



Prologic E Invoice
Web Application VAPT Final Report
For
Prologic Web Solution Private Limited

Prepared By
ESSENTIAL INFOSEC PRIVATE LIMITED

24th July 2024

Disclaimer

this document or any of its content cannot account for, or be included in any form of legal advice. The outcome of a vulnerability scan (or security evaluation) should be utilized to ensure that diligent measures are taken to lower the risk of potential exploits carried out to compromise data. Legal advice must be supplied according to its legal context. All laws and the environments, in which they are applied, are constantly changed and revised. Therefore, no information provided in this document may ever be used as an alternative to a qualified legal body or representative. A portion of the information in this report is taken from OWASP's "The Ten Most Critical Web Application Security Vulnerabilities - 2023 Update" document, that can be found at <https://www.owasp.org>.

The results indicated in this report are reflective of the state of the site and its underlying code at the time of testing. Essential Infosec Pvt Ltd will not be liable for any changes that happen after the submission of this report which might add to vulnerabilities in future.

1. Management Summary

1.1 Document Title

DOCUMENT VERSION CONTROL	
Document Title	Web Application Vulnerability Assessment and Penetration Testing Final Report
Organisation Name	Prologic Web Solution Private Limited
Application Name	Prologic E Invoice
Document Version	1.0
Last Edit Date	24-July-2024

DOCUMENT DISTRIBUTION LIST	
Date	24-July-2024
Classification	Client Confidential
Submitted To	Mr. Muzzammil Kamaal
Designation	
Address	H-183 Sector 63 Noida 201301
Contact Number	+91 9555545345
E-Mail	mmkamaal@prologicwebsolutions.com

1.2 Contact Details

Name	Mr. Pawan Srivastava
Designation	Director
Company	Essential Infosec Private Limited
Address	1st Floor, Plot No. 16, Near SBI BANK Behind Sultanpur Metro Station, New Delhi – 110030
Tel. No.	+91 7398377126
Mobile No.	+91 7985534793
E – Mail	pawan@essentialinfosec.com

Table of Contents

1. Management Summary.....	2
1.1 Document Title	2
1.2 Contact Details	2
2. Scope, Scan (Test) and Report (Creation/Review) Details.....	4
3. Assessment Methodology.....	5
4. Assessment Constraints	8
5. Tools Used	8
6. Standard Followed	9
7. OWASP Top 10 and SANS 25 Application Security Risks.....	10
8. Zero-day (0-day) Application Security Risks.....	12
9. Engagement Scope	13
10. Details of the Auditing team	14
11. Server Details.....	15
11.1 OS / Web Server / Technology Details	15
12. Information Gathering	16
12.1 Identification of Spiders, Robots and Crawler.....	16
12.2 Search Engine Discovery/Reconnaissance.....	17
12.3 Port Scanning.....	19
13. Summary of Key Findings.....	20
14. Graphical Representation	21
15. Detailed Technical Report with Closure PoC.....	22
16. Checklist (Test Cases Performed).....	57
17. General References	60
18. Appendices	61

2. Scope, Scan (Test) and Report (Creation/Review) Details

Following Website is considered as scope of work. During the security assessment we have evaluated security of the modules from the application.

Scope of the work	
Application Name	Prologic E Invoice
Scope	Website Audit
Audit URL	https://gsteinvoice.com/

Audit Activities and Timelines	
Start Date	15-July-2024
End Date	24-July-2024
Scan / Test Time	09 Working Days

Report Created / Reviewed / Approved / Released By	
Report Created By	Mr. Sachin (Information Security Analyst)
Report Reviewed By	Mr. Deepak (Sr. Information Security Analyst)
Report Approved By	Mr. Pawan (Director)
Report Released By	Mr. Sunil (Sr. Information Security Analyst)
Report Released Date	24-July-2024

3. Assessment Methodology

A hybrid approach is followed to perform the assessment that is a combination of tools is used to discover the wide range of vulnerabilities. Additionally, the assessment being adaptive in nature allows us to control the assessment methodology as per the application functionality to focus on the critical areas of the application. The attack vectors are controlled as per the assessment needs and the attack selection ensures maximum coverage of the application.

Following diagram represents the assessment approach:



Figure 1

The table below describes various levels and types of assessment. The type of assessment done for current assessment is available in the “Assessment Scope” section of the document.

Scan/Audit Type		
Level	Type	Information
1	Safe	Safe scan discovers minimum types and instances of vulnerabilities. The safe scan mode avoid fault injection such as Java Scripts, HTML tags, crafted SQL queries etc. to ensure that the application retains its state at the end of the assessment. Any fault injections that may trigger Denial of Service situation are avoided in safe scans. Safe scan suits most when the assessment is to be done on a live application instance, and has already undergone either <i>Standard</i> or <i>Destructive</i> scan/s.
2	Standard	Standard scan discovers and exploits most standard checks such as OWASP Top 10 checks. The standard scan performs fault injection such as Java Scripts injection, HTML tag injection, crafted SQL queries etc. Any fault injections that may trigger Denial of Service situation are avoided in standard scans. Standard scan suits most when the assessment is to be done on a staging/pre-prod/testing application instance.
3	Destructive	Destructive scan discovers and exploits most comprehensive checks including checks that may trigger Denial of Service Attacks situations for the application. Destructive scan is usually done on staging/pre-prod/testing application instance. A destructive scan on a live environment is avoided on live/production systems unless it is really required.

The vulnerabilities discovered are associated with a risk level that indicates how critical the vulnerability is and helps application owners/developers to prioritize the vulnerabilities and choose an appropriate mitigation approach.

Risk Level Information and Necessary Actions




Risk Level	Risk Description and Necessary Action
 <p>High</p>	The high risk level indicates maximum risk associated with a specific vulnerability instance. Such vulnerability may enable an attacker to successfully exploit the underlying application and its data and partially or completely to compromise the application and its data to modify application behaviour to become other than its original intended purpose. The vulnerability marked as "High Risk" is recommended to be handled with utmost priority.
 <p>Medium</p>	The medium risk level indicates considerable risk associated with a specific vulnerability instance. Such vulnerability may enable an attacker to exploit the underlying application and its data to a particular level so that the attacker can gain low level information about the application. Such information can be used by an attacker to craft more specific attacks based on the information collected. The vulnerability marked with "Medium Risk" should be mitigated at the earliest or soon after "High Risk" vulnerabilities are mitigated.
 <p>Low</p>	The low risk level indicates lowest risk associated with a specific vulnerability instance. Such vulnerability may allow an attacker to gain some information about the application which was not intended to be known otherwise. The attacker may not have exploiting techniques available at that instance based on the information revealed by the system. The vulnerability marked with "Low Risk" can be mitigated soon after high and medium risk vulnerabilities are mitigated.

Figure 2

Severity Level Information and Description

SEVERITY	CVSS SCORE	DESCRIPTION
CRITICAL	9.00 – 10.00	Critical Business Impact - e.g., Remote Code Execution, Database Access, System Take Over. Requires fix immediately.
HIGH	7.00 – 8.99	High Business Impact - e.g., Bypassing security controls, arbitrary script execution, takeover any user's account, bypass of user accounts on critical parts of the site. Requires fix as soon as possible
MEDIUM	4.00 – 6.99	Typically, vulnerabilities that requires the attacker to combine it with another vulnerability to cause serious damage
LOW	0.01 – 3.99	Can cause annoyance to the user and be used in a combination with similar vulnerabilities.
INFORMATIONAL	0.0	Bugs that do not create a threat directly or indirectly fall under this category.

Table 1

4. Assessment Constraints

There were no assessment constraints during the security audit.

5. Tools Used

The below tools/scans/scripts were used for security audit:

- BurpSuite Professional (Commercial)
- Nmap (Open Source)
- Kali Linux Tools (Open Source)
- SSL Labs (Open Source)
- Acunetix (Commercial)

6. Standard Followed

Below are the standards followed for VAPT –

1. Open Web Application Security Project (OWASP)
2. SysAdmin, Audit, Network, and Security (SANS)
3. Penetration Testing Execution Standard (PTES)
4. Payment Card Industry Data Security Standard (PCI DSS)
5. Information Systems Security Assessment Framework (ISSAF)
6. Open-Source Security Testing Methodology Manual (OSSTMM)

7. OWASP Top 10 and SANS 25 Application Security Risks

The Common Weakness Enumeration (CWE) is a list of software security vulnerabilities found all throughout the software development industry. It's a community-driven project maintained by MITRE, a non-profit research and development group. For each entry, the CWE provides a description of the vulnerability and steps for mitigating it.

MITRE partnered with the SANS Institute to develop the CWE/25, a list of the 25 most critical software vulnerabilities. A similar list is provided in the Open Web Application Security Project (OWASP) Top 10 Project, which is also a community-driven compilation of software vulnerabilities. Although the CWE/25 and OWASP Top 10 are different, they share many of the same vulnerabilities. Here is a list of the OWASP Top 10 entries for 2021 and their corresponding CWEs.

OWASP Top 10	SANS CWE Top 25
A01:2021-Broken Access Control	1. CWE-787 Out-of-bounds Write
A02:2021-Cryptographic Failures	2. CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
A03:2021-Injection	3. CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
A04:2021-Insecure Design	4. CWE-416 Use After Free
A05:2021-Security Misconfiguration	5. CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
A06:2021-Vulnerable and Outdated Components	6. CWE-20 Improper Input Validation
A07:2021-Identification and Authentication Failures	7. CWE-125 Out-of-bounds Read
A08:2021-Software and Data Integrity Failures	8. CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
A09:2021-Security Logging and Monitoring Failures	9. CWE-352 Cross-Site Request Forgery (CSRF)
A10:2021-Server-Side Request Forgery	10. CWE-434 Unrestricted Upload of File with Dangerous Type
	11. CWE-862 Missing Authorization
	12. CWE-476 NULL Pointer Dereference
	13. CWE-287 Improper Authentication

	<p>14. CWE-190 Integer Overflow or Wraparound</p> <p>15. CWE-502 Deserialization of Untrusted Data</p> <p>16. CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection')</p> <p>17. CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer</p> <p>18. CWE-798 Use of Hard-coded Credentials</p> <p>19. CWE-918 Server-Side Request Forgery (SSRF)</p> <p>20. CWE-306 Missing Authentication for Critical Function</p> <p>21. CWE-362 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')</p> <p>22. CWE-269 Improper Privilege Management</p> <p>23. CWE-94 Improper Control of Generation of Code ('Code Injection')</p> <p>24. CWE-863 Incorrect Authorization</p> <p>25. CWE-276 Incorrect Default Permissions</p>
--	--

Table 2

8. Zero-day (0-day) Application Security Risks

During the security testing, checks were also performed for any zero-day vulnerabilities / attacks.

Below is the brief summary of Zero-day (0-day) security risks –

"Zero-day" is a broad term that describes recently discovered security vulnerabilities that hackers can use to attack systems. The term "zero-day" refers to the fact that the vendor or developer has only just learned of the flaw – which means they have “zero days” to fix it. A zero-day attack takes place when hackers exploit the flaw before developers have a chance to address it.

Zero-day is sometimes written as 0-day. The words vulnerability, exploit, and attack are typically used alongside zero-day, and it's helpful to understand the difference:

A zero-day vulnerability is a software vulnerability discovered by attackers before the vendor has become aware of it. Because the vendors are unaware, no patch exists for zero-day vulnerabilities, making attacks likely to succeed.

A zero-day exploit is the method hackers use to attack systems with a previously unidentified vulnerability.

A zero-day attack is the use of a zero-day exploit to cause damage to or steal data from a system affected by a vulnerability.

Protection against zero-day attacks –

For zero-day protection and to keep your computer and data safe, it's essential for both individuals and organizations to follow cyber security best practices. This includes:

Keep all software and operating systems up to date. This is because the vendors include security patches to cover newly identified vulnerabilities in new releases. Keeping up to date ensures you are more secure.

Use only essential applications. The more software you have, the more potential vulnerabilities you have. You can reduce the risk to your network by using only the applications you need.

Use a firewall. A firewall plays an essential role in protecting your system against zero-day threats. You can ensure maximum protection by configuring it to allow only necessary transactions.

Within organizations, educate users. Many zero-day attacks capitalize on human error. Teaching employees and users' good safety and security habits will help keep them safe online and protect organizations from zero-day exploits and other digital threats.

Use a comprehensive antivirus software solution.

9. Engagement Scope

S. No	URL	Hash Value	Version
1	https://gsteinvoice.com/		Not Available

10. Details of the Auditing team

S. No	Name	Designation	Email Id	Professional Qualifications/ Certifications	Whether the resource has been listed in the Snapshot information published on CERT-In's website (Yes/No)
1	Pawan Srivastava	Director	pawan@essentialinfosec.com	CEH, ISO 27001 LA	YES
2	Deepak Gupta	Senior Security Auditor	deepak@essentialinfosec.com	CEH	YES
3	Sunil	Senior Security Auditor	sunil@essentialinfosec.com	CEH	NO
4	Omkar	Security Auditor	omkar@essentialinfosec.com	LA	NO

11. Server Details

11.1 OS / Web Server / Technology Details

OS Server	Linux CentOS
Web Server	Apache
IP Address	103.129.97.22
Port	443
Technology Used	PHP

12. Information Gathering

12.1 Identification of Spiders, Robots and Crawler

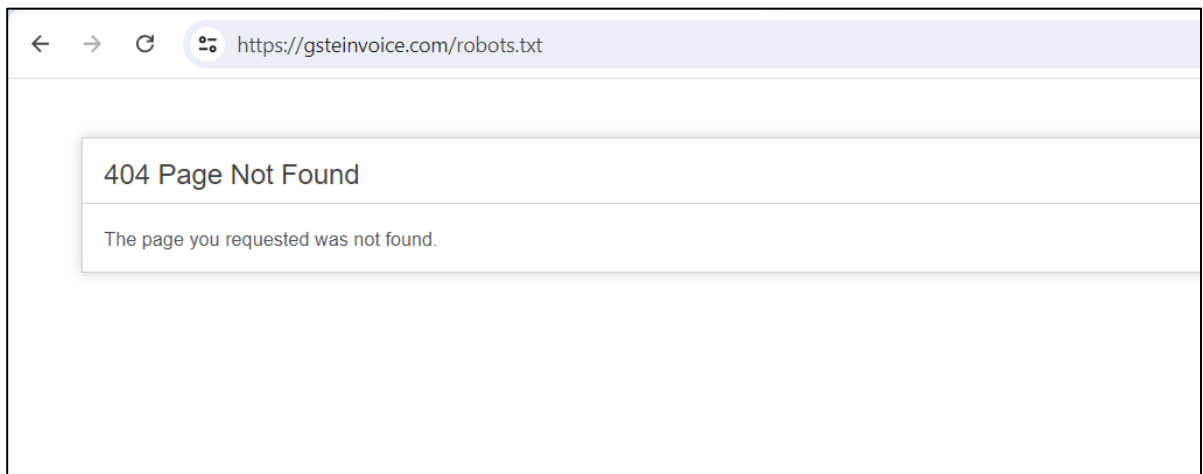
The first phase in security assessment was focused on collecting as much information as possible about a target application.

Tests Conducted:

The site and contains robots.txt or not.

