Module 11

Session Hijacking

23.12.2025

Name : Mugdha Makarand Govilkar

Instructor : Satish Singh

INDEX

1 . What is session hijacking ?

1 . Meaning: Session hijacking is a cyber-attack where an attacker takes control of a valid user session.

2 . Target: The attacker steals the session ID / session cookie used to identify a logged-in user.

3 . Result: Attacker gains unauthorized access without knowing the username or password.

4 . How it happens:

- **Packet sniffing**
- **Cross-Site Scripting (XSS)**
- **Malware or browser exploits**

5 . Types:

- **Active session hijacking**
- **Passive session hijacking**

6 . Common protocols affected: HTTP, FTP, Telnet (non-encrypted).

7 . Impact: Data theft, identity misuse, financial loss.

8 . Example: Attacker steals a session cookie and logs in as the victim.

9 . Prevention: Use HTTPS, secure cookies, logout after use, and session timeouts.

2 . Purpose of session hijacking ?

1 . Gain unauthorized access to a user’s account.

2 . Impersonate a legitimate user without login credentials.

3 . Bypass authentication by using stolen session IDs/cookies.

4 . Access sensitive data (emails, banking, personal info).

5 . Perform actions as the user (transactions, changes, misuse).

6 . Maintain access as long as the session remains active.

3 . prevention of session hijacking ?

1. **Use HTTPS (SSL/TLS):**
   Encrypts data so session IDs cannot be intercepted during transmission.
2. **Secure session management:**
   Use strong, random session IDs and regenerate them after login/logout.
3. **Set secure cookie flags:**
   Enable HttpOnly and Secure flags to prevent cookie theft via scripts or unsecured connections.

4 . Types of Session Hijacking ?

1 . Active Session Hijacking :

- **Attacker takes control of the victim's active session.**
- **Performs actions like sending messages, changing data, or transferring money.**
- **Victim may get logged out suddenly or see unusual activity.**
- **High risk because data can be modified.**
- **Example: Attacker steals session ID and logs in as the user.**

2 . Passive Session Hijacking :

- **Attacker only monitors/sniffs the session traffic.**
- **No modification of data is done.**
- **Used mainly to collect information (usernames, session IDs).**
- **Victim usually does not notice the attack.**
- **Example: Sniffing HTTP traffic to capture cookies.**

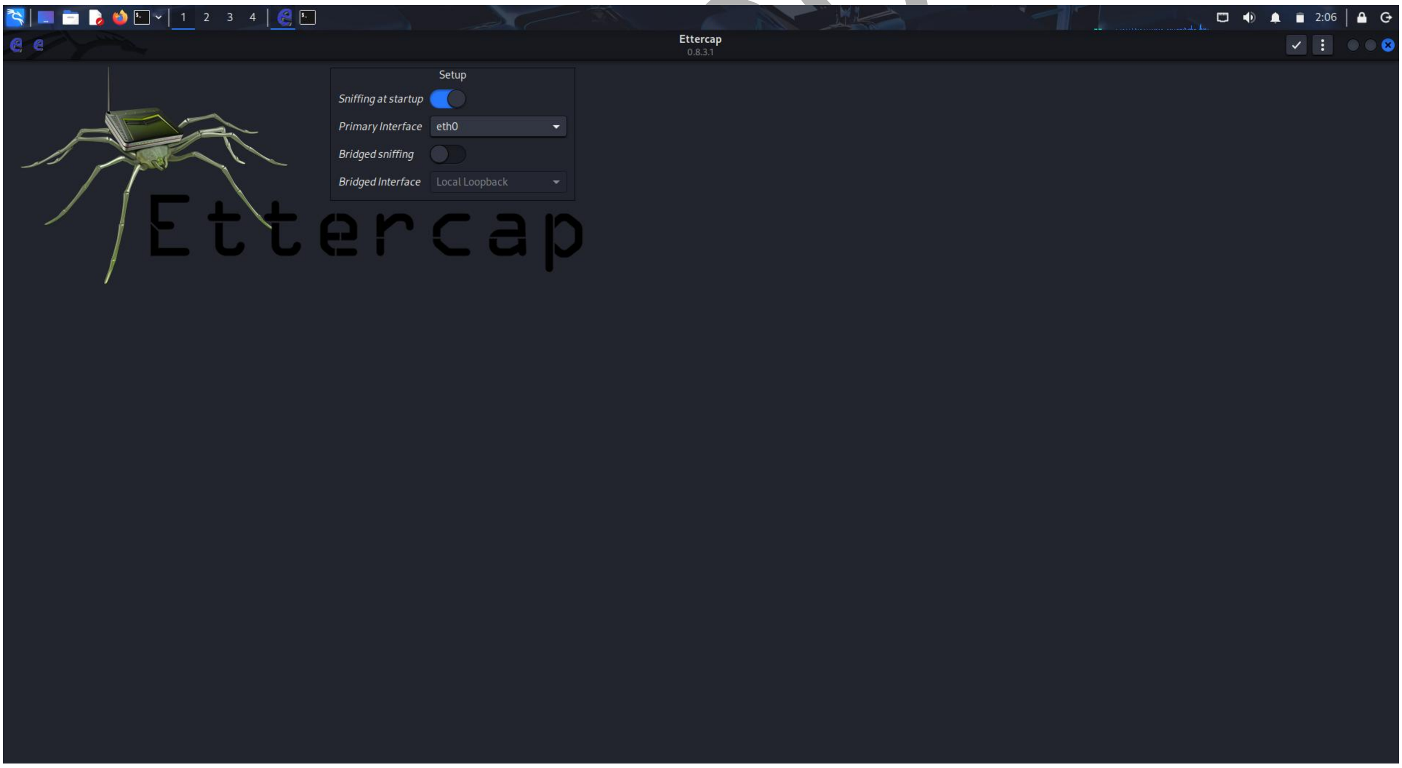
3 . Tools :

1 . Ettercap :

Ettercap is an open-source network security tool that is widely used to perform Man-in-the-Middle (MITM) attacks on local area networks. It is capable of real-time traffic interception, packet filtering, password sniffing, and session hijacking.

Steps :

1 . Click on this icon



Sniffing at startup ●

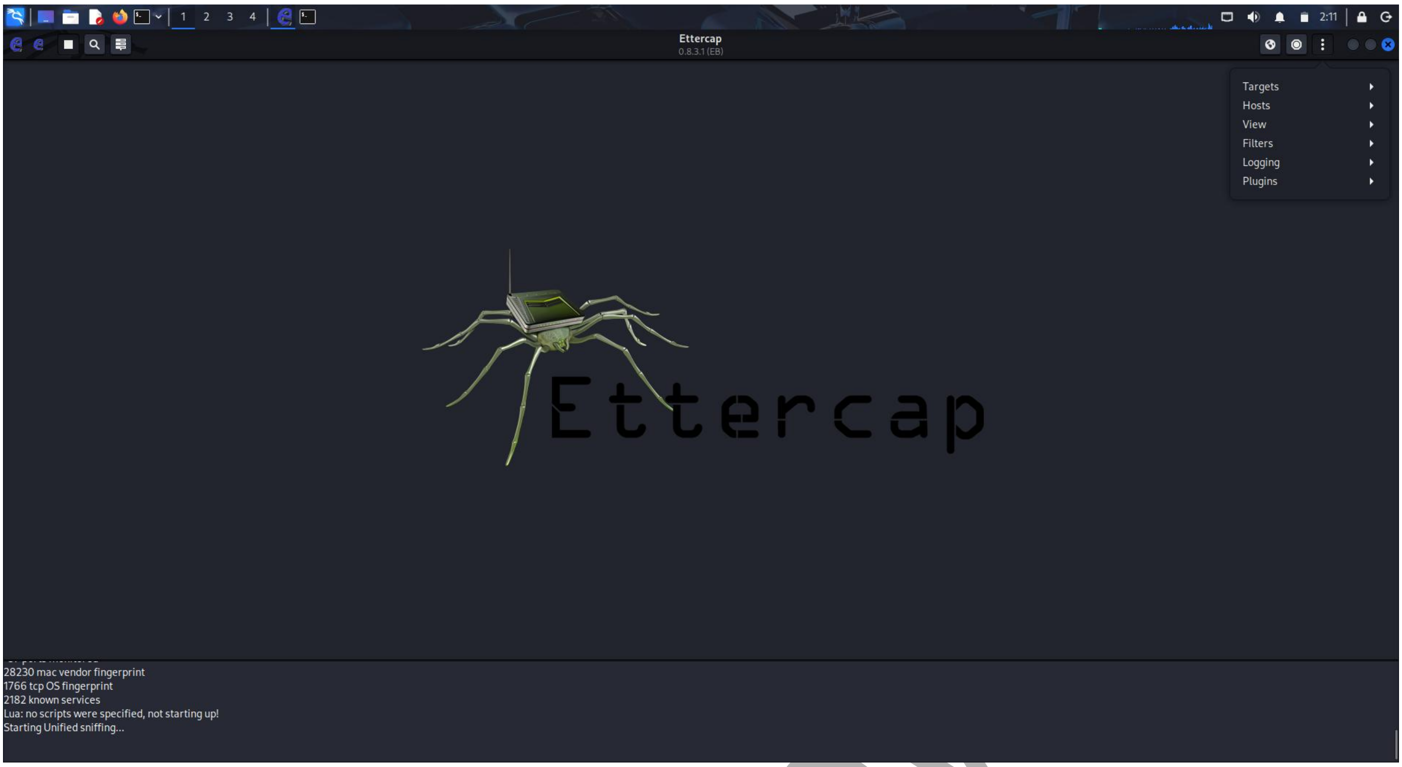
Primary Interface eth0

Bridged sniffing ○

Bridged Interface Local Loopback

1.1

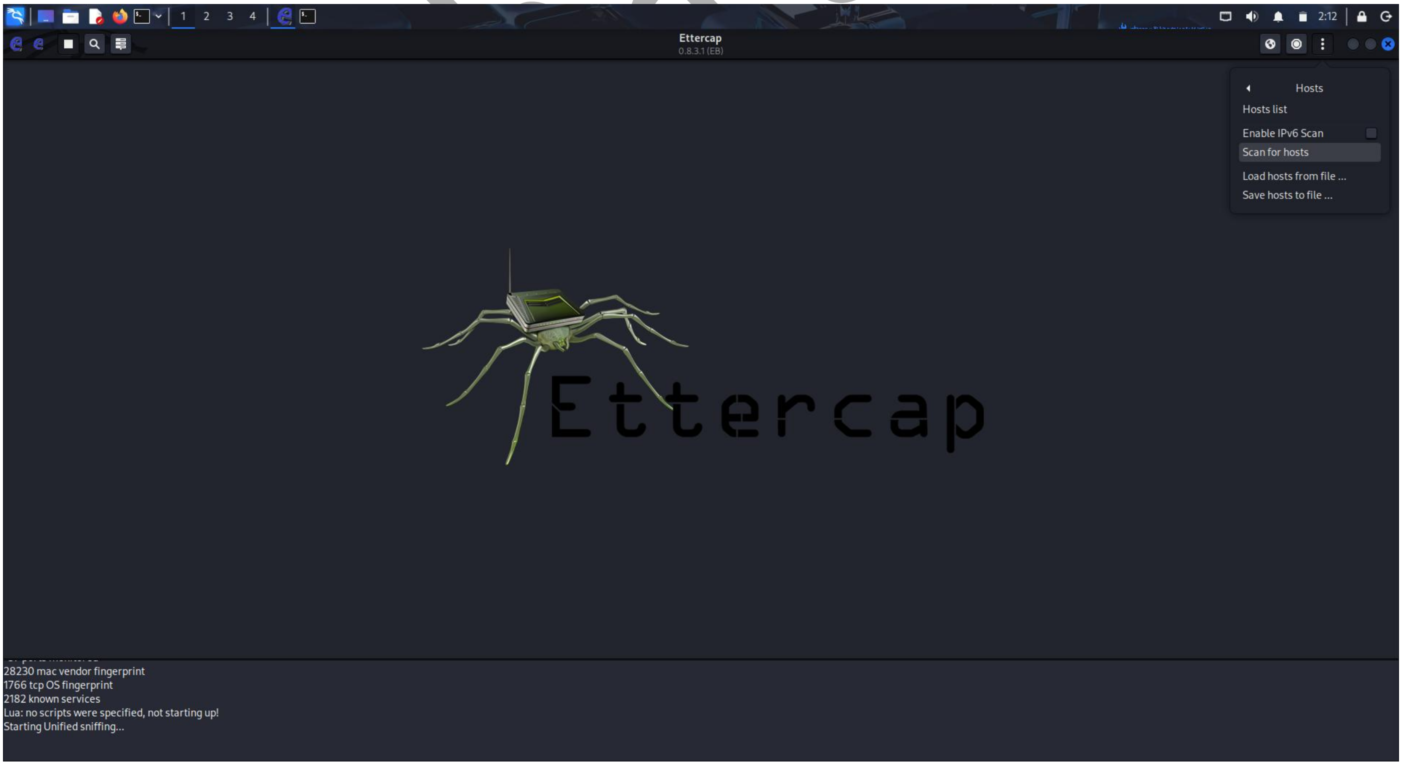
2 . click on three dot and then click on Hosts



```
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

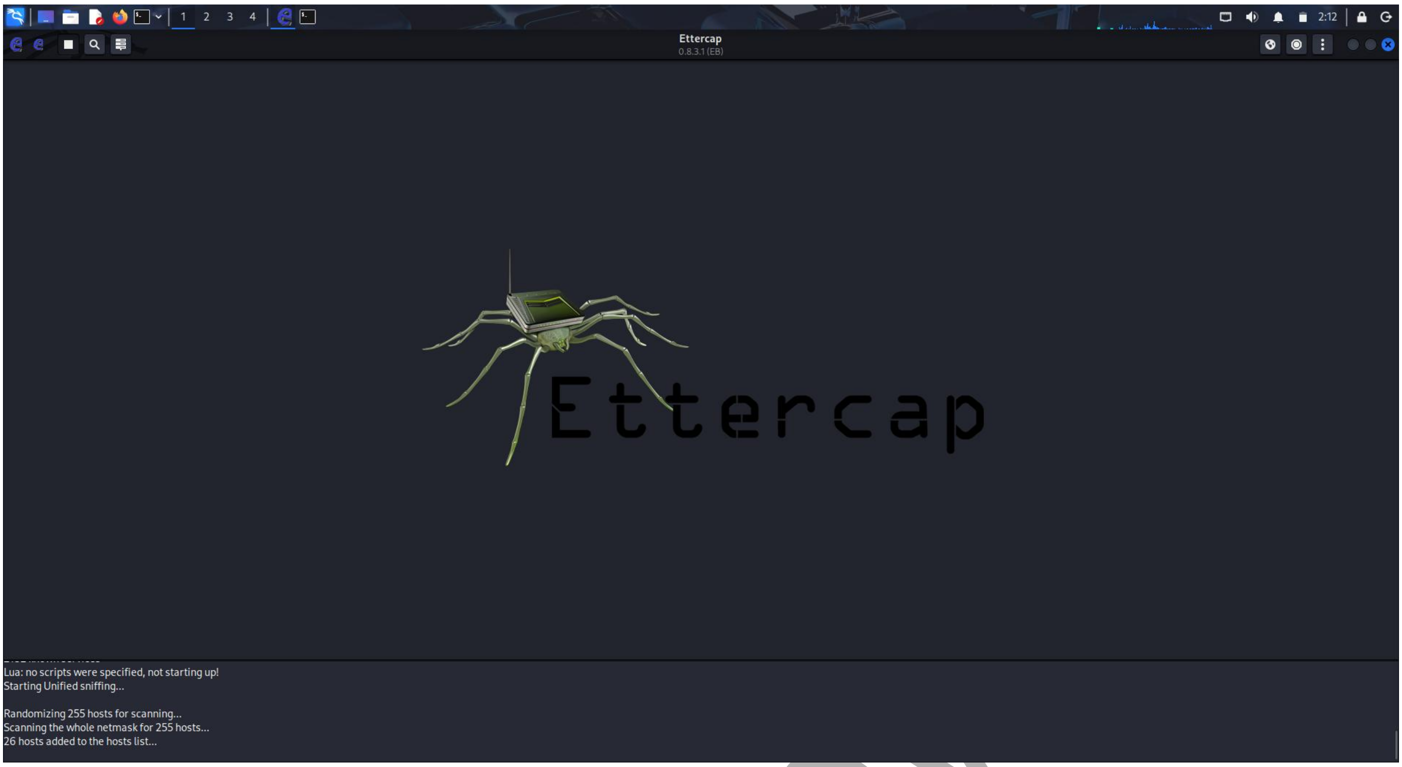
1.2

3 . Click on Scan For Hosts



