CONFIDENTIAL

VulSphere

Application Security Testing

Initial #1023 | Dynamic Application Security Testing | Spoky

The following report provides a comprehensive and professional summary of the initial review process, findings, and recommendations pertaining to the above-mentioned test request. All observations and results are documented in accordance with the standards outlined in the Test Request and Initial Review schemas.

Prepared For:
Application Owner

Prepared By:
CISO

1

Disclaimer

The information shared in this report is confidential and may be legally privileged. It is intended solely for the addressee only and access to this report by anyone else is unauthorized. If you are not the intended recipient, any disclosure, copying, reproduction, distribution or any action taken or omitted to be taken in reliance on it, is prohibited and may be unlawful. Jayaa IT Solution Pvt Ltd. will not be liable to you in respect of any losses arising out of any event or events beyond our reasonable control. We will not be liable to you in respect of any business losses, including without limitation loss of or damage to profits, income, revenue, use, production, anticipated savings, business, contracts, commercial opportunities or goodwill or otherwise arising because of use or any misuse of this report by anyone. All the recommendations and solutions provided in this report are on as is basis and are void of any warranty expressed or implied.

2 Executive Summary

The assessment was conducted in accordance with the recommendations and methodology outlined in OWASP - 2021 and NIST- SWAT frameworks with all tests and actions being conducted under controlled conditions. Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data.

The details of the application are mentioned below:

Application Name	Spoky	**Application Type**	Web Application
Asset Group	Application	**Application Owner**	Application Owner

Test Details

Test Stage	Initial	**Start Date**	Sep 15, 2025
Prepared By	CISO	**End Date**	Sep 15, 2025

The Objective

To identify security vulnerabilities and test the effectiveness of security controls placed on the Spoky application. The assessment was performed without any prior knowledge, assuming an identity of an adversary who can effectively compromise the application.

Overall there were total 3 Observations recorded by security auditors for above Web application, out of which 2 High and 1 Medium observations were found.

Report Issues Statics

Open Issues	Closed Issues	Total Issues
0	3	3

Key Observations Found

Following table presents a list of identified vulnerabilities and their severity levels.

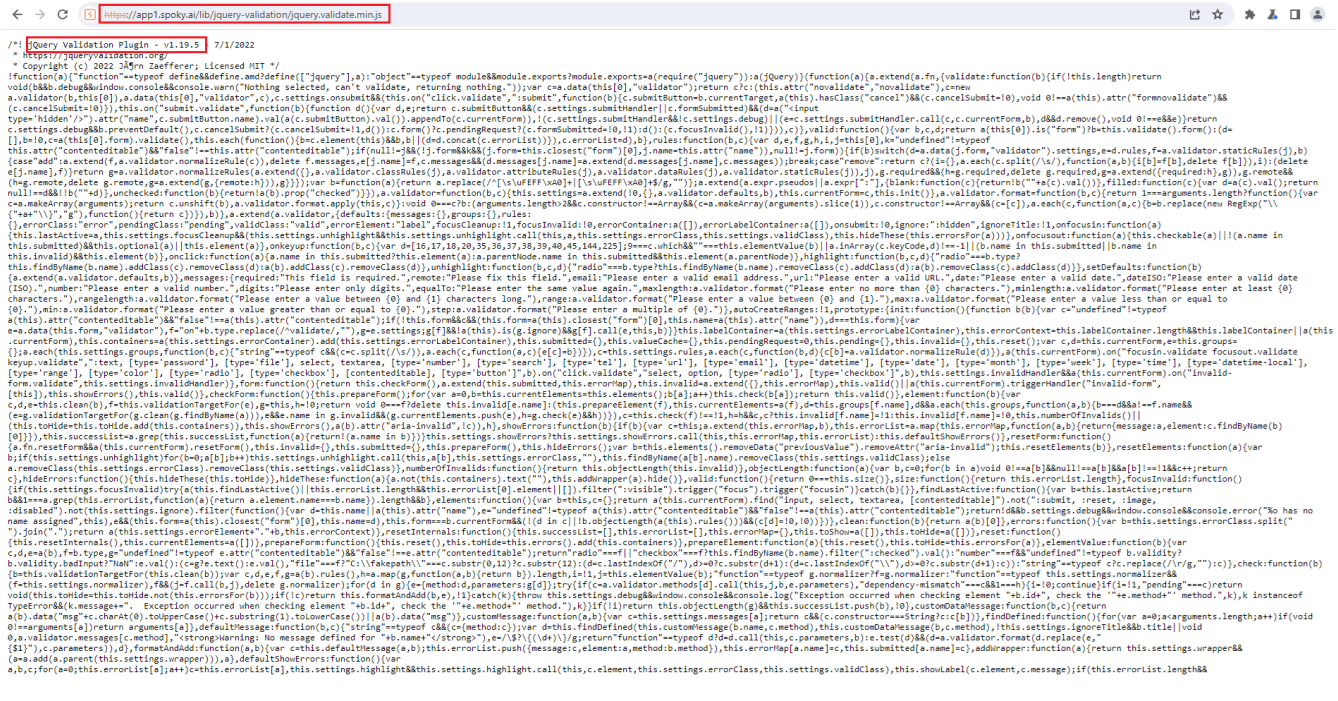
S.No	Vulnerability Title	Severity	Status
1	Using Components with Known Vulnerabilities	HIGH	CLOSED
2	OTP Bypass Using Response Manipulation	HIGH	CLOSED
3	Forced Browsing	MEDIUM	CLOSED