While searching: <https://gstinvoice.com/robots.txt>

Results:



Severity: NIL

12.2 Search Engine Discovery/Reconnaissance

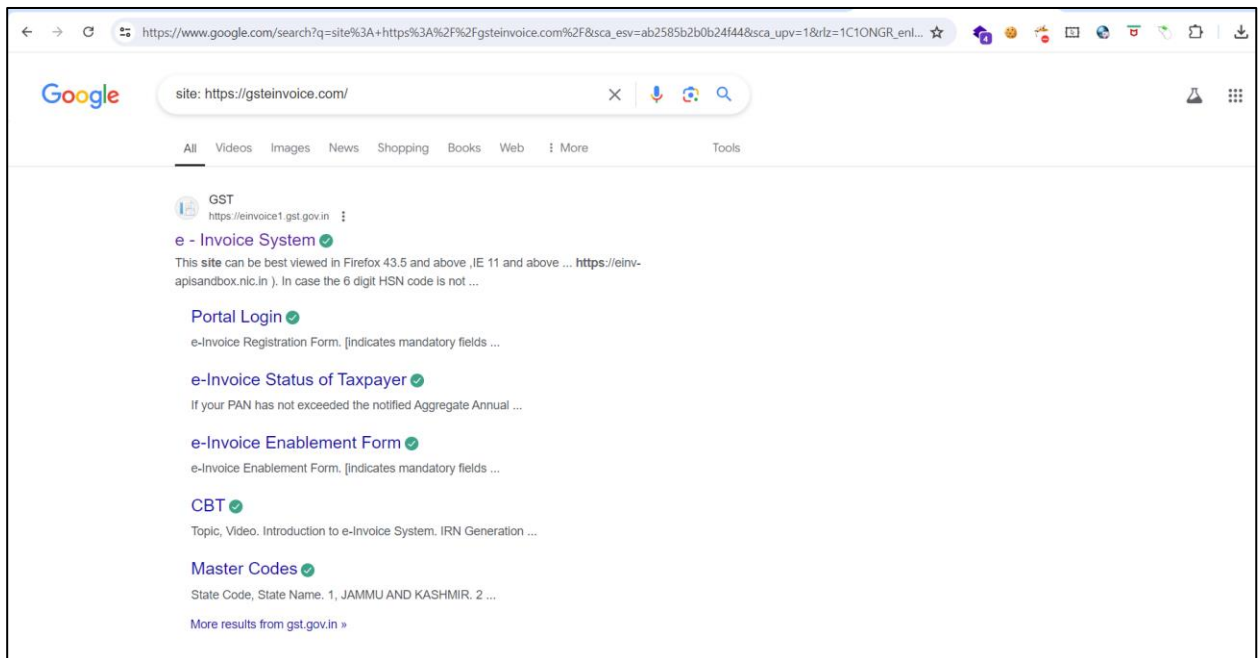
Tests Conducted:

Using the advanced "site:" search operator, it is possible to restrict Search Results to a specific domain.

Results:

To find the web content of site indexed by Google Search, the following Google Search Query is issued:

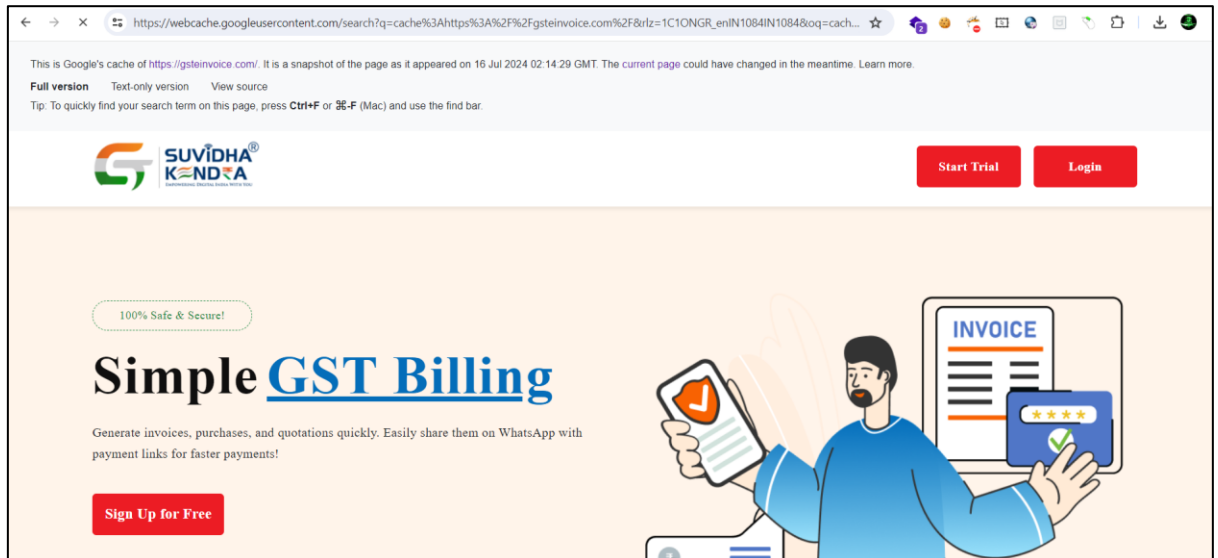
site: <https://gstinvoice.com/>



Severity: NIL

To display the index of Web Application cached by Google, the following Google Search Query is issued

cache:<https://gstinvoice.com/>



Severity: NIL

12.3 Port Scanning

Tests Conducted:

Using the Nmap we checked for Open Ports for the following website.

Results:

site: <https://gsteinvoice.com/>

Hosts		Services		Nmap Output		Ports / Hosts	Topology	Host Details	Scans
OS	Host			Port	Protocol	State	Service	Version	
	gsteinvoice.com (103.129.97.22)			21	tcp	open	ftp	Pure-FTPd	
				25	tcp	open	smtp		
				53	tcp	open	domain	ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)	
				80	tcp	open	http	Apache httpd	
				110	tcp	open	pop3	Dovecot pop3d	
				143	tcp	open	imap	Dovecot imapd	
				443	tcp	open	http	Apache httpd	
				465	tcp	open	smtp	Exim smtpd 4.96.2	
				587	tcp	open	smtp	Exim smtpd 4.96.2	
				993	tcp	open	imaps		
				995	tcp	open	pop3s		
				3306	tcp	open	mysql	MySQL 5.5.5-10.5.25-MariaDB	

Severity: Low

13. Summary of Key Findings

Sr. No.	Vulnerability Name	Severity	Final Status
01	Cross Site Scripting (XSS)	High	CLOSED
02	Weak Encoding Used	Medium	CLOSED
03	HTML Injection	Medium	CLOSED
04	Improper Input Validation	Medium	CLOSED
05	Sensitive Information in URL	Medium	CLOSED
06	Click-Jacking Attack	Medium	CLOSED
07	Possible Brute Force Attack – CAPTCHA Not Found	Medium	CLOSED
08	Credentials Transmitted to Server in Plain Text	Medium	CLOSED
09	Directory Listing	Medium	CLOSED
10	Missing HTTP Strict Transport Security Header (HSTS)	Low	CLOSED
11	Missing X-Frame-Options Header	Low	CLOSED
12	Missing X-Permitted-Cross-Domain-Policies Header	Low	CLOSED
13	Missing Referrer-Policy Header	Low	CLOSED
14	Missing Permissions-Policy Header	Low	CLOSED
15	Missing Content Security Policy (CSP) Header	Low	CLOSED
16	Missing X-Content-Type-Options Header	Low	CLOSED
17	Missing X-XSS-Protection Header	Low	CLOSED
18	Simultaneous Login Allowed	Low	CLOSED
19	Application does not display last login time and date	Low	CLOSED
20	Auto-Complete Enabled	Low	CLOSED
21	Vulnerable and Outdated Components	Low	CLOSED
22	Session Cookie Secure Attribute Not Set	Low	CLOSED
23	Unwanted HTTP Methods Enabled	Low	CLOSED
24	Session Timeout is High or Not Implemented	Low	CLOSED

Table 3

14. Graphical Representation

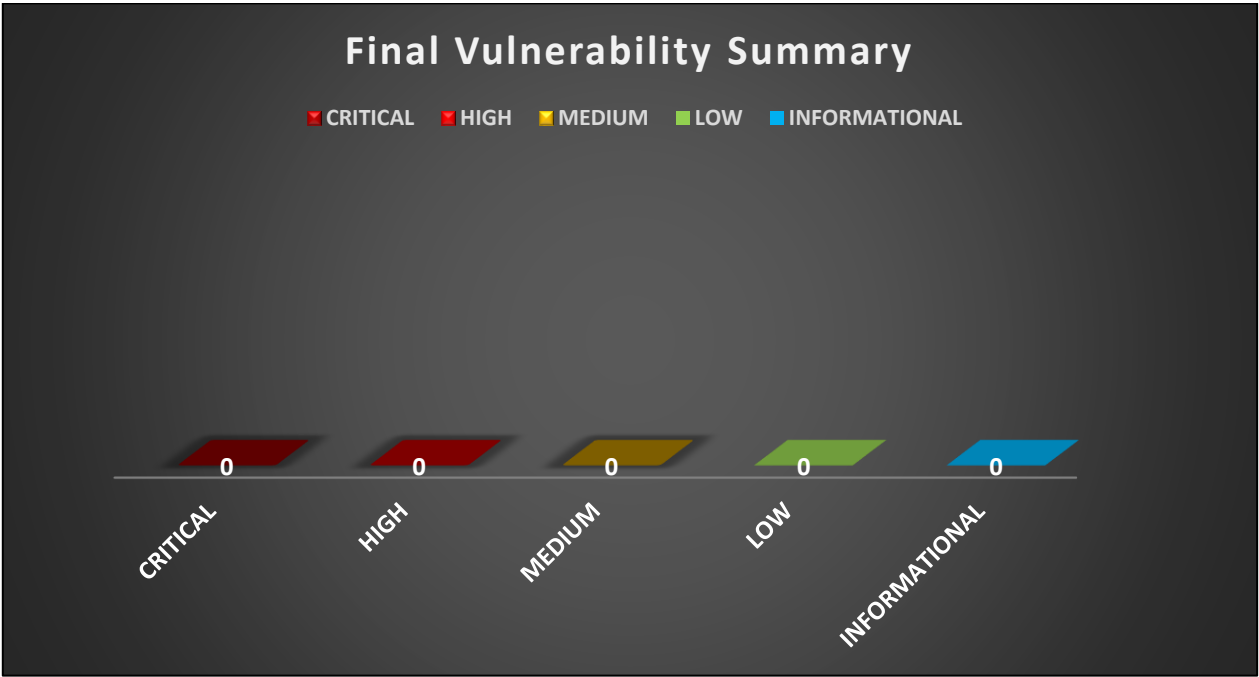


Figure 3

15. Detailed Technical Report with Closure PoC

01: Cross Site Scripting (XSS)

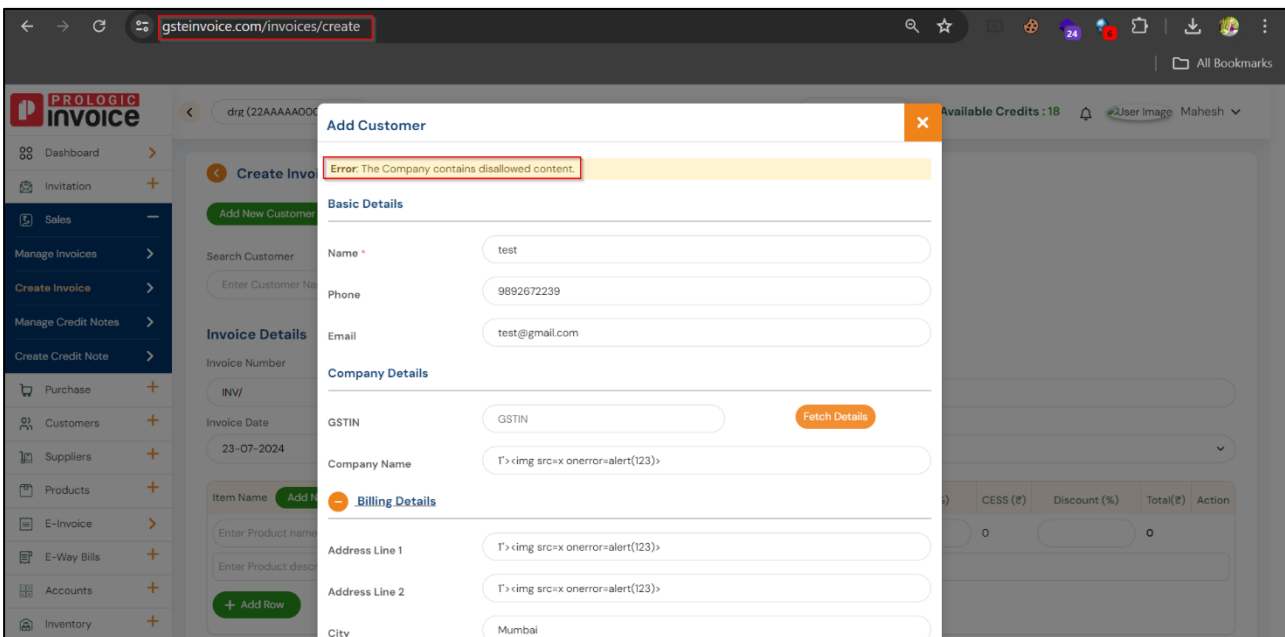
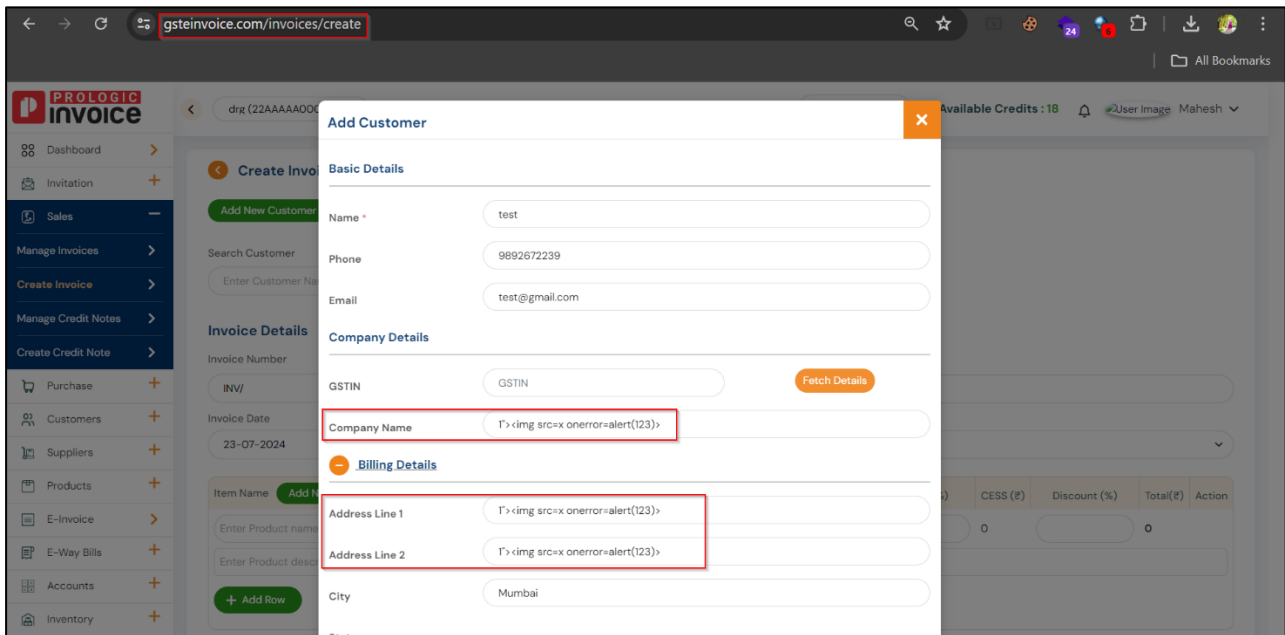
SEVERITY

High

STATUS

CLOSED

CLOSURE PROOF OF CONCEPT



The screenshot shows the 'Prologic Invoice' application interface. On the left is a sidebar with navigation options: Dashboard, Invitation, Sales, Manage Invoices, Manage Credit Notes, Create Invoice, Create Credit Note, Purchase, Customers, Suppliers, Products, E-Invoice, E-Way Bills, Accounts, and Inventory. The main area displays the 'INVOICE' form for 'INV/ 23-07-2024'. The form includes fields for Product Name, HSN/SAC Code, Default TAX Rate, Product Code, CESS, and Additional Details (Product Category, Default Discount Rate). A modal titled 'Add Category' is open, showing fields for Category Name and Description, both with error messages: 'T>'. The modal has 'Save' and 'Cancel' buttons. The background form shows a table for items with columns for CESS, Discount, Total, and Action.