```
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

1.3

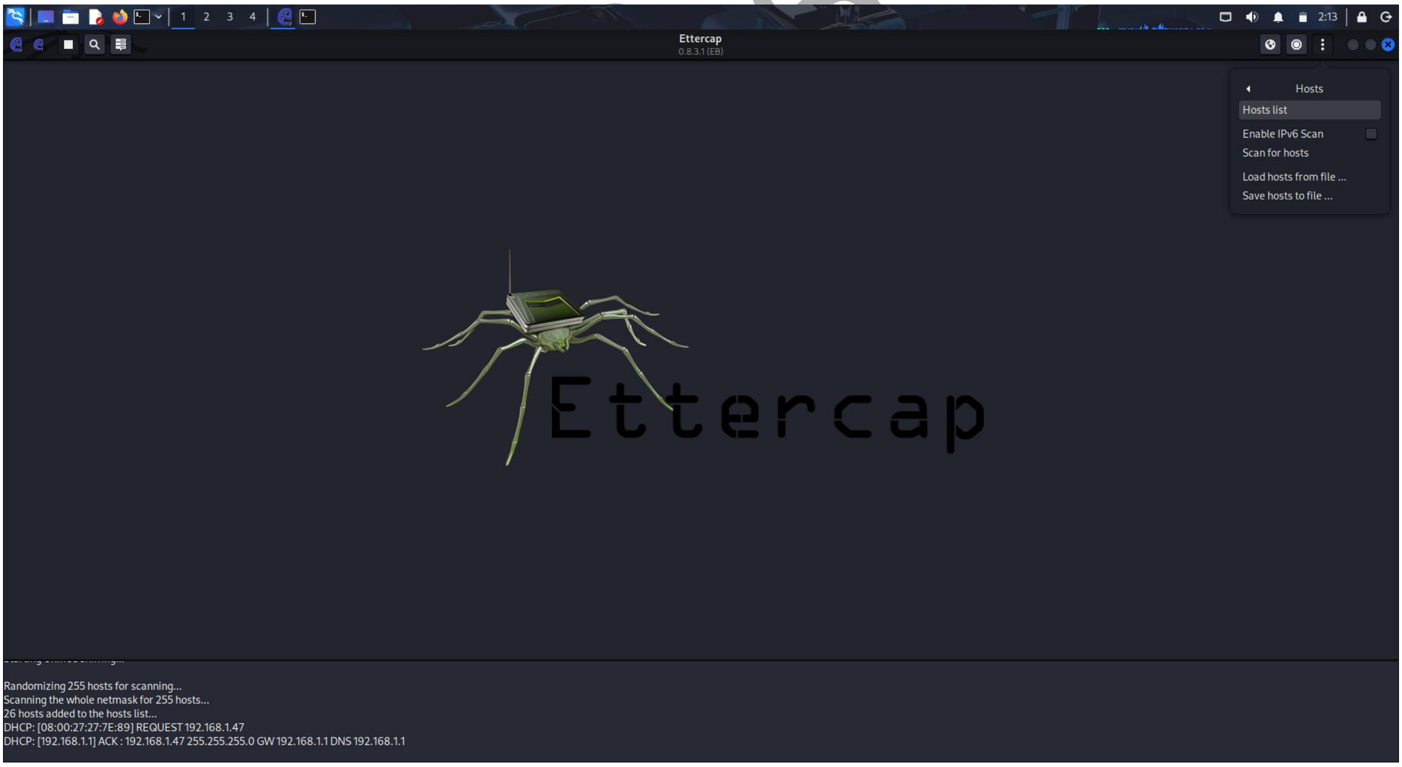


```
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
26 hosts added to the hosts list...
```

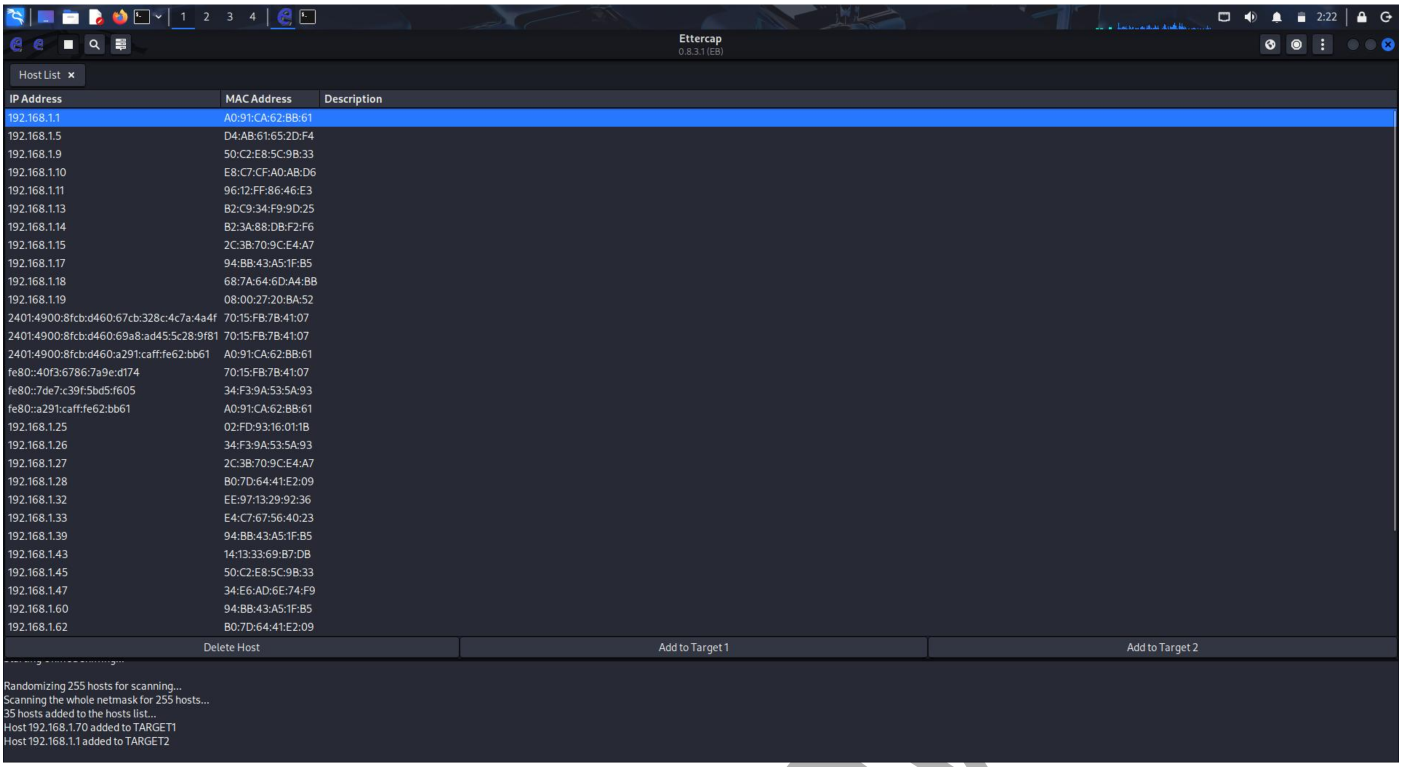
1.4

4 . Once Again click on Three Dot and click on Host List



```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
26 hosts added to the hosts list...
DHCP: [08:00:27:27:7E:89] REQUEST 192.168.1.47
DHCP: [192.168.1.1] ACK : 192.168.1.47 255.255.255.0 GW 192.168.1.1 DNS 192.168.1.1
```

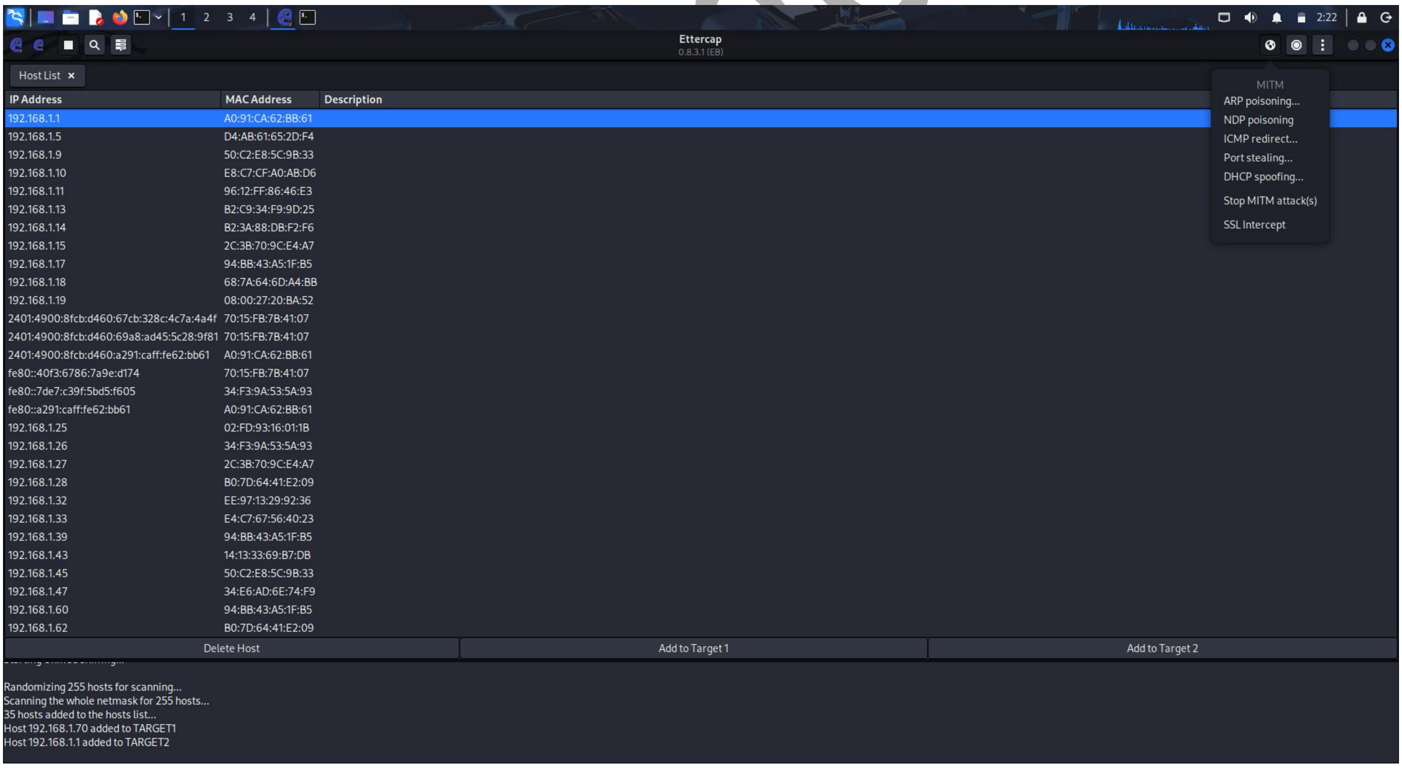
1.5



IP Address	MAC Address	Description
192.168.1.1	A0:91:CA:62:BB:61	
192.168.1.5	D4:AB:61:65:2D:F4	
192.168.1.9	50:C2:E8:5C:9B:33	
192.168.1.10	E8:C7:CF:A0:AB:D6	
192.168.1.11	96:12:FF:86:46:E3	
192.168.1.13	B2:C9:34:F9:9D:25	
192.168.1.14	B2:3A:88:DB:F2:F6	
192.168.1.15	2C:3B:70:9C:E4:A7	
192.168.1.17	94:BB:43:A5:1F:B5	
192.168.1.18	68:7A:64:6D:A4:BB	
192.168.1.19	08:00:27:20:BA:52	
2401:4900:8fcb:d460:67cb:328c:4c7a:4a4f	70:15:FB:7B:41:07	
2401:4900:8fcb:d460:69a8:ad45:5c28:9f81	70:15:FB:7B:41:07	
2401:4900:8fcb:d460:a291:caff:fe62:bb61	A0:91:CA:62:BB:61	
fe80::40f3:6786:7a9e:d174	70:15:FB:7B:41:07	
fe80::7de7:c39f:5bd5:f605	34:F3:9A:53:5A:93	
fe80::a291:caff:fe62:bb61	A0:91:CA:62:BB:61	
192.168.1.25	02:FD:93:16:01:1B	
192.168.1.26	34:F3:9A:53:5A:93	
192.168.1.27	2C:3B:70:9C:E4:A7	
192.168.1.28	B0:7D:64:41:E2:09	
192.168.1.32	EE:97:13:29:92:36	
192.168.1.33	E4:C7:67:56:40:23	
192.168.1.39	94:BB:43:A5:1F:B5	
192.168.1.43	14:13:33:69:B7:DB	
192.168.1.45	50:C2:E8:5C:9B:33	
192.168.1.47	34:E6:AD:6E:74:F9	
192.168.1.60	94:BB:43:A5:1F:B5	
192.168.1.62	B0:7D:64:41:E2:09	