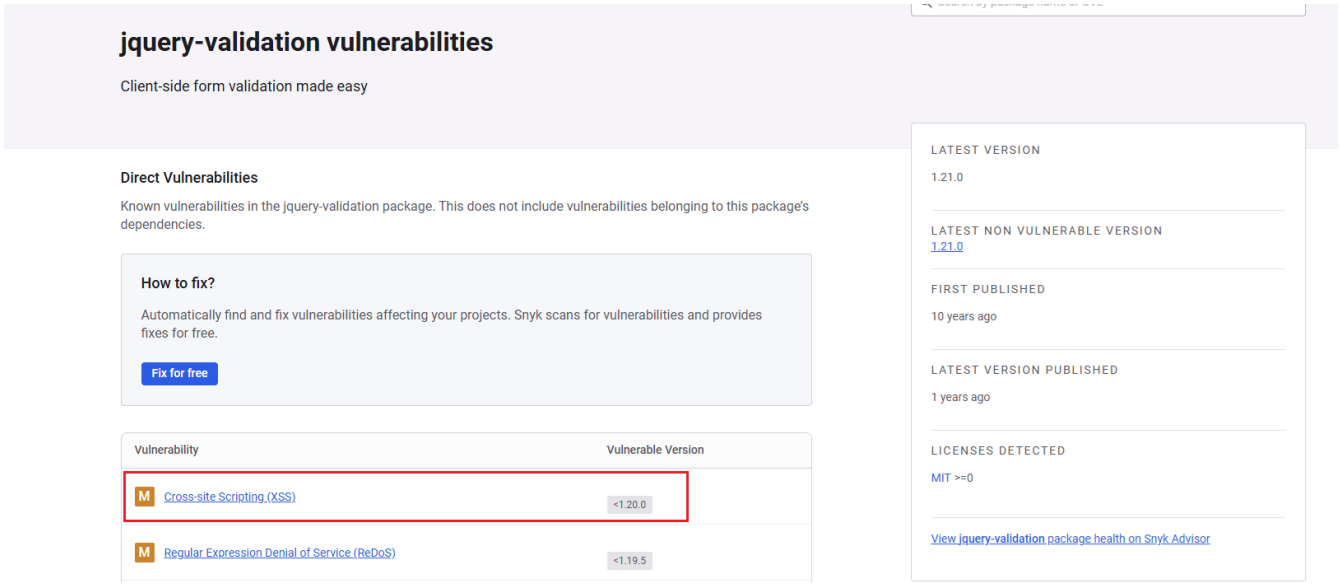
1. Using Components with Known Vulnerabilities

The application uses outdated or vulnerable software components (frameworks, libraries, plugins) with publicly disclosed security issues. Attackers can exploit these known flaws to compromise the system.

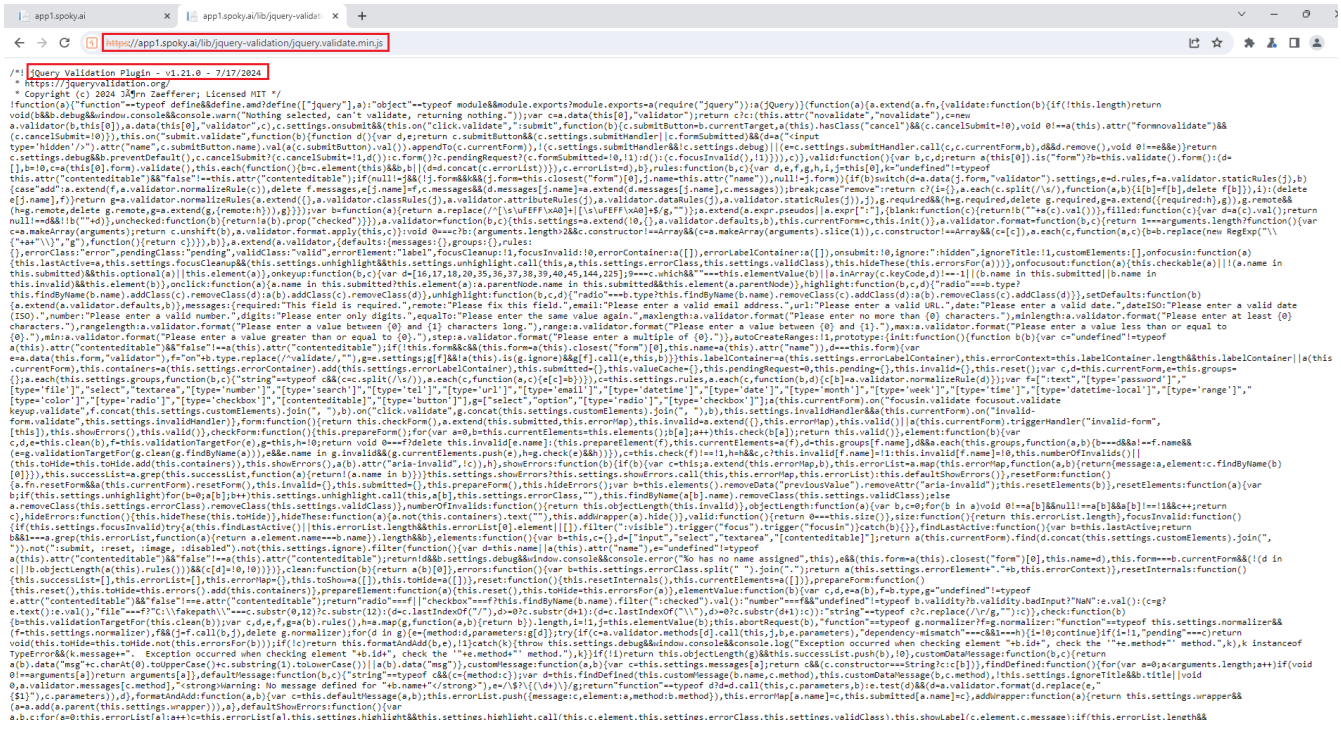
Severity	Status	CVSS
HIGH	CLOSED	7.5 / 10