PROLOGIC
INVOICE

Dashboard

Invitation

Sales

Manage Invoices

Create Invoice

Manage Credit Notes

Create Credit Note

Purchase

Customers

Suppliers

Products

E-Invoice

E-Way Bills

Accounts

Inventory

22AAAAAQQ

Create Invoice

Add New Customer

Search Customer

Enter Customer Name

Invoice Details

Invoice Number

INV/

Invoice Date

23-07-2024

Item Name

Add

Enter Product name

Enter Product description

Add Row

1

Quantity

Product Code

T>

Purchase Price

₹ 0.00

CESS

% 0

Additional Details (Optional Fields)

Product Category

Add Category

Default Discount Rate

Default Discount Rate

%

More Details

Alert For Minimum Stock Quantity

Alert Quantity

Measurement Unit

None

Description

T>

Add Product

Cancel

Available Credits : 18

User Image

Maresh

(%)

CESS (₹)

Discount (%)

Total(₹)

Action

0

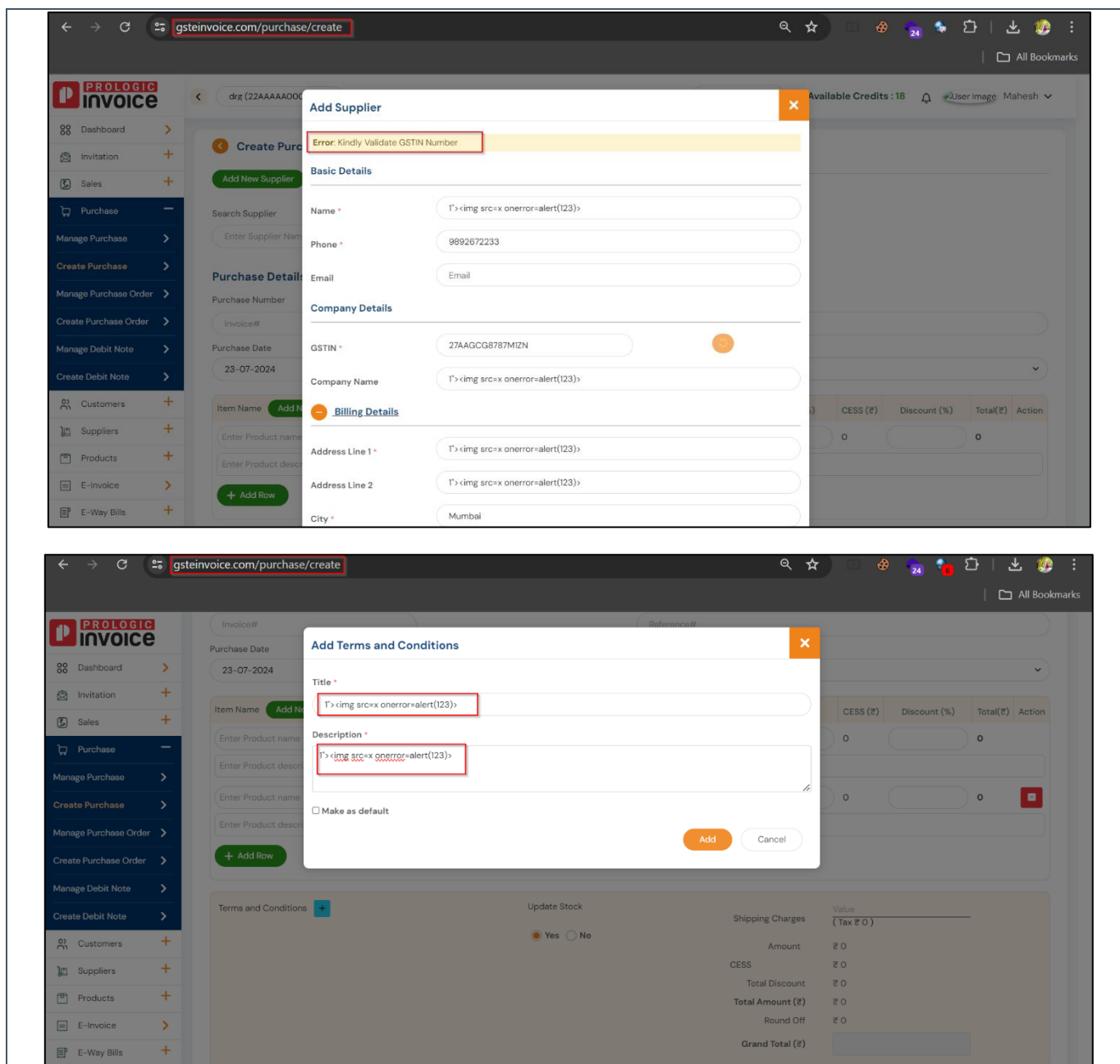
0

The top screenshot shows the 'Add New Product' modal in the Prologic E Invoice Web Application. The modal contains the following fields and values:

- Product Name:** Placeholder text: ``
- Selling Price:** 34
- HSN/SAC Code:** 0901
- Default TAX Rate:** 1
- Quantity:** Placeholder text: ``
- Product Code:** Placeholder text: ``
- Purchase Price:** 0.00
- CESS:** 0

The bottom screenshot shows the 'Add Customer' modal in the Prologic E Invoice Web Application. The modal contains the following fields and values:

- Name:** Placeholder text: ``
- Phone:** 9892672233
- Email:** Placeholder text: ``
- GSTIN:** 27AAGCG8787M1ZN
- Company Name:** Placeholder text: ``
- Address Line 1:** Placeholder text: ``
- Address Line 2:** Placeholder text: ``
- City:** Mumbai



Prologic Web Solution Private Limited - Prologic E Invoice Web Application VAPT Final Report

gsteinvoice.com/purchase/create

PROLOGIC INVOICE

Dashboard > Invitation > Sales > **Purchase** > Manage Purchase > **Create Purchase** > Manage Purchase Order > Create Purchase Order > Manage Debit Note > Create Debit Note > Customers > Suppliers > Products > E-Invoice > E-Way Bills >

Item Name	Quantity	Rate	Amount	HSN/SAC	Tax (%)	Tax (₹)	CESS (%)	CESS (₹)	Discount (%)	Total(₹)	Action
Enter Product name	1		₹ 0.00			0		0		0	
Enter Product description (Optional)											
Enter Product name	1		0			0		0		0	
Enter Product description											

+ Add Row

Terms and Conditions: T's Description: T's

Update Stock: Yes No

Shipping Charges: Value (Tax ₹ 0)

Amount: ₹ 0

CESS: ₹ 0

Total Discount: ₹ 0

Total Amount (₹): ₹ 0

Round Off: ₹ 0

Grand Total (₹):

Generate Purchase Cancel

© Powered by Prologic Web Solutions. All rights reserved

gsteinvoice.com/expense/addexpense

PROLOGIC INVOICE

drq (22AAAAA0000A1Z5) Create Available Credits : 17 User Image Mahesh

Add Expense / Income

Name: T's GST: GSTIN

Address: T's State: Maharashtra

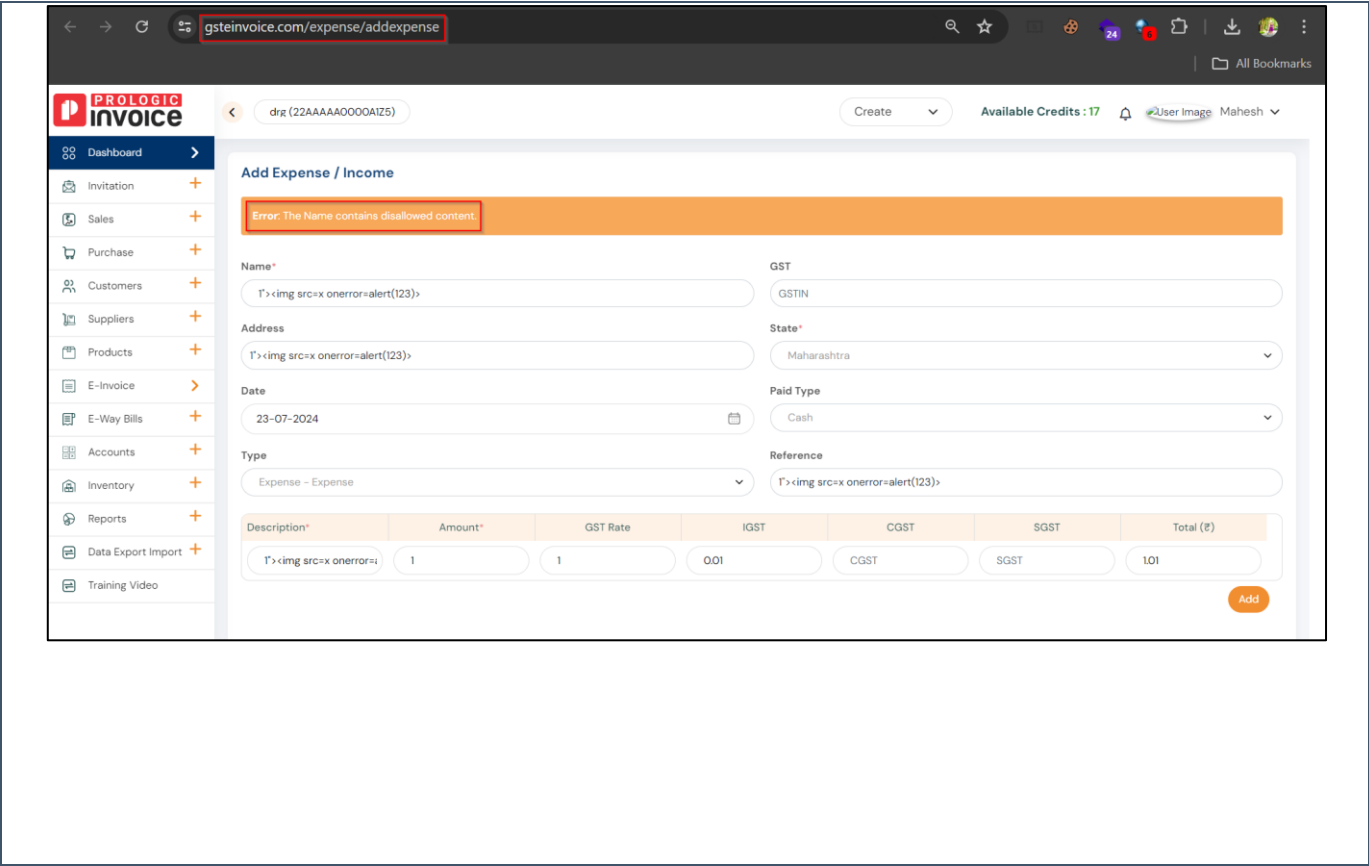
Date: 23-07-2024 Paid Type: Cash

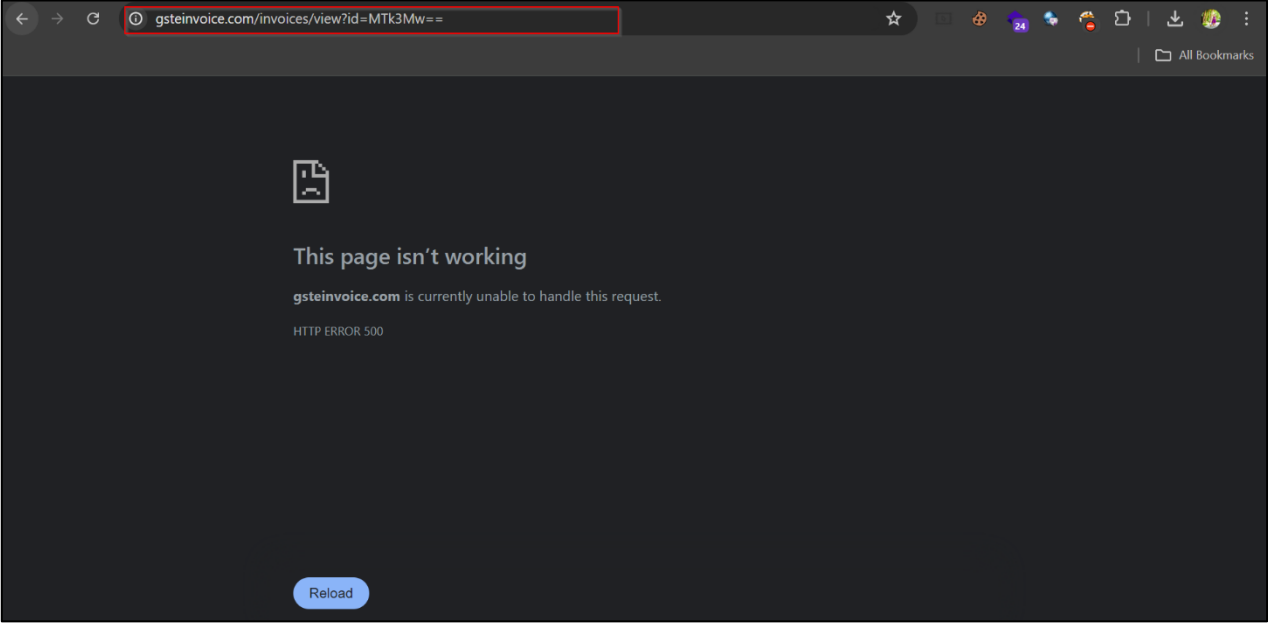
Type: Expense - Expense Reference: T's

Description*	Amount*	GST Rate	IGST	CGST	SGST	Total (₹)
T's 	1	1	0.01	CGST	SGST	1.01

Add

© Powered by Prologic Web Solutions. All rights reserved



02: Weak Encoding Used	
SEVERITY	Medium
STATUS	CLOSED
CLOSURE PROOF OF CONCEPT	
	

03: HTML Injection

SEVERITY

Medium

STATUS

CLOSED

CLOSURE PROOF OF CONCEPT

The screenshot shows the 'Update Profile' page of the Prologic E Invoice application. The browser address bar displays 'gstinvoice.com/user/update'. The page has a sidebar with navigation links: Dashboard, Invitation, Sales, Purchase, Customers, Suppliers, Products, E-Invoice, E-Way Bills, Accounts, Inventory, Reports, Data Export Import, and Training Video. The main content area is titled 'Update Profile Picture' and 'Update Your Signature'. Below these are input fields for Name, Address, City, State, PIN Code, Country, Email, Aadhaar, and Phone. The 'Address' field contains the HTML payload: `<h1>HTML INJECTION</h1>`, which is highlighted with a red box. The 'Country' field is set to 'India'. The 'Email' field is 'maheshthite107@gmail.com'. The 'Aadhaar' field is '841780759725'. The 'Phone' field is '7004771608'. The 'PIN Code' field is '533216'. The 'City' field is 'test'. The 'State' field is '30-GOA'. The 'Update Profile' button is visible at the bottom right.

The screenshot shows the 'Update Profile' page of the Prologic E Invoice application after the HTML injection. The browser address bar displays 'gstinvoice.com/user/update'. The page has a sidebar with navigation links: Dashboard, Invitation, Sales, Purchase, Customers, Suppliers, Products, E-Invoice, E-Way Bills, Accounts, Inventory, Reports, Data Export Import, and Training Video. The main content area is titled 'Update Your Details (Mahesh)'. Below the title is an orange error message: 'Error The Address contains disallowed content.' The 'Address' field contains the HTML payload: `<h1>HTML INJECTION</h1>`. The 'Country' field is set to 'India'. The 'Email' field is 'maheshthite107@gmail.com'. The 'Aadhaar' field is '841780759725'. The 'Phone' field is '7004771608'. The 'PIN Code' field is '533216'. The 'City' field is 'test'. The 'State' field is '30-GOA'. The 'Update Profile' button is visible at the bottom right.