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
35 hosts added to the hosts list...
Host 192.168.1.70 added to TARGET1
Host 192.168.1.1 added to TARGET2
```

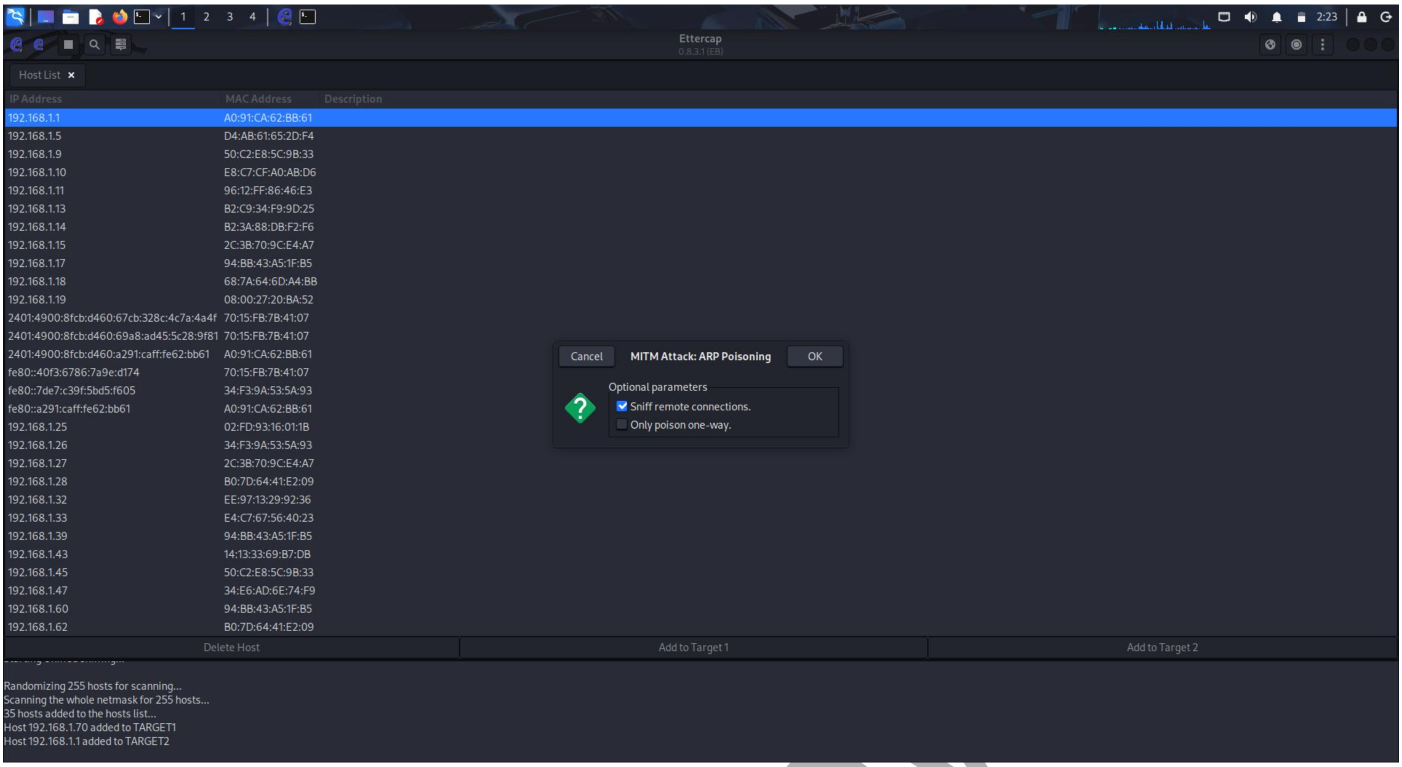
1.6



IP Address	MAC Address	Description
192.168.1.1	A0:91:CA:62:BB:61	
192.168.1.5	D4:AB:61:65:2D:F4	
192.168.1.9	50:C2:E8:5C:9B:33	
192.168.1.10	E8:C7:CF:A0:AB:D6	
192.168.1.11	96:12:FF:86:46:E3	
192.168.1.13	B2:C9:34:F9:9D:25	
192.168.1.14	B2:3A:88:DB:F2:F6	
192.168.1.15	2C:3B:70:9C:E4:A7	
192.168.1.17	94:BB:43:A5:1F:B5	
192.168.1.18	68:7A:64:6D:A4:BB	
192.168.1.19	08:00:27:20:BA:52	
2401:4900:8fcb:d460:67cb:328c:4c7a:4a4f	70:15:FB:7B:41:07	
2401:4900:8fcb:d460:69a8:ad45:5c28:9f81	70:15:FB:7B:41:07	
2401:4900:8fcb:d460:a291:caff:fe62:bb61	A0:91:CA:62:BB:61	
fe80::40f3:6786:7a9e:d174	70:15:FB:7B:41:07	
fe80::7de7:c39f:5bd5:f605	34:F3:9A:53:5A:93	
fe80::a291:caff:fe62:bb61	A0:91:CA:62:BB:61	
192.168.1.25	02:FD:93:16:01:1B	
192.168.1.26	34:F3:9A:53:5A:93	
192.168.1.27	2C:3B:70:9C:E4:A7	
192.168.1.28	B0:7D:64:41:E2:09	
192.168.1.32	EE:97:13:29:92:36	
192.168.1.33	E4:C7:67:56:40:23	
192.168.1.39	94:BB:43:A5:1F:B5	
192.168.1.43	14:13:33:69:B7:DB	
192.168.1.45	50:C2:E8:5C:9B:33	
192.168.1.47	34:E6:AD:6E:74:F9	
192.168.1.60	94:BB:43:A5:1F:B5	
192.168.1.62	B0:7D:64:41:E2:09	

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
35 hosts added to the hosts list...
Host 192.168.1.70 added to TARGET1
Host 192.168.1.1 added to TARGET2
```

1.7



IP Address	MAC Address	Description
192.168.1.1	A0:91:CA:62:BB:61	
192.168.1.5	D4:AB:61:65:2D:F4	
192.168.1.9	50:C2:E8:5C:9B:33	
192.168.1.10	E8:C7:CF:A0:AB:D6	
192.168.1.11	96:12:FF:86:46:E3	
192.168.1.13	B2:C9:34:F9:9D:25	
192.168.1.14	B2:3A:88:DB:F2:F6	
192.168.1.15	2C:3B:70:9C:E4:A7	
192.168.1.17	94:BB:43:A5:1F:B5	
192.168.1.18	68:7A:64:6D:A4:BB	
192.168.1.19	08:00:27:20:BA:52	
2401:4900:8fcb:d460:67cb:328c:4c7a:4a4f	70:15:FB:7B:41:07	
2401:4900:8fcb:d460:69a8:ad45:5c28:9f81	70:15:FB:7B:41:07	
2401:4900:8fcb:d460:a291:caff:fe62:bb61	A0:91:CA:62:BB:61	
fe80::40f3:6786:7a9e:d174	70:15:FB:7B:41:07	
fe80::7de7:c39f:5bd5:f605	34:F3:9A:53:5A:93	
fe80::a291:caff:fe62:bb61	A0:91:CA:62:BB:61	
192.168.1.25	02:FD:93:16:01:1B	
192.168.1.26	34:F3:9A:53:5A:93	
192.168.1.27	2C:3B:70:9C:E4:A7	
192.168.1.28	B0:7D:64:41:E2:09	
192.168.1.32	EE:97:13:29:92:36	
192.168.1.33	E4:C7:67:56:40:23	
192.168.1.39	94:BB:43:A5:1F:B5	
192.168.1.43	14:13:33:69:B7:DB	
192.168.1.45	50:C2:E8:5C:9B:33	
192.168.1.47	34:E6:AD:6E:74:F9	
192.168.1.60	94:BB:43:A5:1F:B5	
192.168.1.62	B0:7D:64:41:E2:09	

Cancel **MITM Attack: ARP Poisoning** OK

Optional parameters

☑ Sniff remote connections.

□ Only poison one-way.

