Walkthrough - Template

Contents

[Host Discovery 2](#_Toc147678928)

[Nmap 2](#_Toc147678929)

[Nikto 2](#_Toc147678930)

[Dirb 2](#_Toc147678931)

[FFuf 2](#_Toc147678932)

[Gobuster 3](#_Toc147678933)

[Burp Suite 3](#_Toc147678934)

[Viewing Website 4](#_Toc147678935)

[Exploitation 4](#_Toc147678936)

[Escalation 5](#_Toc147678937)

[Upgrade Shell 5](#_Toc147678938)

[Flag 1 5](#_Toc147678939)

[Flag 2 5](#_Toc147678940)

[Sudo -l 5](#_Toc147678941)

# Host Discovery

A black and white screen with numbers

Description automatically generated

**Kali**: 192.168.56.101

**Victim**: 192.168.56.155

# Nmap

A black background with white text

Description automatically generated



# Nikto



It found nothing interesting.

# Dirb



# FFuf

# Gobuster

# Burp Suite

A screenshot of a computer code

Description automatically generatedI don’t quite understand why, however adding “X-Forwarded-fo” to the request can bypass something.

A screenshot of a computer program

Description automatically generated

The response I need, -------->

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedRight click the response then click request in browser > current browser session.

A screenshot of a computer

Description automatically generated

I will try some basic credentials admin:admin, and it worked.

Move this result to the main web-browser and see now you have logged in.

# Viewing Website

A screenshot of a computer

Description automatically generated

The website shows that it can allow file uploads. I tried upload my reverse php shell however the extension is not permitted. I will try and modify it.

# Exploitation

I now will upload my reverse php3 shell.

A screenshot of a computer

Description automatically generated



A computer screen shot of white text

Description automatically generatedIn the url: <http://192.168.56.155/adminstration/upload/files> The file was located.

# Escalation

## Upgrade Shell



A computer screen with white text

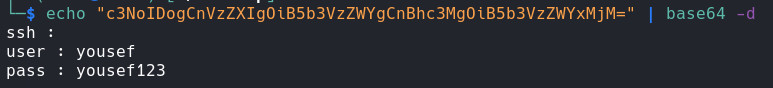
Description automatically generated



# Flag 1

It is a base64 text.





# Flag 2

## A screen shot of a computer Description automatically generatedSudo -l

A screenshot of a computer screen

Description automatically generated