04: Improper Input Validation

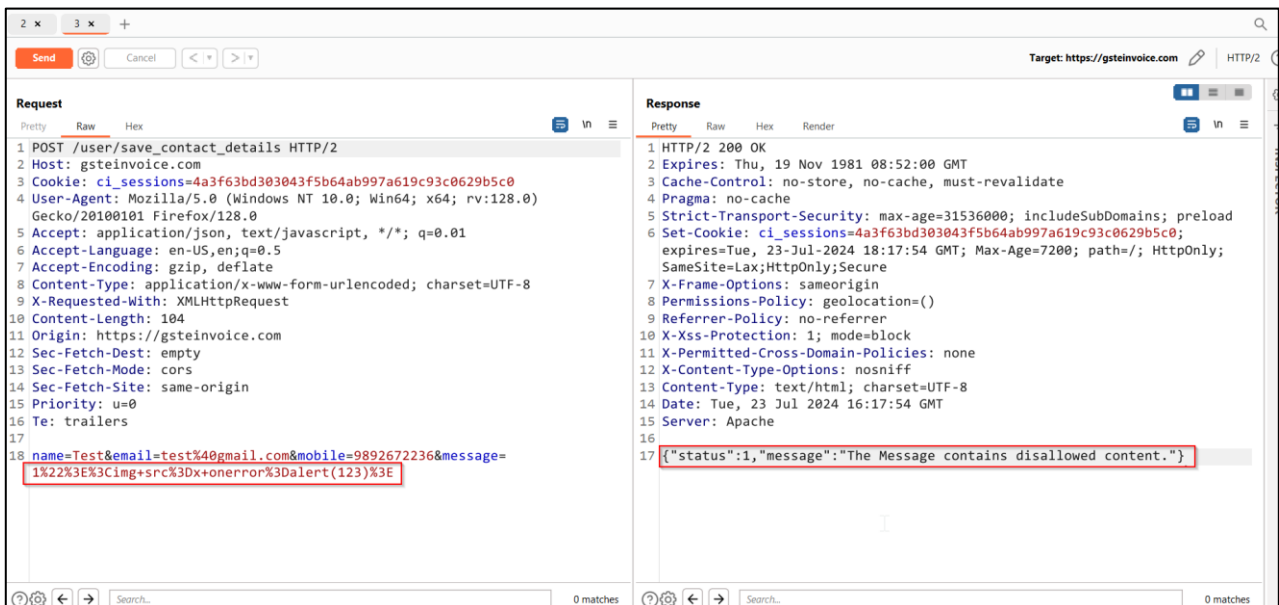
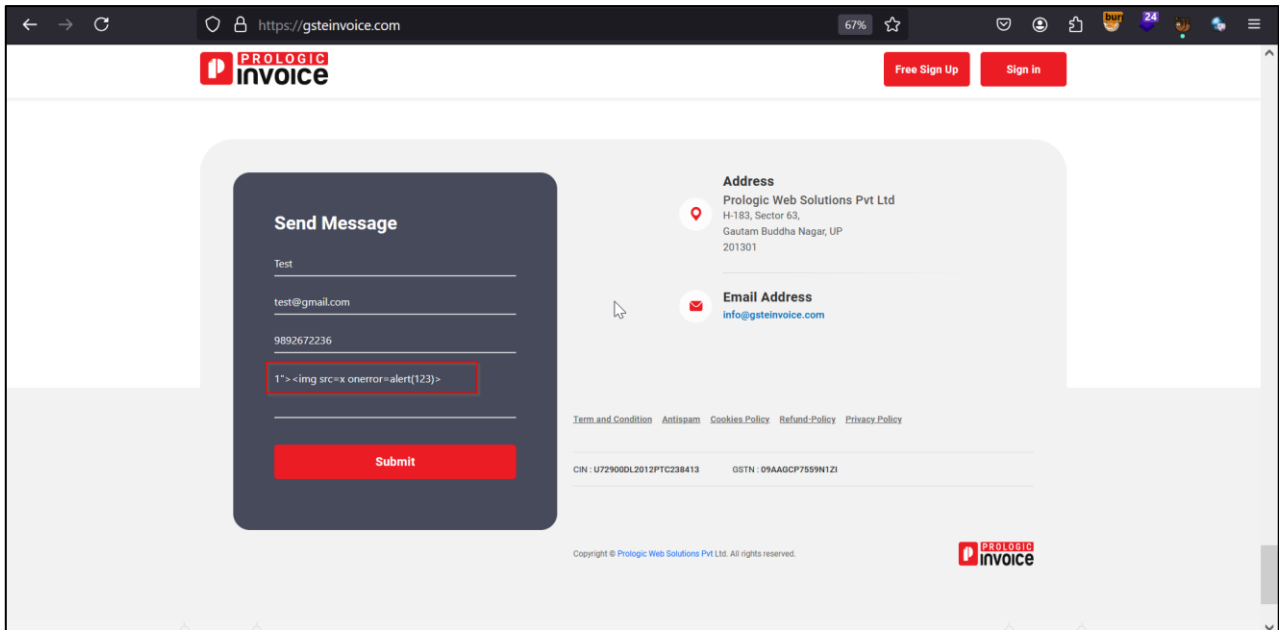
SEVERITY

Medium

STATUS

CLOSED

CLOSURE PROOF OF CONCEPT



gsteinvoice.com/accounts/add

PROLOGIC Invoice

drp (22AAAAA0000AIZ5)

Create Available Credits : 17 User Image Mahesh

Dashboard

Invitation Sales Purchase Customers Suppliers Products E-Invoice E-Way Bills Accounts Inventory Reports Data Export Import

Add New Account

Account No* 123

Name* test

Initial Balance* 1

Account Type Savings

Bank Name* HDFC BANK

IFSC Code* HDFC0000967

Note

`">`

Add Account

© Powered by Prologic Web Solutions. All rights reserved

gsteinvoice.com/accounts/add

PROLOGIC Invoice

drp (22AAAAA0000AIZ5)

Create Available Credits : 17 User Image Mahesh

Dashboard

Invitation Sales Purchase Customers Suppliers Products E-Invoice E-Way Bills Accounts Inventory Reports Data Export Import

Add New Account

Error: The Note contains disallowed content.

Account No* 123

Name* test

Initial Balance* 1

Account Type Savings

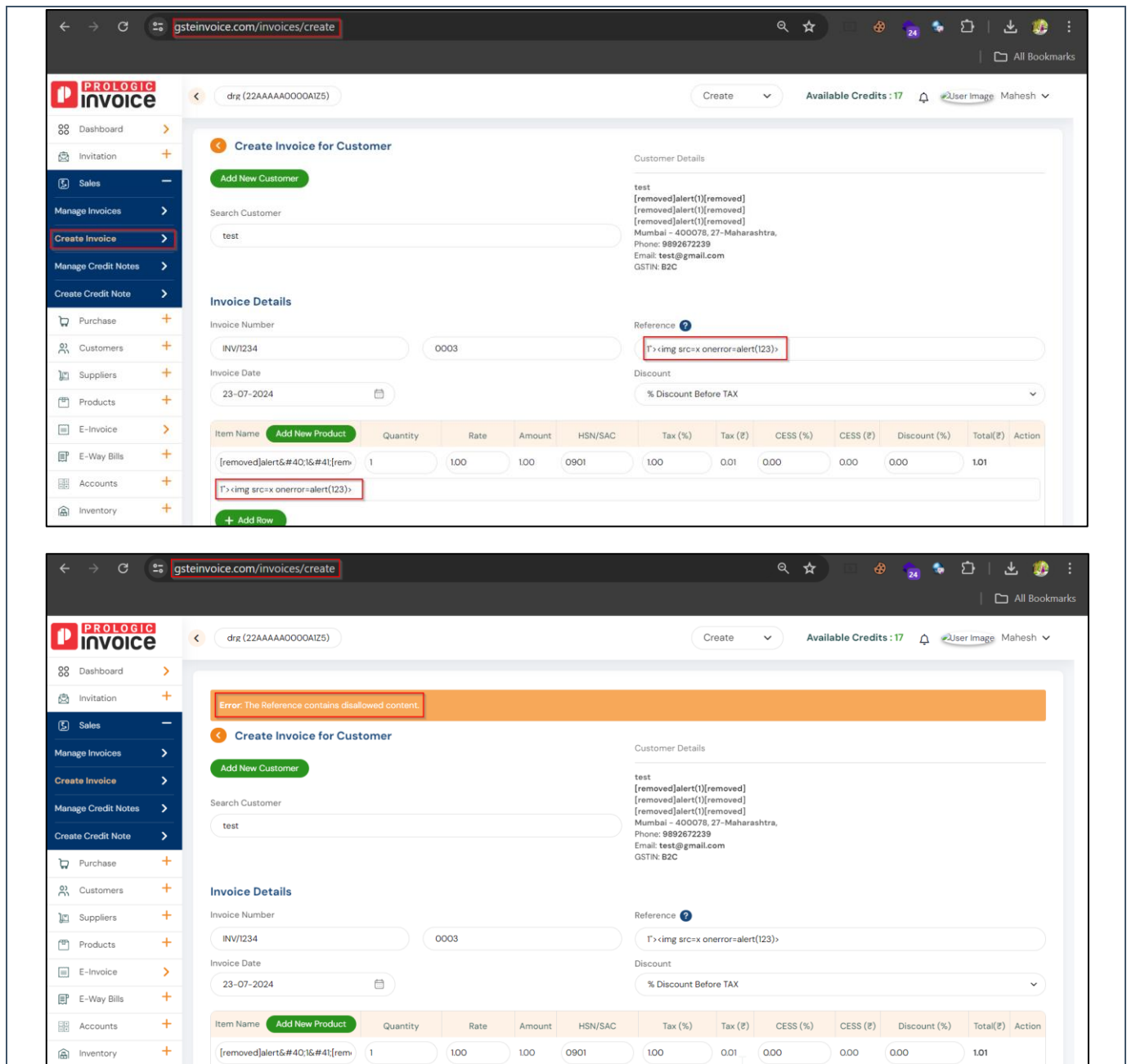
Bank Name* HDFC BANK

IFSC Code* HDFC0000967

Note

`">`

Add Account



gsteinvoice.com/purchase/create

PROLOGIC INVOICE

drgr (22AAAAA0000AIZ5)

Create Available Credits : 17 User Image Mahesh

Dashboard Invitation Sales Purchase Manage Purchase Create Purchase Manage Purchase Order Create Purchase Order Manage Debit Note Create Debit Note Customers Suppliers Products E-Invoice E-Way Bills

Create Purchase

Add New Supplier

Search Supplier

Enter Supplier Name or Mobile Number to search

Purchase Details

Purchase Number: rrr

Purchase Date: 23-07-2024

Reference: T'

Discount: % Discount Before TAX

Item Name	Quantity	Rate	Amount	HSN/SAC	Tax (%)	Tax (₹)	CESS (%)	CESS (₹)	Discount (%)	Total(₹)	Action
chai	1	100	100	0901	100	0.01	0.00	0.00	0.00	1.01	
T'											

+ Add Row

Error: The Reference contains disallowed content.

Create Purchase

Add New Supplier

Search Supplier

Enter Supplier Name or Mobile Number to search

Purchase Details

Purchase Number: rrr

Purchase Date: 23-07-2024

Reference: T'

Discount: % Discount Before TAX

Item Name	Quantity	Rate	Amount	HSN/SAC	Tax (%)	Tax (₹)	CESS (%)	CESS (₹)	Discount (%)	Total(₹)	Action
chai	1	100	100	0901	100	0.01	0.00	0.00	0.00	1.01	
T'											

Prologic Web Solution Private Limited - Prologic E Invoice Web Application VAPT Final Report

gsteinvoice.com/purchaseOrder/create

Success: Product added successfully!

PROLOGIC invoice

Dashboard > Invitation > Sales > **Purchase** > Manage Purchase > Create Purchase > Manage Purchase Order > Create Purchase Order > Manage Debit Note > Create Debit Note > Customers > Suppliers > Products > E-Invoice > E-Way Bills

Create Purchase Order

Supplier Details

Add New Supplier

Search Supplier

Enter Supplier Name or Mobile Number to search

Purchase Order Details

Purchase Order Number

PO/ 0002

Reference ?

!>

Purchase Order Date

23-07-2024

Discount

% Discount Before TAX

Item Name	Quantity	Rate	Amount	HSN/SAC	Tax (%)	Tax (₹)	CESS (%)	CESS (₹)	Discount (%)	Total(₹)	Action
chai	1	89	89.00	1006	0.1	0.01		0.00	90	8.91	
!>											

+ Add Row

gsteinvoice.com/purchaseOrder/create

drp (22AAAAA0000AI25)

Create Available Credits : 17 User Image Mahesh

PROLOGIC invoice

Dashboard > Invitation > Sales > **Purchase** > Manage Purchase > Create Purchase > Manage Purchase Order > Create Purchase Order > Manage Debit Note > Create Debit Note > Customers > Suppliers > Products > E-Invoice > E-Way Bills

Create Purchase Order

Supplier Details

Add New Supplier

Search Supplier

Enter Supplier Name or Mobile Number to search

Purchase Order Details

Purchase Order Number

PO/ 0002

Reference ?

!>

Purchase Order Date

23-07-2024

Discount

% Discount Before TAX

Item Name	Quantity	Rate	Amount	HSN/SAC	Tax (%)	Tax (₹)	CESS (%)	CESS (₹)	Discount (%)	Total(₹)	Action
chai	1	89	89.00	1006	0.1	0.01		0.00	90	8.91	
!>											

Error: The Reference contains disallowed content.

05: Sensitive Information in URL

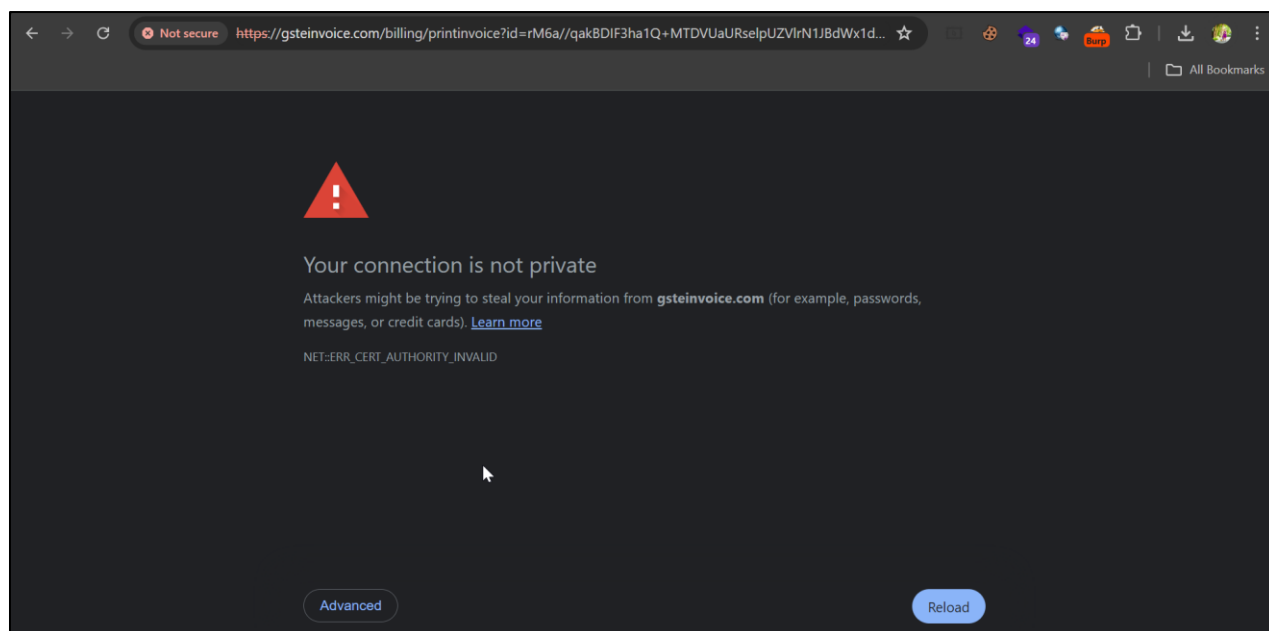
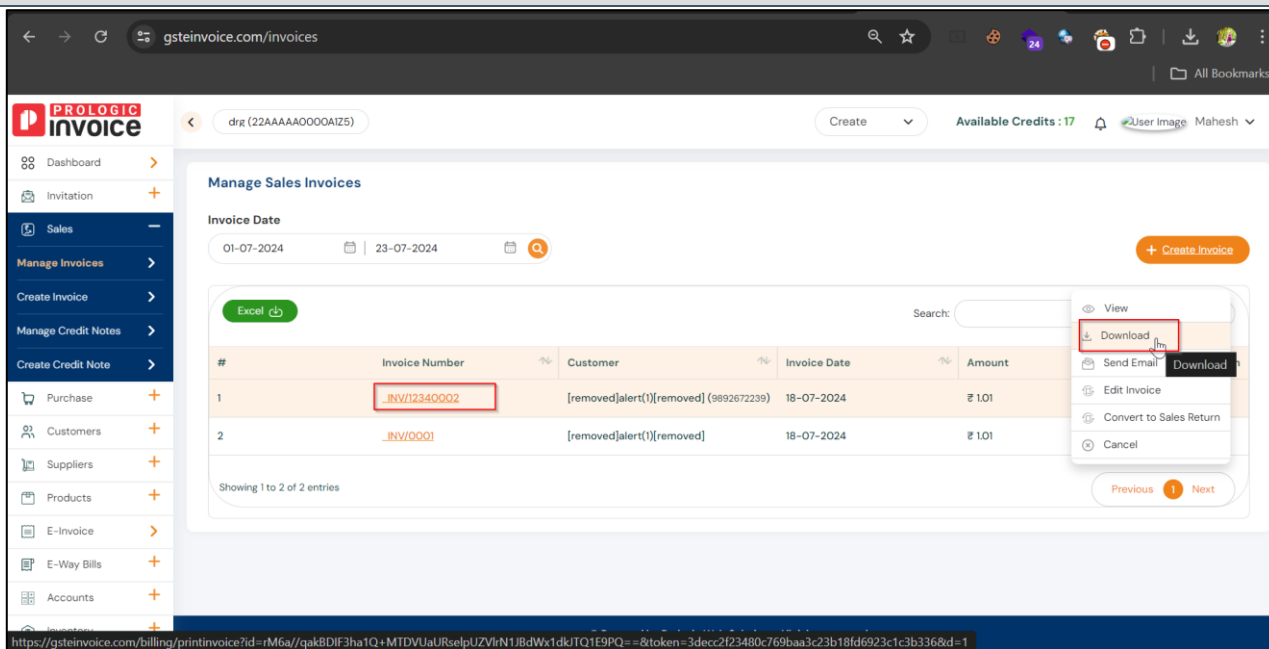
SEVERITY