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
35 hosts added to the hosts list...
Host 192.168.1.70 added to TARGET1
Host 192.168.1.1 added to TARGET2
```

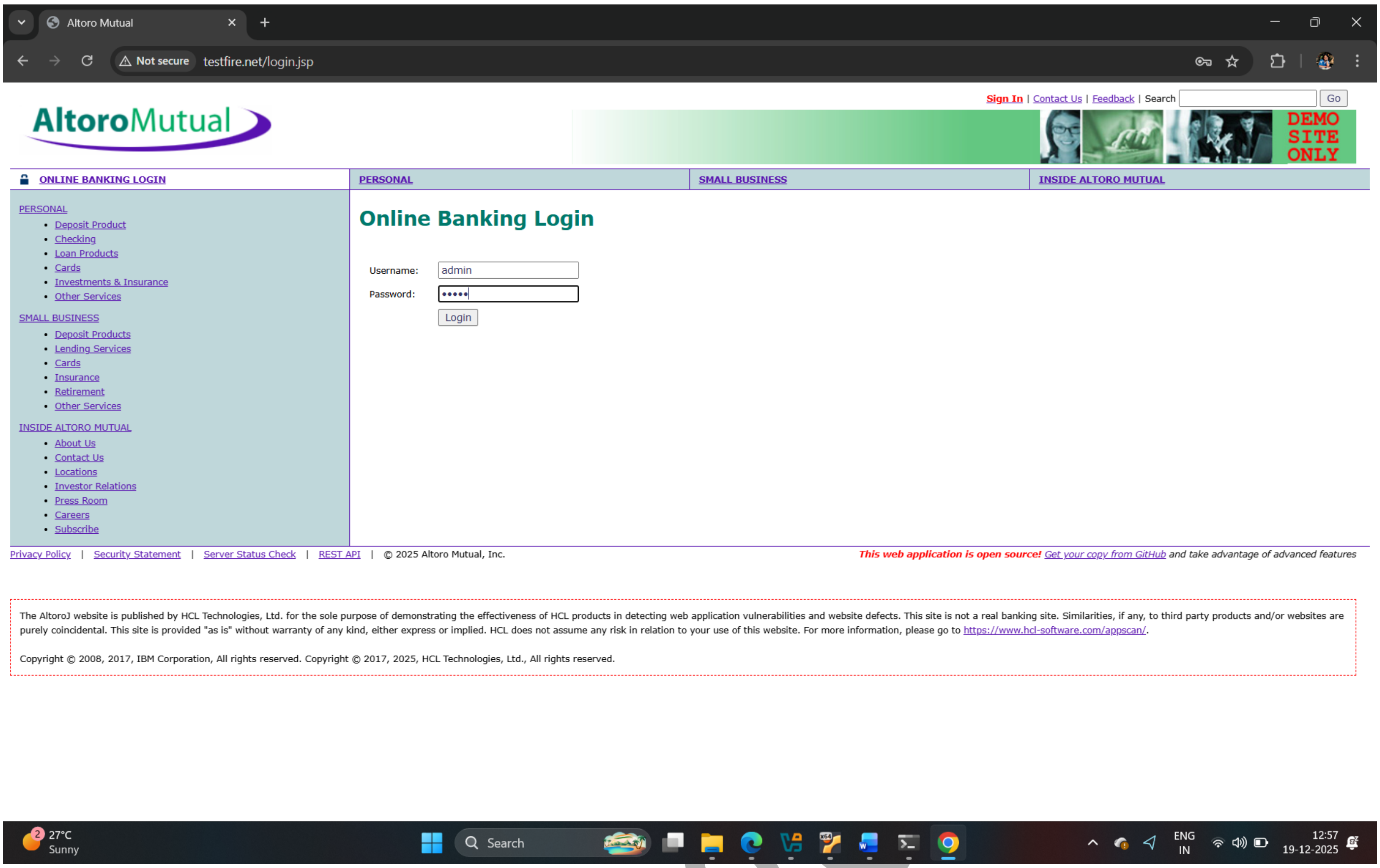
1.8

5 . Now , Assume That Your Target will sign in some website and you want to hijack their session and cookies .

Target Website

Login Process

Login Successful



Online Banking Login

Username: admin

Password: •••••

Login

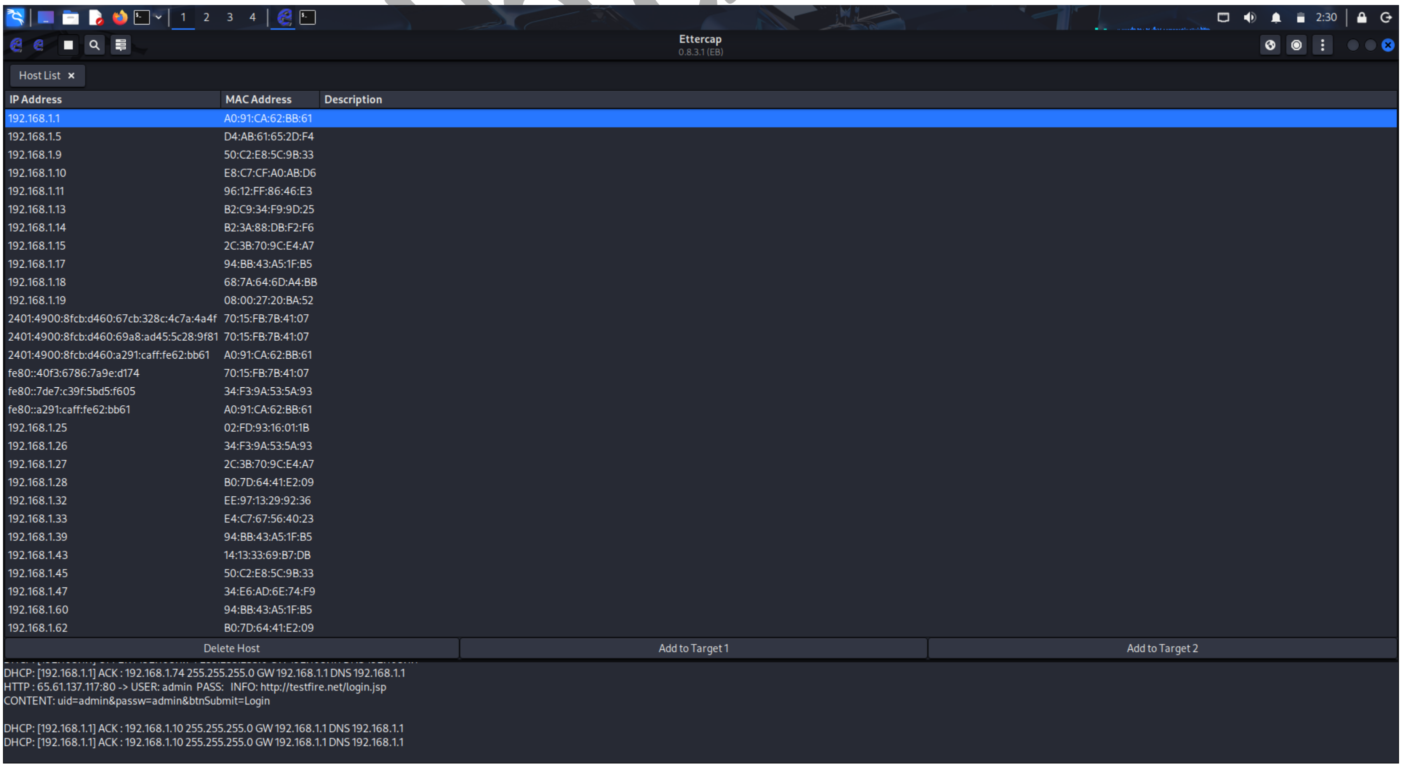
Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.

1.9



IP Address	MAC Address	Description
192.168.1.1	A0:91:CA:62:BB:61	
192.168.1.5	D4:AB:61:65:2D:F4	
192.168.1.9	50:C2:E8:5C:9B:33	
192.168.1.10	E8:C7:CF:A0:AB:D6	
192.168.1.11	96:12:FF:86:46:E3	
192.168.1.13	B2:C9:34:F9:9D:25	
192.168.1.14	B2:3A:88:DB:F2:F6	
192.168.1.15	2C:3B:70:9C:E4:A7	
192.168.1.17	94:BB:43:A5:1F:B5	
192.168.1.18	68:7A:64:6D:A4:BB	
192.168.1.19	08:00:27:20:BA:52	
2401:4900:8fcb:d460:67cb:328c:4c7a:4a4f	70:15:FB:7B:41:07	
2401:4900:8fcb:d460:69a8:ad45:5c28:9f81	70:15:FB:7B:41:07	
2401:4900:8fcb:d460:a291:caff:fe62:bb61	A0:91:CA:62:BB:61	
fe80::40f3:6786:7a9e:d174	70:15:FB:7B:41:07	
fe80::7de7:c39f:5bd5:f605	34:F3:9A:53:5A:93	
fe80::a291:caff:fe62:bb61	A0:91:CA:62:BB:61	
192.168.1.25	02:FD:93:16:01:1B	
192.168.1.26	34:F3:9A:53:5A:93	
192.168.1.27	2C:3B:70:9C:E4:A7	
192.168.1.28	B0:7D:64:41:E2:09	
192.168.1.32	EE:97:13:29:92:36	
192.168.1.33	E4:C7:67:56:40:23	
192.168.1.39	94:BB:43:A5:1F:B5	
192.168.1.43	14:13:33:69:B7:DB	
192.168.1.45	50:C2:E8:5C:9B:33	
192.168.1.47	34:E6:AD:6E:74:F9	
192.168.1.60	94:BB:43:A5:1F:B5	
192.168.1.62	B0:7D:64:41:E2:09	

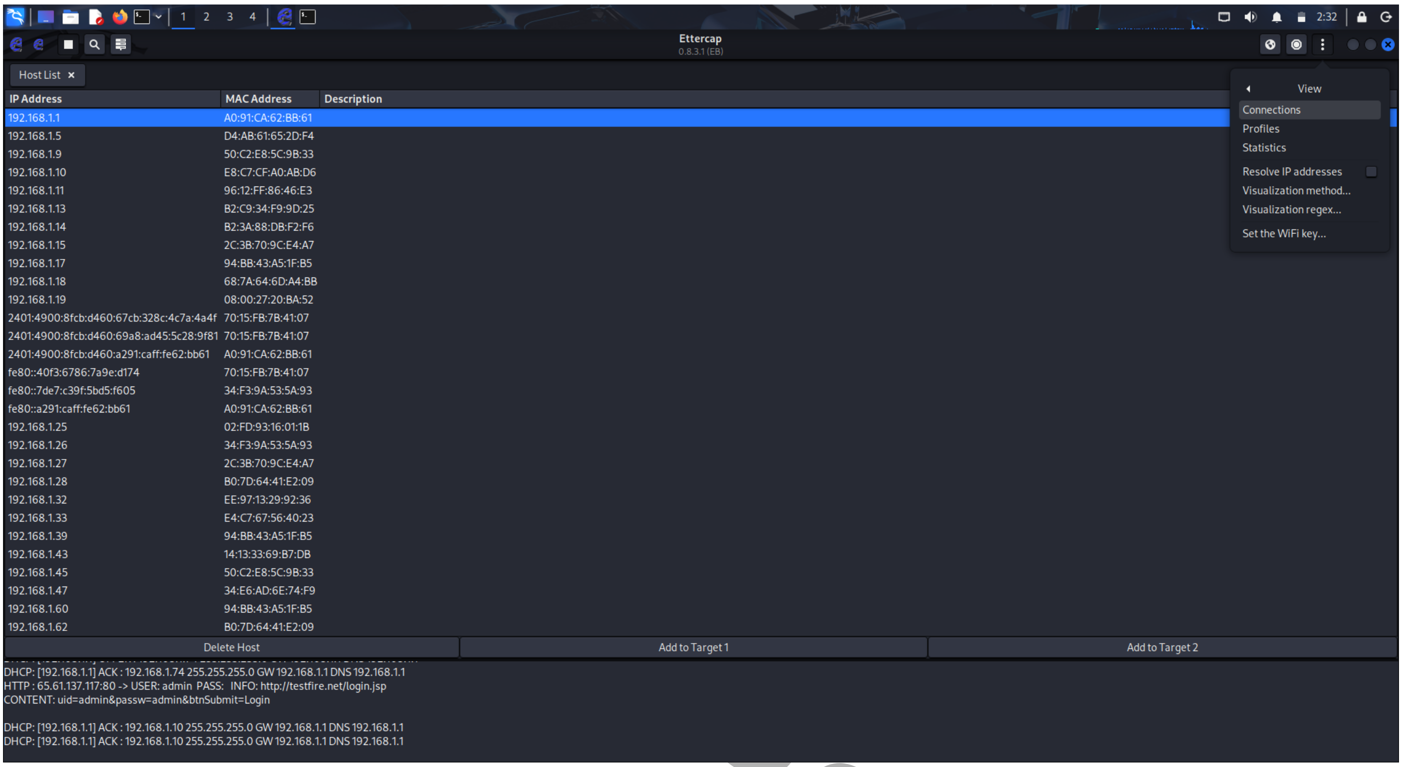
```
DHCP: [192.168.1.1] ACK : 192.168.1.74 255.255.255.0 GW 192.168.1.1 DNS 192.168.1.1
HTTP : 65.61.137.117:80 -> USER: admin  PASS:   INFO: http://testfire.net/login.jsp
CONTENT: uid=admin&passw=admin&btnSubmit=Login

DHCP: [192.168.1.1] ACK : 192.168.1.10 255.255.255.0 GW 192.168.1.1 DNS 192.168.1.1
DHCP: [192.168.1.1] ACK : 192.168.1.10 255.255.255.0 GW 192.168.1.1 DNS 192.168.1.1
```

2.0

6 . it capture Many packets .

7 . Search Using Target Ip address .



IP Address	MAC Address	Description
192.168.1.1	A0:91:CA:62:BB:61	
192.168.1.5	D4:AB:61:65:2D:F4	
192.168.1.9	50:C2:E8:5C:9B:33	
192.168.1.10	E8:C7:CF:A0:AB:D6	
192.168.1.11	96:12:FF:86:46:E3	
192.168.1.13	B2:C9:34:F9:9D:25	
192.168.1.14	B2:3A:88:DB:F2:F6	
192.168.1.15	2C:3B:70:9C:E4:A7	
192.168.1.17	94:BB:43:A5:1F:B5	
192.168.1.18	68:7A:64:6D:A4:BB	
192.168.1.19	08:00:27:20:BA:52	
2401:4900:8fcb:d460:67cb:328c:4c7a:4a4f	70:15:FB:7B:41:07	
2401:4900:8fcb:d460:69a8:ad45:5c28:9f81	70:15:FB:7B:41:07	
2401:4900:8fcb:d460:a291:caff:fe62:bb61	A0:91:CA:62:BB:61	
fe80::40f3:6786:7a9e:d174	70:15:FB:7B:41:07	
fe80::7de7:c39f:5bd5:f605	34:F3:9A:53:5A:93	
fe80::a291:caff:fe62:bb61	A0:91:CA:62:BB:61	
192.168.1.25	02:FD:93:16:01:1B	
192.168.1.26	34:F3:9A:53:5A:93	
192.168.1.27	2C:3B:70:9C:E4:A7	
192.168.1.28	B0:7D:64:41:E2:09	
192.168.1.32	EE:97:13:29:92:36	
192.168.1.33	E4:C7:67:56:40:23	
192.168.1.39	94:BB:43:A5:1F:B5	
192.168.1.43	14:13:33:69:B7:DB	
192.168.1.45	50:C2:E8:5C:9B:33	
192.168.1.47	34:E6:AD:6E:74:F9	
192.168.1.60	94:BB:43:A5:1F:B5	
192.168.1.62	B0:7D:64:41:E2:09	

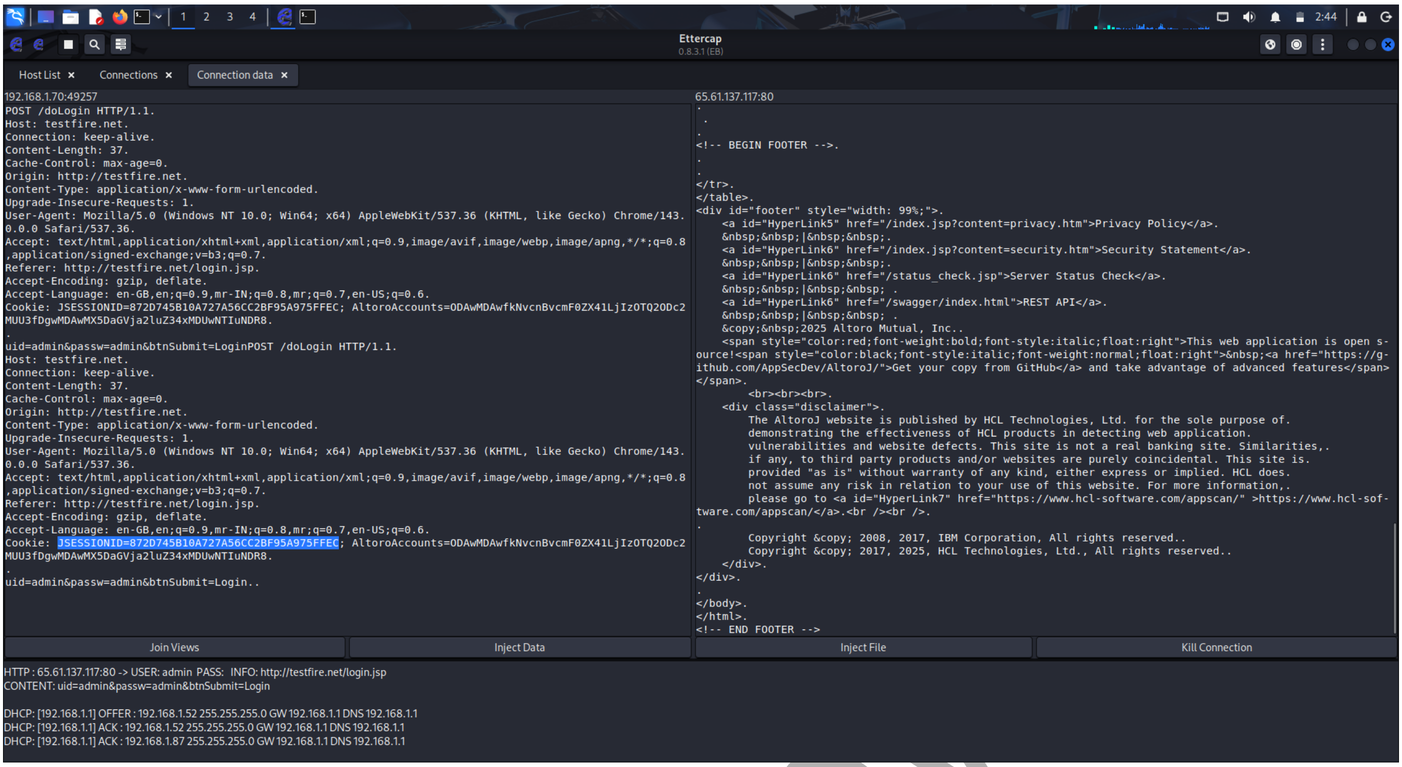
```
DHCP: [192.168.1.1] ACK : 192.168.1.74 255.255.255.0 GW 192.168.1.1 DNS 192.168.1.1
HTTP : 65.61.137.117:80 -> USER: admin  PASS:   INFO: http://testfire.net/login.jsp
CONTENT: uid=admin&passw=admin&btnSubmit=Login

