# Red Team: Summary of Operations

## 

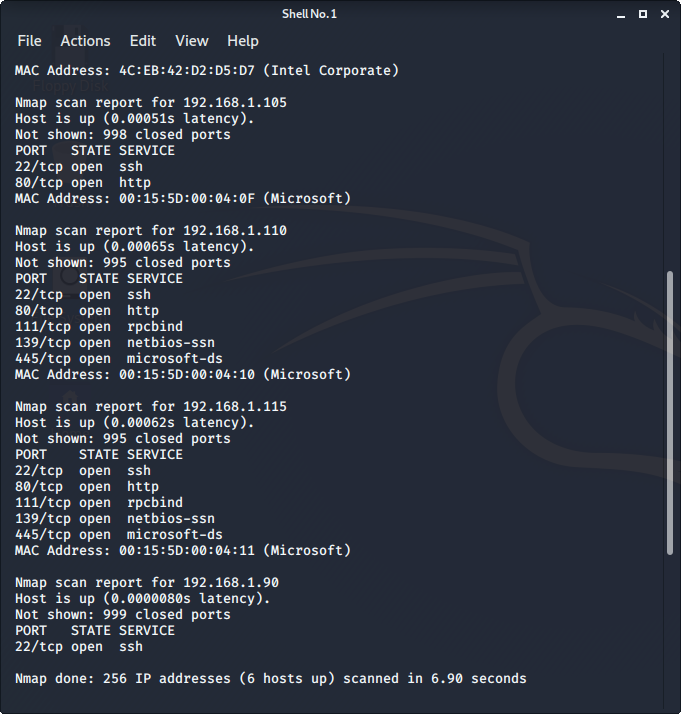
## Table of Contents

* Exposed Services
* Critical Vulnerabilities
* Exploitation

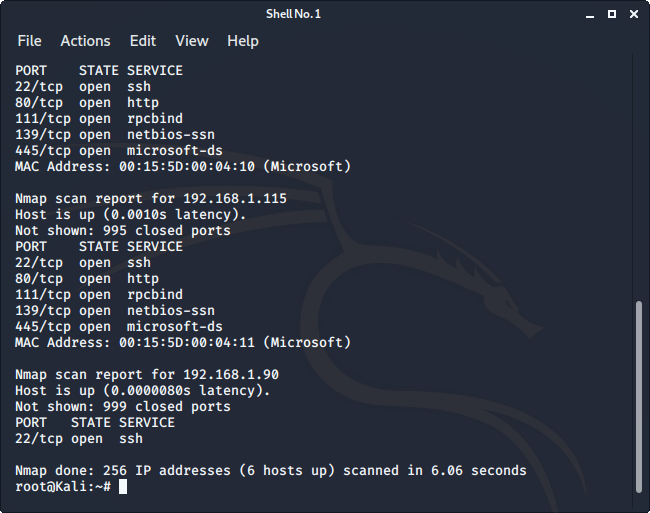
### Exposed Services

Nmap scan results for each machine reveal the below services and OS details:

$ nmap 192.168.1.110



$ nmap 192.168.1.115



This scan identifies the services below as potential points of entry:

**Target 1**

1. Port 22: ssh into system
2. Port 80: access to webserver
3. Port 445: File-sharing

**Target 2**

1. Port 22: ssh into system
2. Port 80: access to webserver
3. Port 445: File-sharing

### Critical Vulnerabilities

The following vulnerabilities were identified on each target:

**Target 1**

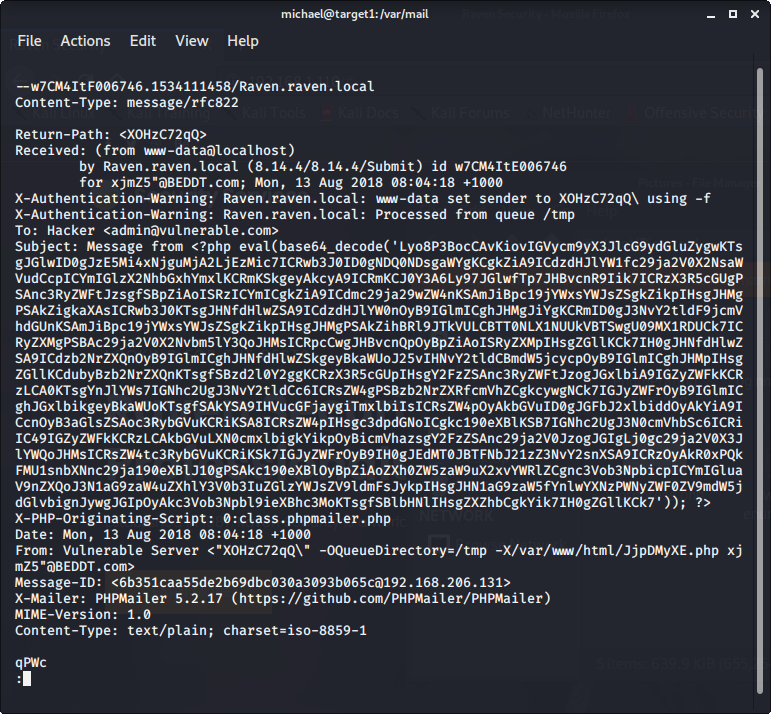
1. **CWE-200: Exposure of Sensitive Information to an Unauthorised Actor**

<https://cwe.mitre.org/data/definitions/200.html>

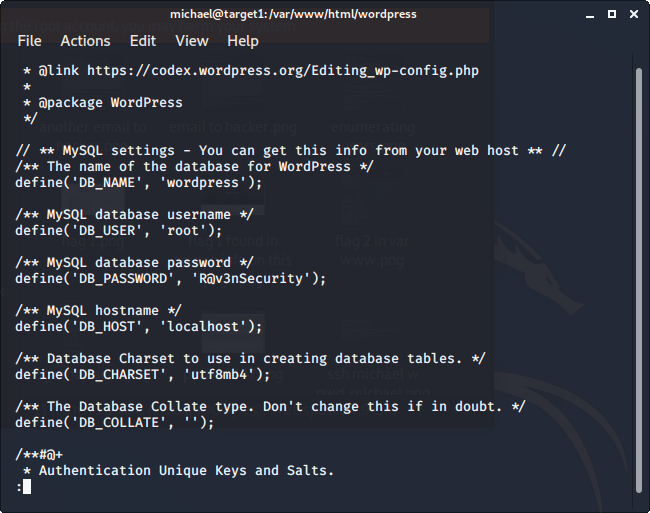
**Description:** The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.

**Impact:** An attacker can attain sensitive data and can use this to perform an exploit.

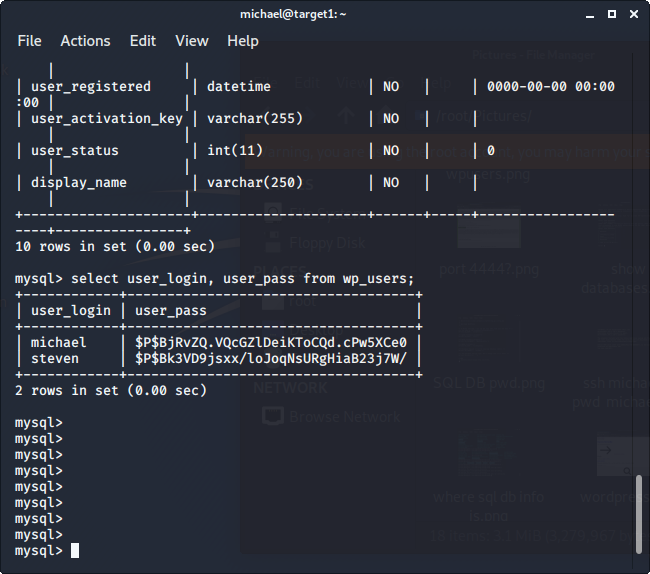
In the target 1 machine, we gained access to Michael’s mail and could read sensitive information.



The username and password for access onto the MYSQL database was stored in plaintext in an easily accessible account, which allowed us access to the database to perform further exploits.



