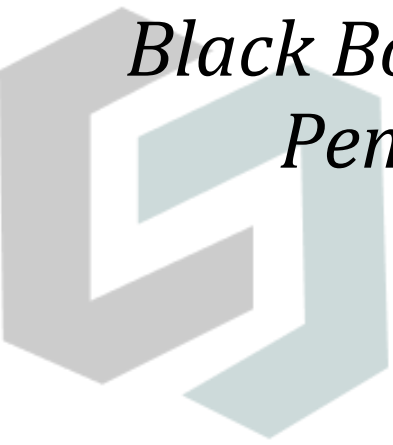




Black Box - Vulnerability Assessment and Penetration Test (VAPT) Report

SECURIFY

EDGE UP YOUR SECURITY

Table of Contents

Section	Page No.
1. Executive Summary	1
2. Background & Methodology	1
3. Detailed Findings	2
3.1 Critical Findings	2
3.1.1 Exposed Swagger UI & Unauthenticated Access to Sensitive User Data	2
3.2 High Findings	7
3.2.1 Hyperlink Injection	7
3.3 Medium Findings	8
3.3.1 Content Spoofing	9
3.3.2 Click jacking	10
3.3.3 Unencrypted Communication	11
3.3.4 Information Disclosure (Server Version)	12
3.3.5 Portal Exposed (ReportServer)	13
3.3.6 Outdated JavaScript Library	14
3.4 Low Findings	15
3.4.1 Missing Security Headers	16
3.4.2 Arbitrary Method Allowed	17
4. Conclusion & Remediation Summary	18

1. Executive Summary

This report summarizes the findings of a security assessment conducted on the application. The assessment identified eight vulnerabilities, resulting in an overall risk rating of **High**, primarily due to one **Critical** finding.

The most severe issue is the **Exposed Swagger UI and Unauthenticated Access to Sensitive User Data**. An attacker can bypass authentication, enumerate user IDs, and retrieve confidential user documents (containing account numbers, mobile numbers, and NIC details) via a publicly exposed API endpoint. This poses an immediate and unacceptable risk of massive data leakage and regulatory non-compliance.

Mandatory Remediation Priority:

1. **Immediate Lockdown:** Restrict public access to the Swagger UI and enforce strict authentication/authorization on all sensitive API endpoints.
2. **Enforce Encryption:** Immediately enforce HTTPS/TLS across the entire application to secure credential transmission.
3. **Strategic Hardening:** Address High and Medium findings through input validation, output encoding, and deploying critical HTTP security headers.

2. Background & Methodology

Background

This security assessment evaluated the application's resilience against common web application vulnerabilities. The scope included all publicly accessible components, API endpoints, and core user workflows. The objective was to identify configuration weaknesses and flaws before they could be exploited.

Methodology

The assessment followed a **Black Box assessment** approach, simulating an external attacker with no prior knowledge of the application's internal source code or architecture. The methodology was guided by industry-standard practices, primarily the **Open Web Application Security Project (OWASP) Testing Guide**. Key testing activities included:

1. **Information Gathering:** Directory enumeration and analysis of exposed components (e.g., Swagger UI, ReportServer).
2. **Configuration Review:** Checking for server information leakage and default settings.
3. **Authentication/Authorization Testing:** Verifying access control mechanisms against IDOR (Insecure Direct Object Reference) and access bypass.
4. **Injection Testing:** Testing inputs for flaws like Content Spoofing and Hyperlink Injection.
5. **Communication Review:** Verifying the enforcement of HTTPS and the presence of critical security headers.

3. Detailed Findings

3.1 Critical Findings

Critical findings represent the highest risk, allowing for easy exploitation and resulting in severe consequences, such as mass data leakage or system compromise.

3.1.1 Exposed Swagger UI & Unauthenticated Access to Sensitive User Data

Description:

During directory brute forcing, I found that the Swagger UI was publicly accessible, exposing all available API endpoints. While checking one of these endpoints, I noticed that by changing the ID parameter, it was possible to retrieve user details. The response returned a PDF file containing sensitive information such as the user's account number, mobile number, and NIC number

Severity:

