



CLOUD SEK

Cyber Security, Machine Intelligence company

Capture The Flag Report

Start Date: Feb 14th, 2022
End Date: Feb 15th, 2022

Table of Contents

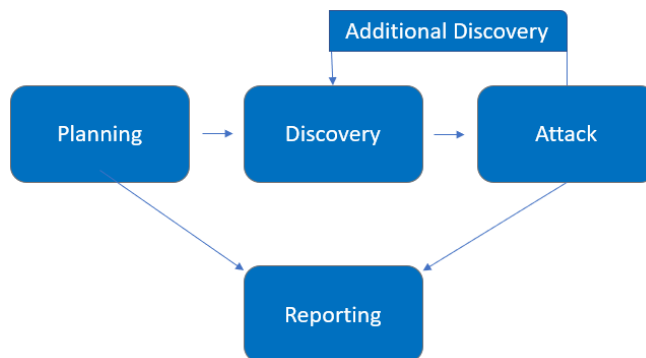
Table of Contents	1
Assessment Overview	2
Scope	2
Executive Summary	3
Attack Summary	3
Findings	
1. Wizardry.txt	4
2. Nmap Enumeration	5
3. Fuzzing with ID parameter in id3nt1ty_card.php	6
Thank You and Contact Info	10

Assessment Overview

From Feb 14th, 2022 to Feb 15th, 2022, I was engaged to find CTF flags and other vulnerabilities that included an external penetration test. All testing performed is based on the NIST SP 800-115 *Technical Guide to Information Security Testing and Assessment*, OWASP Testing Guide (v4).

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Scope

Assessment	Details
Penetration Test	13.235.95.179/24

Per client request, I did not perform any Denial of Service, brute force attacks on the CTF server.

Executive Summary

I was assigned to evaluate security posture and find flags on the given scope by CloudSEK by engaging in a 1-day penetration test that was conducted on 5pm Feb 14th, 2022 - 6pm Feb 15th, 2022. The goal of the “pentest” is to act as a threat-actor by performing cyber-attacks against CTF server. This will serve to discover any present vulnerabilities that could result in a breach and be leveraged to access sensitive data by a real-world attacker. All issues discovered are achieved and verified through network evaluation, system vulnerability scanning and assessment, and both automated and manual exploitation (where applicable) of found vulnerabilities.

Attack Summary

Step	Action
1	After reaching the gateway, a path to wizardry.txt is found and a cryptic message is shown.
2	After decoding it with base64, an esoteric programming language text was the result which was JSFuck. After executing esoteric text, an alert popped up with a page name “id3nt1ty_card.php”
3	After reaching http://13.235.95.179/id3nt1ty_card.php there was a lot of emphasis on ID. After trying with the ID parameter till “4”, a clue was given to go to 212.
4	Meanwhile started a simple nmap enumeration scan revealed an open port: 5000 http://13.235.95.179:5000
5	Upon visiting http://13.235.95.179/id3nt1ty_card.php?id=212 two peculiar variables are found (x,y) one of them is hex value and the other is a link to password protected ControlC pate bin. When the source is viewed of the same page, we also find a hidden php code card image explaining about the possible password combinations for controlC.