Initial:





Confirmatory 1:



Solution / Remediation

Maintain an inventory of components (SBOM – Software Bill of Materials).Regularly update and patch all libraries, frameworks, and third- party dependencies.Subscribe to vendor security advisories and OWASP Dependency-Check alerts.Use automated tools (e.g., Snyk, OWASP Dependency-Track, NPM Audit) to scan for vulnerable components.Replace unsupported or end-of-life components.

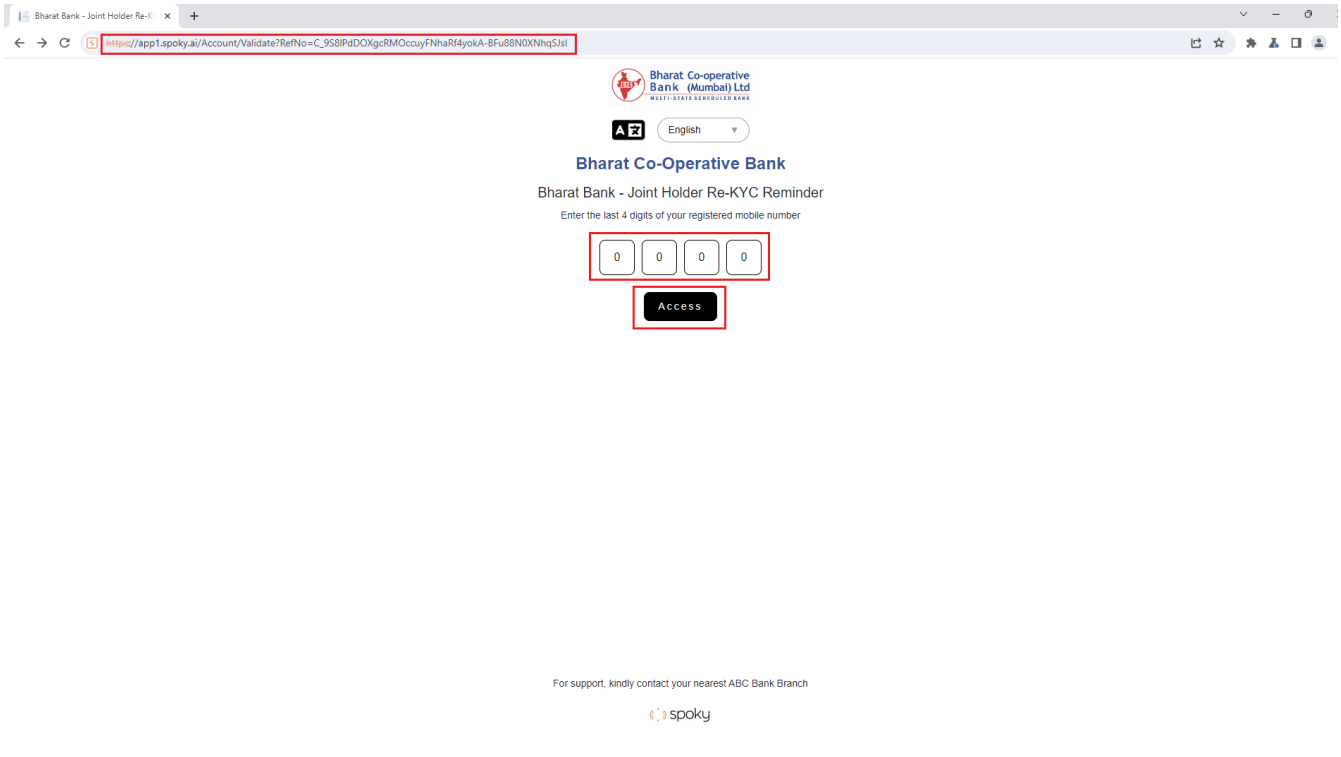
2. OTP Bypass Using Response Manipulation