Critical

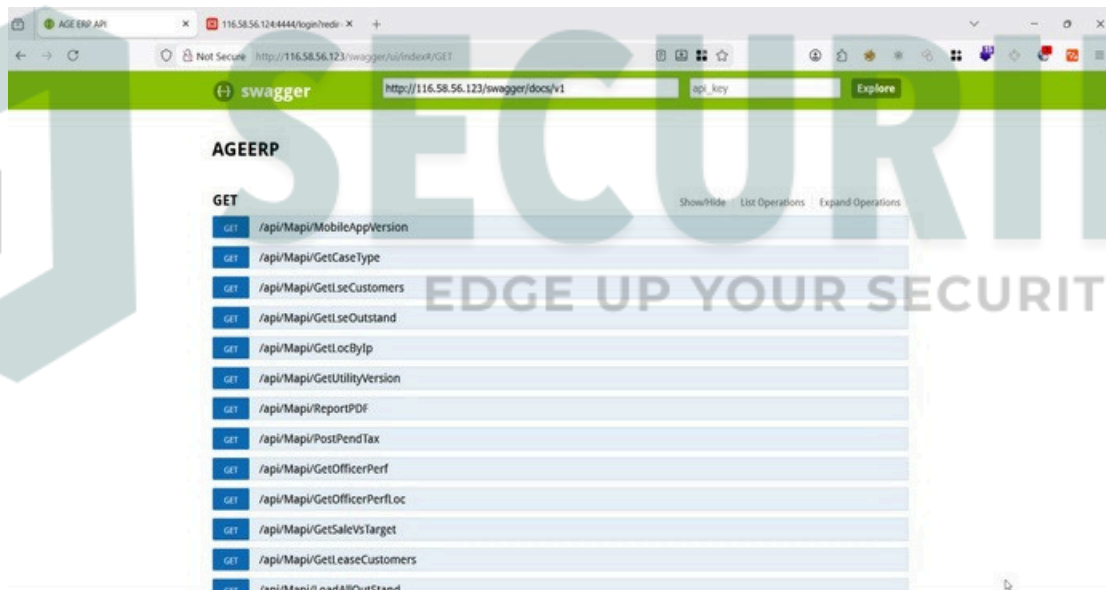
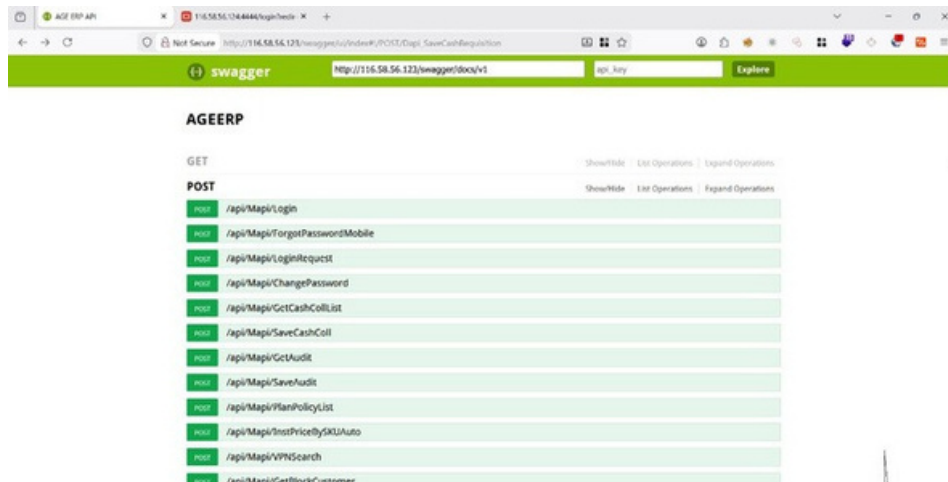
Impact

- Public access to the Swagger UI and unrestricted ID manipulation allowed attackers to obtain confidential user information, including account numbers, mobile numbers, and NIC details.
- The leaked personal and financial identifiers could enable malicious actors to impersonate users, initiate fraudulent transactions, or exploit the data for social-engineering attacks.
- The exposure of unprotected personal data may violate data-protection laws (e.g., GDPR, local privacy acts), potentially resulting in legal penalties, reputational damage, and mandatory incident disclosures.

Remediation:

- Immediate actions must be taken to lock down access and protect sensitive information:
 - o Disable Swagger UI in Production
 - o Swagger documentation should be removed or restricted to internal IPs via network access controls.
 - o If Swagger is necessary, enforce authentication with developer-level permissions only.
- Deploy WAF Rules and Rate-limiting
 - o Use a Web Application Firewall to monitor and block unusual traffic patterns, including automated directory bruteforcing.
- Audit Logging
 - o Enable logging and alerting for access to sensitive endpoints to monitor potential abuse.

Evidence



AGE ERP API x 116.58.56.124/4444/login?redir= X Untitled.pdf x +

Not Secure http://116.58.56.123/api/Map/ReportPDF?TransId=0021212

1 of 1 93%

Customer Account Information Detail Page 1 of 1

Print Date : 24-Nov-2025
Print Time : [REDACTED]

Account No.: 10597 Date: 05-Mar-2019 FQMS AccNo.: 7650

Cust. Name: [REDACTED]

F/H Name: [REDACTED]

Residential: Personal Repeat as Customer: 3 Repeat as Guarantor: 1

Occupation: Owner-Driver

Rest. Addr.: [REDACTED]

Office Addr.: [REDACTED]

Pres. A.C.#.: [REDACTED]

Mobile 1.#: [REDACTED] Company: [REDACTED] SRM: [REDACTED]
Mobile 2.#: [REDACTED] Product: [REDACTED] RM: [REDACTED]
NIC #: [REDACTED] Model: [REDACTED] CRC (J): [REDACTED]
Gender: Male Serial No.: [REDACTED] Deb. Mng.: [REDACTED]
Inst. Price: 36,300 Fine Time: 0 2nd Mng.: [REDACTED]
Act. Install.: 3,025 Fine Rcv.: 0 Insv. Off.: [REDACTED]
Advance Rcv.: 3,025 Fine Exp.: 0 Mark Off.: [REDACTED]
Advance Rcv.: 3,050.00 Duration: 11 DO: Administrator
Total Rcv.: 36,300 100% Inst. Rcv.: 11 Process At: OutDoor Process Fee: 0
Discount: 0 0% Inst. Rem.: 0 Defaulter: No Salary/Income: 40,000
Balance: 0 0% Status: Close PTO: No VPN: Yes

Employee Status: Not Employee
DBM Remarks: [REDACTED]
CRC Remarks: CRC remarks hidden by HO

Criteria	Guarantor # 3	Guarantor # 4
Name :	[REDACTED]	[REDACTED]
F/H Name :	[REDACTED]	[REDACTED]
Rest. Ph. # :	[REDACTED]	[REDACTED]
Office Ph. # :	[REDACTED]	[REDACTED]
NIC # :	[REDACTED]	[REDACTED]
Rest. Addr. :	[REDACTED]	[REDACTED]
Office Addr. :	[REDACTED]	[REDACTED]
Occupation :	[REDACTED]	[REDACTED]
Relation :	[REDACTED]	[REDACTED]
Outstand Month	Outstand Amt	Received Amt
	n	n
	Month Status	

Not Secure http://116.58.56.123/api/Map/ReportPDF?TransId=000001

1 of 2 105%

Customer Account Information Detail Page 1 of 2

Print Date : 24-Nov-2025
Print Time : [REDACTED]

Account No.: 2549 Date: 11-Sep-2017 FQMS AccNo.: 3022

Cust. Name: [REDACTED]