Findings

1. Wizardry.txt

Url: <http://13.235.95.179/wizardry.txt>

```
13.235.95.179[wizardry.txt]
Hi Cloudster! I'm Dobby. I once served the Dark Wizards who treated me cruelly but soon a legendary wizard broke my slavery and YES! I am no longer a slave.
That legendary wizard, gave me this code but till now, I have no idea about it.
Take this! Might be useful for you at your journey.

W1lbKCFbXstbXSlbKltdXSsoIvtdKltdKvshKltdKyErW1ldKygHw10rW10pWyshKltdXSsoISfBXstbXSlbKltdXVlbfKtDwYghW10rW10pWytbXV0rKCFbXstbXSlbIStbXShhKltdXSsoIvtdKltdKVsrbXV0rKCEHw10rW10pWytbXVldKltdKvshKltdKyErW10rIStbXV0rKCEHw10rW1lbKCFbXstbXSlbKltdXSsoIvtdKltdKvshKltdKyErW1ldKygHw10rW10pWyshKltdXSsoISfBXstbXSlbKltdXV0pWysdkVsrW1ldXSsoW1lbW1ldKltdKvSrIStbXV0rKCFbXstbXSlbIStbXShhKltdKyErW1ldKygHIVtdKltdKVsrbW1ldKygHIVtdKltdKVsrbIStbXV0rKfTdGw1tdXStbXSlbKltdXSsoW1lbKCFbXstbXSlbKltdXSsoIvtdKltdKvshKltdKyErW1ldKygHw10rW10pWyshKltdXSsoISfBXstbXSlbKltdXV0rW10pWYdYErW10rIStbXShhKltdXSsoISfBXstbXSlbKltdXSsoISfBXstbXVsoIvtdKltdKVsrbW1ldKygHw10rWYErW10rIStbXV0rKCFbXstbXSlbIStbXShhKltdKyErW1ldKygHIVtdKltdKVsrbW1ldKlSlbKyErW10rWYtbXVldKygHIVtdKltdKVsrbIStbXVldKfDwYghW10rW10pWytbXV0rKCFbXstbXSlbIStbXShhKltdXSsoIvtdKVsrbXV0rKCEHw10rW10pWytbXVldwYhbXVsoIvtdKltdKVsrbW1ldKygHw10rW10pWYdYErW10rIStbXV0rKCFbXstbXSlbKyErW1ldKygHIVtdKltdKVsrbW1ldXStbXSlbIStbXShhKltdKyErW1ldKygHtdKltdWYghW10rW10pWYtbXV0rKCFbXstbXSlbIStbXShhKltdXSsoIvtdKltdKVsrbIStbXV0rKCEHw10rW10pWYtbXVldKVsrbIStbXstbXSlbKltdXV0rKfTdGw1tdXStbXSlbKyErW1ldKygHw10rW10pWYdYErW1ldXStbXSlbKltdXSsoISfBXstbXSlbKltdXSsoISfBXstbXSlbKyErW1ldKygHw10rW10pWYtbXV0rKfTdWYghW10rW10pWYtbXV0rKCFbXstbXSlbIStbXShhKltdXSsoIvtdKltdKVsrbIStbXV0rKCEH
```

- **“cloudster”** maybe the username for the getaway to Realm of Magic
- After decoding the above text with base64, we get:

[illegible]

- Which is a JSFuck text, after executing it with <https://jsfuck.com>
- An alert with an identity card page is shown:



2. Nmap Enumeration

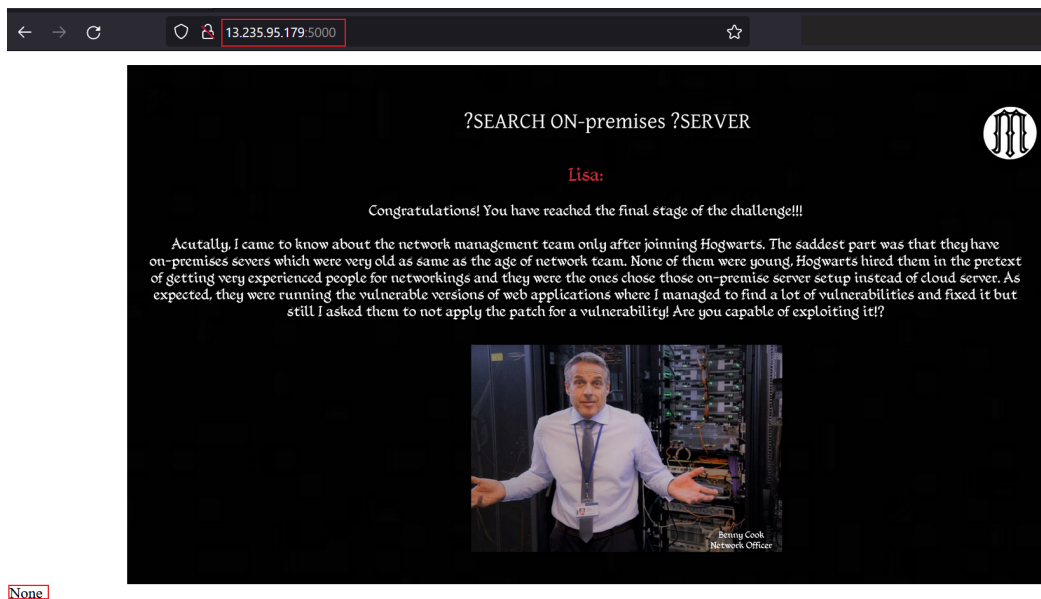
Url: <http://13.235.95.179:5000>

- After doing a simple nmap scan, we find an interesting open port: 5000

```
# nmap 13.235.95.179 -T4 -A -v -oA nmap
```