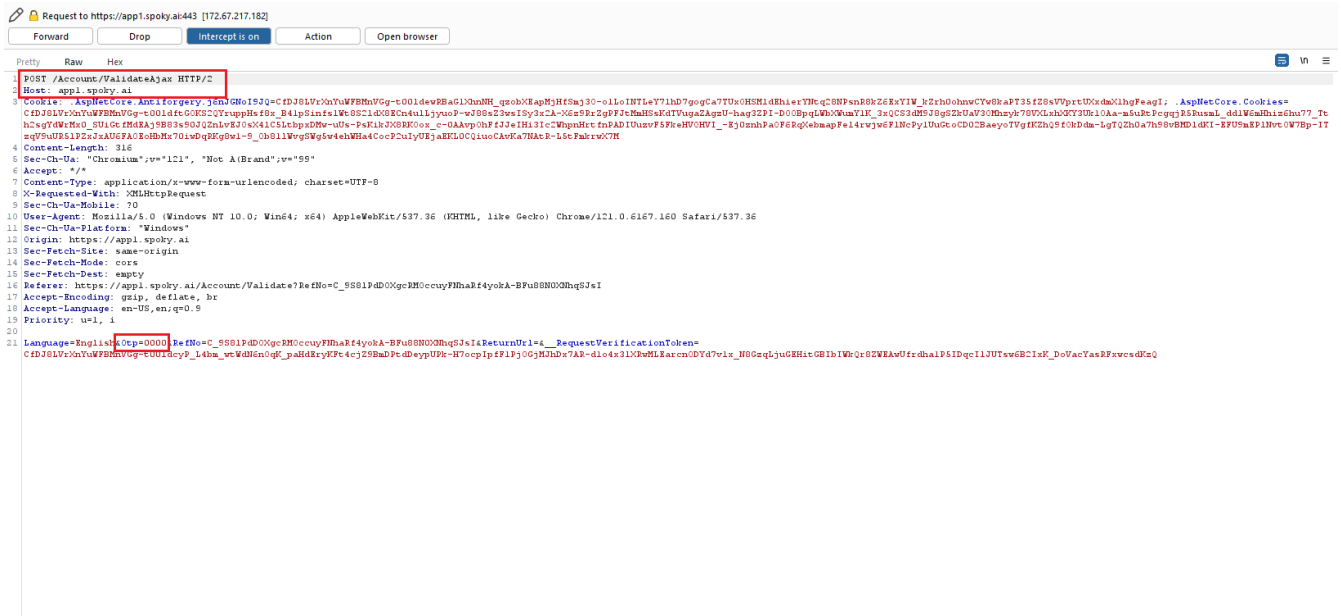
The application's OTP (One-Time Password) validation mechanism can be bypassed by tampering with client-

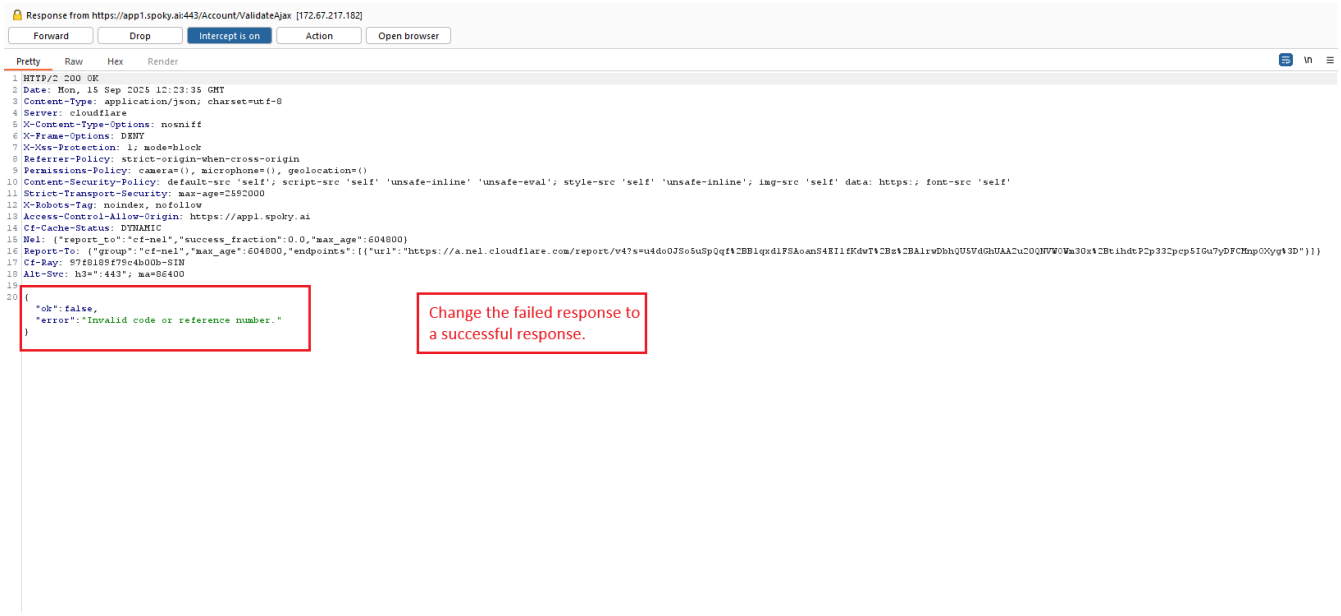
side responses (e.g., intercepting API calls via a proxy and modifying the server's response or request payload). This indicates insufficient server-side validation and reliance on client inputs for authentication flow.