F/H Name: [REDACTED]

Residential: Personal Repeat as Customer: 0 Repeat as Guarantor: 0

Occupation: Owner

Rest. Addr.: [REDACTED]

Office Addr.: [REDACTED]

Pres. A.C.#.: [REDACTED]

Mobile 1.#: [REDACTED] Company: [REDACTED] SRM: [REDACTED]
Mobile 2.#: [REDACTED] Product: [REDACTED] RM: [REDACTED]
NIC #: [REDACTED] Model: [REDACTED] CRC (J): [REDACTED]
Gender: Male Serial No.: [REDACTED] Deb. Mng.: [REDACTED]
Inst. Price: 67,100 Fine Time: 21 2nd Mng.: [REDACTED]
Act. Install.: 2,550 Fine Rcv.: 0 Insv. Off.: [REDACTED]
Advance Rcv.: 13,550 Fine Exp.: 21 Mark Off.: [REDACTED]
Advance Rcv.: 13,550.00 Duration: 21 DO: Administrator
Total Rcv.: 67,100 100% Inst. Rcv.: 21 Process At: Indoor Process Fee: 0
Discount: 0 0% Inst. Rem.: 0 Defaulter: No Salary/Income: 80,000
Balance: 0 0% Status: Close PTO: No VPN: Yes

Employee Status: Not Employee
DBM Remarks: 21 cheque monthly
CRC Remarks: CRC remarks hidden by HO

Criteria	Guarantor # 1	Guarantor # 2	Guarantor # 3	Guarantor # 4
Name :	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
F/H Name :	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Rest. Ph. # :	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Office Ph. # :	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
NIC # :	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Rest. Addr. :	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Office Addr. :	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

AGE ERP API x 116.58.56.124/444/login?rede= x Untitled.pdf x +

← → ↻ Not Secure http://116.58.56.123/api/Map/ReportPDF?TransId=0021212

1 of 1 99%

Print Date: 24-Nov-2025
Print Time: [Redacted]

Account No.: 70051 Date: 26-Jun-2018 TQMS AccNo: 10743
Cust. Name: [Redacted]
FBI Name: [Redacted]
Residential: Personal Repeat as Customer: 0 Repeat as Guarantor: 0
Occupation: [Redacted]
Rest. Addr.: [Redacted]
Office Addr.: [Redacted]
Pres. A.C. #: [Redacted]

Mobile 1 #: [Redacted] Company: [Redacted] SRM: [Redacted]
Mobile 2 #: [Redacted] Product: [Redacted] RM: [Redacted]
NIC #: [Redacted] Model: [Redacted] CRC ID: [Redacted]
Gender: Male Serial No.: [Redacted] Delv. Mtg.: [Redacted]
Inst. Price: 18,500 Fine Time: 15 2nd Mtg.: [Redacted]
Act. Install.: 3,000 Fine Ecs.: 0 Insv. Off.: [Redacted]
Adv. Advance: 13,500 Fine Exp.: 15 Mark Off.: [Redacted]
Advance Rec.: 13,500.00 Duration: 15 RO: Administrator
Total Ecs.: 18,500 100% Inst. Ecs.: 15 Present Mtg.: OutDoor Process Fee: 0
Discount: 0% Inst. Rem.: 0 Defaulter: No Salary/Income: 40,000
Balance: 0 0% Status: Close FTO: No YPN: No

Employee Status: Not Employee
DSM Remarks: [Redacted]
CRC Remarks: CRC remarks hidden by HO

Criteria	Guarantor # 3	Guarantor # 4
Name:	[Redacted]	[Redacted]
FBI Name:	[Redacted]	[Redacted]
Rest. Ph. #:	[Redacted]	[Redacted]
Office Ph. #:	[Redacted]	[Redacted]
NIC #:	[Redacted]	[Redacted]
Rest. Addr.:	[Redacted]	[Redacted]
Office Addr.:	[Redacted]	[Redacted]
Occupation:	[Redacted]	[Redacted]
Relation:	[Redacted]	[Redacted]
Outstand Month	[Redacted]	[Redacted]
Outstand Amt	[Redacted]	[Redacted]
Received Amt	[Redacted]	[Redacted]
Due Amt	[Redacted]	[Redacted]
Month Status	[Redacted]	[Redacted]

← → ↻ Not Secure http://116.58.56.123/api/Map/ReportPDF?TransId=0021212

1 of 1 76%

Customer Account Information Detail Page 1 of 1

Print Date: 24-Nov-2025
Print Time: [Redacted]

Account No.: 10897 Date: 05-May-2019 TQMS AccNo: 7650
Cust. Name: [Redacted]
FBI Name: [Redacted]
Residential: Personal Repeat as Customer: 3 Repeat as Guarantor: 1
Occupation: Owner/Driver
Rest. Addr.: [Redacted]
Office Addr.: [Redacted]
Pres. A.C. #: [Redacted]

Mobile 1 #: [Redacted] Company: [Redacted] SRM: [Redacted]
Mobile 2 #: [Redacted] Product: [Redacted] RM: [Redacted]
NIC #: [Redacted] Model: [Redacted] CRC ID: [Redacted]
Gender: Male Serial No.: 20197 Delv. Mtg.: [Redacted]
Inst. Price: 16,500 Fine Time: 4 2nd Mtg.: [Redacted]
Act. Install.: 3,025 Fine Ecs.: 0 Insv. Off.: [Redacted]
Adv. Advance: 3,025 Fine Exp.: 4 Mark Off.: [Redacted]
Advance Rec.: 3,050.00 Duration: 11 RO: Administrator
Total Ecs.: 16,500 100% Inst. Ecs.: 11 Present Mtg.: OutDoor Process Fee: 0
Discount: 0% Inst. Rem.: 0 Defaulter: No Salary/Income: 40,000
Balance: 0 0% Status: Close FTO: No YPN: Yes