DHCP: [192.168.1.1] ACK : 192.168.1.10 255.255.255.0 GW 192.168.1.1 DNS 192.168.1.1
DHCP: [192.168.1.1] ACK : 192.168.1.10 255.255.255.0 GW 192.168.1.1 DNS 192.168.1.1
```

2.1

8 . here , it capture session id and all like website and other things

Session Id • Now , copy this Session Id



```
192.168.1.70:49257
POST /doLogin HTTP/1.1.
Host: testfire.net.
Connection: keep-alive.
Content-Length: 37.
Cache-Control: max-age=0.
Origin: http://testfire.net.
Content-Type: application/x-www-form-urlencoded.
Upgrade-Insecure-Requests: 1.
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.
0.0.0 Safari/537.36.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
,application/signed-exchange;v=b3;q=0.7.
Referer: http://testfire.net/login.jsp.
Accept-Encoding: gzip, deflate.
Accept-Language: en-GB,en;q=0.9,mr-IN;q=0.8,mr;q=0.7,en-US;q=0.6.
Cookie: JSESSIONID=872D745B10A727A56CC2BF95A975FFEC; AltoroAccounts=ODAwMDAwfkNvcnBvcmF0ZX41LjIzOTQ2ODc2
MUU3fDgwMDAwMX5DaGVja2luZ34xMDUwNTIuNDR8.
.
uid=admin&passw=admin&btnSubmit=LoginPOST /doLogin HTTP/1.1.
Host: testfire.net.
Connection: keep-alive.
Content-Length: 37.
Cache-Control: max-age=0.
Origin: http://testfire.net.
Content-Type: application/x-www-form-urlencoded.
Upgrade-Insecure-Requests: 1.
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.
0.0.0 Safari/537.36.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
,application/signed-exchange;v=b3;q=0.7.
Referer: http://testfire.net/login.jsp.
Accept-Encoding: gzip, deflate.
Accept-Language: en-GB,en;q=0.9,mr-IN;q=0.8,mr;q=0.7,en-US;q=0.6.
Cookie: JSESSIONID=872D745B10A727A56CC2BF95A975FFEC; AltoroAccounts=ODAwMDAwfkNvcnBvcmF0ZX41LjIzOTQ2ODc2
MUU3fDgwMDAwMX5DaGVja2luZ34xMDUwNTIuNDR8.
.
uid=admin&passw=admin&btnSubmit=Login..
```

```
65.61.137.117:80
.
 .
.
<!-- BEGIN FOOTER -->.
.
.
</tr>.
</table>.
<div id="footer" style="width: 99%;">.
    <a id="HyperLink5" href="/index.jsp?content=privacy.htm">Privacy Policy</a>.
    &nbsp;&nbsp;|&nbsp;&nbsp;.
    <a id="HyperLink6" href="/index.jsp?content=security.htm">Security Statement</a>.
    &nbsp;&nbsp;|&nbsp;&nbsp;.
    <a id="HyperLink6" href="/status_check.jsp">Server Status Check</a>.
    &nbsp;&nbsp;|&nbsp;&nbsp; .
    <a id="HyperLink6" href="/swagger/index.html">REST API</a>.
    &nbsp;&nbsp;|&nbsp;&nbsp; .
    &copy;&nbsp;2025 Altoro Mutual, Inc..
    <span style="color:red;font-weight:bold;font-style:italic;float:right">This web application is open s-
ource!<span style="color:black;font-style:italic;font-weight:normal;float:right">&nbsp;<a href="https://g-
ithub.com/AppSecDev/AltoroJ/">Get your copy from GitHub</a> and take advantage of advanced features</span>
</span>.
        <br><br><br>.
    <div class="disclaimer">.
        The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of.
        demonstrating the effectiveness of HCL products in detecting web application.
        vulnerabilities and website defects. This site is not a real banking site. Similarities,.
        if any, to third party products and/or websites are purely coincidental. This site is.
        provided "as is" without warranty of any kind, either express or implied. HCL does.
        not assume any risk in relation to your use of this website. For more information,.
        please go to <a id="HyperLink7" href="https://www.hcl-software.com/appscan/" >https://www.hcl-sof-
tware.com/appscan/</a>.<br /><br />.
.
        Copyright &copy; 2008, 2017, IBM Corporation, All rights reserved..
        Copyright &copy; 2017, 2025, HCL Technologies, Ltd., All rights reserved..
    </div>.
</div>.
.
</body>.
</html>.
<!-- END FOOTER -->
```

```
HTTP : 65.61.137.117:80 -> USER: admin  PASS:   INFO: http://testfire.net/login.jsp
CONTENT: uid=admin&passw=admin&btnSubmit=Login

DHCP: [192.168.1.1] OFFER : 192.168.1.52 255.255.255.0 GW 192.168.1.1 DNS 192.168.1.1
DHCP: [192.168.1.1] ACK : 192.168.1.52 255.255.255.0 GW 192.168.1.1 DNS 192.168.1.1
DHCP: [192.168.1.1] ACK : 192.168.1.87 255.255.255.0 GW 192.168.1.1 DNS 192.168.1.1
```

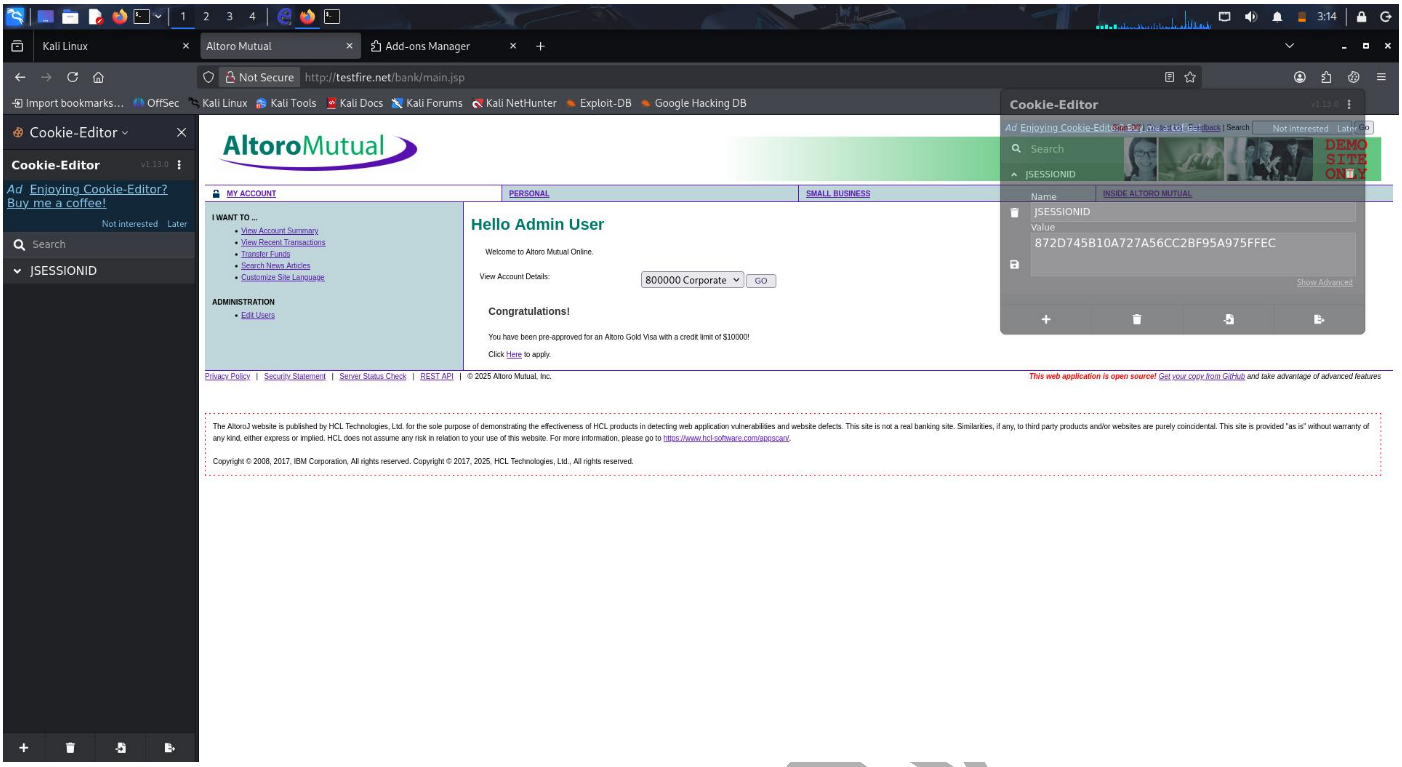
2.2

9 . Open target Website

10 . Go to Extensions and open Cookies Editor • Replace this session id

To this , that you copy from Ettercap

Login



Cookie-Editor

JSESSIONID

Name: JSESSIONID

Value: 872D745B10A727A56CC2BF95A975FFEC

http://testfire.net/bank/main.jsp

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.

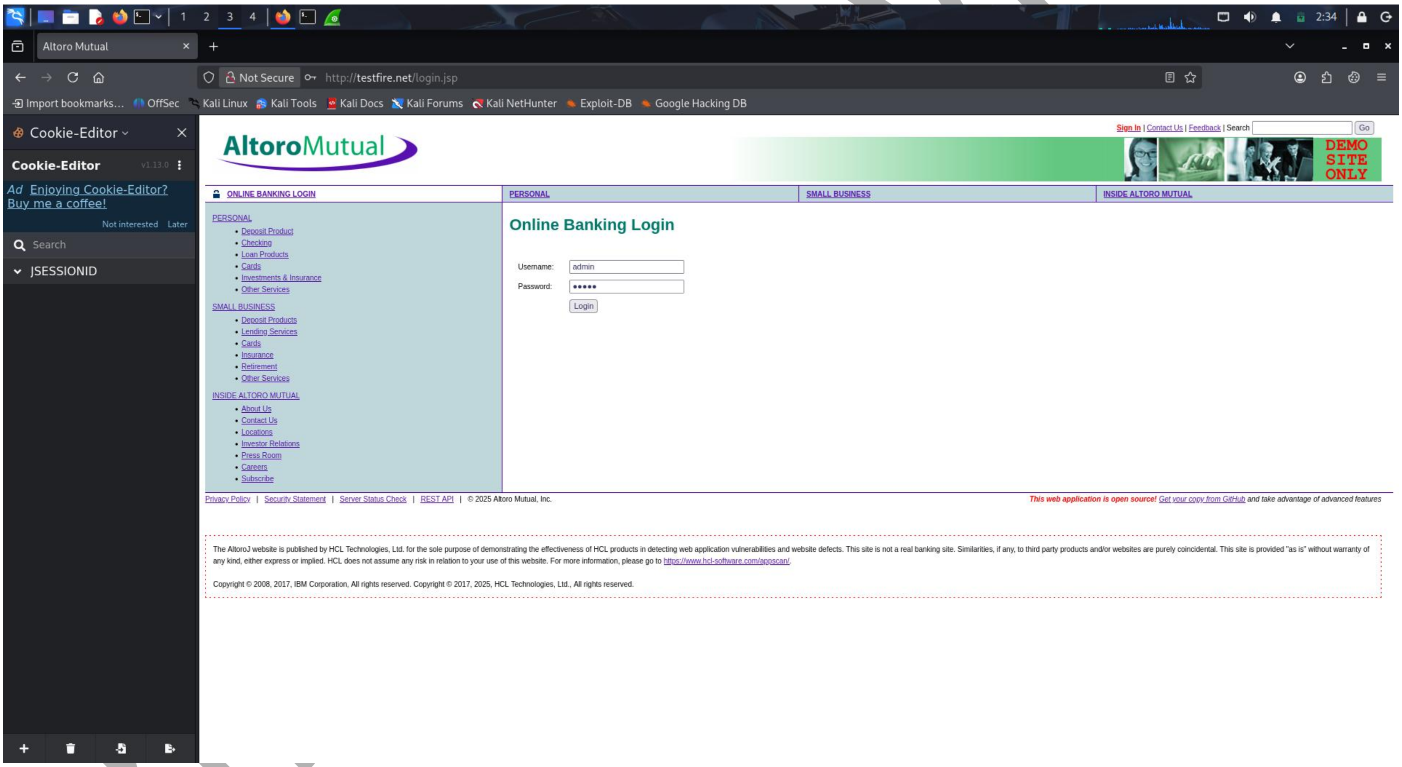
2.3

2 . wireshark :

Wireshark is a packet analyzer. It does not hijack sessions by itself, but it can be used to observe network traffic. If traffic is not encrypted, sensitive session data may be visible.

Steps :

1 . Target Website



http://testfire.net/login.jsp

Online Banking Login

Username: admin

Password: •••••

This web application is open source! Get your copy from GitHub and take advantage of advanced features

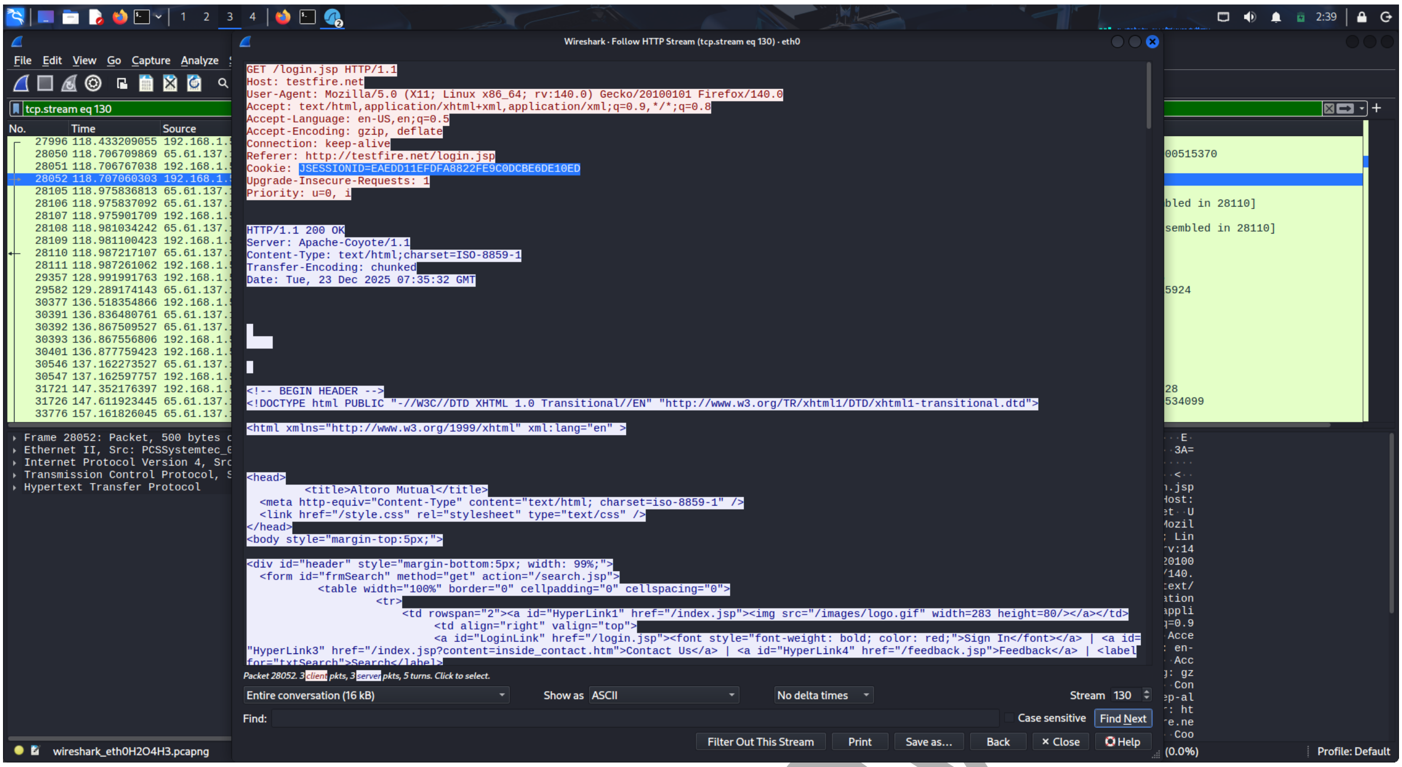
The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.

1.1

2 . Open wireshark and find http Post Request

Now , copy JSESSIONID



Wireshark · Follow HTTP Stream (tcp.stream eq 130) · eth0