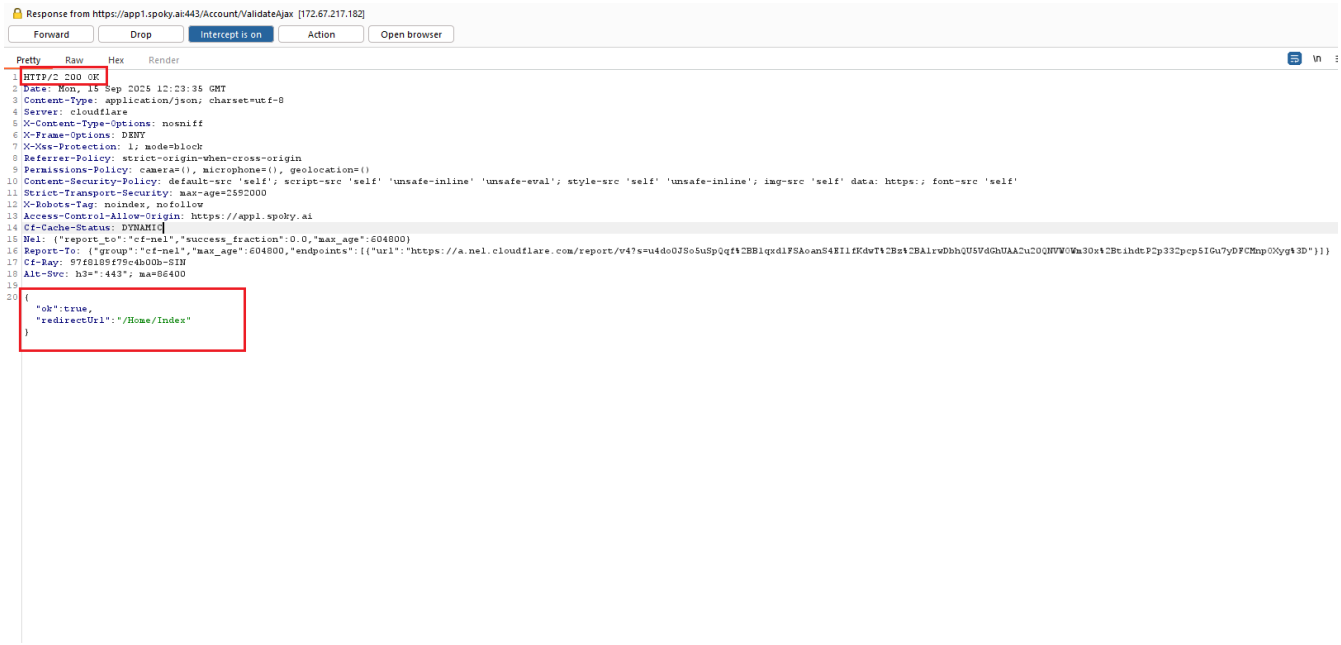
Severity	Status	CVSS
HIGH	CLOSED	8.5 / 10

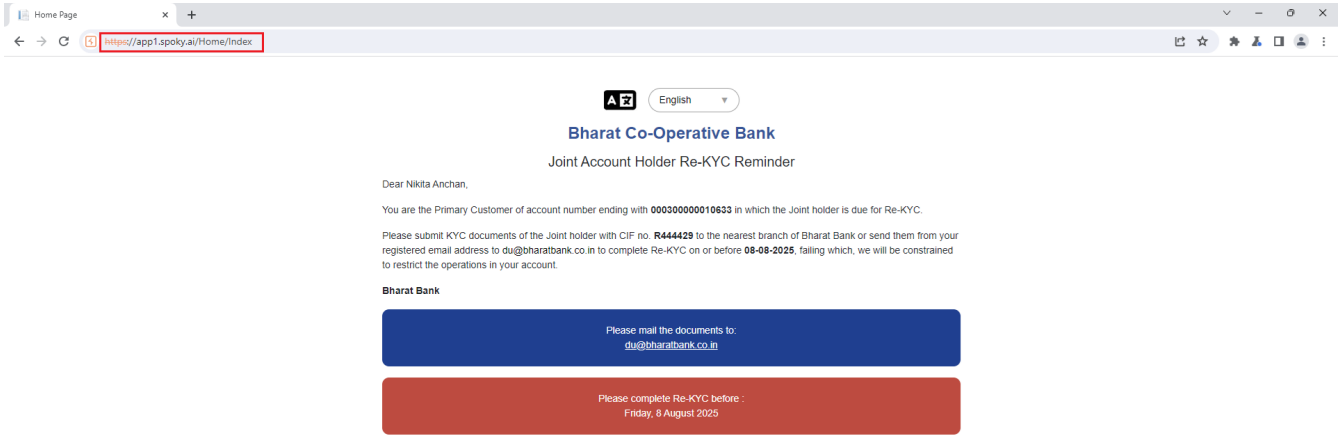
Initial:



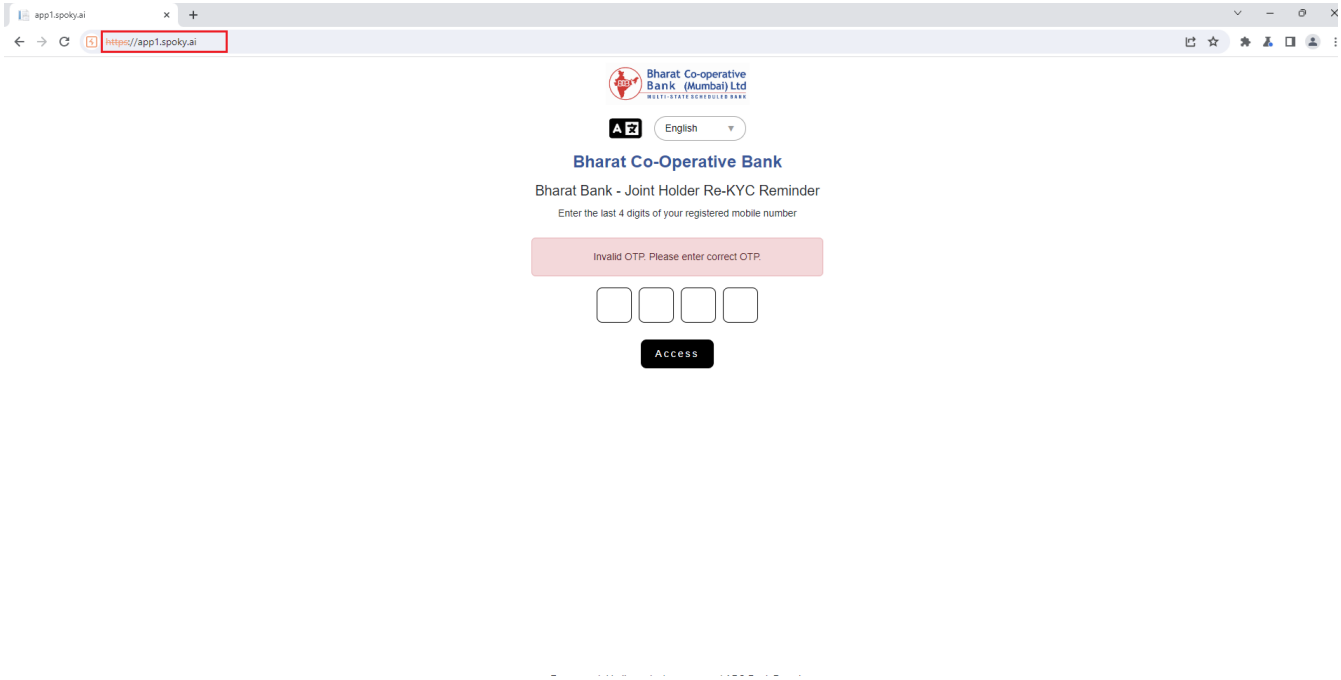



Response from https://app1.spoky.ai:443/Account/ValidateAjax [172.67.217.182]
Forward
Drop
Intercept is on
Action
Open browser
Pretty
Raw
Hex
Render
HTTP/2 200 OK
Date: Mon, 15 Sep 2025 12:23:35 GMT
Content-Type: application/json; charset=utf-8
Server: cloudflare
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Xss-Protection: 1; mode=block
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: camera=(), microphone=(), geolocation=()
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline'; img-src 'self' data: https:; font-src 'self'
Strict-Transport-Security: max-age=2592000
X-Robots-Tag: noindex, nofollow
Access-Control-Allow-Origin: https://app1.spoky.ai
Cf-Cache-Status: DYNAMIC
Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=u4do0JSo5uSpQqf%2BBlqxdlFSAoanS4EIlfKdwT%2Bs%2BAlrwDbhQU5VdGhUAA2u20QNVW0Wm30x%2BtihdtP2p33Zpcp5IGu7yDFCMnp0Xyg%3D"}]}
Cf-Ray: 97f8189f79c4b00b-SIN
Alt-Svc: h3=":443"; ma=86400
{
"ok":false,
"error":"Invalid code or reference number."
}
Change the failed response to a successful response.


Response from https://app1.spoky.ai:443/Account/ValidateAjax [172.67.217.182]
Forward
Drop
Intercept is on
Action
Open browser
Pretty
Raw
Hex
Render
HTTP/2 200 OK
Date: Mon, 15 Sep 2025 12:23:35 GMT
Content-Type: application/json; charset=utf-8
Server: cloudflare
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Xss-Protection: 1; mode=block
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: camera=(), microphone=(), geolocation=()
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline'; img-src 'self' data: https:; font-src 'self'
Strict-Transport-Security: max-age=2592000
X-Robots-Tag: noindex, nofollow
Access-Control-Allow-Origin: https://app1.spoky.ai
Cf-Cache-Status: DYNAMIC
Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=u4do0JSo5uSpQqf%2BBlqxdlFSAoanS4EIlfKdwT%2Bs%2BAlrwDbhQU5VdGhUAA2u20QNVW0Wm30x%2BtihdtP2p33Zpcp5IGu7yDFCMnp0Xyg%3D"}]}
Cf-Ray: 97f8189f79c4b00b-SIN
Alt-Svc: h3=":443"; ma=86400
{
"ok":true,
"redirectUrl":"/Home/Index"
}