Medium

STATUS

CLOSED

CLOSURE PROOF OF CONCEPT



06: Click-Jacking Attack

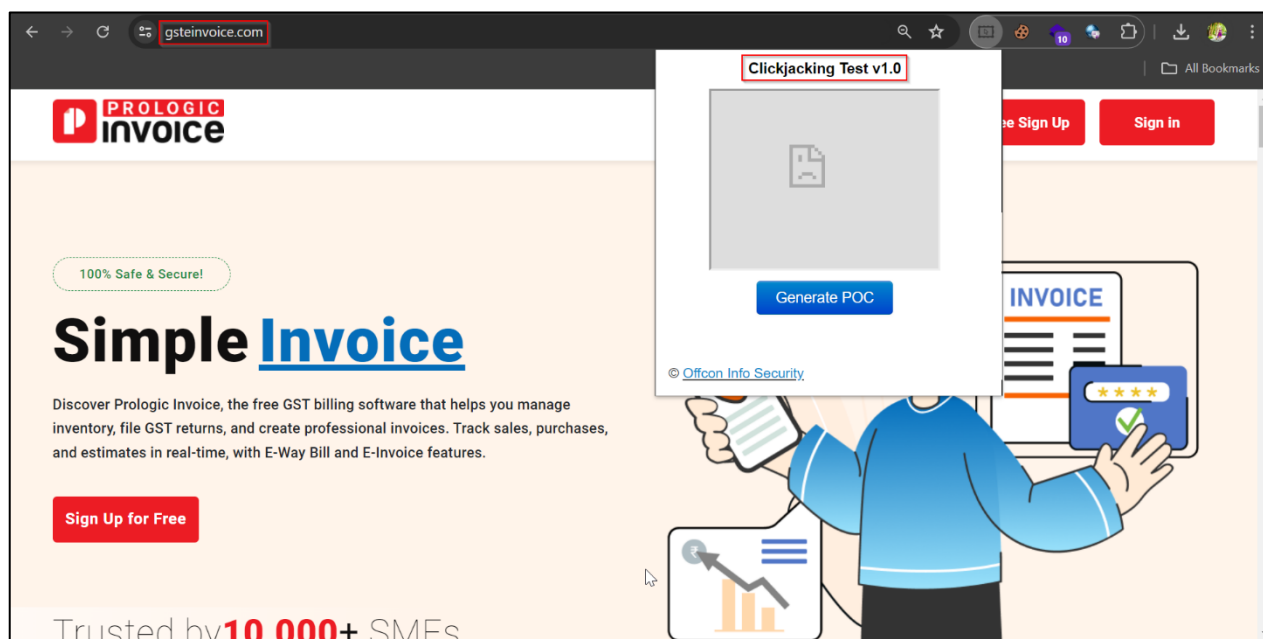
SEVERITY

Medium

STATUS

CLOSED

CLOSURE PROOF OF CONCEPT



07: Possible Brute Force Attack – CAPTCHA Not Found

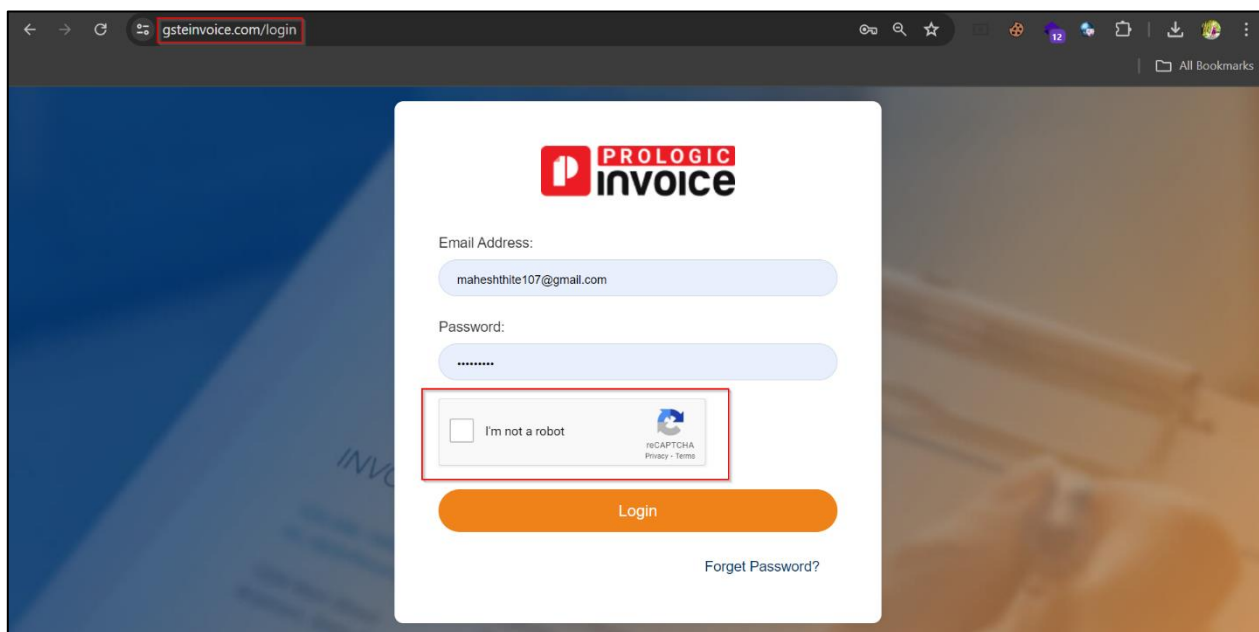
SEVERITY

Medium

STATUS

CLOSED

CLOSURE PROOF OF CONCEPT



08: Credentials Transmitted to Server in Plain Text

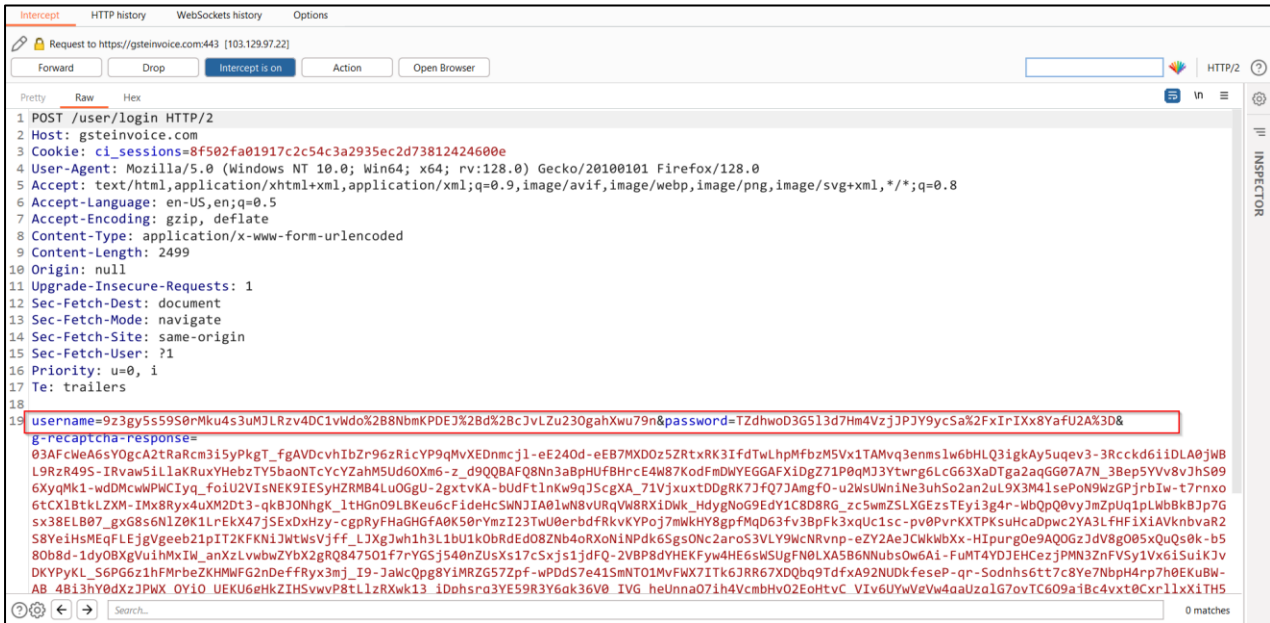
SEVERITY

Medium

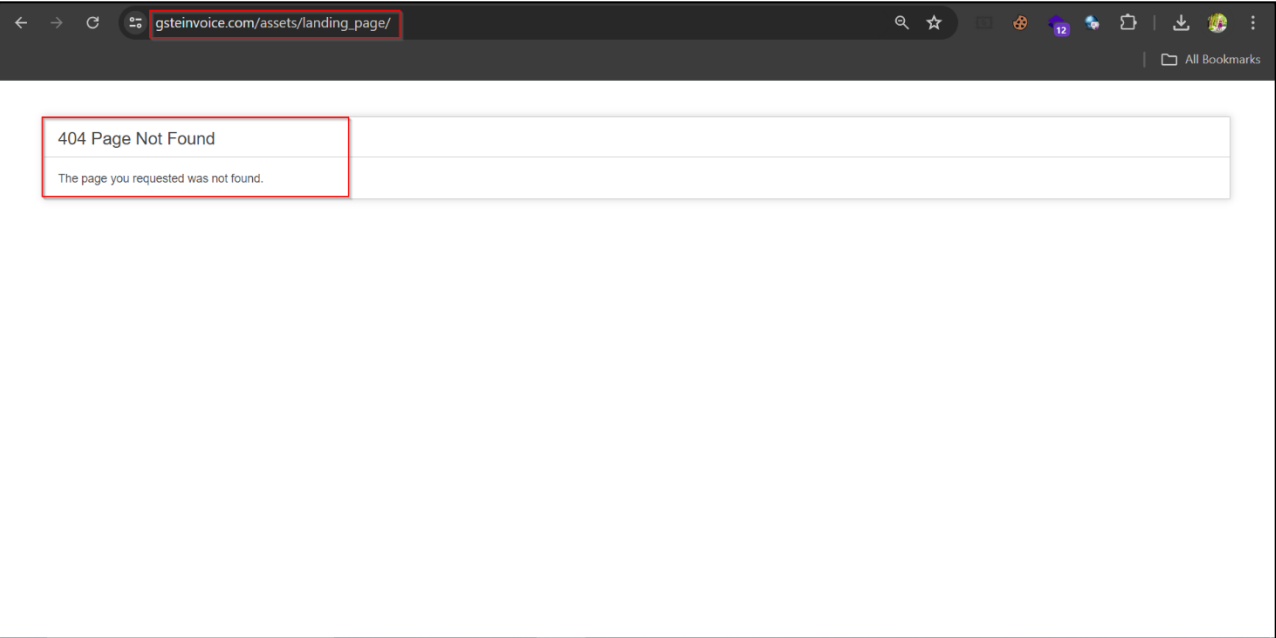
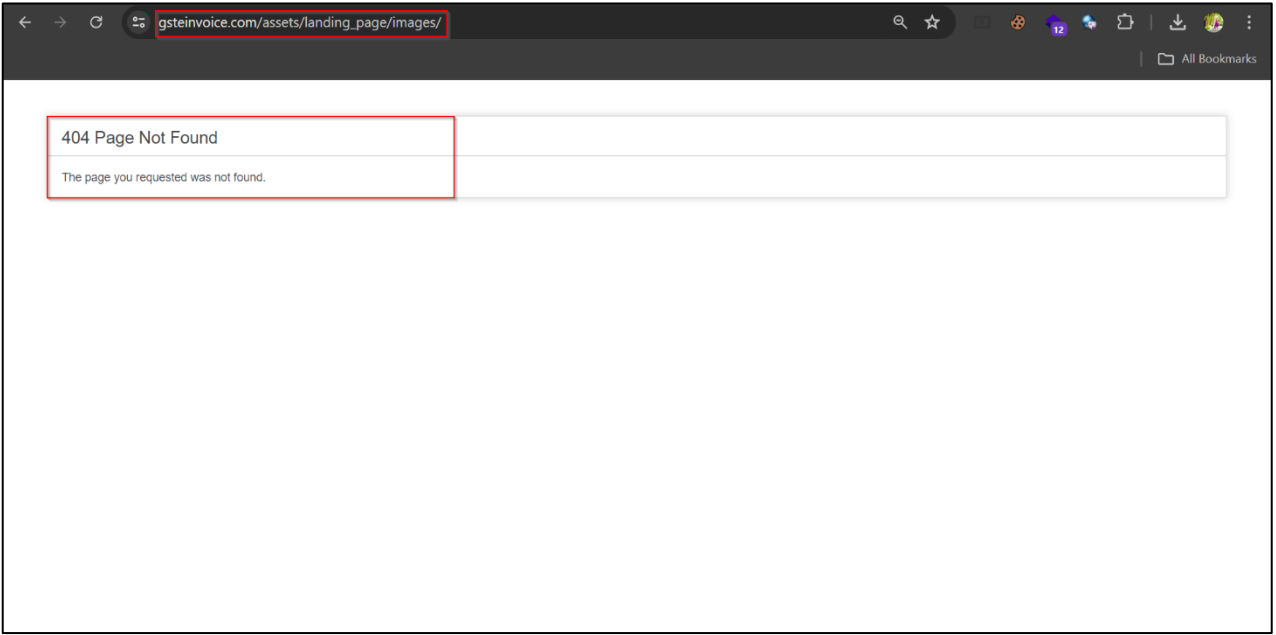
STATUS

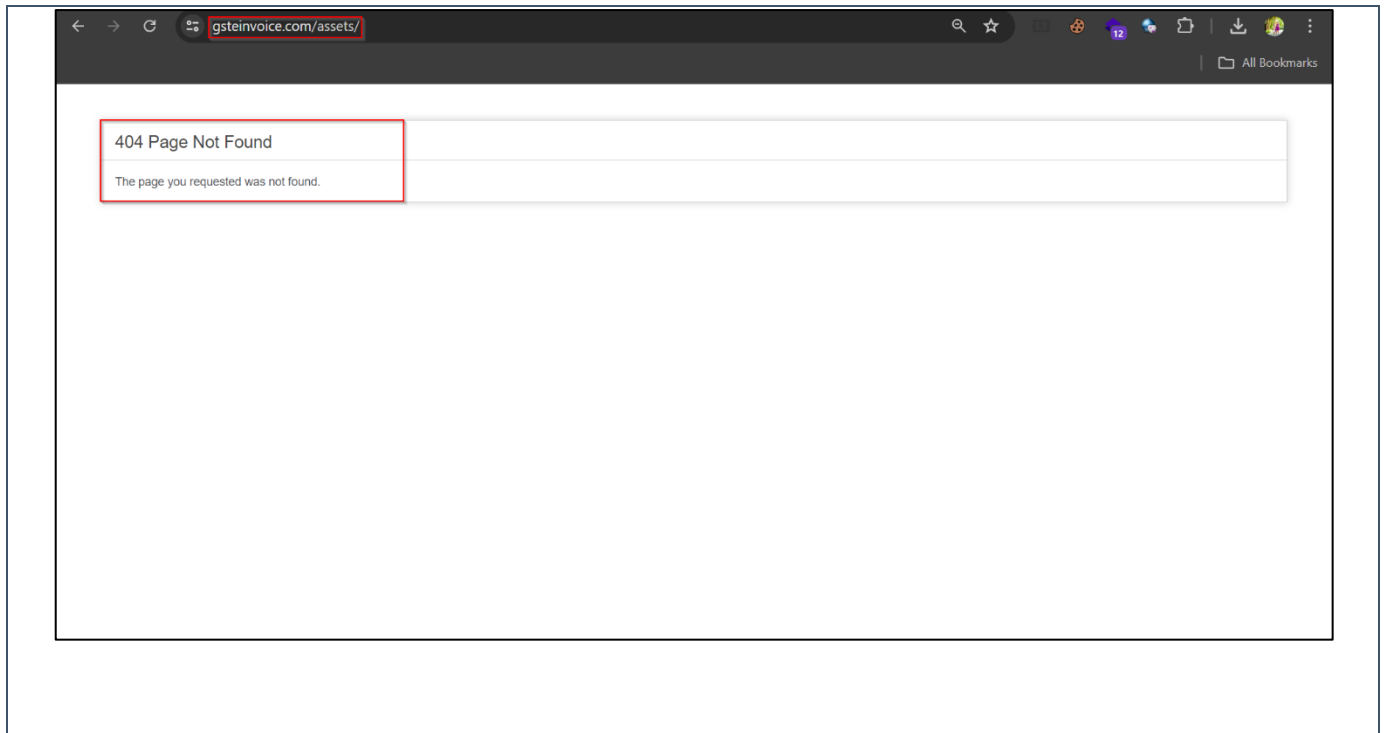
CLOSED

CLOSURE PROOF OF CONCEPT



09: Directory Listing	
SEVERITY	Medium
STATUS	CLOSED
CLOSURE PROOF OF CONCEPT	





10: Missing HTTP Strict Transport Security Header (HSTS)