```
GET /login.jsp HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=EAEDD11EFDFA8822FE9C0DCBE6DE10ED
Upgrade-Insecure-Requests: 1
Priority: u=0, i


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Tue, 23 Dec 2025 07:35:32 GMT



<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
         <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
           <table width="100%" border="0" cellpadding="0" cellspacing="0">
                    <tr>
                        <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
                             <td align="right" valign="top">
                             <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id=
"HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label
for="txtSearch">Search</label>
```

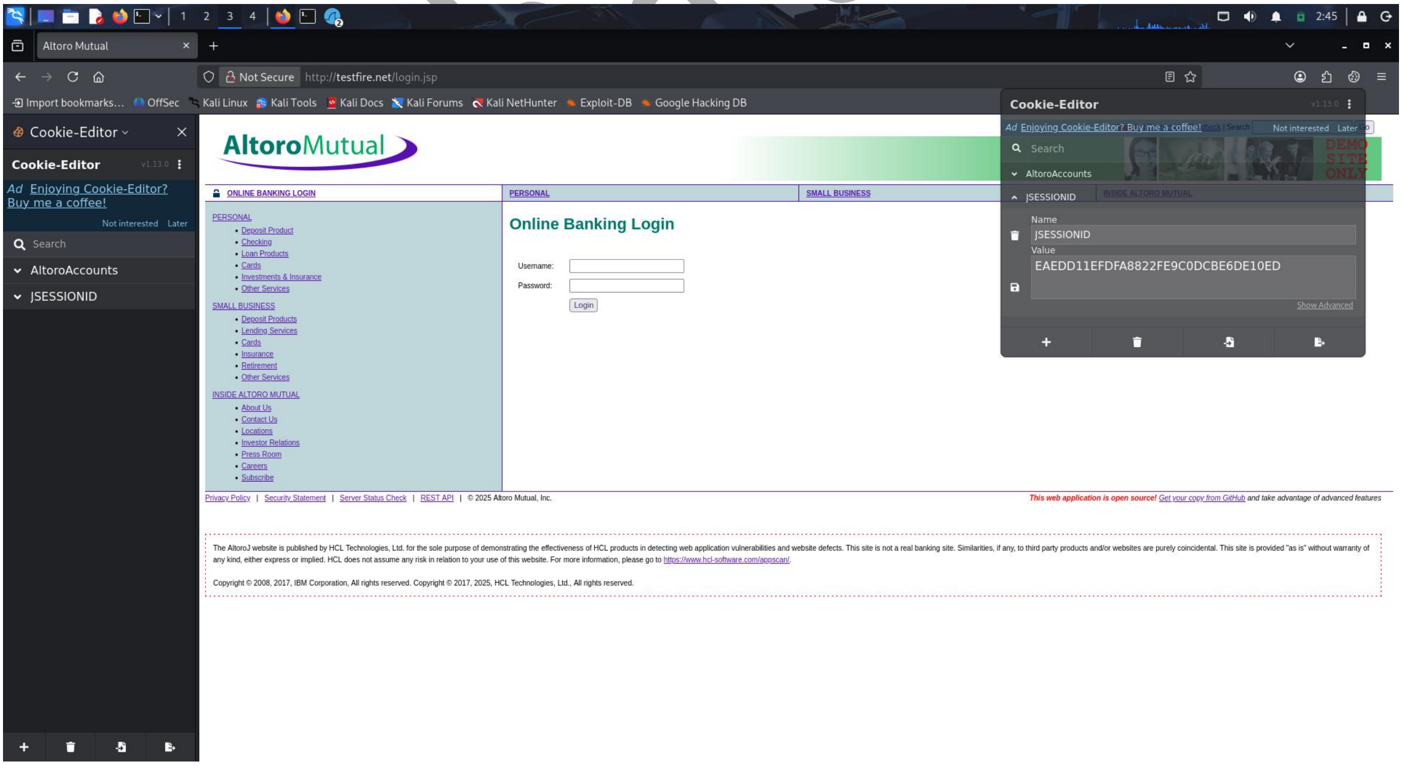
Packet 28052. 3 client pkts, 3 server pkts, 5 turns. Click to select.

Entire conversation (16 kB) | Show as ASCII | No delta times | Stream 130

1.2

3 . Now , go to another browser and open target website , sign in Option

Now open cookies editor extention and replace this JSESSIONID



Cookie-Editor

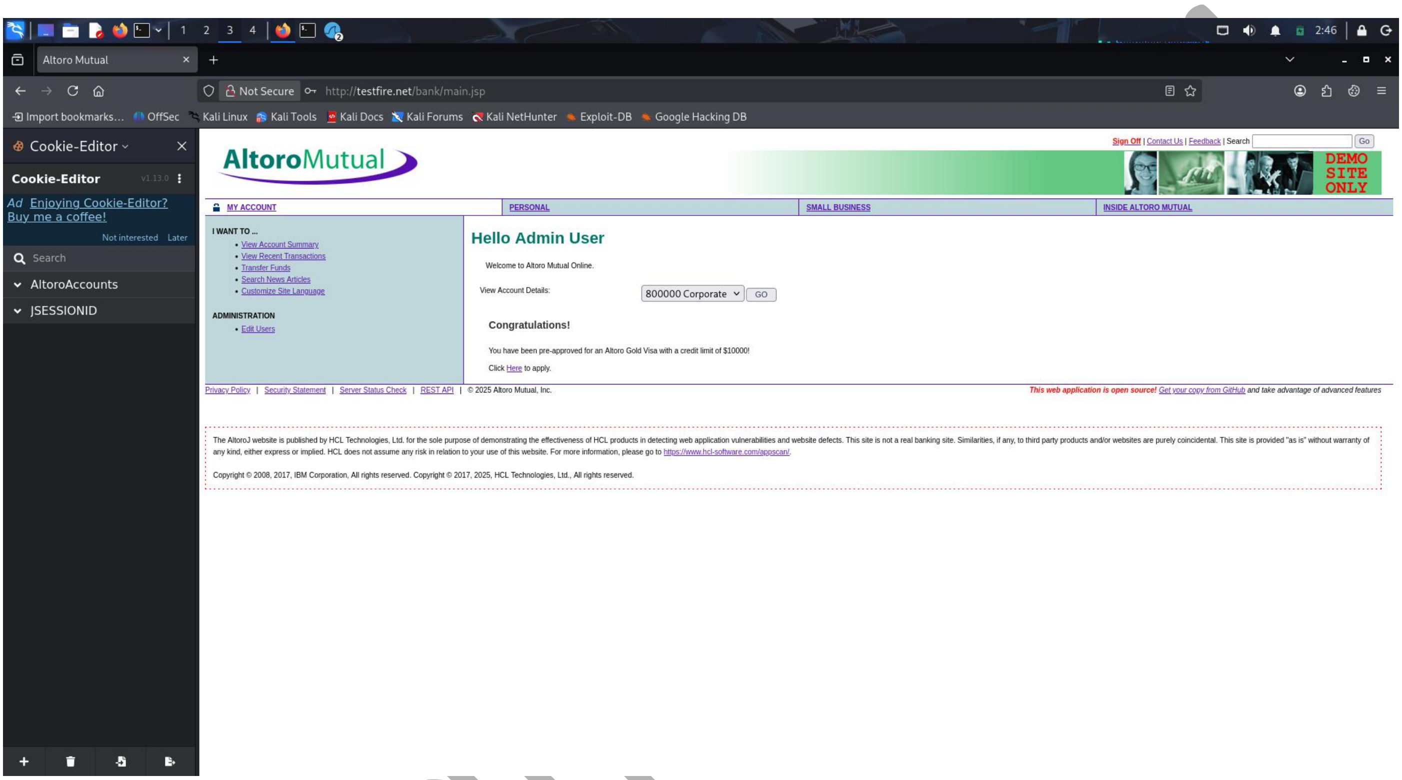
Name: JSESSIONID

Value: EAEDD11EFDFA8822FE9C0DCBE6DE10ED

1.3

4 . And then refresh browser , if cookies replace successfully , sign in option change to sign off option • Sign in to sign off without username and password

Login Successfully



I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.

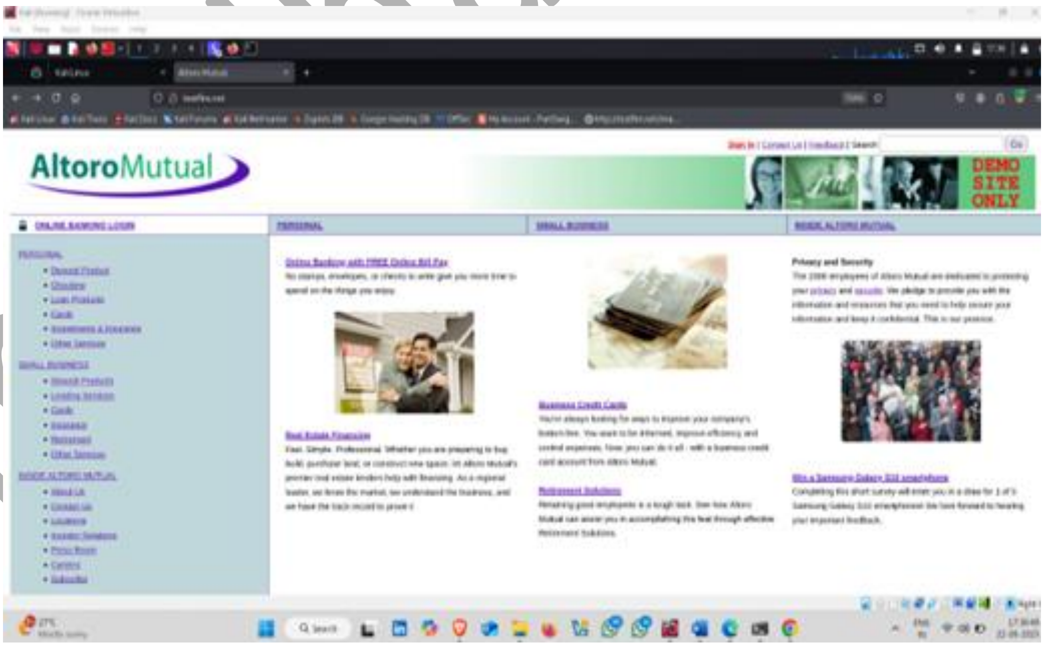
1.4

3 . Burp suite :

The Burp Suite Sequencer tool is used to assess the strength and unpredictability of session tokens generated by web applications. By capturing multiple session IDs, Sequencer analyzes the randomness and entropy to determine if the tokens can be predicted by an attacker. In this test, session cookies were collected and analyzed to check whether the application is using sufficiently strong, random, and unique tokens. Weak or predictable session IDs can lead to session hijacking and unauthorized access. This analysis helps ensure that the session management mechanism is secure and resistant to token prediction attacks.

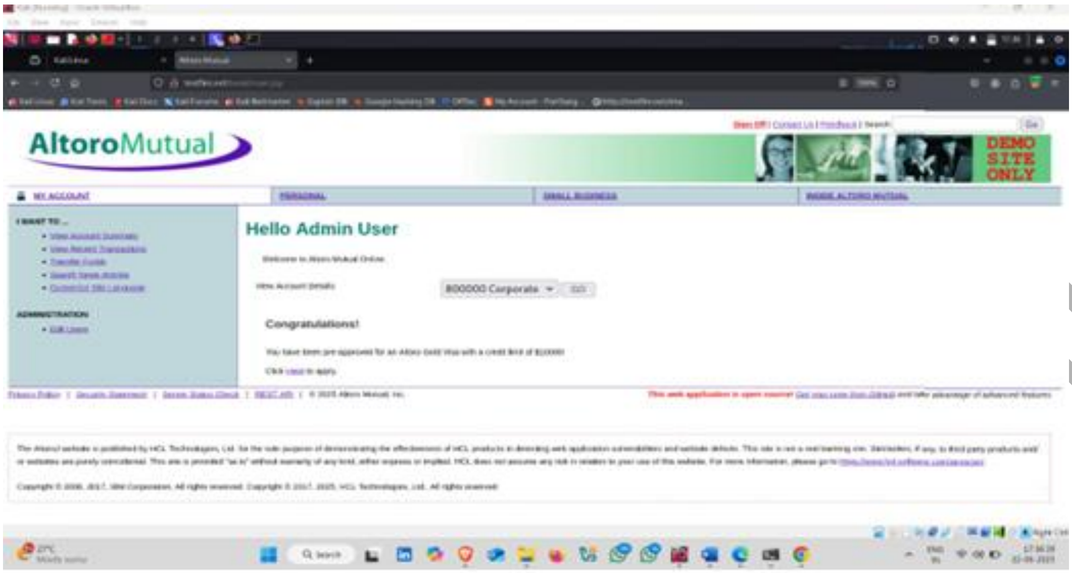
Steps :

1 . Target Website



1.1

2 . Enter username and password and click on login



AltoroMutual

DEMO SITE ONLY

MY ACCOUNT | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

I WANT TO ...

ADMINISTRATION

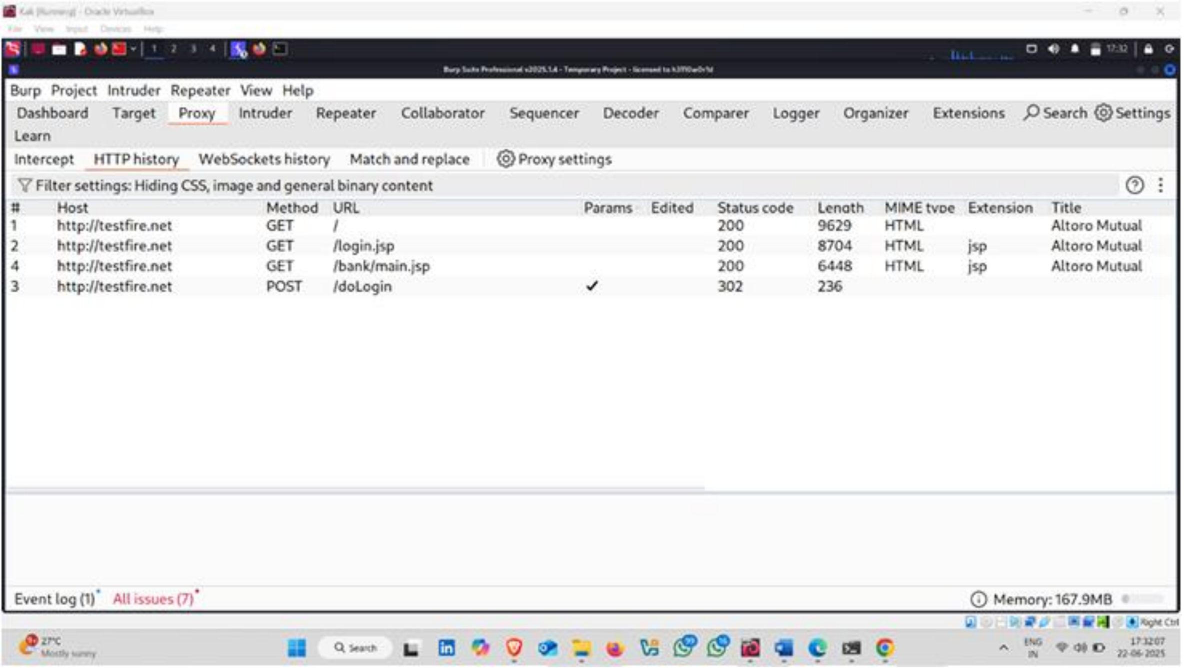
Hello Admin User

800000 Corporate

Congratulations!

1.2

3 . Open burp suite and click on target option



Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Search Settings
Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings

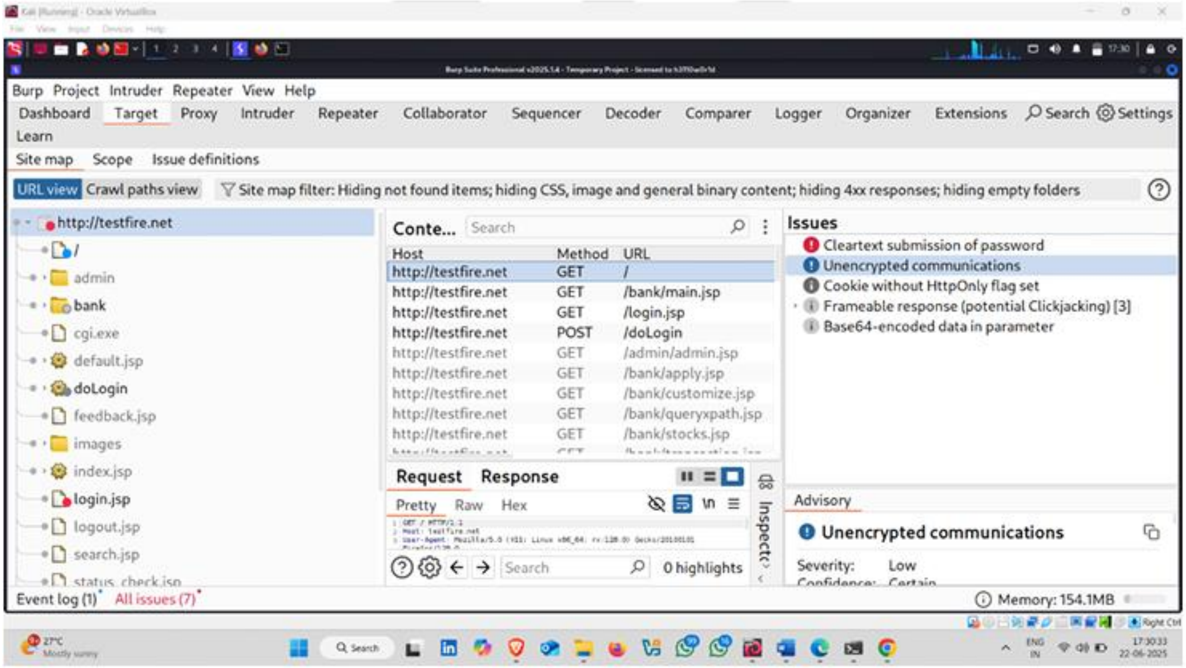
Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME tvoe	Extension	Title
1	http://testfire.net	GET	/			200	9629	HTML		Altoro Mutual
2	http://testfire.net	GET	/login.jsp			200	8704	HTML	jsp	Altoro Mutual
4	http://testfire.net	GET	/bank/main.jsp			200	6448	HTML	jsp	Altoro Mutual
3	http://testfire.net	POST	/doLogin	✓		302	236			

Event log (1)
All issues (7)
Memory: 167.9MB

1.3

4 . Now click on doLogin Option


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Search Settings
Learn
Site map Scope Issue definitions
URL view Crawl paths view
Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://testfire.net
/
admin
bank
cgi.exe
default.jsp
doLogin
feedback.jsp
images
index.jsp
login.jsp
logout.jsp
search.jsp
status_check.jsp
Conte... Search
Request Response
Pretty Raw Hex
Search 0 highlights
Inspector
Issues
Advisory
Event log (1) All issues (7)
Memory: 154.1MB

Host	Method	URL
http://testfire.net	GET	/
http://testfire.net	GET	/bank/main.jsp
http://testfire.net	GET	/login.jsp
http://testfire.net	POST	/doLogin
http://testfire.net	GET	/admin/admin.jsp
http://testfire.net	GET	/bank/apply.jsp
http://testfire.net	GET	/bank/customize.jsp
http://testfire.net	GET	/bank/queryxpath.jsp
http://testfire.net	GET	/bank/stocks.jsp

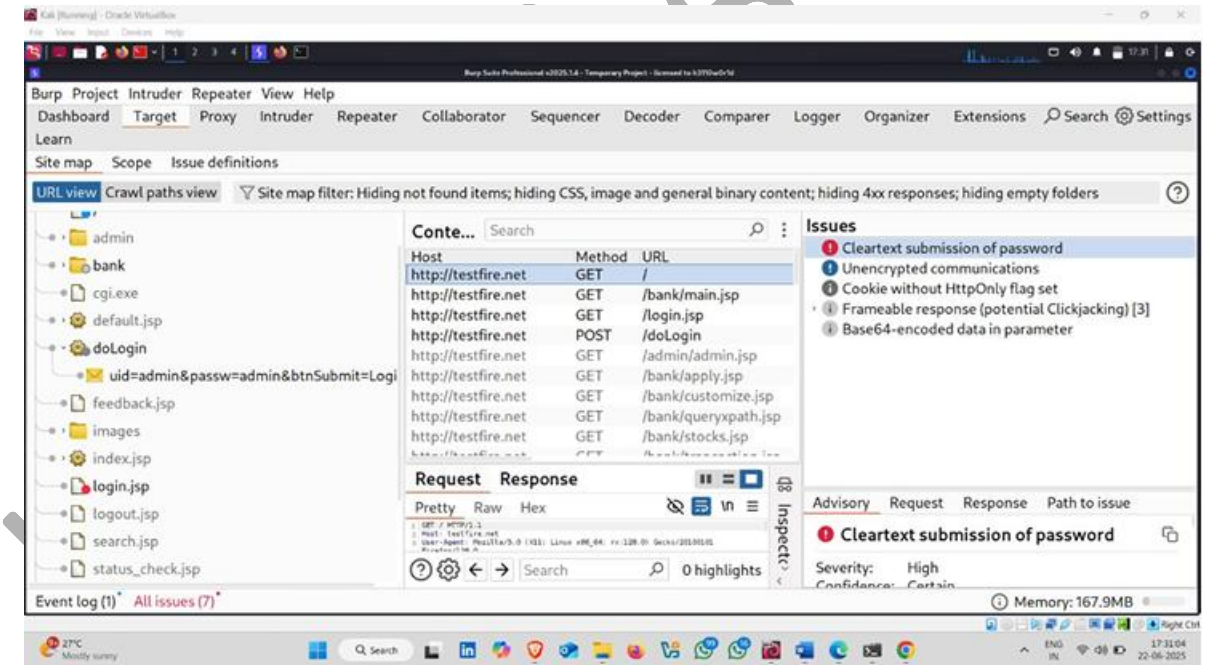
Issues
- Cleartext submission of password
- Unencrypted communications
- Cookie without HttpOnly flag set
- Frameable response (potential Clickjacking) [3]
- Base64-encoded data in parameter

Unencrypted communications

Severity: Low

1.4

5 . Now , right click on uid and passw section


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Search Settings
Learn
Site map Scope Issue definitions
URL view Crawl paths view
Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
admin
bank
cgi.exe
default.jsp
doLogin
uid=admin&passw=admin&btnSubmit=Logi
feedback.jsp
images
index.jsp
login.jsp
logout.jsp
search.jsp
status_check.jsp
Conte... Search
Request Response
Pretty Raw Hex
Search 0 highlights
Inspector
Issues
Advisory Request Response Path to issue
Event log (1) All issues (7)
Memory: 167.9MB

Host	Method	URL
http://testfire.net	GET	/
http://testfire.net	GET	/bank/main.jsp
http://testfire.net	GET	/login.jsp
http://testfire.net	POST	/doLogin
http://testfire.net	GET	/admin/admin.jsp
http://testfire.net	GET	/bank/apply.jsp
http://testfire.net	GET	/bank/customize.jsp
