Walkthrough - Template

Contents

[Host Discovery 2](#_Toc149135383)

[Nmap 2](#_Toc149135384)

[Nikto 2](#_Toc149135385)

[Dirb 2](#_Toc149135386)

[Viewing Website 3](#_Toc149135387)

[FTP 3](#_Toc149135388)

[Gobuster 3](#_Toc149135389)

[WPScan 4](#_Toc149135390)

[HTTPIE 4](#_Toc149135391)

[WPSCAN 2 5](#_Toc149135392)

[Login 5](#_Toc149135393)

[Escalation 5](#_Toc149135394)

[Upgrade Shell 5](#_Toc149135395)

[/Var/Mail 6](#_Toc149135396)

[/Var/www/html/so-dev-wordpress/ 6](#_Toc149135397)

[MYSQL 6](#_Toc149135398)

[John 6](#_Toc149135399)

[/etc/Passwd 6](#_Toc149135400)

[Joes Home Directory 7](#_Toc149135401)

[Find SUID Binaries 7](#_Toc149135402)

[Flag 7](#_Toc149135403)

# Host Discovery



# Nmap



# Nikto

A black background with white text

Description automatically generated

# Dirb





# Viewing Website

A close-up of a computer screen

Description automatically generated

The website has a default apache 2 webpage.

# FTP

Using the default credentials ‘anonymous’ and no password, I was able to get into ftp. There was a file.

# A screen shot of a computer code Description automatically generatedA screen shot of a computer Description automatically generatedGobuster

One thing I notice was that index.php is returning a status code which is common with directories found. So I will investigate this.

It just gave me a bunch of random items.

Now I will go back to the root directory (home default apache 2 webpage).

A screenshot of a computer

Description automatically generatedI just noticed that index.html is actually index.htnl.

A screenshot of a computer

Description automatically generatedNow there is a gif on a webpage. Clicking on the image reveals an upload page.

It requires image only files, so I know a way to bypass this.

A screen shot of a computer

Description automatically generatedAppend the GIF tag to the beginning of the file.

# WPScan



Wordpress scan revealed nothing of importance.

# HTTPIE

A screen shot of a computer

Description automatically generatedThis tool help me look at the request.

Base64 is found.

# WPSCAN 2

A screenshot of a computer

Description automatically generatedNow performing another wordpress scan.



# Login







# Escalation

## Upgrade Shell



A close up of a text

Description automatically generated with medium confidence





A screen shot of a computer

Description automatically generated

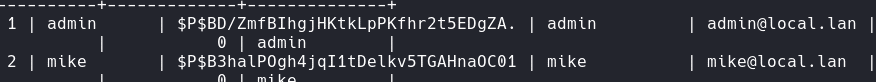
# /Var/Mail

# /Var/www/html/so-dev-wordpress/

A screen shot of a computer screen

Description automatically generated

# MYSQL

I used the password provided above.

# John





# /etc/Passwd



A quick google showed that this rule uses a hyphen to join two words.



Files ending in a hyphen were showing up. So I investigated.





Opening the files contents, I see the password.

# Joes Home Directory

# Find SUID Binaries

This doesn’t look like a regular available suid binary, so I looked at the permissions. There was a plus next to it. This means there is ACLs attached to this binary.

A screen shot of a computer

Description automatically generated

As you can see, any other user, other than www-data and mike and rwx.



# Flag

A screen shot of a computer screen

Description automatically generated