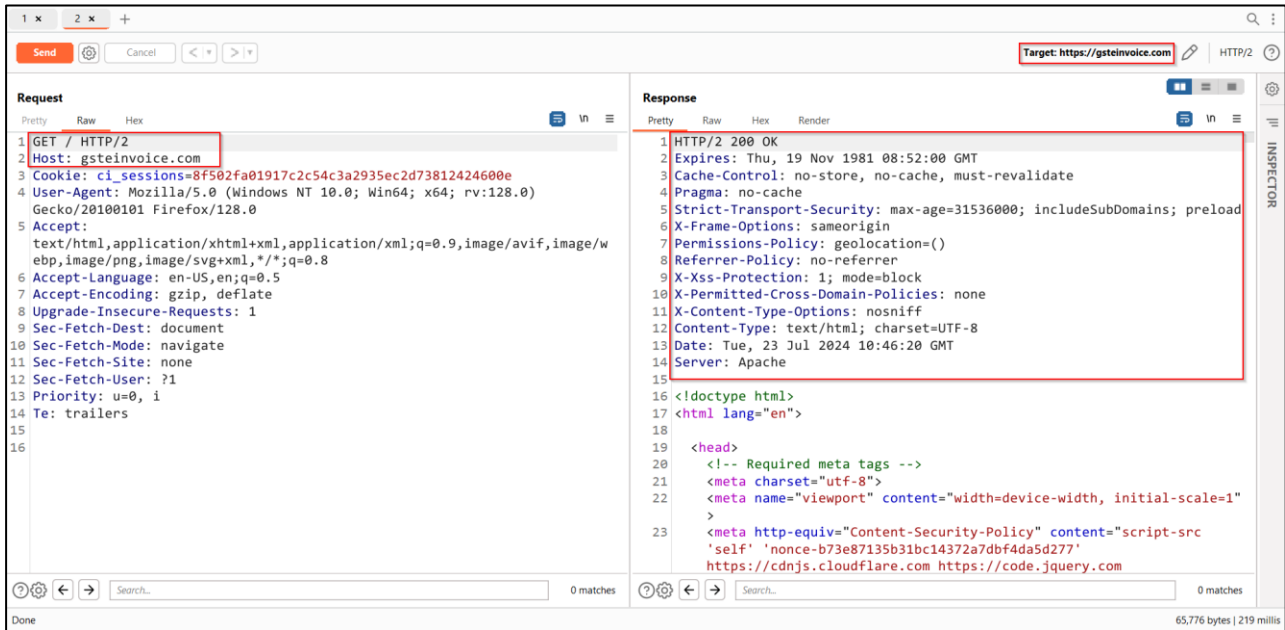
SEVERITY

Low

STATUS

CLOSED

CLOSURE PROOF OF CONCEPT



11: Missing X-Frame-Options Header

SEVERITY

Low

STATUS

CLOSED

CLOSURE PROOF OF CONCEPT

The screenshot displays the browser's developer tools with the 'Request' and 'Response' tabs selected. The 'Request' tab shows a GET request to `https://gstinvoice.com`. The 'Response' tab shows the server's response, which includes the following headers:

- `HTTP/2 200 OK`
- `Expires: Thu, 19 Nov 1981 08:52:00 GMT`
- `Cache-Control: no-store, no-cache, must-revalidate`
- `Pragma: no-cache`
- `Strict-Transport-Security: max-age=31536000; includeSubDomains; preload`
- `X-Frame-Options: sameorigin`
- `Permissions-Policy: geolocation=()`
- `Referrer-Policy: no-referrer`
- `X-Xss-Protection: 1; mode=block`
- `X-Permitted-Cross-Domain-Policies: none`
- `X-Content-Type-Options: nosniff`
- `Content-Type: text/html; charset=UTF-8`
- `Date: Tue, 23 Jul 2024 10:46:20 GMT`
- `Server: Apache`

The response body shows the HTML structure of the page, including meta tags and a script source. The 'X-Frame-Options: sameorigin' header is highlighted in red, indicating the missing X-Frame-Options header.

