Purvashare E-voting Website POC Document

1. Email Spoofing

Affected URL: https://uat-evoting.purvashare.com/

It is observed that emails originating from the domain (e.g., evoting@purvashare.com) can be spoofed due to the absence or misconfiguration of email authentication controls. During testing, the domain's DMARC policy was found to be missing or not enforced, and a spoofed email was successfully sent impersonating the same email address to a user without being rejected or flagged. This indicates that necessary protections such as DMARC, and potentially SPF and DKIM, are not properly implemented, allowing unauthorized parties to send emails that appear to originate from the legitimate domain.

Step I: Identify and copy the target email address (e.g., scrutinizer email) used by the application.
Step II: Verify the DMARC configuration for the target domain using online tools or DNS lookup.
Step III: Observe that the domain does not have a properly configured DMARC policy.
Step IV: Using an email spoofing tool, send a spoofed email using the target domain as the sender address.(Refer to Fig. 2.1 to 2.4)

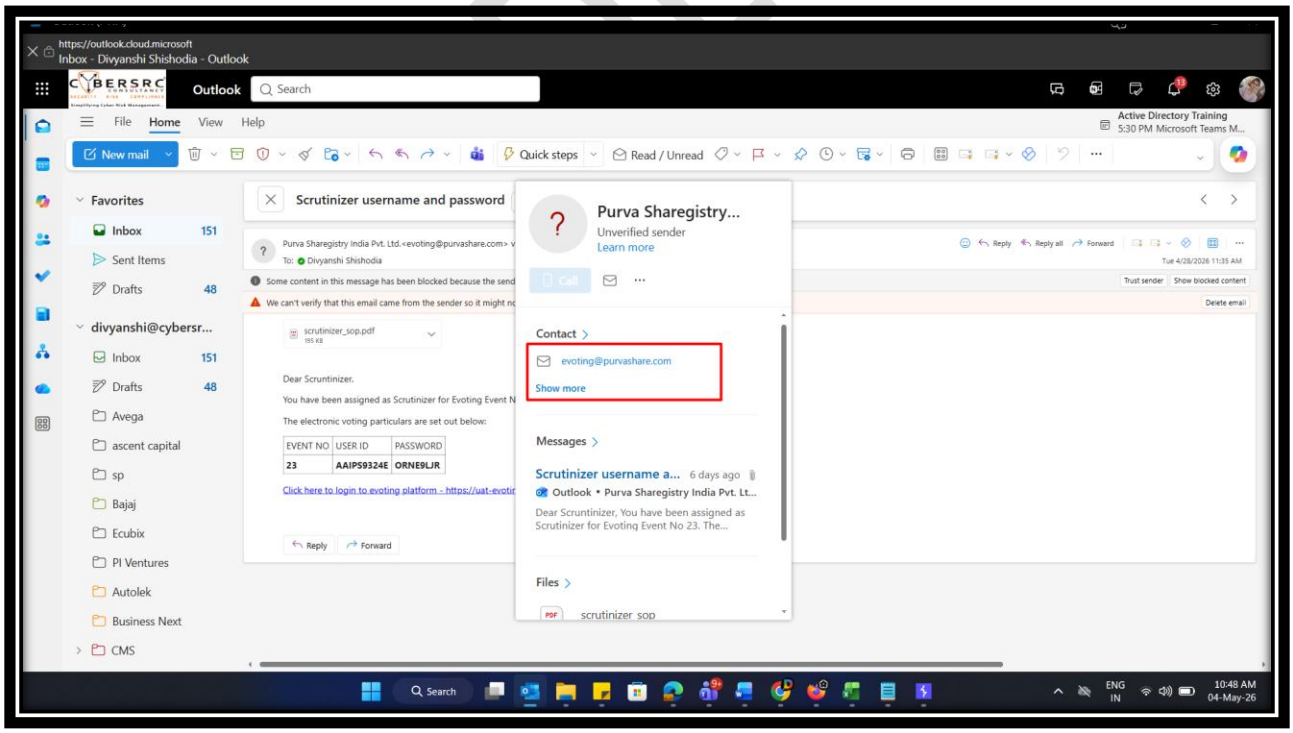


Fig. 1.1

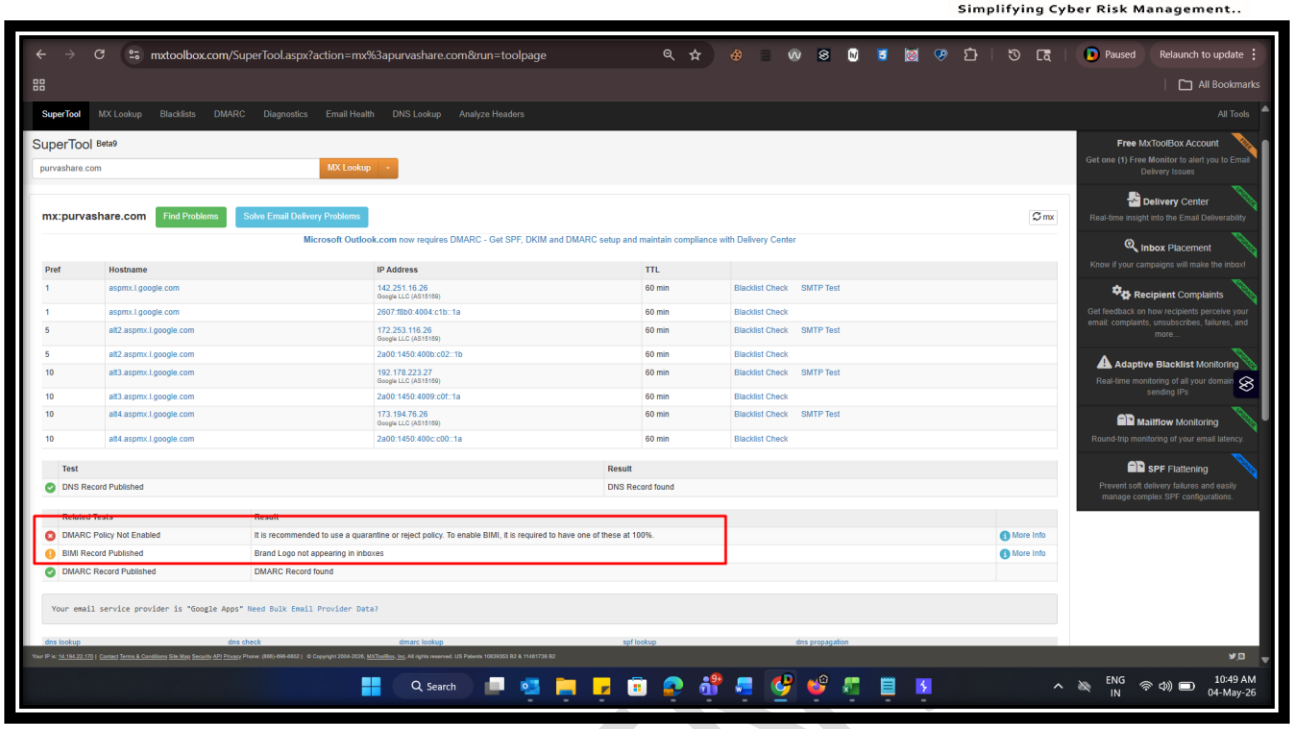

mxtoolbox.com/SuperTool.aspx?action=mx%3apurvashare.com&run=toolpage
SuperTool Beta9
purvashare.com
MX Lookup
mx:purvashare.com
Find Problems
Solve Email Delivery Problems
Microsoft Outlook.com now requires DMARC - Get SPF, DKIM and DMARC setup and maintain compliance with Delivery Center
DMARC Policy Not Enabled
It is recommended to use a quarantine or reject policy. To enable BIMI, it is required to have one of these at 100%.
BIMI Record Published
Brand Logo not appearing in inboxes
DMARC Record Published
DMARC Record found
Your email service provider is "Google Apps"

