Capture The Flag Penetration Testing

Walkthrough

Alert

09th of Jan 2025

Version 1.0

# Table of Contents

[Table of Contents 2](#_Toc199072203)

[Statement of Confidentiality 3](#_Toc199072204)

[Engagement Contacts 4](#_Toc199072205)

[Executive Summary 5](#_Toc199072206)

[Approach 5](#_Toc199072207)

[Scope 6](#_Toc199072208)

[Detailed Walkthrough 6](#_Toc199072209)

# Statement of Confidentiality

The contents of this document have been developed during a capture the flag exercise. The contents of the document may be shared or used for educational and training purposes only. Exercising the any of the techniques of this document without prior written consent by the owner of the internet assets may be considered as an offence and may bear legal responsibility.

The contents of this document do not constitute legal advice. 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 real company’s external or internal infrastructure.

# Engagement Contacts

|  |  |  |
| --- | --- | --- |
| Customer Contacts | | |
| Primary contact | Title | Primary contact email |
| Example name | Example title | example@bar.com |
| Secondary contact | Title | Secondary contact email |
| Example name | Example title | example@bar.com |

|  |  |  |
| --- | --- | --- |
| Assessor Contacts | | |
| Assessor name | Title | Assessor email |
| SvetozarP | Example title | example@bar.com |

# Executive Summary

The below described penetration test has been conducted as part of a “capture the flag” training exercise, assessing the security of internet asset, provided by Hack The Box and documenting the findings in clear and repeatable manner. This document aims to provide the detailed path of exploitation.

## Approach

The below described exercise was performed on 09th of January 2025 under a “black box” approach without any credentials or any advance knowledge of the target’s structure or environment, besides that the system is running a Linux operational system. Testing was performed with the aim of securing a shell to the system and capturing the user and the root user’s flags. The testing was performed remotely. Detailed walkthrough can be found in the Detailed Walkthrough section of this document.

## Scope

The scope of this assessment is the Alert machine, provisioned by Hack The Box.

|  |  |
| --- | --- |
| Host / URL / IP Address | Description |
| alert.htb / 10.10.11.44 | Hack The Box testing machine |

Table 1 Scope details

## Detailed Walkthrough

The tester performed the following to fully compromise the Codify machine.

1. Using a stored XSS vulnerability on the webpage, the tester was able to obtain password hash from the .htaccess file of the system.
2. The password hash was successfully cracked and the tester was able to obtain credentials and authorised shell access
3. Enumerating the system uncovered that software (Website monitor) was running with administrative privileges locally on the machine
4. The software had writeable monitors directory, in which the tester was able to insert code for reverse shell
5. The tester was able to obtain reverse shell as the administrative user, which led to full control of the system.

#### Detailed reproduction of the steps above:

The website was running a markdown viewer, which was found to be software to view and share markdown files

A screenshot of a computer

AI-generated content may be incorrect.

Figure 1 alert.htb website

The tester noted that all messages are reviewed by the administrator

A screenshot of a website

AI-generated content may be incorrect.

Figure 2 disclaimer that all messages are reviewed

Through enumeration of the host, the tester was able to find a statistics subdomain, which led to a .htpasswd protected page

A screenshot of a computer

AI-generated content may be incorrect.

Figure 3 statistics subdomain discovered

A screenshot of a computer

AI-generated content may be incorrect.

Figure 4 uncovered .htpasswd protection

The tester then checked the upload page for XSS, by creating a .md file using payload <script>alert("XSS attack!")</script>

A screenshot of a computer

AI-generated content may be incorrect.

Figure 5 XSS confirmed

The tester then generated a file targeting messages.php which was obtaining the messages, stored as text files. The tester attempted getting the .htpasswd from the statistics subdomain

A screen shot of a computer

AI-generated content may be incorrect.

Figure 6 payload to obtain the .htpasswd file and send it to the listener started on port 8000 on the local machine

Link to the MD file was obtained through the “Share Markdown” button within the upload page

A red rectangle with a white background

AI-generated content may be incorrect.

The tester then sent a link to the markdown file via the ‘contact us’ page of the website

A screenshot of a contact us

AI-generated content may be incorrect.

This yielded response from the machine, containing the hash from the .htpasswd file



Figure 7 Response containing the .htpasswd contents

The tester was then able to obtain credentials by executing a brute force attack on the hash

A screen shot of a computer

AI-generated content may be incorrect.

Figure 8 obtained password for user albert

This led to authorised shell access to the system

A screenshot of a computer

AI-generated content may be incorrect.

Figure 9 successful connection

Service enumeration uncovered software running on port 8080

A screen shot of a computer

AI-generated content may be incorrect.

Figure 10 machine’s open ports

The tester discovered a Website monitor software running on this port

A computer screen shot of a computer program

AI-generated content may be incorrect.

Figure 11 Enumeration of port 8080

Files were discovered in /opt/website-monitor folder with writeable monitors directory

A screenshot of a computer

AI-generated content may be incorrect.

Figure 12 contents of /opt/website-monitor

The tester then constructed a .php file containing reverse shell payload and inserted it in the monitors folder



Figure 13 Reverse shell payload



Figure 14 Payload execution

This led to the tester obtaining full control of the machine

A black screen with white text

AI-generated content may be incorrect.

Figure 15 Successful connection