Employee Status: Not Employee
DSM Remarks: [Redacted]
CRC Remarks: [Redacted]

Criteria	Guarantor # 3	Guarantor # 4
Name:	[Redacted]	[Redacted]
FBI Name:	[Redacted]	[Redacted]
Rest. Ph. #:	[Redacted]	[Redacted]
Office Ph. #:	[Redacted]	[Redacted]
NIC #:	[Redacted]	[Redacted]
Rest. Addr.:	[Redacted]	[Redacted]
Office Addr.:	[Redacted]	[Redacted]
Occupation:	[Redacted]	[Redacted]
Relation:	[Redacted]	[Redacted]
Outstand Month	[Redacted]	[Redacted]
Outstand Amt	[Redacted]	[Redacted]
Received Amt	[Redacted]	[Redacted]
Due Amt	[Redacted]	[Redacted]
Month Status	[Redacted]	[Redacted]

Sl	Date	Rev. #	Rev. Bal.	Month	Disc.	Balance	Fine	Exempt	Remarks
1	02-04-2019	112426	33,250	3,025	0	30,225	0	Exempt	
2	10-05-2019	112423	30,225	3,025	0	27,200	300	Exempt	
3	14-06-2019	112427	27,200	3,000	0	24,200	300	Exempt	
4	01-07-2019	112430	24,200	3,025	0	21,175	0	Exempt	
5	10-08-2019	112429	21,175	3,025	0	18,150	300	Exempt	
6	04-09-2019	112428	18,150	3,025	0	15,125	0	Exempt	
7	10-10-2019	112422	15,125	3,025	0	12,100	0	Exempt	
8	20-11-2019	112423	12,100	3,025	0	9,075	300	Exempt	
9	10-12-2019	112424	9,075	3,025	0	6,050	0	Exempt	

← → ↻ Not Secure http://116.58.56.123/api/Mapi/ReportPDF?TransId=000001 105%

2 of 2

Customer Account Information Detail Page 2 of 2

Print Date : 24-Nov-2025
Print Time : [REDACTED]

Account No.: 2549 Date: 11-Sep-2017 FQMS AccNo.: 3022

Cust. Name: [REDACTED]

F/H Name: [REDACTED]

Residential: Personal Repeat as Customer: 0 Repeat as Guarantor: 0

Occupation: Owner

Rest. Addr.: [REDACTED]

Office Addr.: [REDACTED]

Prev. A/C #: [REDACTED]

Mobile 1 #: [REDACTED] Company: [REDACTED] SRM: [REDACTED]

Mobile 2 #: [REDACTED] Product: [REDACTED] RML: [REDACTED]

NIC #: [REDACTED] Model: [REDACTED] CRC (L): [REDACTED]

Gender: Male Serial No.: [REDACTED] Deb. Mng.: [REDACTED]

Inst. Price: 67,100 Fin. Time: 21 2nd Mng.: [REDACTED]

Act. Install: 2,550 Fin. Rcv.: 0 Inst. Off: [REDACTED]

Act. Advance: 13,550 Fin. Exp.: 21 Mark Off: [REDACTED]

Advance Rcv.: 13,550.00 Duration: 21 DO: Administrator

Total Rcv.: 67,100 100% Inst. Rcv.: 21 Process AL: Indow Process Fee: 0

Discont.: 0 0% Inst. Rem.: 0 Defaulter: No Salary/Income: 80,000

Balance: 0 0% Status: Close PTO: No YPN: Yes

Employee Status: Not Employee

DBM Remarks: 21 cheque monthly

CRC Remarks: CRC remarks hidden by HO

Criteria	Guarantor # 1	Guarantor # 2	Guarantor # 3	Guarantor # 4
Name :	[REDACTED]	[REDACTED]		
F/H Name :	[REDACTED]	[REDACTED]		
Rest. Ph. # :	[REDACTED]	[REDACTED]		
Office Ph. # :	[REDACTED]	[REDACTED]		
NIC # :	[REDACTED]	[REDACTED]		
Rest. Addr. :	[REDACTED]	[REDACTED]		
Office Addr. :	[REDACTED]	[REDACTED]		

EDGE UP YOUR SECURITY

3.2 High Finding 3.2.1 Hyperlink injection

Description:

A hyperlink injection vulnerability was identified in the application's user interface. The application reflected the external domain **evil.com** within the UI, and when the user right-clicked on the injected link, it redirected the browser to **evil.com**

Severity:

High

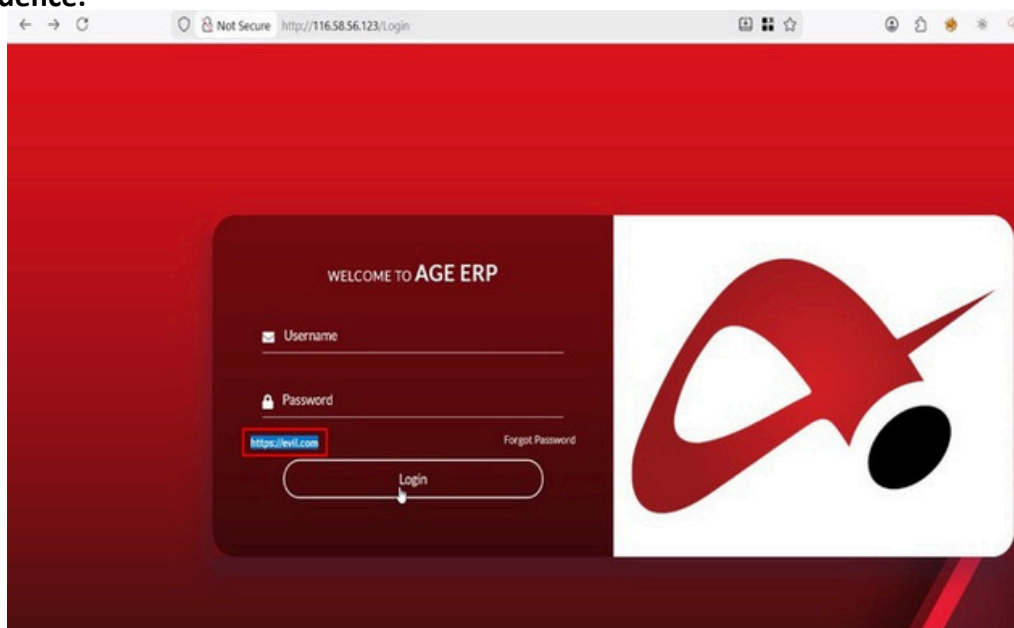
Impact

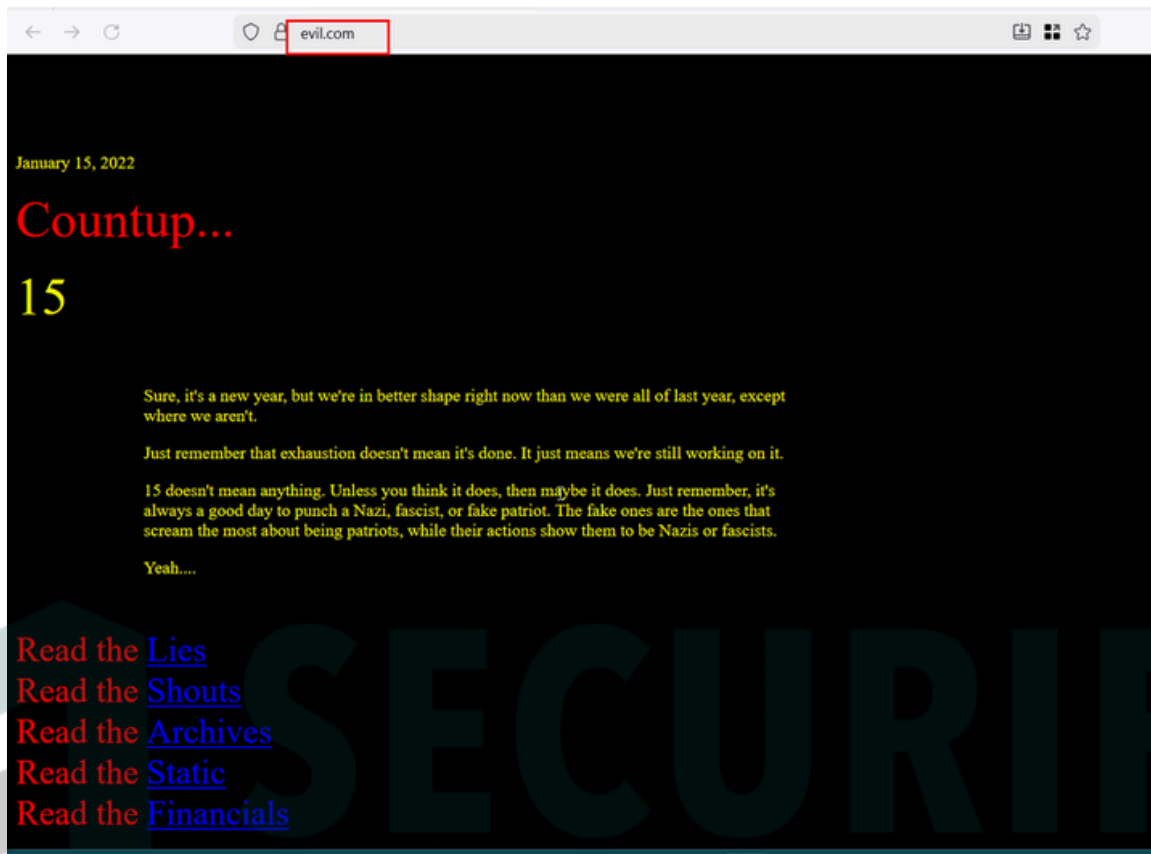
- Users may be redirected to malicious websites designed to steal credentials or personal information.
- Attackers can exploit injected links to impersonate the legitimate application, harming user confidence
- Malicious redirect links may lead to sites hosting malware, putting user devices at risk

Remediation

- Ensure all user-supplied data is sanitized and cannot be rendered as active hyperlinks unless explicitly intended.
- Only permit redirects to domains that are part of an approved and controlled allow-list
- Use proper output encoding (e.g., HTML encoding) to prevent user input from being interpreted as clickable HTML links.

Evidence:





3.3MediumFindings:

3.3.1Contentspoofing:

Description:

The application allows malicious payloads to be injected into the UI. When these payloads are entered, they are displayed back to the user without proper validation or sanitization, potentially misleading the user into trusting malicious content. This type of vulnerability is commonly referred to as Content Spoofing or UI Spoofing

Severity:

Medium

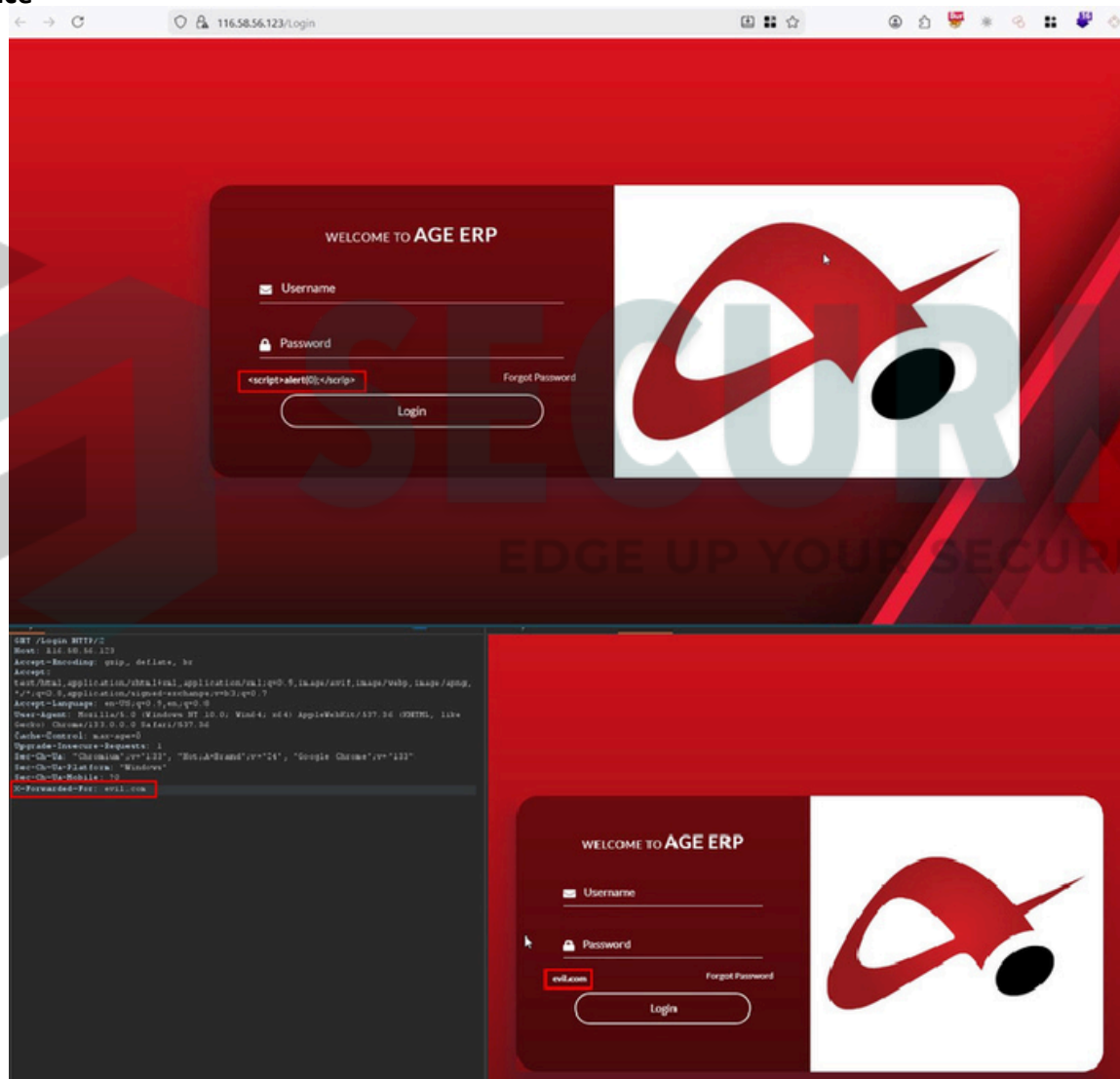
Impact

- Users can be tricked into performing unintended actions by interacting with maliciously crafted UI elements
- It can lead to phishing attacks, social engineering exploits, or data disclosure
- May damage the application's trustworthiness and reputation, causing loss of user confidence

Remediation:

- Implement proper input validation and sanitize all user-provided content before rendering it in the UI.
- Use secure coding frameworks and libraries that automatically encode output to prevent malicious content from being executed.

Evidence



3.3.2 Clickjacking

Description:

Clickjacking is a web-based attack in which an attacker tricks a user into clicking on a malicious or hidden element while they believe they are interacting with a legitimate webpage. This is typically achieved by overlaying invisible frames, buttons, or page elements on top of trusted content. As a result, the user unknowingly performs actions that can compromise security, such as enabling settings, submitting sensitive information, or initiating unintended transactions

Severity:

Medium

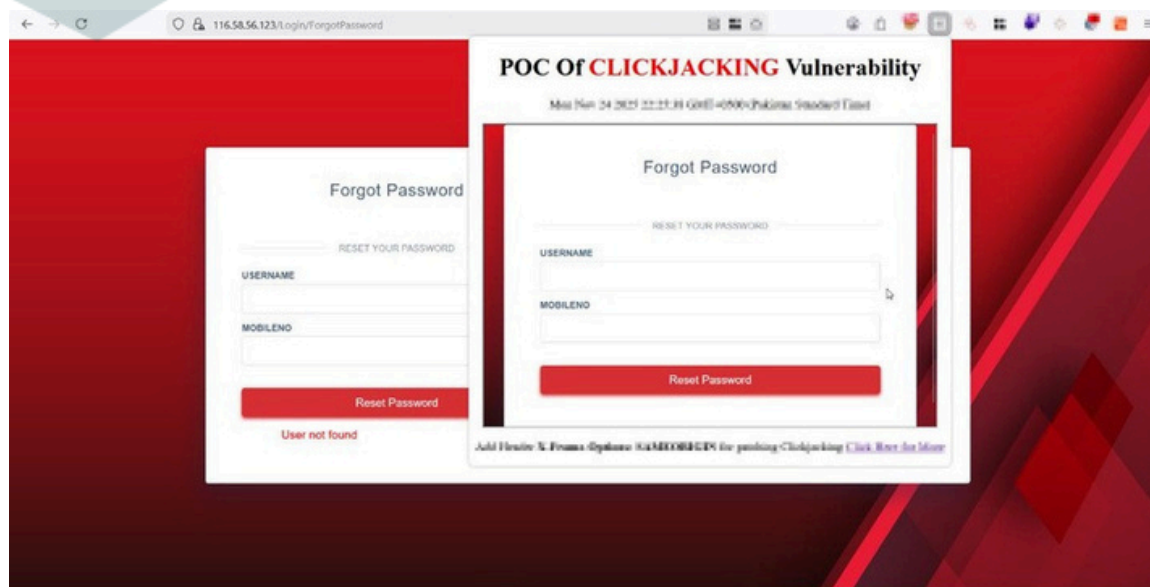
Impact

Unauthorized actions can be performed on behalf of the victim without their knowledge. Sensitive user information or account controls may be exposed or modified.