This allowed us access into the MYSQL database where the password hashes for users on the network were stored.



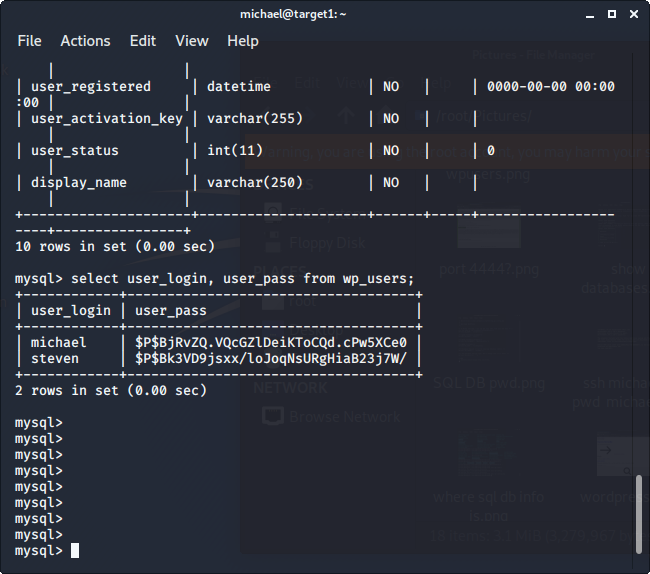
1. **CWE-261: Weak Encoding for Password**

<https://cwe.mitre.org/data/definitions/261.html>

**Description:** Obscuring a password with a trivial encoding does not protect the password.

**Impact:** An attacker can gain privileges to a system or assume an identity.

In target 1, the passwords were encoded with a hash that was easy to reverse and the passwords were easily discovered.



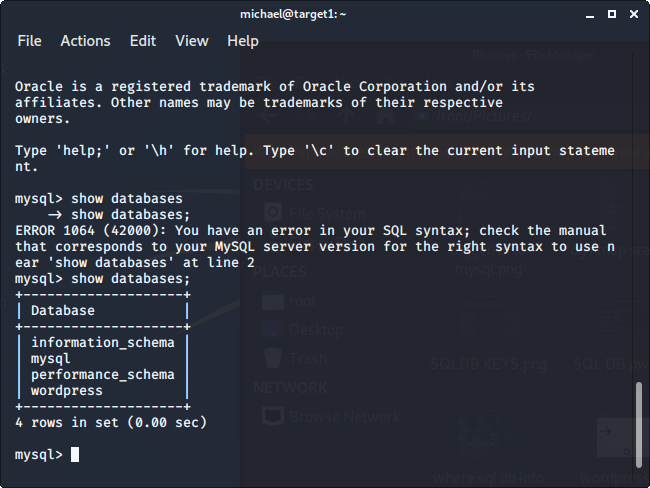
1. **CWE-284: Improper Access Control**

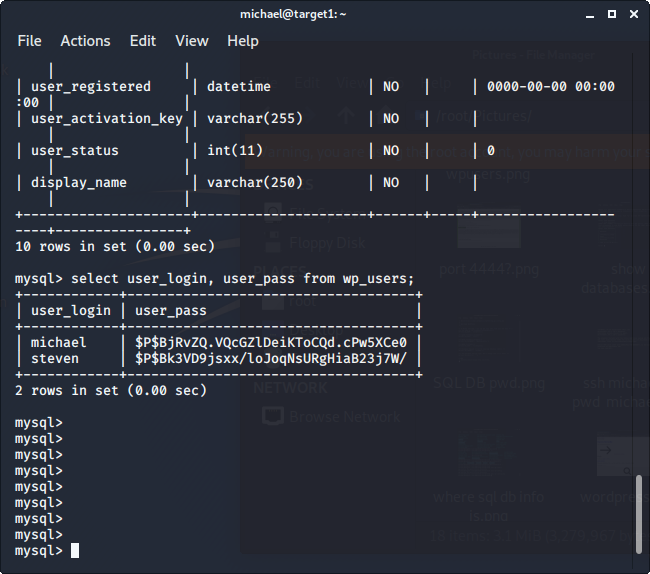
<https://cwe.mitre.org/data/definitions/284.html>