http://testfire.net	GET	/bank/queryxpath.jsp
http://testfire.net	GET	/bank/stocks.jsp

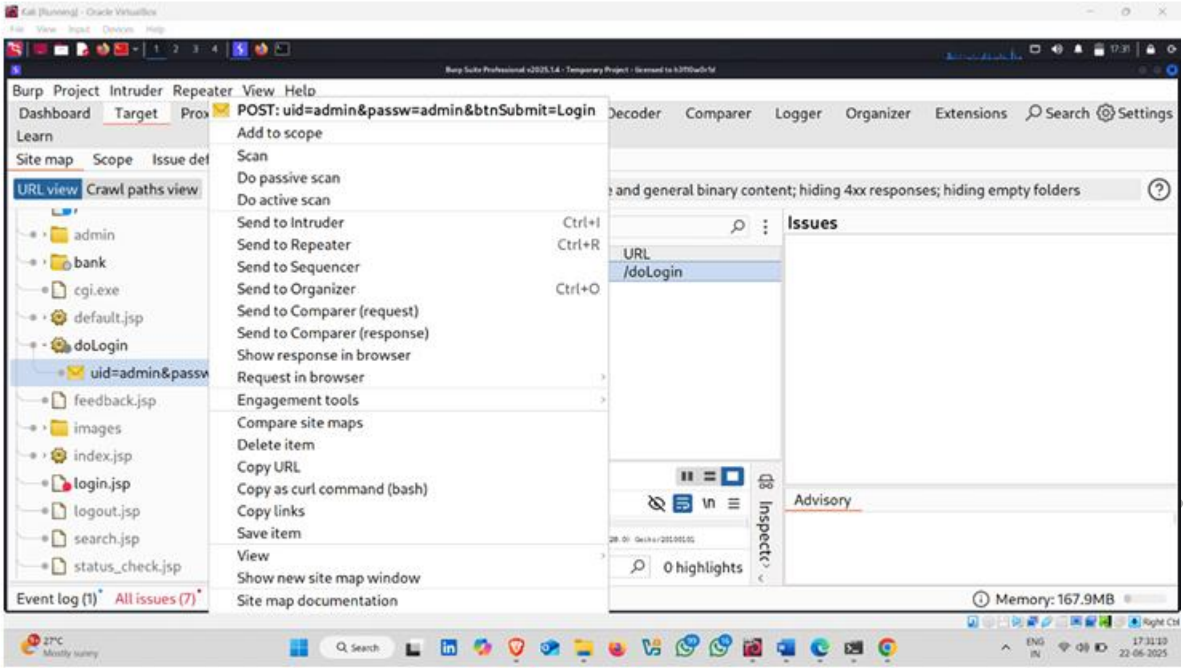
Issues
- Cleartext submission of password
- Unencrypted communications
- Cookie without HttpOnly flag set
- Frameable response (potential Clickjacking) [3]
- Base64-encoded data in parameter

Cleartext submission of password

Severity: High

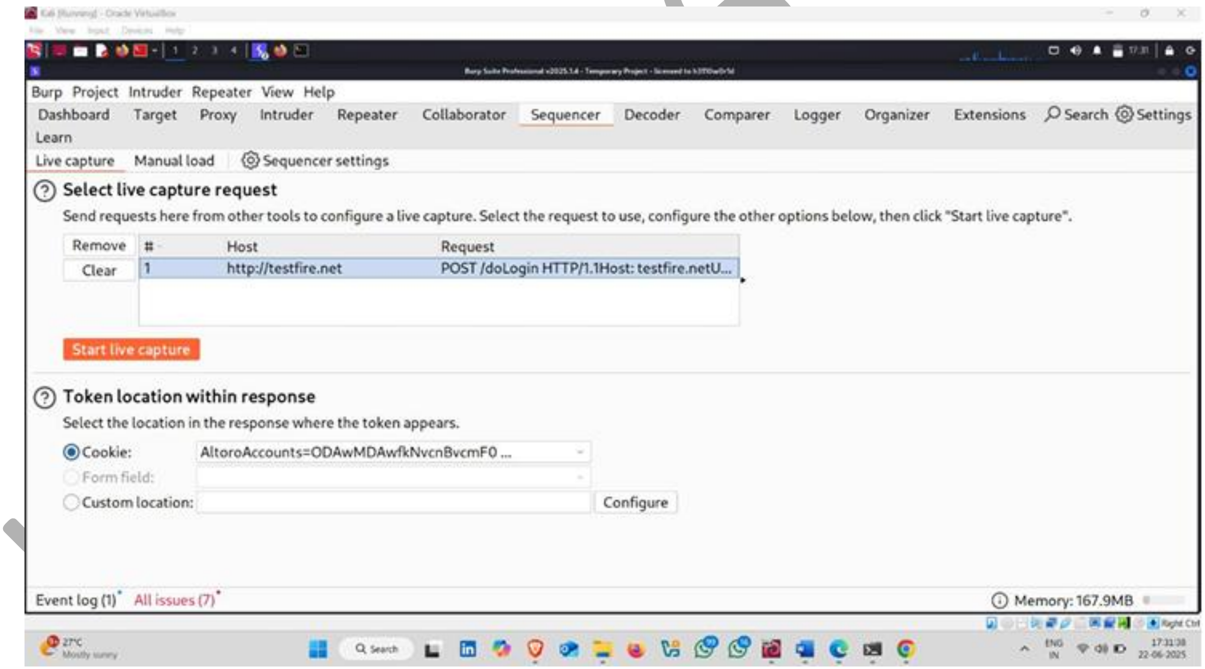
1.5

6 . Send to Sequencer



1.6

7 . Click on Start live capture


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Search Settings
Learn
Live capture Manual load Sequencer settings

Select live capture request

Send requests here from other tools to configure a live capture. Select the request to use, configure the other options below, then click "Start live capture".

#	Host	Request
1	http://testfire.net	POST /doLogin HTTP/1.1Host: testfire.netU...

Remove
Clear
Start live capture

Token location within response

Select the location in the response where the token appears.

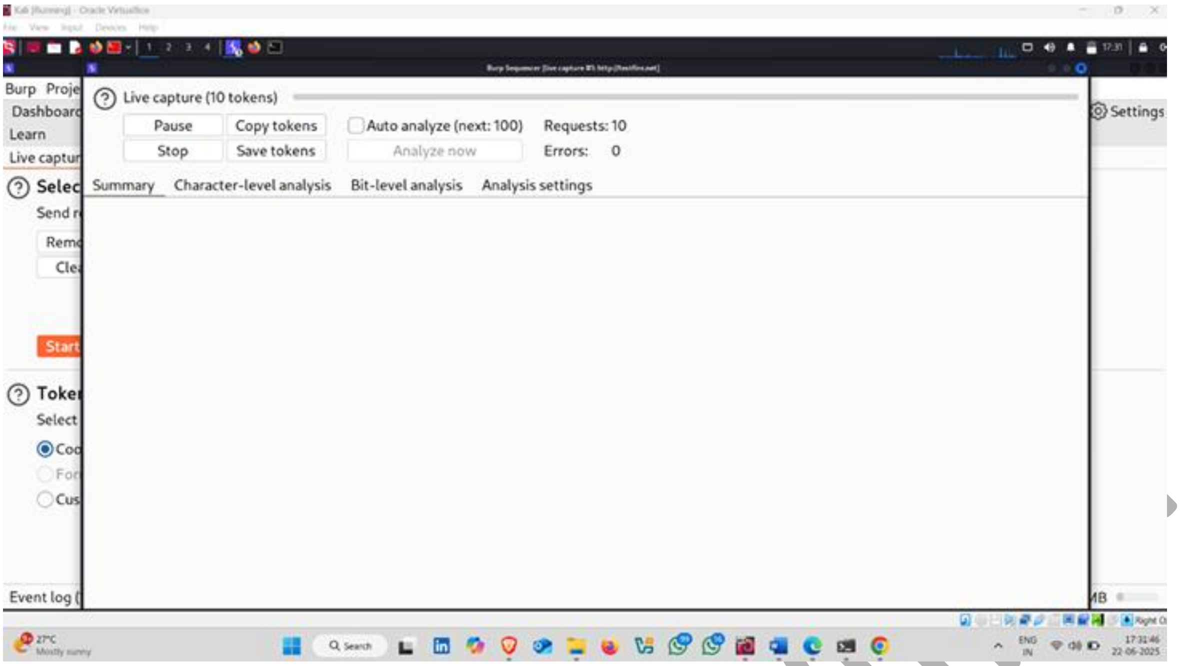
● Cookie: AltoroAccounts=ODAwMDAwfkNvcnBvcmF0 ...

○ Form field:

○ Custom location: Configure

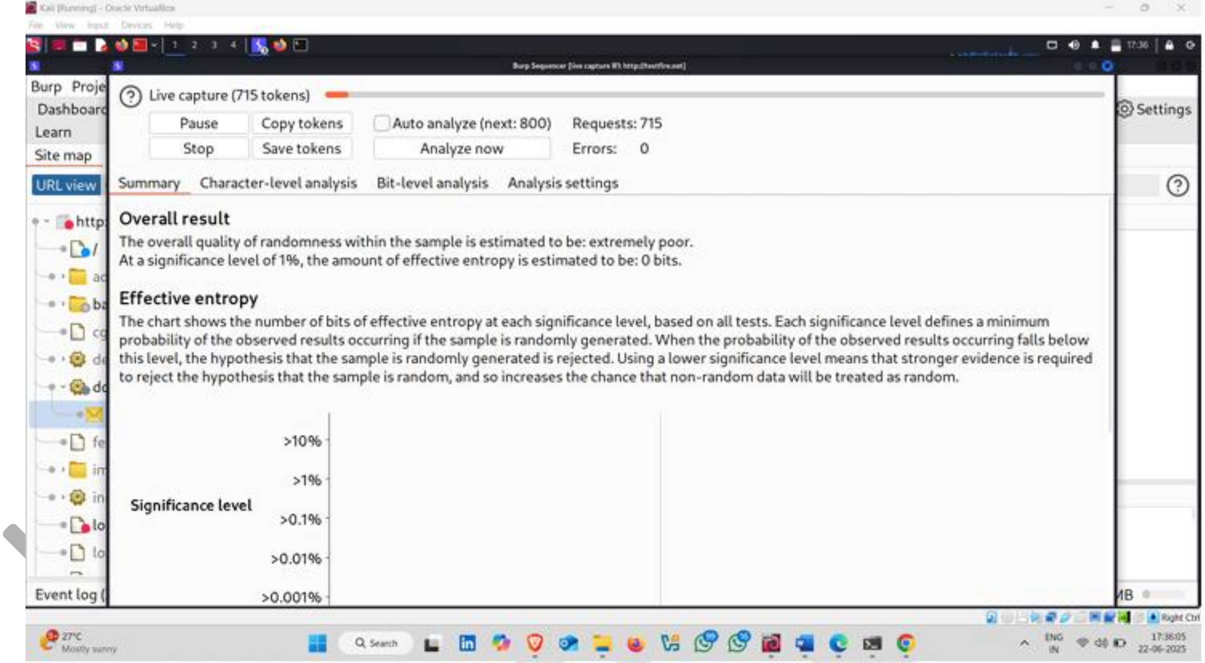
1.7

8 . Started



1.8

9 . Now click on Analyze now • Here , result



Overall result

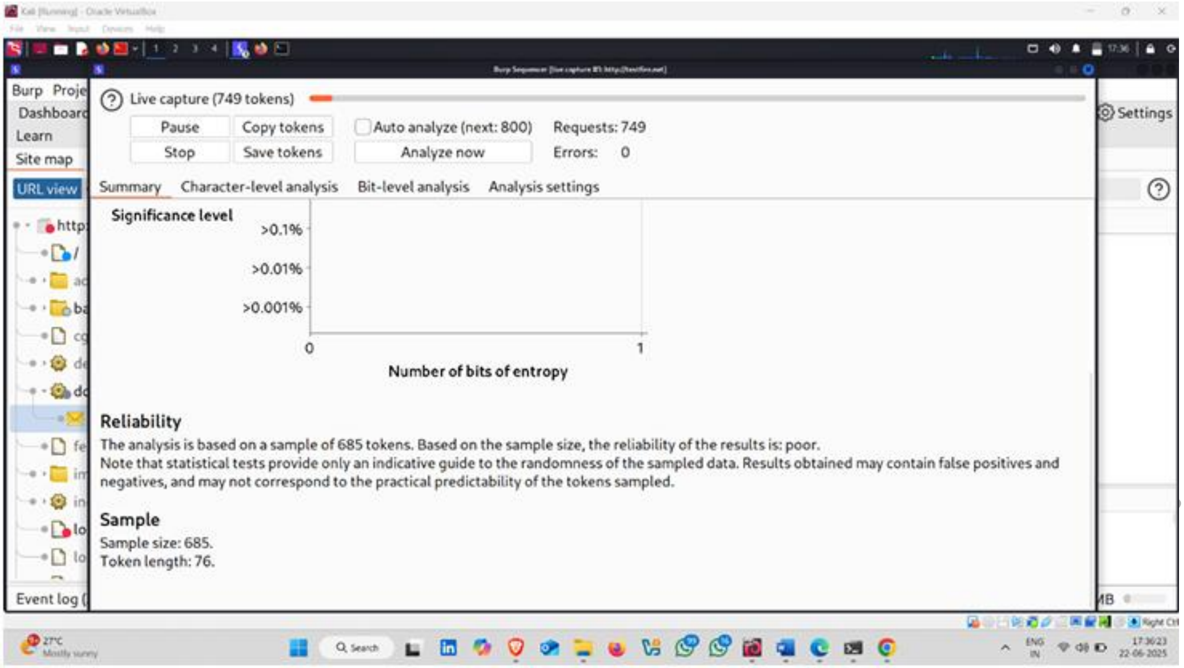
The overall quality of randomness within the sample is estimated to be: extremely poor.
At a significance level of 1%, the amount of effective entropy is estimated to be: 0 bits.

Effective entropy

The chart shows the number of bits of effective entropy at each significance level, based on all tests. Each significance level defines a minimum probability of the observed results occurring if the sample is randomly generated. When the probability of the observed results occurring falls below this level, the hypothesis that the sample is randomly generated is rejected. Using a lower significance level means that stronger evidence is required to reject the hypothesis that the sample is random, and so increases the chance that non-random data will be treated as random.

1.9

10 . Reliability is poor



Live capture (749 tokens)

Reliability

The analysis is based on a sample of 685 tokens. Based on the sample size, the reliability of the results is: poor.

Note that statistical tests provide only an indicative guide to the randomness of the sampled data. Results obtained may contain false positives and negatives, and may not correspond to the practical predictability of the tokens sampled.

Sample

Sample size: 685.

Token length: 76.

2.0