Walkthrough - Venus

Contents

[Host Discovery 2](#_Toc147747355)

[Nmap 2](#_Toc147747356)

[Nikto 2](#_Toc147747357)

[Dirb 2](#_Toc147747358)

[Viewing Website 2](#_Toc147747359)

[Exploitation 2](#_Toc147747360)

[Escalation 2](#_Toc147747361)

# Host Discovery

A black and white screen with white text

Description automatically generated

**Kali**: 192.168.56.101

**Victim**: 192.168.56.157

# Nmap

A black background with white text

Description automatically generated



I could not get a result. It stays on loading.

# Nikto



# Dirb





# Burp Suite

A close-up of a text

Description automatically generatedThe response of the credentials guest:guest show this cookie being set.

The base64 is translated to the following.

A close up of a black background

Description automatically generated

A screenshot of a computer code

Description automatically generatedThe second part of the string appears to match the same length of the username guest, so it might be the password encoded. So if I can find other usernames, I might be able to get their passwords!

I was able to find a valid username. I was looking through the source code of the home directory and found the username venus, through trial and error.

They used the same id to identify both password and username.

# Hydra

Using hydra you can brute force and potentially find usernames and passwords.

I found another username.

# Back to Burp Suite



DO NOT USE INBUILT ONE! THAT ENCODER IS WRONG!

A screenshot of a computer

Description automatically generatedI used the same base64 as found earlier, however I replaced guest with venus.

Sending that request, changes the cookie on the right hand side (response).

A screenshot of a computer

Description automatically generatedI repeated it again.

I now used the Magellan username and modified the cookie to have Magellan:irahf. I then replaced the auth cookie and sent it. The response (right) showed the final cookie.

magellan:irahfvnatrbybtl1989

A screenshot of a computer code

Description automatically generated

Now I have ssh login. (venusiangeology1989)

# Escalation

# Flag 1

A screenshot of a computer

Description automatically generated

# Sudo -L



A black background with white text

Description automatically generated

# Ps aux

# Strings



This is the one line that stands out: loveandbeauty (password?)

I STOPPED HERE BECAUSE ITS BUFFER OVERFLOW STUFF (NEXT SEM).