12: Missing X-Permitted-Cross-Domain-Policies Header

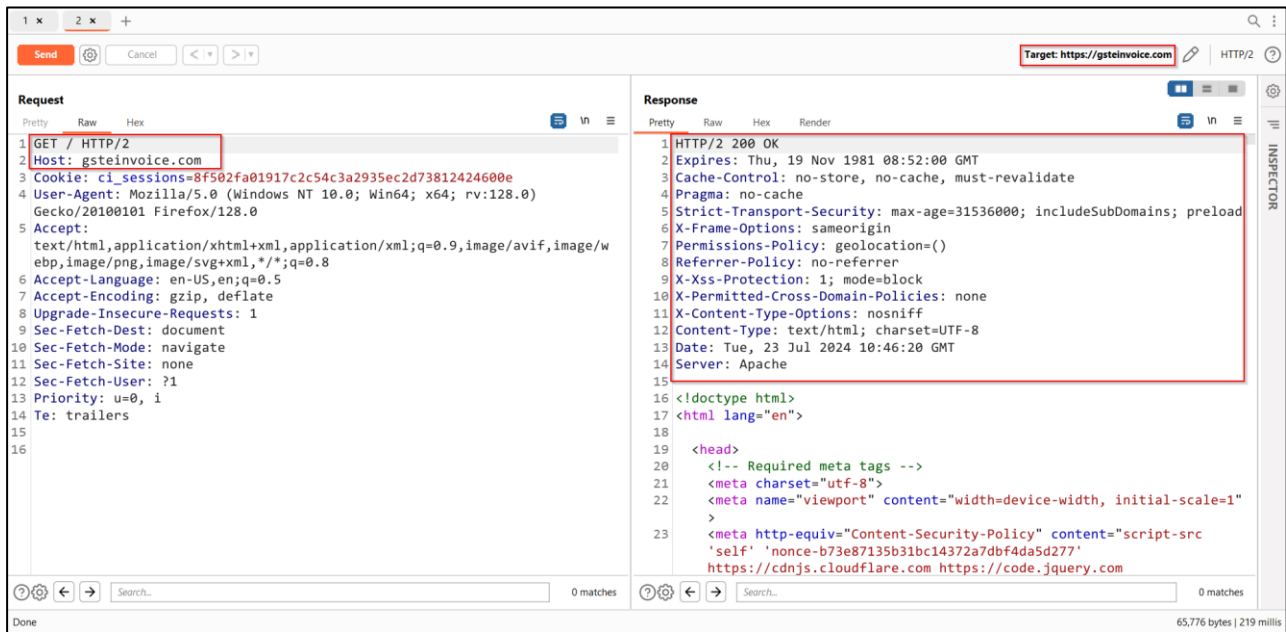
SEVERITY

Low

STATUS

CLOSED

CLOSURE PROOF OF CONCEPT



13: Missing Referrer-Policy Header

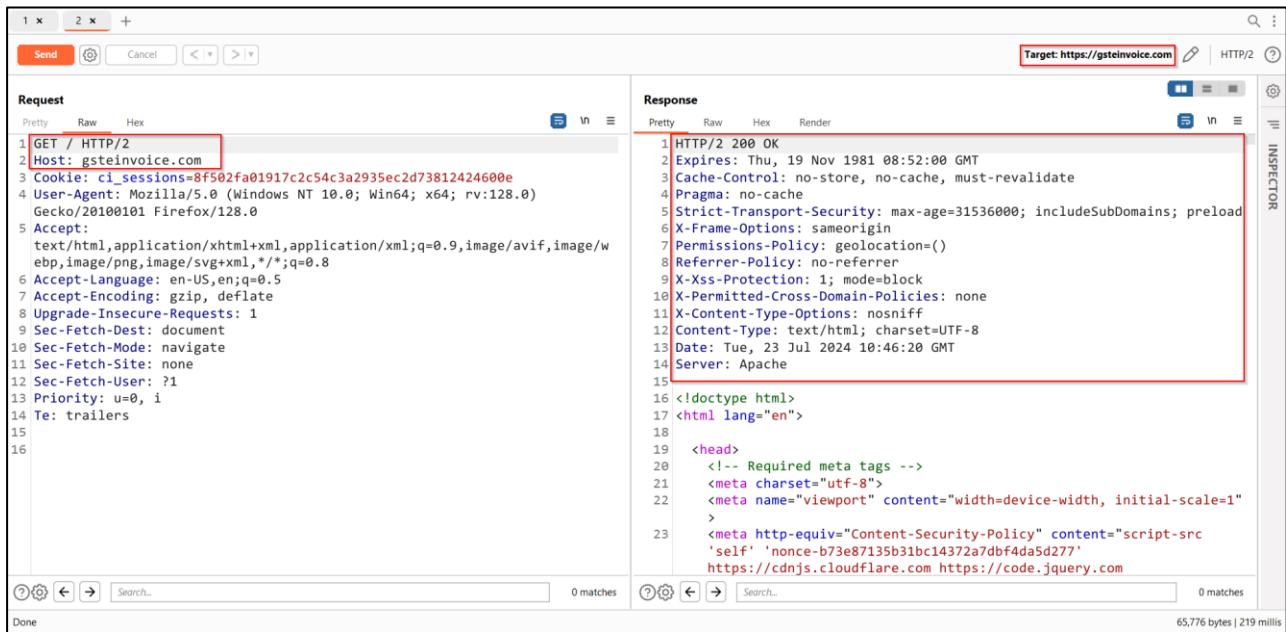
SEVERITY

Low

STATUS

CLOSED

CLOSURE PROOF OF CONCEPT



14: Missing Permissions-Policy Header

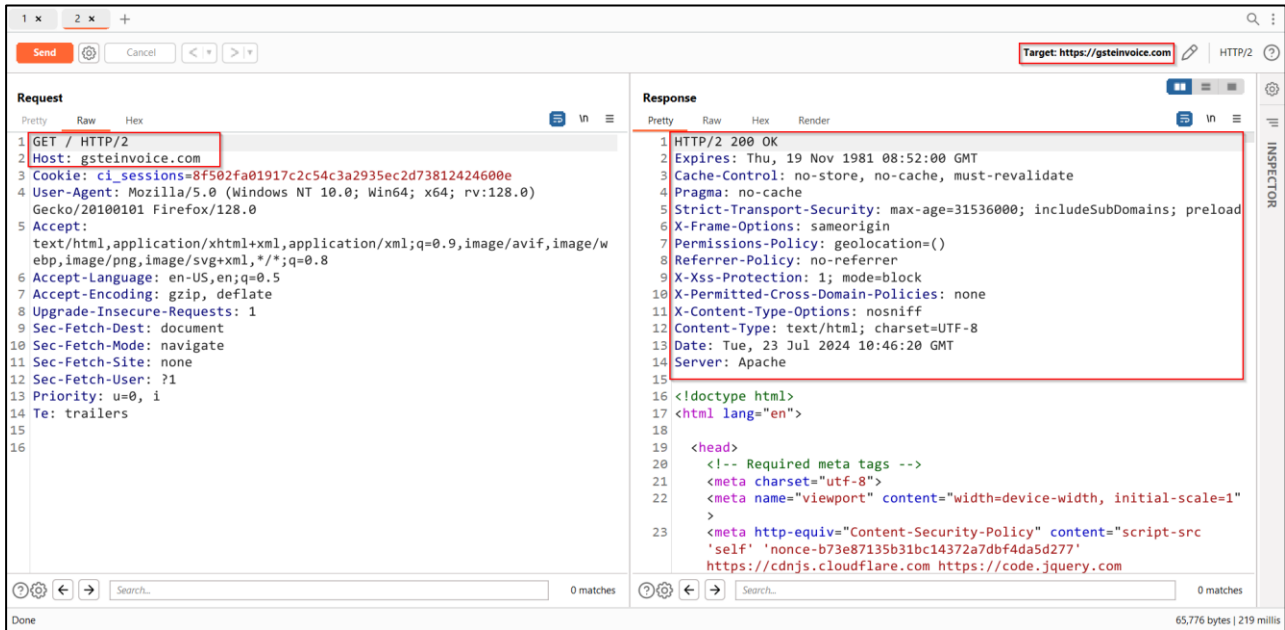
SEVERITY

Low

STATUS

CLOSED

CLOSURE PROOF OF CONCEPT



15: Missing Content Security Policy (CSP) Header

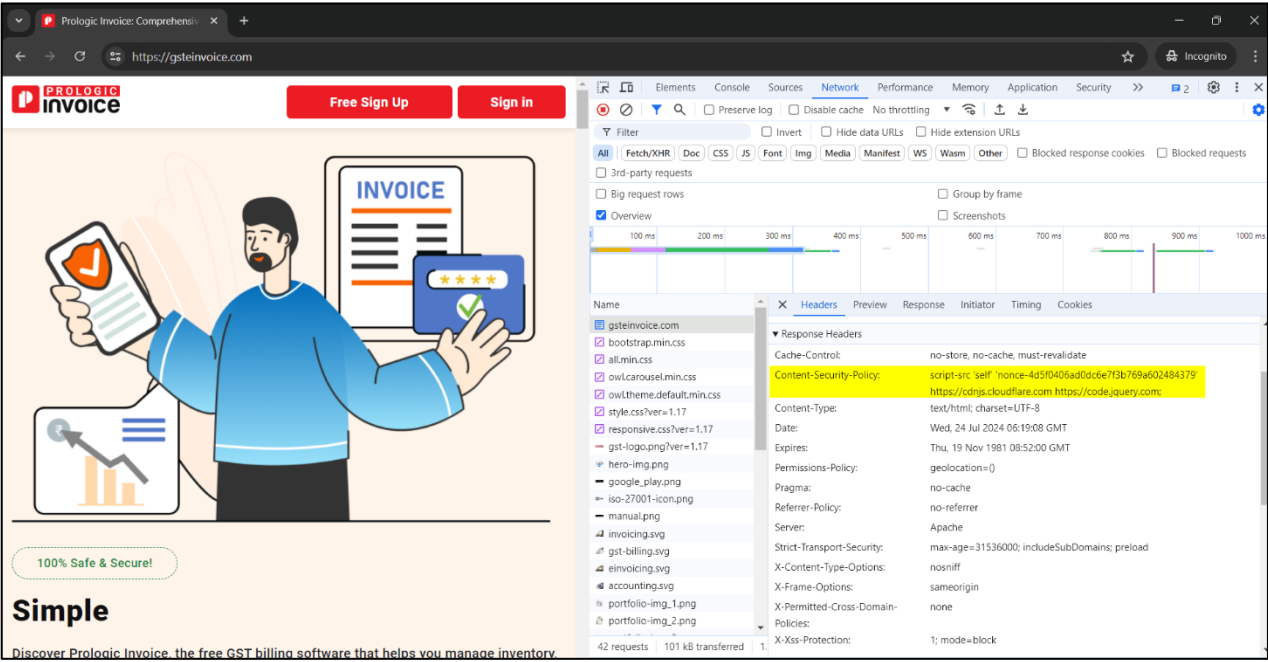
SEVERITY

Low

STATUS

CLOSED

CLOSURE PROOF OF CONCEPT



16: Missing X-Content-Type-Options Header

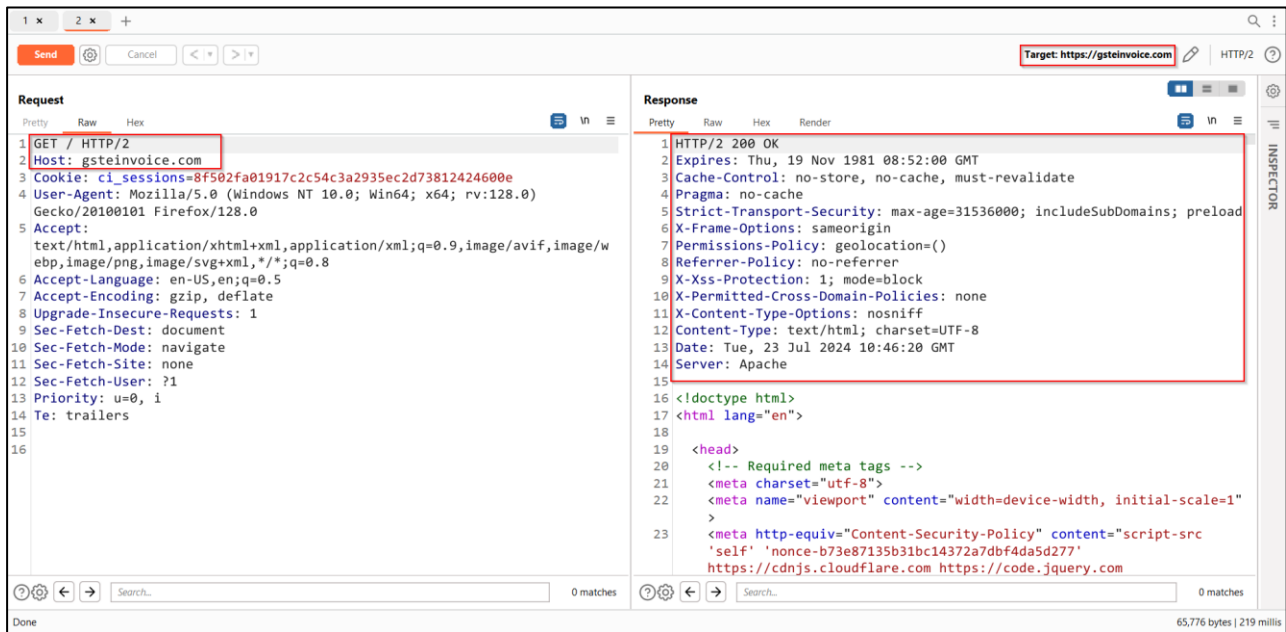
SEVERITY

Low

STATUS

CLOSED

CLOSURE PROOF OF CONCEPT



17: Missing X-XSS-Protection Header

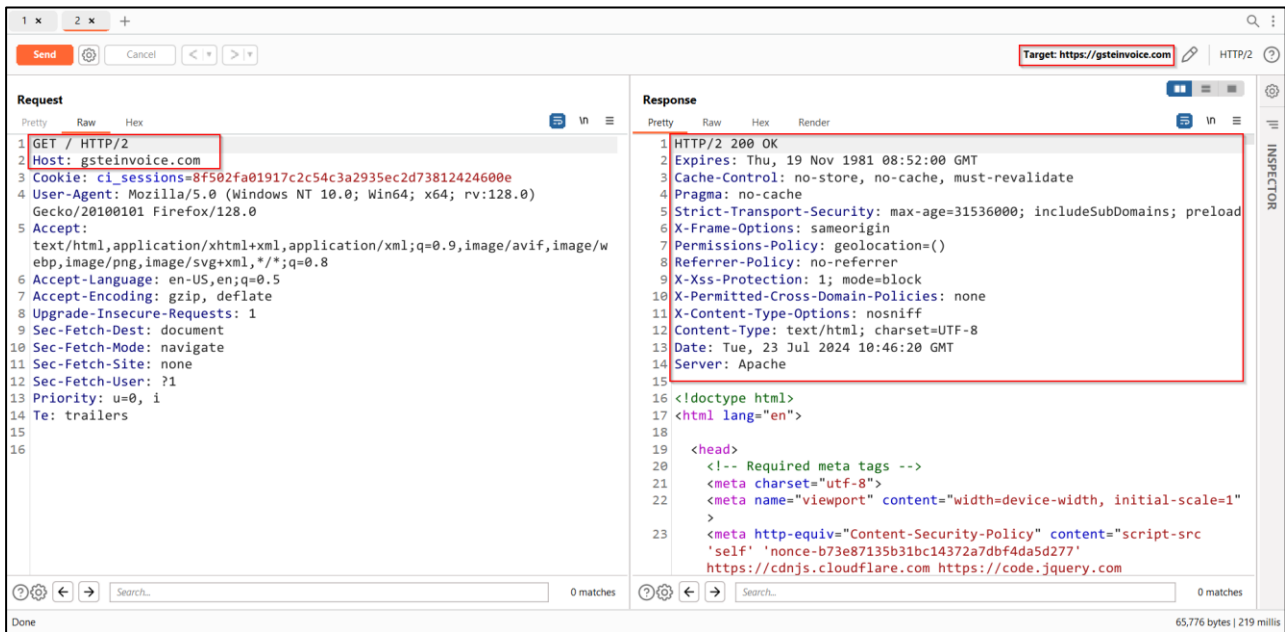
SEVERITY

Low

STATUS

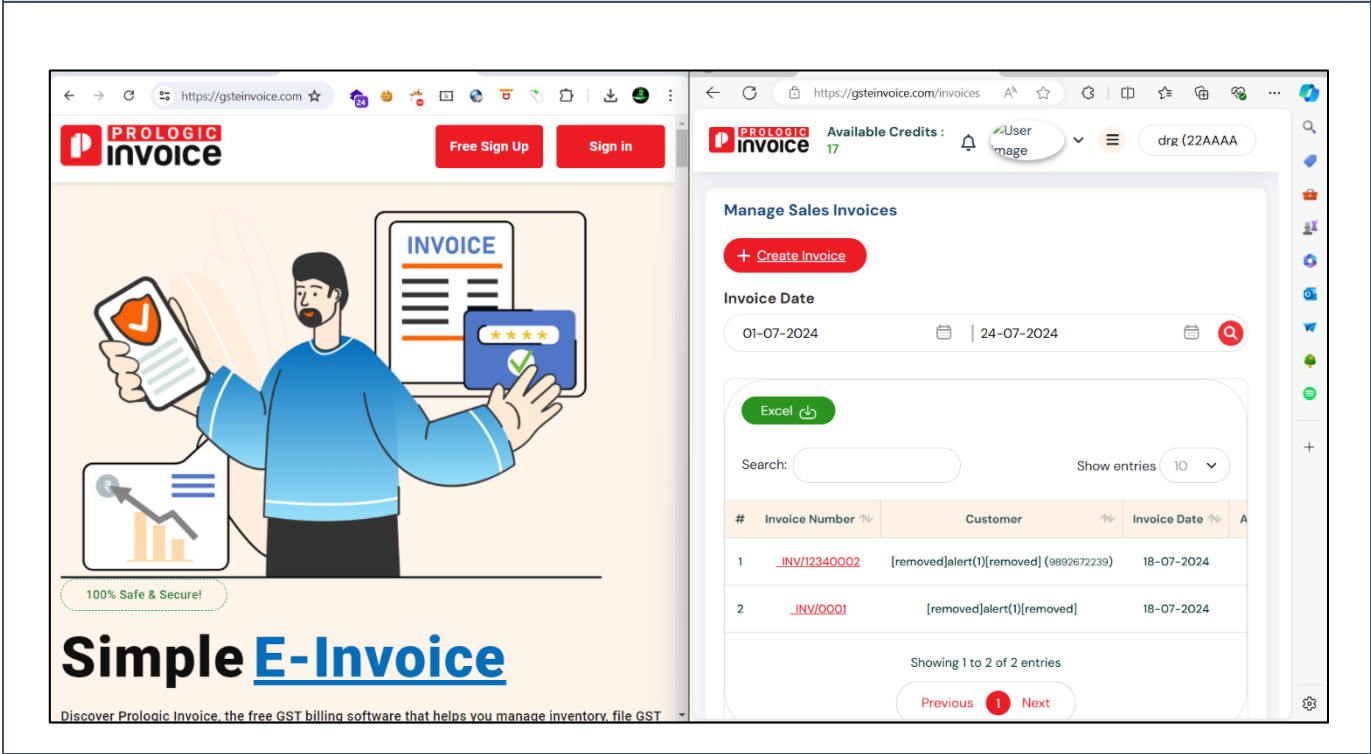
CLOSED

CLOSURE PROOF OF CONCEPT



18: Simultaneous Login Allowed

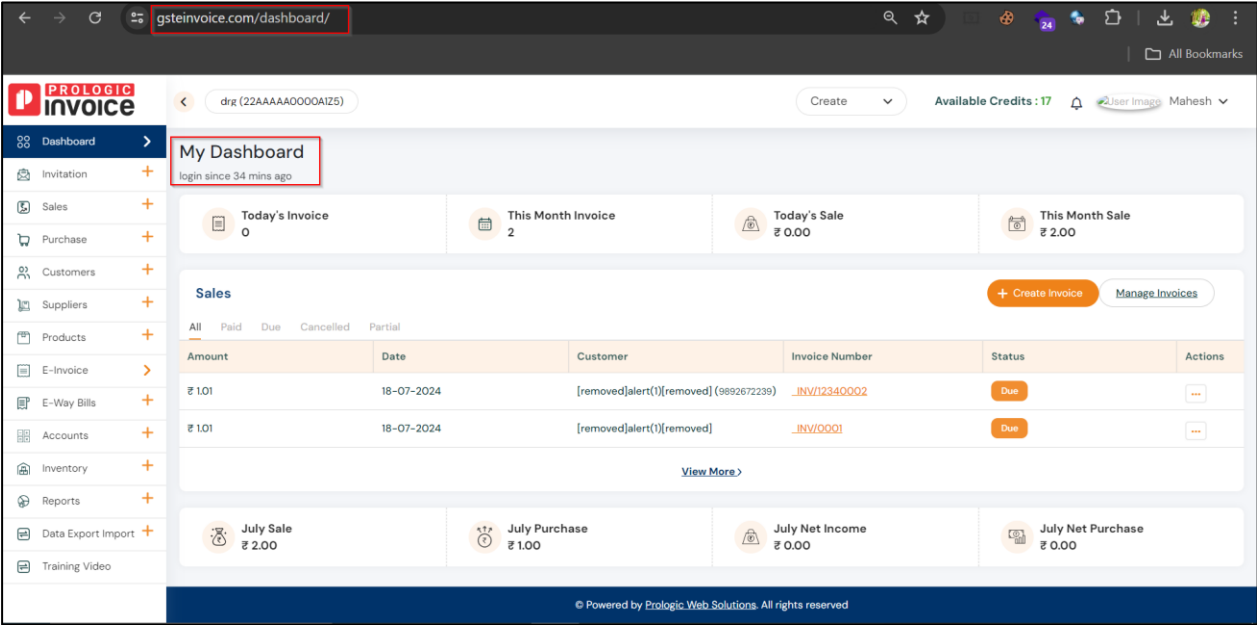
SEVERITY	Low
STATUS	CLOSED
CLOSURE PROOF OF CONCEPT	



19: Application does not display last login time and date

SEVERITY	Low
STATUS	CLOSED

CLOSURE PROOF OF CONCEPT



20: Auto Complete Enabled

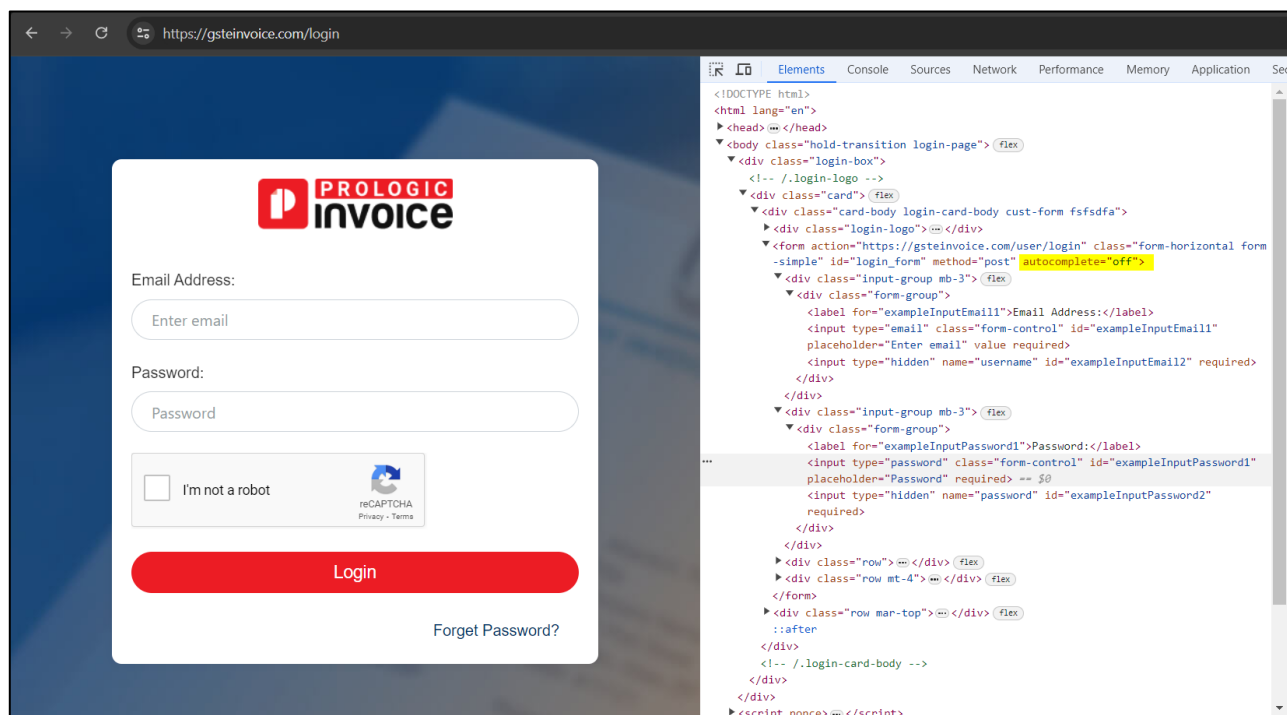
SEVERITY

Low

STATUS

CLOSED

PROOF OF CONCEPT



21: Vulnerable and Outdated Components

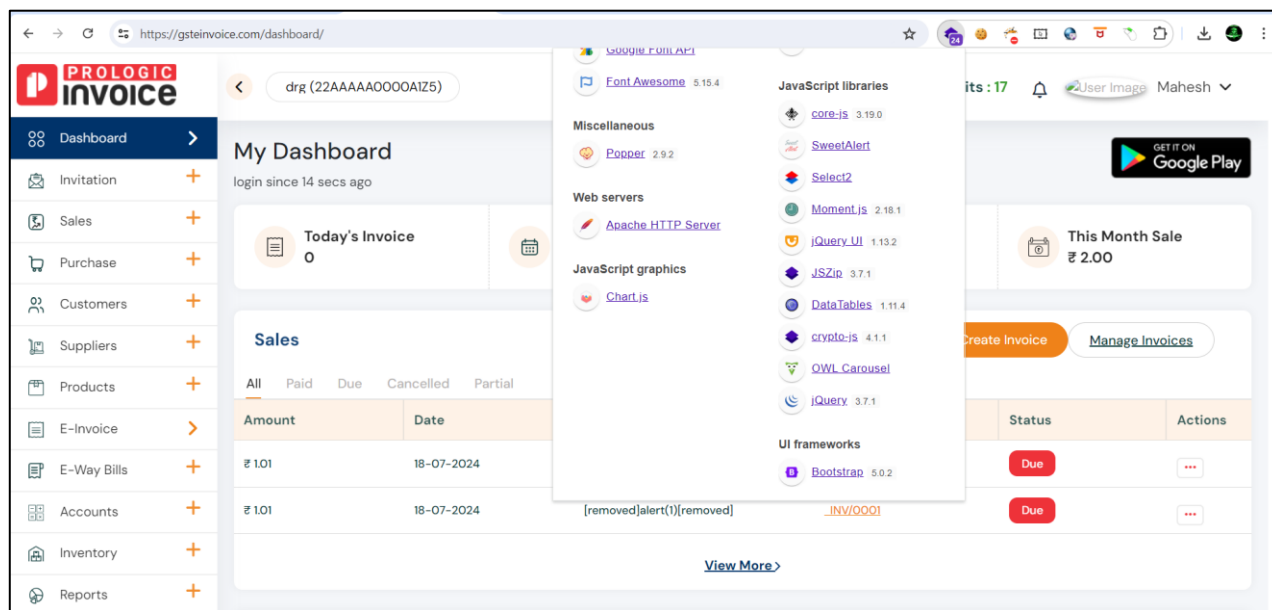
SEVERITY

Low

STATUS

CLOSED

CLOSURE PROOF OF CONCEPT



22: Session Cookie Secure Attribute Not Set

SEVERITY

LOW

STATUS

CLOSED

CLOSURE PROOF OF CONCEPT

The screenshot displays the Network tab of a web browser's developer tools. The target URL is <https://gstinvoice.com>. The request is a GET method. The response is an HTTP/2 200 OK. The 'Set-Cookie' header is highlighted, showing the cookie: `ci_sessions=2aa258f7f29184ac792666d6763042d2383c95e2; expires=Tue, 23-Jul-2024 12:50:16 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=Lax; HttpOnly:Secure`. The 'Secure' attribute is missing, which is the vulnerability being demonstrated.

```
Request
1 GET / HTTP/2
2 Host: gstinvoice.com
3 Cookie: ci_sessions=8f502fa01917c2c54c3a2935ec2d73812424600
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Priority: u=0, i
14 Te: trailers
15
16

Response
1 HTTP/2 200 OK
2 Expires: Thu, 19 Nov 1981 08:52:00 GMT
3 Cache-Control: no-store, no-cache, must-revalidate
4 Pragma: no-cache
5 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
6 Set-Cookie: ci_sessions=2aa258f7f29184ac792666d6763042d2383c95e2; expires=Tue, 23-Jul-2024 12:50:16 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=Lax; HttpOnly:Secure
7 X-Frame-Options: sameorigin
8 Permissions-Policy: geolocation=()
9 Referrer-Policy: no-referrer
10 X-Xss-Protection: 1; mode=block
11 X-Permitted-Cross-Domain-Policies: none
12 X-Content-Type-Options: nosniff
13 Content-Type: text/html; charset=UTF-8
14 Date: Tue, 23 Jul 2024 10:50:16 GMT
15 Server: Apache
16
17 <!doctype html>
18 <html lang="en">
19
20 <head>
21 <!-- Required meta tags -->
22 <meta charset="utf-8">
23 <meta name="viewport" content="width=device-width, initial-scale=1">
24 </head>
```

