Walkthrough - Template

Contents

[Host Discovery 2](#_Toc147658896)

[Nmap 2](#_Toc147658897)

[Nikto 2](#_Toc147658898)

[Viewing Website 3](#_Toc147658899)

[JS File 3](#_Toc147658900)

[WFuzz 3](#_Toc147658901)

[Exploitation 3](#_Toc147658902)

[Curl 3](#_Toc147658903)

[John 4](#_Toc147658904)

[WFUZZ 4](#_Toc147658905)

[Escalation 4](#_Toc147658906)

[Curl 2 4](#_Toc147658907)

[Sudo -l 5](#_Toc147658908)

[Upgrade Shell 5](#_Toc147658909)

[Switching Accounts 5](#_Toc147658910)

[Flag 1 5](#_Toc147658911)

[Flag 2 5](#_Toc147658912)

# Host Discovery

A black and white screen with white text

Description automatically generated

**Kali**:192.168.56.101

**Victim**: 192.168.56.152

# Nmap

A close up of white text

Description automatically generated



# Nikto







# Viewing Website



The contents of /secret/ contain a jpg which may need to be extracted.

# JS File

I was browsing through javascript files and I noticed that one of the files contained some info.



I know though about injecting ../../etc/passwd which didn’t result in anything (despite adding ../ many times)

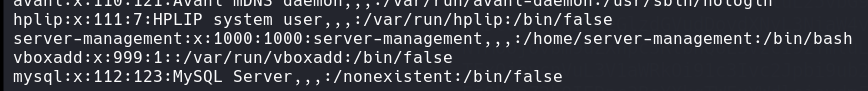
# WFuzz

I decided to check for more possible domains. That didn’t really help.

# Exploitation

# Curl

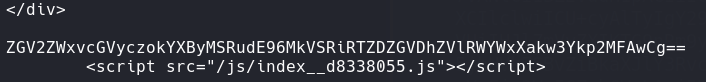
<http://192.168.56.152/index.php?referer=php://filter/convert.base64-encode/resource=/etc/passwd>

I continued trying to use this and eventually I used curl to see if I could get anything useful (could also use burp suite)

This gave me some insights (I had to decode the base64).

A black background with white text

Description automatically generatedI then read this config file for apache. I also found a piece that said htaccess if a key file. If .htaccess doesn’t work, I can try .htpasswd.

I read .htaccess and nothing of interest came, but then .htpasswd saw a base64 password.

**Decode the base64**.

developers:$apr1$ntOz2ERF$Sd6FT8YVTValWjL7bJv0P0

# John



developers:9972761drmfsls

# A screenshot of a computer screen Description automatically generatedWFUZZ

Add it to the /etc/hosts file.

Login with the credentials cracked.

# Escalation

I was greted with ClipBucket webpage and googled for some exploits.

<https://www.exploit-db.com/exploits/44250?ref=infosecarticles.com>

## Curl 2



A computer screen shot of white text

Description automatically generatedThen set up a netcat and click the php file that was created in the index listing.

## Sudo -l

This showed I could run npm binary as server-management.

## Upgrade Shell



A computer screen shot of a computer code

Description automatically generated

## Switching Accounts

I created a file called check.sh

A screen shot of a computer

Description automatically generatedI then created package.json

I then used npm to run package.json.



Now I am a different user. 

# Flag 1



# Flag 2

I used a program called pspy64.



These are some interesting.

A screenshot of a computer program

Description automatically generated

Under “what to back” the files are taken via a wild card. This gives me an idea of wild card injection.

**Resource**: <https://systemweakness.com/privilege-escalation-using-wildcard-injection-tar-wildcard-injection-a57bc81df61c>

This is the order of the commands I ran.

echo 'echo "server-management ALL=(root) NOPASSWD: ALL" >> /etc/sudoers' > demo.sh

touch -- "--checkpoint-action=exec=sh demo.sh"

A screen shot of a computer

Description automatically generated

After about 1 minute, you can try ‘sudo su’ and you will have sudo privs.

A screen shot of a computer

Description automatically generated