**Description:** The software does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

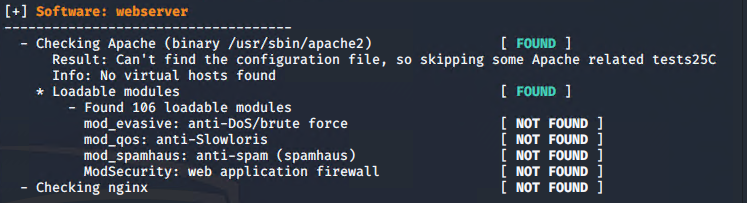
**Impact:** Attackers can gain access to resources within a system that allow them to gain sensitive information or execute exploits.

In target 1, we could gain access to the MYSQL database which contained sensitive user details.

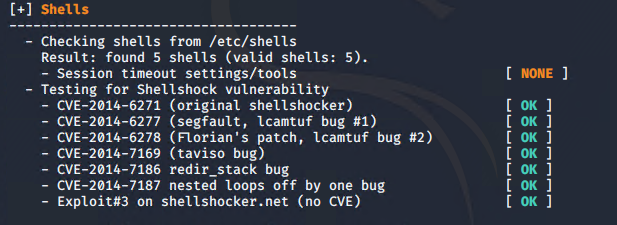




A Lynis scan of target 1 also showed no web application firewall was installed meaning there is no proper restriction to the webserver from an unauthorised actor.



Also found there is no session timeout for shells so an ssh into the system was not stopped after a while and unauthorised access could remain indefinitely.

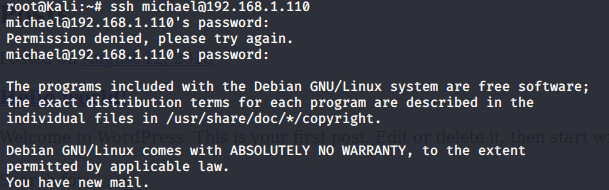


1. **CWE-306: Missing Authentication for Critical Function**

<https://cwe.mitre.org/data/definitions/306.html>

**Description:** The software does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources.

**Impact:** Exposing critical functionality essentially provides an attacker with the privilege level of that functionality. The consequences will depend on the associated functionality, but they can range from reading or modifying sensitive data, access to administrative or other privileged functionality, or possibly even execution of arbitrary code.

In target 1, weak passwords lead to access into the command shell of the network and hence access to sensitive documents within the network.

1. **CWE-307: Improper Restriction of Excessive Authentication Attempts**

<https://cwe.mitre.org/data/definitions/307.html>

**Description:** Software has insufficient measures to prevent multiple failed authentication attempts in a short time frame.

**Impact:** An attacker can perform any amount of authentication attempts and eventually gain access to an account.

In target 1, we gained access to the user steven’s account using brute force via john the ripper.



1. **CWE-326: Inadequate Encryption Strength**

<https://cwe.mitre.org/data/definitions/326.html>

**Description:** The software stores or transmits sensitive data using an encryption scheme that is theoretically sound but is not strong enough for the level of protection required.

**Impact:** An attacker may be able to decrypt the data using brute force attacks.

In target 1, this is exactly what happened, and we were able to brute force our way into stevens account due to his password information having low encryption strength.