23: Unwanted HTTP Methods Enabled

SEVERITY

Low

STATUS

CLOSED

CLOSURE PROOF OF CONCEPT

Attack Save Columns 3. Intruder attack of <https://gteinvoice.com> Temporary attack - Not saved to project file

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			65776	
1	GET	200			65776	
2	POST	200			65776	
3	HEAD	200			495	
4	CONNECT		<input checked="" type="checkbox"/>			
5	PUT	403			65783	
6	TRACE	405			65792	
7	OPTIONS	403			65783	
8	DELETE	403			65950	
9	ACL	403			65783	
10	ARBITRARY	403			65783	
11	BASELINE-CONTROL	403			65783	
12	BCOPY	403			65783	
13	BDELETE	403			65783	
14	BIND	403			65783	
15	BMOVE	403			65783	
16	BPROPFIND	403			65783	
17	BPROPPATCH	403			65783	

Request Response

Pretty Raw Hex Render

```
1 HTTP/2 403 Forbidden
2 Expires: Thu, 19 Nov 1981 08:52:00 GMT
3 Cache-Control: no-store, no-cache, must-revalidate
4 Pragma: no-cache
5 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
6 X-Frame-Options: sameorigin
7 Permissions-Policy: geolocation=()
8 Referrer-Policy: no-referrer
9 X-Xss-Protection: 1; mode=block
10 X-Permitted-Cross-Domain-Policies: none
11 X-Content-Type-Options: nosniff
```

Finished

Attack Save Columns 3. Intruder attack of <https://gteinvoice.com> Temporary attack - Not saved to project file

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
18	CHECKIN	403			65783	
19	CHECKOUT	403			65783	
20	COPY	403			65783	
21	DEBUG	403			65783	
22	INDEX	403			65783	
23	LABEL	403			65783	
24	LINK	403			65783	
25	LOCK	403			65783	
26	MERGE	403			65778	
27	MKACTIVITY	403			65783	
28	MKCALENDAR	403			65783	
29	MKCOL	403			65783	
30	MKREDIRECTREF	403			65778	
31	MKWORKSPACE	403			65783	
32	MOVE	403			65783	
33	NOTIFY	403			65783	
34	ORDERPATCH	403			65783	
35	PATCH	403			65783	

Request Response

Pretty Raw Hex Render

```
1 HTTP/2 403 Forbidden
2 Expires: Thu, 19 Nov 1981 08:52:00 GMT
3 Cache-Control: no-store, no-cache, must-revalidate
4 Pragma: no-cache
5 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
6 X-Frame-Options: sameorigin
7 Permissions-Policy: geolocation=()
8 Referrer-Policy: no-referrer
9 X-Xss-Protection: 1; mode=block
10 X-Permitted-Cross-Domain-Policies: none
11 X-Content-Type-Options: nosniff
```

Finished

Prologic Web Solution Private Limited - Prologic E Invoice Web Application VAPT Final Report

Attack Save Columns 3. Intruder attack on <https://gstinvoice.com> Temporary attack - Not saved to project file

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
37	PROPFIND	403			65783	
38	PROPPATCH	403			65783	
39	REBIND	403			65783	
40	REPORT	403			65783	
41	RPC_IN_DATA	403			65783	
42	RPC_OUT_DATA	403			65783	
43	SEARCH	403			65783	
44	SUBSCRIBE	403			65783	
45	TRACK	403			65783	
46	UNBIND	403			65783	
47	UNCHECKOUT	403			65783	
48	UNLINK	403			65783	
49	UNLOCK	403			65783	
50	UNSUBSCRIBE	403			65783	
51	UPDATE	403			65783	
52	UPDATEDIRECTREF	403			65783	
53	VERSION-CONTROL	403			65783	
54	X-MS-ENUMATTS	403			65778	

Request Response

Pretty Raw Hex Render

```
1 HTTP/2 403 Forbidden
2 Expires: Thu, 19 Nov 1981 08:52:00 GMT
3 Cache-Control: no-store, no-cache, must-revalidate
4 Pragma: no-cache
5 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
6 X-Frame-Options: sameorigin
7 Permissions-Policy: geolocation=()
8 Referrer-Policy: no-referrer
9 X-Xss-Protection: 1; mode=block
10 X-Permitted-Cross-Domain-Policies: none
11 X-Content-Type-Options: nosniff
```

0 matches

Finished

Attack Save Columns 3. Intruder attack on <https://gstinvoice.com> Temporary attack - Not saved to project file

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
32	MOVE	403			65783	
33	NOTIFY	403			65783	
34	ORDERPATCH	403			65783	
35	PATCH	403			65783	
36	POLL	403			65783	
37	PROPFIND	403			65783	
38	PROPPATCH	403			65783	
39	REBIND	403			65783	
40	REPORT	403			65783	
41	RPC_IN_DATA	403			65783	
42	RPC_OUT_DATA	403			65783	
43	SEARCH	403			65783	
44	SUBSCRIBE	403			65783	
45	TRACK	403			65783	
46	UNBIND	403			65783	
47	UNCHECKOUT	403			65783	
48	UNLINK	403			65783	
49	UNLOCK	403			65783	

Request Response

Pretty Raw Hex Render

```
1 HTTP/2 403 Forbidden
2 Expires: Thu, 19 Nov 1981 08:52:00 GMT
3 Cache-Control: no-store, no-cache, must-revalidate
4 Pragma: no-cache
5 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
6 X-Frame-Options: sameorigin
7 Permissions-Policy: geolocation=()
8 Referrer-Policy: no-referrer
9 X-Xss-Protection: 1; mode=block
10 X-Permitted-Cross-Domain-Policies: none
11 X-Content-Type-Options: nosniff
```

0 matches

Finished

24: Session Timeout is High or Not Implemented

SEVERITY

Low

STATUS

CLOSED

CLOSURE PROOF OF CONCEPT

The screenshot shows the Prologic Invoice dashboard. The browser address bar displays 'gstinvoice.com/dashboard/'. The dashboard header includes the Prologic Invoice logo, a user profile dropdown for 'Mahesh', and 'Available Credits : 18'. The main content area is titled 'My Dashboard' and shows 'login since 0 sec ago'. It features four summary cards: 'Today's Invoice' (0), 'This Month Invoice' (2), 'Today's Sale' (₹ 0.00), and 'This Month Sale' (₹ 2.00). Below these is a 'Sales' section with a table of invoices. The table has columns for Amount, Date, Customer, Invoice Number, Status, and Actions. Two invoices are listed, both with a status of 'Due'. The Windows taskbar at the bottom shows the time as 04:40 PM on 23-07-2024.

The screenshot shows the Prologic Invoice landing page. The browser address bar displays 'gstinvoice.com'. The page features the Prologic Invoice logo, 'Free Sign Up' and 'Sign in' buttons, and a large illustration of a man holding a smartphone and a tablet. The text on the page reads: '100% Safe & Secure!', 'Simple InvoiceBill', 'Discover Prologic Invoice, the free GST billing software that helps you manage inventory, file GST returns, and create professional invoices. Track sales, purchases, and estimates in real-time, with E-Way Bill and E-Invoice features.', and 'Sign Up for Free'. At the bottom, it says 'Trusted by 10,000+ SMEs'. The Windows taskbar at the bottom shows the time as 05:26 PM on 23-07-2024.

16. Checklist (Test Cases Performed)

Sr. No.	Vulnerability Name	Vulnerable (Yes/No)
1	Account Lockout Policy Not Implemented	No
2	An application sent Sensitive data in URL (GET)	No
3	Anti-CSRF Token Missing	No
4	Application Accepts Arbitrary Methods	No
5	Application does not display Last Login Date and Time	No
6	Application is accessible by IP address	No
7	Application is Vulnerable to BEAST Attack	No
8	Application is Vulnerable to BREACH Attack	No
9	Application is Vulnerable to LOGJAM Attack	No
10	Application is Vulnerable to LUCKY13 Attack	No
11	Application is vulnerable to Non-HTML page accessible	No
12	Application is Vulnerable to POODLE Attack	No
13	Application is Vulnerable to RC4 Attack	No
14	Application is Vulnerable to ROBOT Attack	No
15	Application is Vulnerable to Secure Renegotiation	No
16	Application is Vulnerable to SWEET32 Attack	No
17	Application is Vulnerable to TLS_FALLBACK_SCSV Attack	No
18	ASP.NET Debugging Enabled	No
19	Authentication Bypass (Blind SQL Injection)	No
20	Authentication Bypass by Response Manipulation	No
21	Auto-Complete Enabled	No
22	Back Button Policy Enabled (Browser Back Refresh Attack)	No
23	Banner Grabbing	No
24	Broken Access Control (Improper Authorization)	No
25	Broken Authentication (Forced Browsing)	No
26	Broken Authentication (Improper Session Management)	No
27	Broken Links	No
28	Buffer Overflow	No
29	Business Logic Error (Business Logic Flaw)	No
30	CAPTCHA Bypass	No
31	Click-Jacking Attack	No
32	Content Spooking Attack	No
33	CORS Misconfiguration	No
34	Credentials Transmitted to Server in Plain Text	No
35	Cross Site Scripting (XSS)	No
36	CSRF (Cross-Site Request Forgery)	No
37	Database Dump using sqlmap	No
38	Database is Unencrypted	No
39	Default Credentials been Used	No
40	Directory Listing	No
41	Directory Traversal	No
42	Documentation File Found	No
43	Email Harvesting	No
44	File Upload - Content-Type Restriction Bypass	No

45	File Upload - Double Extension File Upload Vulnerability	No
46	File Upload - Magic Number File Upload	No
47	File Upload - Malicious File Upload	No
48	File Upload - No Size Restriction	No
49	File Upload - Null Byte Extension	No
50	File Upload - Unrestricted File Upload	No
51	Functionality Issue	No
52	Hardcoded Secret	No
53	HTTP Parameter Pollution	No
54	HTTP Request Smuggling	No
55	IDOR	No
56	Improper Error Handling	No
57	Improper Input Validation	No
58	Information Disclosure	No
59	Information Disclosure (Hardcoded Version)	No
60	Information Exposure through Query Strings in URL	No
61	Injection - CSS Injection	No
62	Injection - CSV Injection	No
63	Injection - Host Header Injection	No
64	Injection - HTML Injection	No
65	Injection - iFrame Injection	No
66	Injection - Link Injection	No
67	Injection - OS Command Injection	No
68	Injection - Server-side Template Injection (SSTI)	No
69	Injection - XML Injection	No
70	Insecure Change Password Functionality	No
71	Insecure Communication (SSL is Not Implemented)	No
72	Internal Full Path Disclosure	No
73	Internal IP Disclosure	No
74	Local File Inclusion (LFI)	No
75	Method Interchange Attack (POST to GET)	No
76	Missing Cache-Control Header	No
77	Missing Content Security Policy (CSP) Header	No
78	Missing Expires Header	No
79	Missing HTTP Strict-Transport-Security (HSTS) Header	No
80	Missing Permissions-Policy Header	No
81	Missing Pragma Header	No
82	Missing Referrer-Policy Header	No
83	Missing X-Content-Type-Options Header	No
84	Missing X-Frame-Options Header	No
85	Missing X-Permitted-Cross-Domain-Policies	No
86	Missing X-XSS-Protection Header	No
87	OTP can be Brute Force	No
88	Out-Of-Date Component Version	No
89	Parameter Tampering	No
90	Password Revealed in Response	No
91	Possible Brute Force Attack – CAPTCHA Not Found	No
92	Privilege Escalation	No

93	Race Condition	No
94	Rate Limit is Not Implemented	No
95	Remote Code Execution (RCE)	No
96	Remote File Inclusion (RFI)	No
97	Second Factor Authentication (2FA) Not Implemented	No
98	Security Misconfiguration	No
99	Sensitive Files Disclosure	No
100	Sensitive Information Disclosed in Response	No
101	Sensitive Page Disclosure	No
102	Server Returns 403 Forbidden Response or Error	No
103	Server-Side Validations are not in Place	No
104	Session Cookie HttpOnly Attribute Not Set	No
105	Session Cookie SameSite Attribute Not Set	No
106	Session Cookie Secure Attribute Not Set	No
107	Session Fixation	No
108	Session ID remains constant before login and after logout	No
109	Session Timeout is High or Not Implemented	No
110	Simultaneous Login Enabled (Concurrent Login Allowed)	No
111	SQL Injection (Boolean-based Blind SQL Injection)	No
112	SQL Injection (Error Based SQL Injection)	No
113	SQL Injection (Time-based Blind SQL Injection)	No
114	SQL Injection (Union Based SQL Injection)	No
115	SQL Wildcard Attack	No
116	SSL Version 2.0 Protocol Detection	No
117	SSL Version 3.0 Protocol Detection	No
118	SSRF	No
119	Stack Trace Error	No
120	Test Script Page Available on Server	No
121	TLS Version 1.0 Protocol Detection	No
122	TLS Version 1.1 Protocol Detection	No
123	Unrestricted Field Length	No
124	Unwanted HTTP Methods Enabled	No
125	User can set New Password as Old Password	No
126	User Enumeration	No
127	Version Disclosure	No
128	Vulnerable Component Used	No
129	Weak Ciphers Enabled	No
130	Weak Encoding is Used	No
131	Weak Password Policy	No
132	XML External Entity (XXE)	No
133	XMLRPC.php File Found	No

Table 4

17. General References

Application Security Standard –

<https://owasp.org/Top10/>

<https://www.sans.org/top25-software-errors/>

<https://cert-in.org.in/>

Hardening of Servers –

<https://geekflare.com/apache-web-server-hardening-security/>

<https://geekflare.com/apache-tomcat-hardening-and-security-guide/>

<https://geekflare.com/nginx-webserver-security-hardening-guide/>

<https://geekflare.com/ibm-http-server-security-guide/>

18. Appendices

Table 1: SEVERITY LEVEL INFORMATION AND DESCRIPTION (CVSS SCORE)

Table 2: OWASP TOP 10 AND SANS CWE TOP 25

Table 3: VULNERABILITY SUMMARY KEY FINDINGS

Table 4: CHECKLIST (TEST CASES SUMMARY)

Figure 1: ASSESSMENT APPROACH

Figure 2: RISK LEVEL INFORMATION AND NECESSARY ACTIONS

Figure 3: GRAPHICAL REPRESENTATION OF VULNERABILITY SUMMARY

THE END OF DOCUMENT