Remediation

Implement X-Frame-Options headers such as DENY or SAMEORIGIN to block unauthorized framing. Use Content Security Policy (CSP) frame-ancestors directive to strictly control which domains may embed the site.

Evidence



3.3.3 Unencrypted communication

Description:

The application transmits sensitive information—specifically the username and password—over an unencrypted HTTP connection. Because the communication channel is not secured, the credentials are sent in plain text.

Severity:

Medium

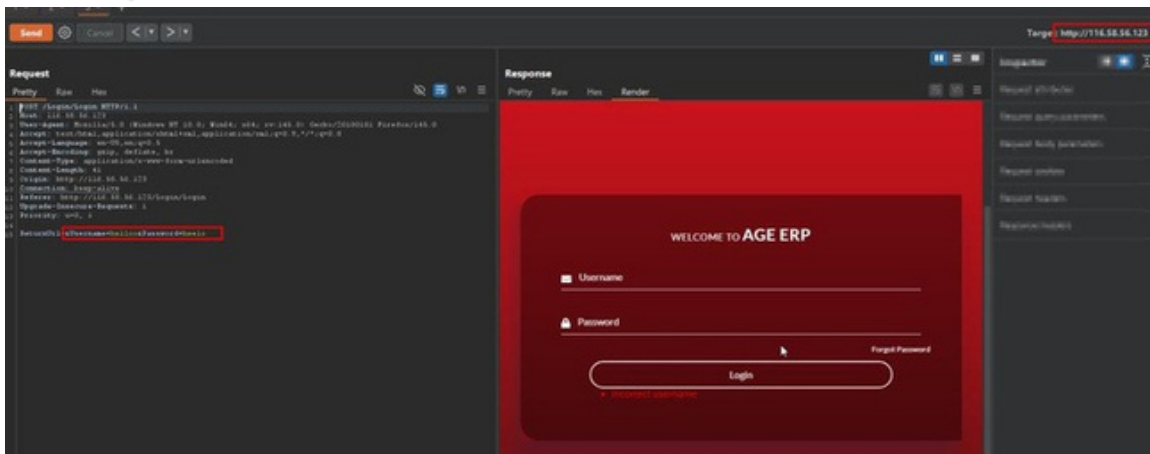
Impact:

- Unauthorized individuals can intercept and steal user credentials.
- Compromised accounts may lead to unauthorized access to internal systems and data.
- increases the risk of broader security breaches, including data theft, privilege escalation, and account takeover.

Remediation

Implement HTTPS using TLS/SSL to encrypt all communication between client and server.

Evidence



3.3.4 Information Discloser:

Description

It was observed that the server version and name disclose through response headers

Severity:

Medium

Impact

Attackers can identify the exact version of the server and map it against known exploits.

Remediation

- Configure your server to prevent Information leakage from the Header of its https Response.
- Disable disclosure of server version response headers and error messages

Evidence

```
Server: Microsoft-IIS/10.0  
/: Retrieved x-aspnet-version header: 4.0.30319.  
/: Retrieved x-powered-by header: ASP.NET.
```

EDGE UP YOUR SECURITY

3.3.5 Portal Exposed Description

Directory brute-forcing enumeration identified an accessible endpoint:

ReportServer/Pages/ReportViewer.aspx This endpoint exposes the Reporting Services portal, which prompts for authentication but is directly reachable from the internet/internal network.

Severity:

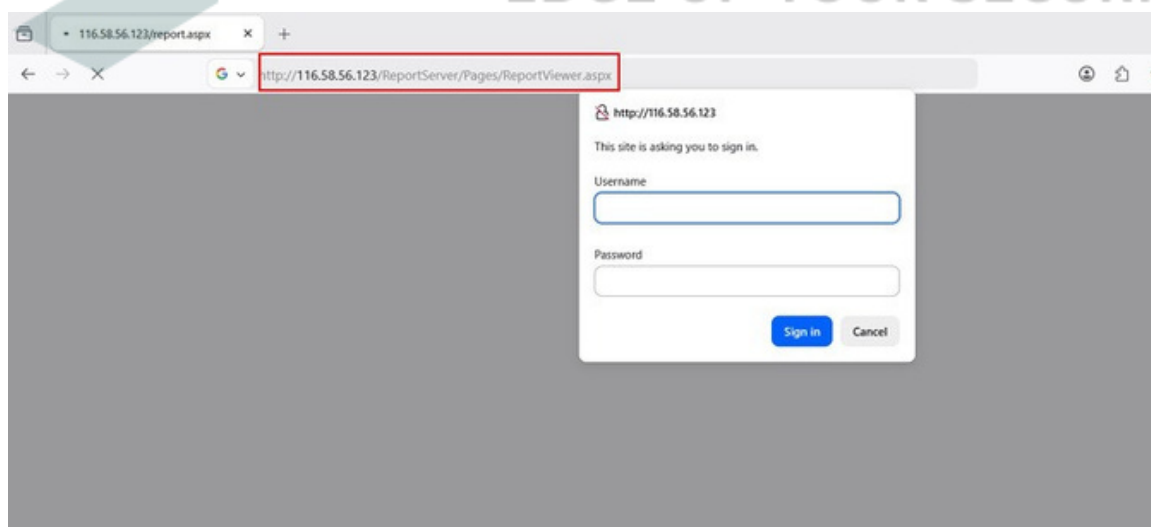
Medium

Impact:

- Gain unauthorized access to sensitive business reports
- Enumerate internal paths, users, or server configurations
- Use the server as an entry point for lateral movement

Remediation

Disable publicly and only access to legitimate user only.