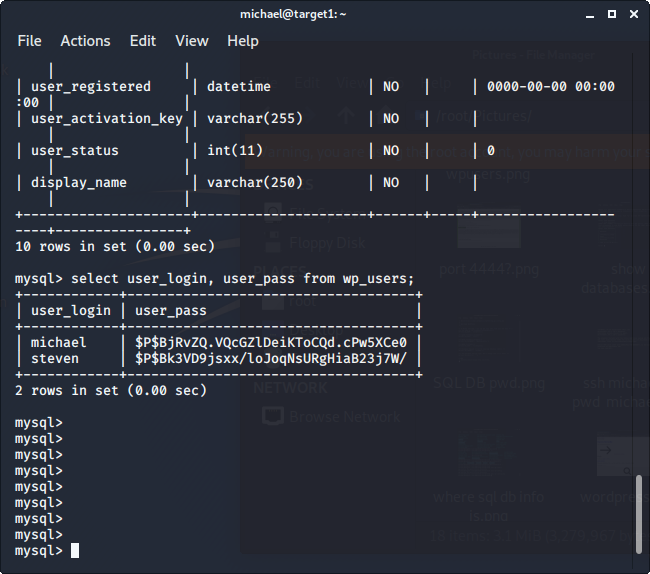


1. **CWE-328: Reversible One-Way Hash**

<https://cwe.mitre.org/data/definitions/328.html>

**Description:** The product uses a hashing algorithm that produces a hash value that can be used to determine the original input.

**Impact:** Attackers can bypass the protection mechanism and gain access to sensitive information that is supposed to be protected by this one-way hash.





1. **CWE-521: Weak Password Requirements**

<https://cwe.mitre.org/data/definitions/521.html>

**Description:** The product does not require that users should have strong passwords, which makes it easier for attackers to compromise user accounts.

**Impact:** An attacker could easily guess user passwords and gain access user accounts.

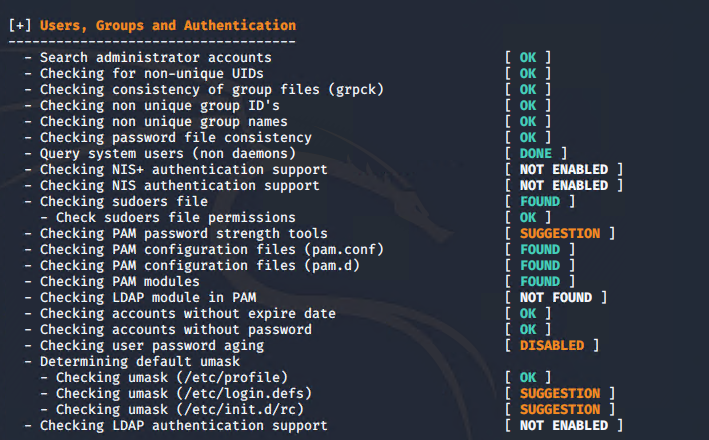
In target1, access to each user’s account was gained due to their weak passwords. Michael and root user’s password were guessed, as they were both commonly used passwords. Steven’s password was easily cracked using john and a wordlist of common passwords.

michael:michael

root:toor



A lynis scan showed that there was no user password ageing set.