Confirmatory 1:



Solution / Remediation

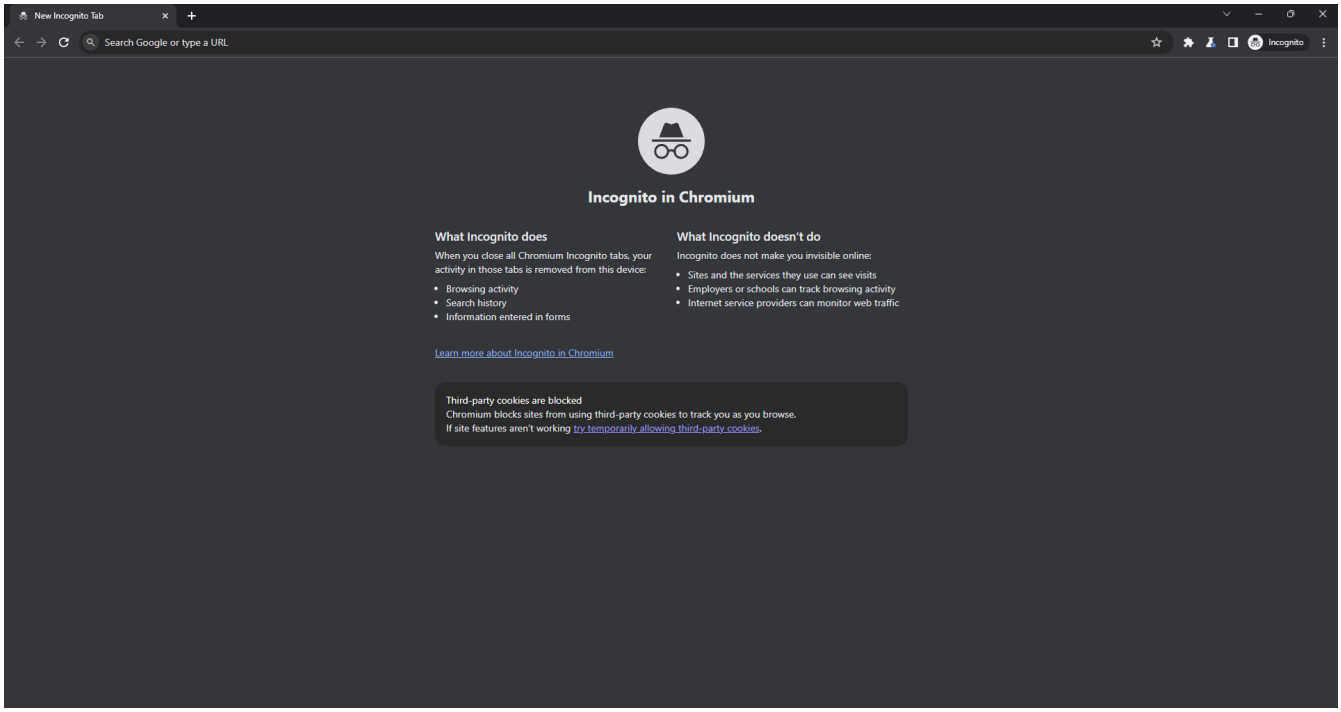
Implement strict server- side validation of OTP values.Ensure OTPs are single- use, time- bound, and cryptographically random.Use rate limiting and account lockout after multiple failed OTP attempts.Avoid sending authentication status in client-controllable responses.

