Walkthrough – RTB1

Contents

[Host Discovery 2](#_Toc147409801)

[Nmap 2](#_Toc147409802)

[Nikto 2](#_Toc147409803)

[Viewing Website 2](#_Toc147409804)

[Dirb 3](#_Toc147409805)

[WPScan 3](#_Toc147409806)

[Searchsploit 3](#_Toc147409807)

[Exploitation 3](#_Toc147409808)

[SQLMap 3](#_Toc147409809)

[Escalation 4](#_Toc147409810)

[Upgrade Shell 5](#_Toc147409811)

[Kernel Exploit 5](#_Toc147409812)

[Flag 5](#_Toc147409813)

# Host Discovery

A black and white screen with white text

Description automatically generated

**Kali**: 192.168.56.101

**Victim**: 192.168.56.154

# Nmap







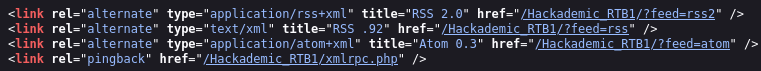
# Nikto







# Viewing Website

The main website source code reveals this data.

I can now kind of see the url structure.



# Dirb

Note: I quickly viewed the website source code before I did this scan.

A screen shot of a computer code

Description automatically generated

# WPScan



# Searchsploit



These are 3 that I found.

This version is vulnerable to sql injection.

# Exploitation

## SQLMap

A black background with white text

Description automatically generated



A screen shot of a computer program

Description automatically generated



A screenshot of a computer program

Description automatically generated

A green and grey striped background

Description automatically generated

I used the credentials NickJames:admin (admin dashboard account). This got me inside the dash board.

Looking around I found nothing. I will try another account. I see George has a level 10 account.

Yes this is the account to use. He must be the website admin.

A close-up of a website

Description automatically generated

I can now put php code to establish a reverse shell, I will modify the original file hello.php.

# Escalation

A screen shot of a computer code

Description automatically generatedUsing this as a guideline I was able to locate hello.php

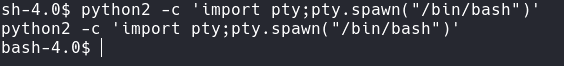




A computer screen with white text

Description automatically generated

## Upgrade Shell

Victim machine:

A close up of a text

Description automatically generated with medium confidenceKali Machine:

Victim:

I did look around for a bit and found nothing really of interest.

## Kernel Exploit

This one didn’t work.

After quite some time I found: <https://www.exploit-db.com/exploits/15285>



A close up of a black background

Description automatically generated

# A screen shot of a computer Description automatically generatedFlag