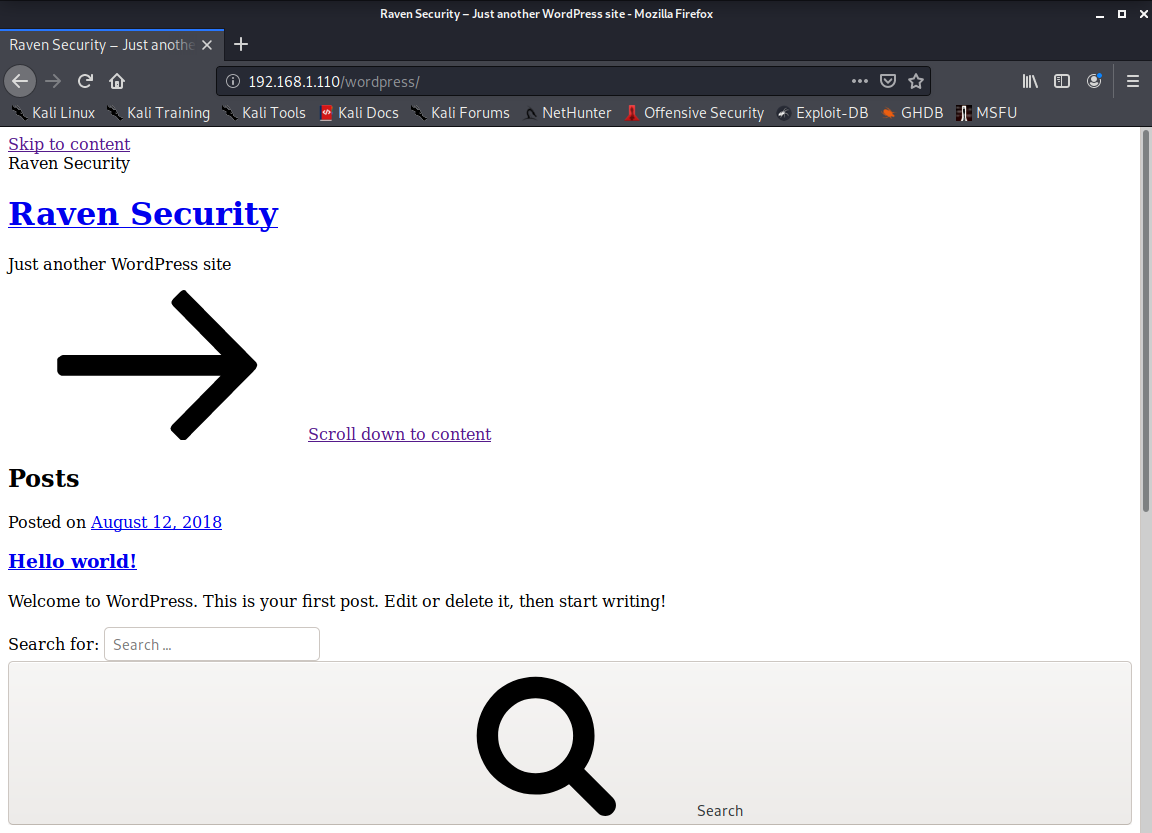
1. **CWE-552: Files or Directories Accessible to External Parties**

<https://cwe.mitre.org/data/definitions/552.html>

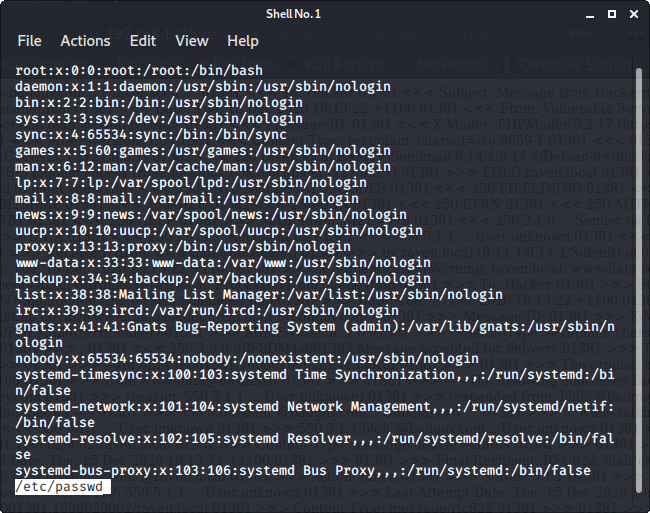
**Description:** The product makes files or directories accessible to unauthorized actors, even though they should not be.

**Impact:** Unauthorised actors can read files or directories; modify files or directories.

In target 1, we had access to directories on the webserver by appending to the end of the web address.



4

We also had access to the /etc/passwd file through stevens account.

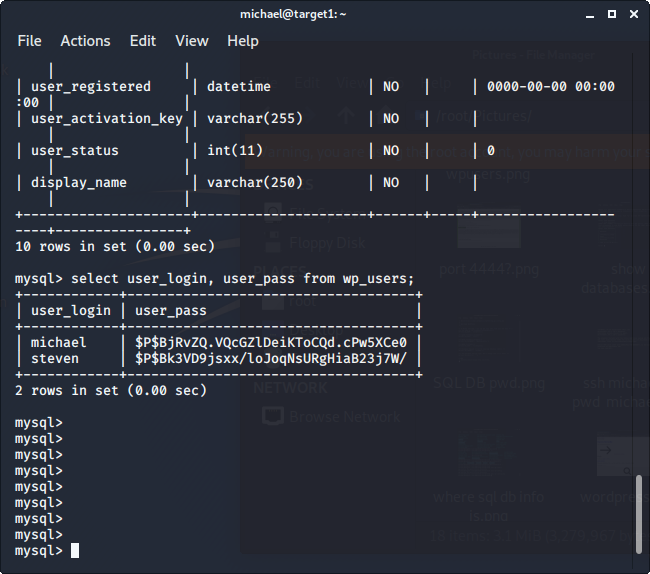
1. **CWE-916: Use of Password Hash with Insufficient Computational Effort**