3.3.6 Outdated JavaScript library

Description

It was observed that the application is using an outdated version of a JavaScript library with publicly known security vulnerabilities. This version has not been updated or patched

Severity:

Medium

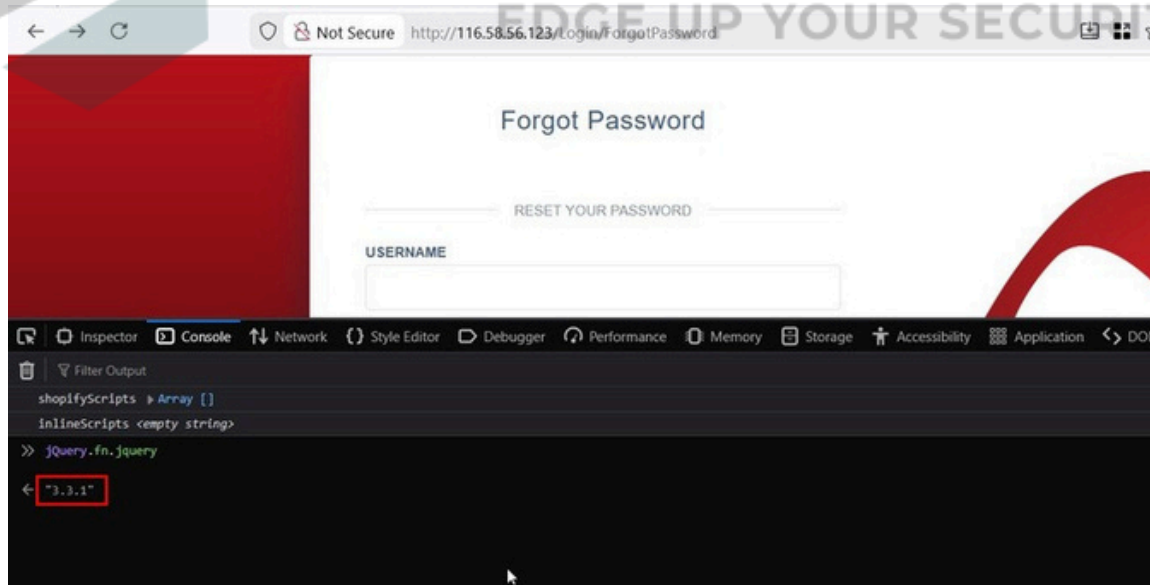
Impact

- Can lead to client-side script execution, compromising user sessions and data.
- Potential to compromise user data and overall application integrity.
- May allow attackers to exploit known vulnerabilities for XSS

Remediation

Identify and upgrade the vulnerable JavaScript library to the latest stable and secure version.

Evidence



3.4 Low Findings:

3.4.1 Missing Security header

Description

During the assessment, it was observed that several critical HTTP security headers, such as Strict-Transport-Security (HSTS), Content-Security-Policy (CSP), X-Content-Type-Options, and X-Frame-Options, were missing from the HTTP responses. This lack of security headers leaves the application vulnerable to a variety of attacks, including man-in-the-middle (MITM), cross-site scripting (XSS), and clickjacking attacks.

Severity

Low

Impact

The absence of security headers increases the risk of attacks like clickjacking, content-type sniffing, and man-in-the-middle interception. It reduces the browser's ability to enforce safe behavior.

Solution

- Implement the Strict-Transport-Security (HSTS) header to enforce HTTPS connections and prevent downgrade attacks
- Set up Content-Security-Policy (CSP) to restrict the sources of executable content and mitigate XSS risks.
- Use the X-Content-Type-Options header to prevent MIME type sniffing and the X-Frame-Options header to defend against clickjacking attacks.

3.4.2 Arbitrary method Allowed

Description:

During assessment, it was observed that the server responds to non-standard HTTP methods (e.g., DEBUG, TRACK, PUT) without proper validation or restriction.

Severity:

Low

Impact

- May allow an attacker to upload or overwrite files using the PUT method.
- Can lead to cross-site tracing (XST) attacks using the TRACE method.
- Increases the attack surface of the application by supporting unnecessary functionalities.

Remediation

- Disable all unnecessary HTTP methods on the server or application level. Only allow required methods such as GET and POST. For all other unsupported methods (e.g., PUT, DELETE, OPTIONS, TRACE, CONNECT), the server should return an HTTP 405 Method Not Allowed response

Evidence

Method	Status	Size
GET	200	32
POST	400	31
HEAD	400	30
CONNECT	400	24
PUT	400	25
TRACE	400	26
OPTIONS	400	26
DELETE	400	25

```
Request: TRACE /Login/Login HTTP/1.1
Host: 116.50.56.123
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:145.0) Gecko/20100101 Firefox/145.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Origin: http://116.50.56.123
Connection: keep-alive
Referer: http://116.50.56.123/Login/Login
Upgrade-Insecure-Requests: 1
Priority: u=0, i

ReturnUrl=4Username=hello&Password=hello

Response: 200 OK
Content-Type: text/html; charset=utf-8
Date: Mon, 24 Nov 2025 19:29:46 GMT
Connection: close
Content-Length: 324

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<HTML>
<HEAD>
<TITLE>
Bad Request
</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=utf-8">
</HEAD>
<BODY>
Bad Request - Invalid Verb
<div>
<div>
<p>
HTTP Error 400. The request verb is invalid.
</p>
</div>
</BODY>
</HTML>
```

4. Conclusion & Remediation Summary

overall risk as **High**. The most urgent issue remains the **Critical** exposure of sensitive user data through This security assessment identified a significant vulnerability footprint in the application, classifying the

the publicly accessible Swagger UI and inadequate authorization controls.

Failure to immediately address the critical findings will leave the organization vulnerable to a large-scale data breach, leading to severe regulatory fines and irreversible damage to user trust.