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 9c:03:63:af:46:f9:d6:4c:a5:77:66:00:3c:8f:be:34 (RSA)
|   256 2f:55:13:0e:bc:07:8e:d2:bd:a0:33:a2:d7:fd:f0:74 (ECDSA)
|_  256 54:f0:01:7b:98:04:9f:2b:e5:e1:89:81:a9:51:13:96 (ED25519)
80/tcp    open  http     Apache httpd 2.4.52 (( ) PHP/7.2.34)
|_ http-methods:
|   Supported Methods: OPTIONS HEAD GET POST TRACE
|_  Potentially risky methods: TRACE
|_ http-title: Hogwarts Staff Recruitment - Cyber
|_ http-server-header: Apache/2.4.52 ( ) PHP/7.2.34
5000/tcp  open  http     Werkzeug httpd 2.0.3 (Python 3.7.10)
|_ http-title: ?SEARCH ON-premises ?SERVER
|_ http-methods:
|   Supported Methods: GET OPTIONS HEAD
|_ http-server-header: Werkzeug/2.0.3 Python/3.7.10
```

- The scan also gives it's running Werkzeug 2.0.3
- After visiting the open port:



- And some peculiar text “None”. Not sure if it has any significance.

3. Fuzzing with ID parameter in id3nt1ty_card.php

Url: http://13.235.95.179/id3nt1ty_card.php?id=*

Affected Parameters: id [GET]


Payload: id=1

- When the payload “id=1” inserted, we get something interesting, hinting that we’re on the right track.

13.235.95.179/id3nt1ty_card.php?id=1

☆

Ministry of Magic Identity Card



Lisa:


Great. Keep up with the process & dont forget to look the image with clear eyes

From my experience, being a non-wizard staff is not so easy at Hogwarts. The wizards here just cast a spell to refill their cup of coffee and I am here grinding and preparing my own coffee as the expresso machine is yet to be delivered. By the way, the Ministry of Magic has decided to issue Identity Cards for non-wizard staffs. So that they come under the exclusive protection of Aurors from Ministry of Magic.

Seriously! How did you find this thing!?

- After giving 2,3 as payloads in the id parameter, we get a clue on “id=4” payload.

13.235.95.179/id3nt1ty_card.php?id=4



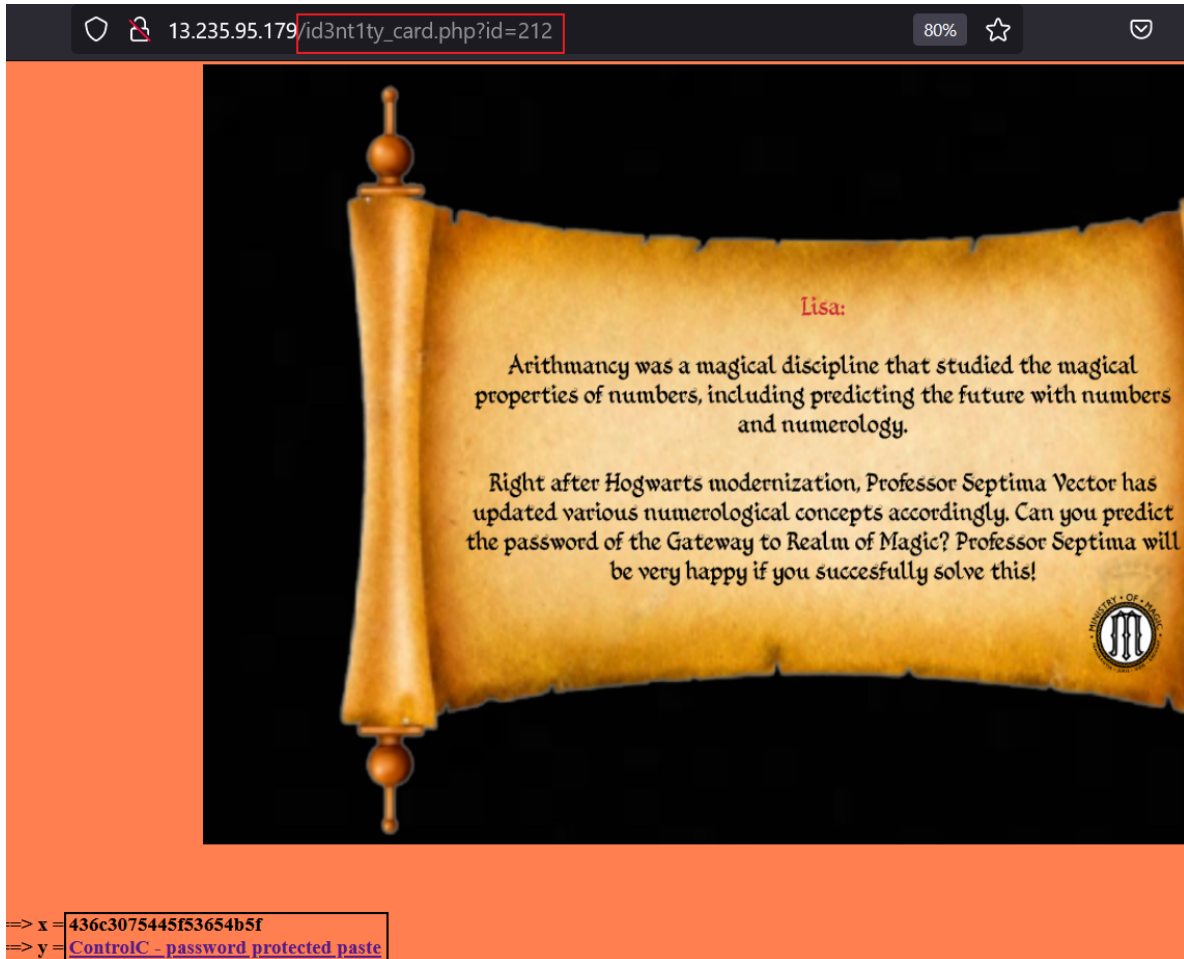
Lisa:

Great. Keep up with the process & dont forget to look the image with clear eyes