<https://cwe.mitre.org/data/definitions/916.html>

**Description:** The software generates a hash for a password, but it uses a scheme that does not provide a sufficient level of computational effort that would make password cracking attacks infeasible or expensive.

**Impact:** If an attacker can gain access to the hashes, then the lack of sufficient computational effort will make it easier to conduct brute force attacks using techniques such as rainbow tables, or specialized hardware such as GPUs, which can be much faster than general-purpose CPUs for computing hashes.

In target 1, we gained access to the hashes and then used John the Ripper to conduct a brute force attack and gained access to stevens account.



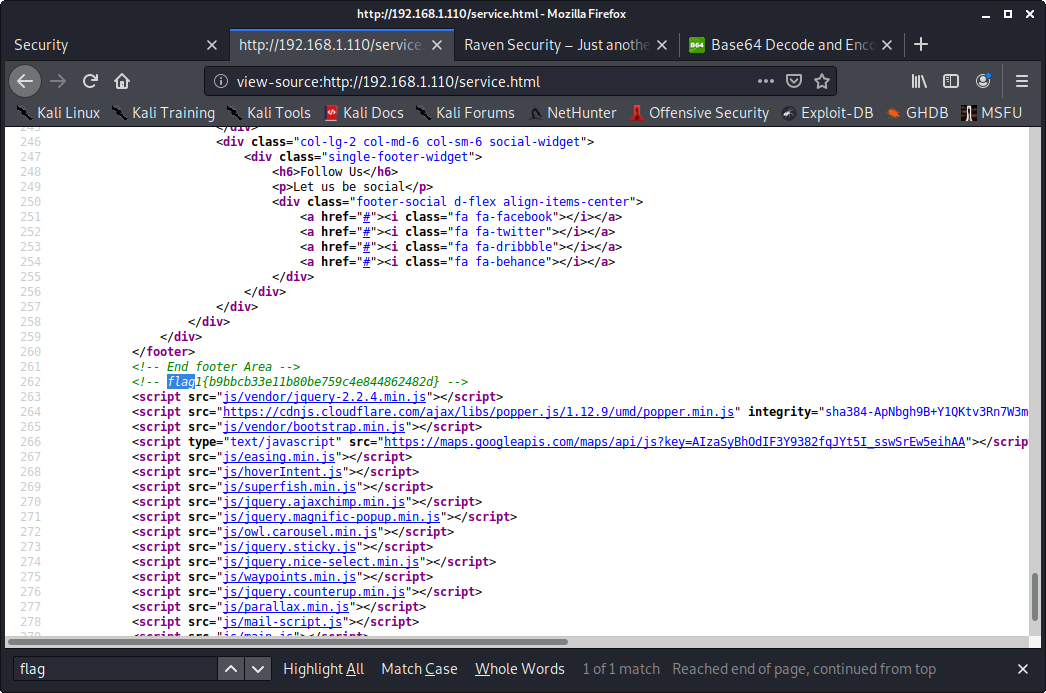


Exploitation

The Red Team was able to penetrate both Target 1 and Target 2 and retrieve the following confidential data:

**Target 1**

* flag1.txt: b9bbcb3ellb80be759c4e844862482d
* Exploit Used
  + Accessed the webserver through port 80 and looked at the source code of the service page on the webserver.
  + Right click -> source code  
    Ctrl+F: flag





* flag2.txt: fc3fd58dcdad9ab23faca6e9a36e581c
* Exploit Used
  + Accessed files and directories that were accessible to unauthorised actors
  + Cd /var/www/