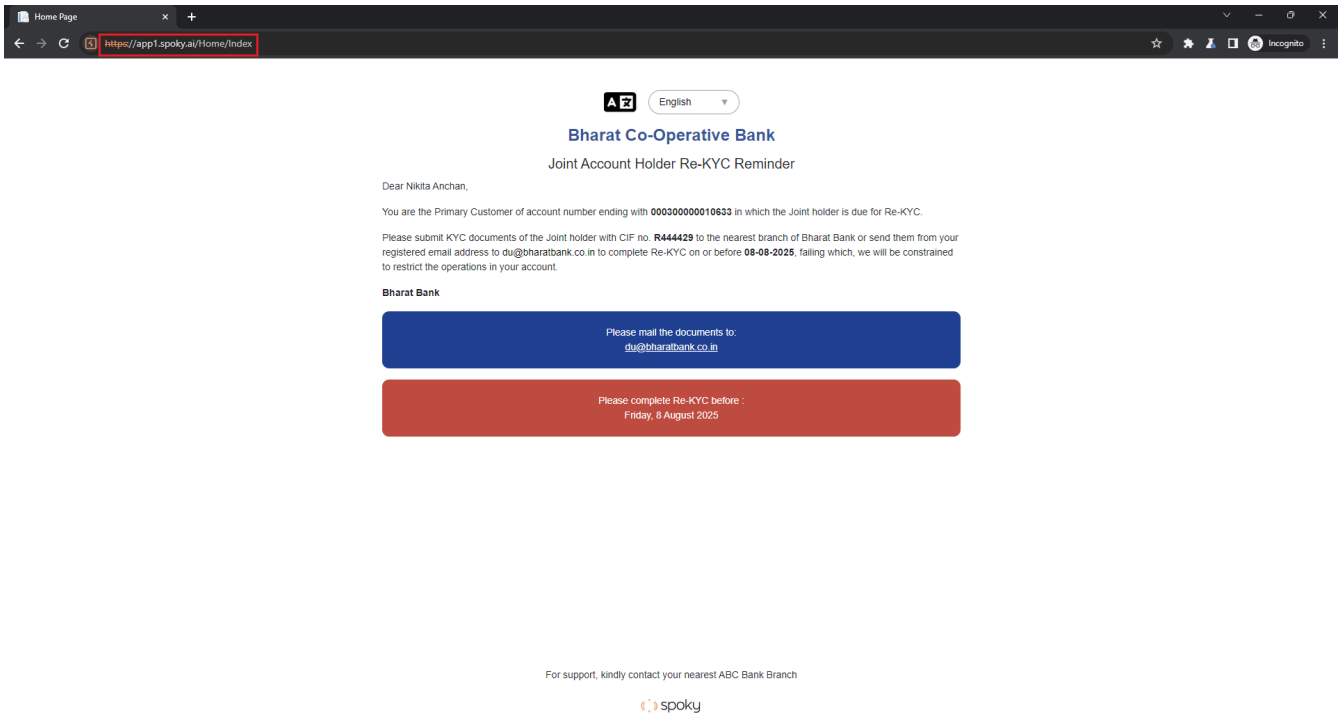
3. Forced Browsing

The application allows attackers to directly access restricted resources (URLs, API endpoints, files) by manipulating the URL or path without proper authorization checks. Attackers can gain access to sensitive information or perform unauthorized actions by accessing hidden or unlinked resources. Depending on the application, this could expose PII, financial records, or administrative functions.

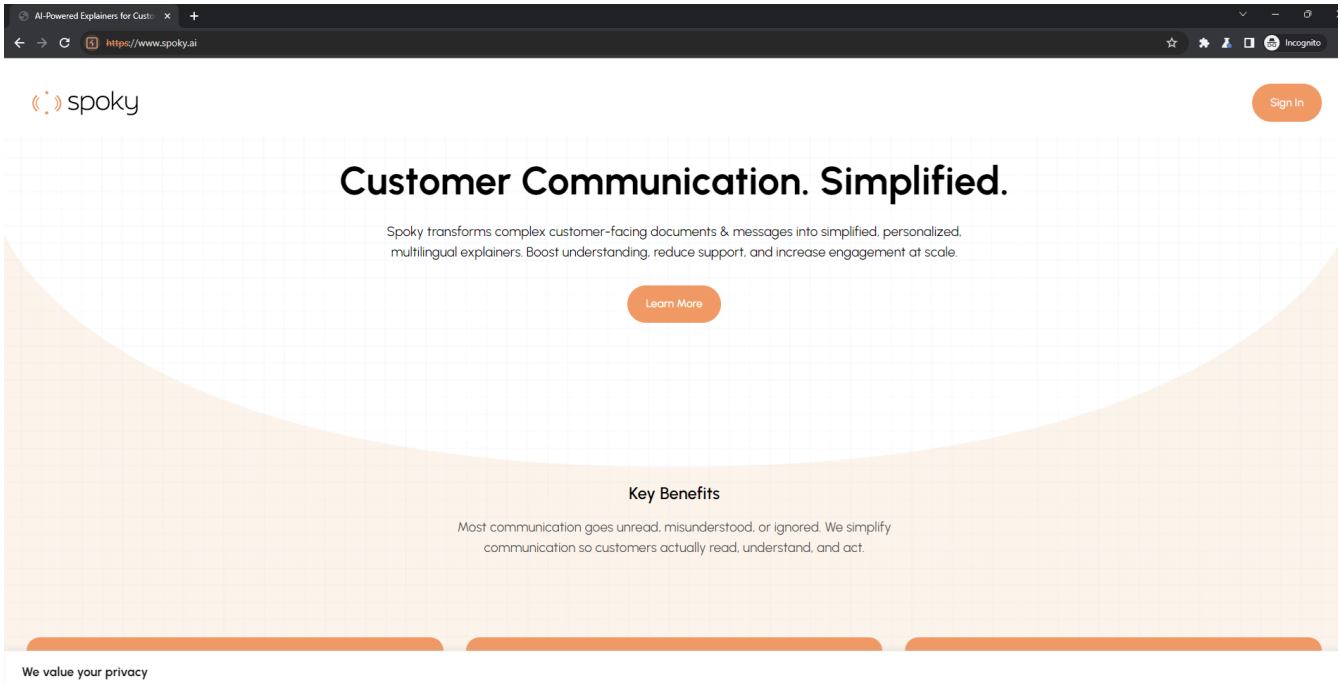
Severity	Status	CVSS
MEDIUM	CLOSED	5.8 / 10

Initial:





Confirmatory 1:



Solution / Remediation

Implement deny-by-default security posture for sensitive resources.Avoid relying on client-side “hidden” URLs for security.Conduct periodic authorization testing as part of development and QA.