From my experience, being a non-wizard staff is not so easy at Hogwarts. The wizards here just cast a spell to refill their cup of coffee and I am here grinding and preparing my own coffee as the expresso machine is yet to be delivered. By the way, the Ministry of Magic has decided to issue Identity Cards for non-wizard staffs. So that they come under the exclusive protection of Aurors from Ministry of Magic.

Anyways, have a look at this before you bruteforce..zweihundertzwölf

- After translating the text “zweihundertzwölf” from German to English, we get: two hundred twelve
- After putting the value “212” in the id parameter, we see a scroll and two variables: x and y, assigned with a hex and a link to controlC paste bin respectively.



- Converting the hex to text gives us a half password to gateway: **ClOuD_SeK_**

436c3075445f53654b5f

hex numbers to text

ClOuD_SeK_

- When looked at source code, we see a hidden image tag with this image:

```
/*Analyze the code & predict the password to ControlC Paste within the range of numbers at condition*/
<?php
    if(array_key_exists("passphrase",$REQUEST)){
        if(strpos($_REQUEST["passphrase"],"carbonblack") && ($_REQUEST["passphrase"] > 22) && ($_REQUEST["passphrase"] < 55)){
            alert("The password to pastebin: <HIDDEN>");
        }
        else{
            echo "<br>Try again!<br>";
        }
    }
}
```

- Hinting that the password of ContolC can be predicted when this piece of php code is understood.

Password Required

The paste you are trying to view (#0e1fbc43) has been password protected. Enter the correct password below to view it.

Password:

- When the php code is analysed, we can understand that password is submitted with “passphrase” parameter through either GET or POST request and must contain the word “carbonblack” and the password length should be greater than 22 but less than 55.



Thank You!

Contact:

Jaswanth Sunkara

+91 8074346267

jaswanthsunkara@protonmail.com

<https://github.com/KickAss101>