Fig. 1.2

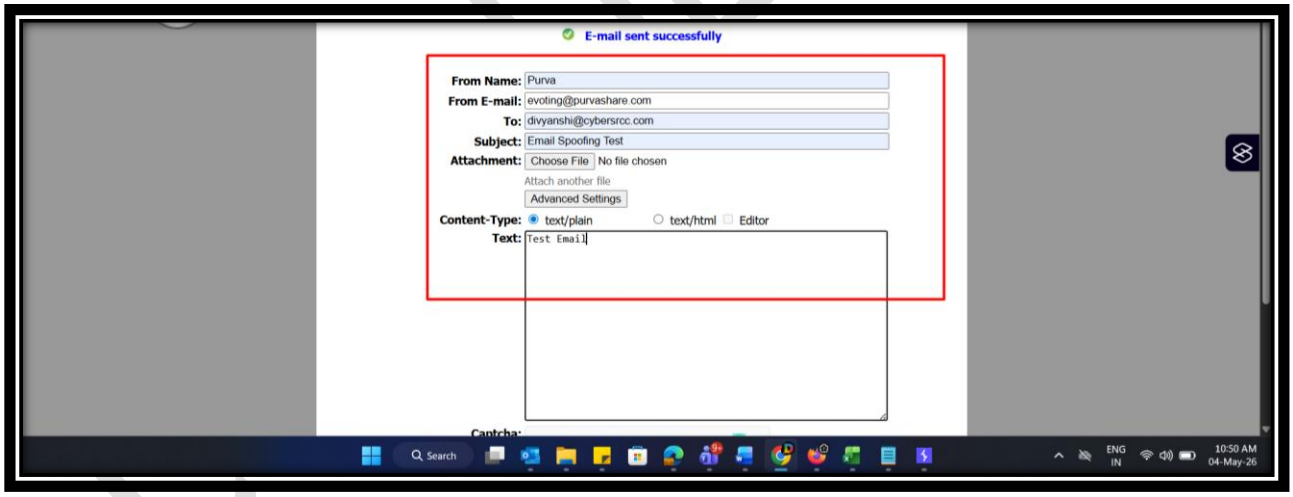

E-mail sent successfully
From Name: Purva
From E-mail: evoting@purvashare.com
To: divyanshi@cybersrcc.com
Subject: Email Spoofing Test
Attachment: Choose File No file chosen
Attach another file
Advanced Settings
Content-Type: text/plain text/html Editor
Text: Test Email
Captcha:

Fig. 1.3

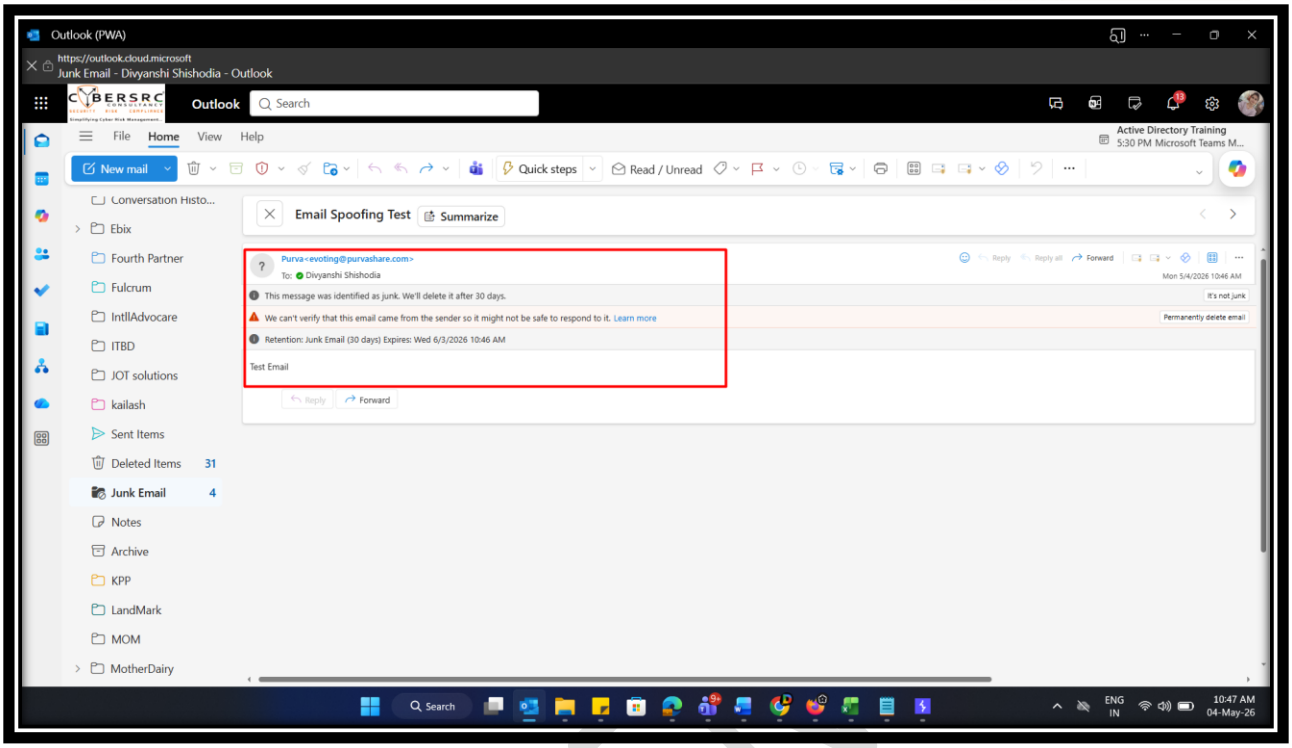
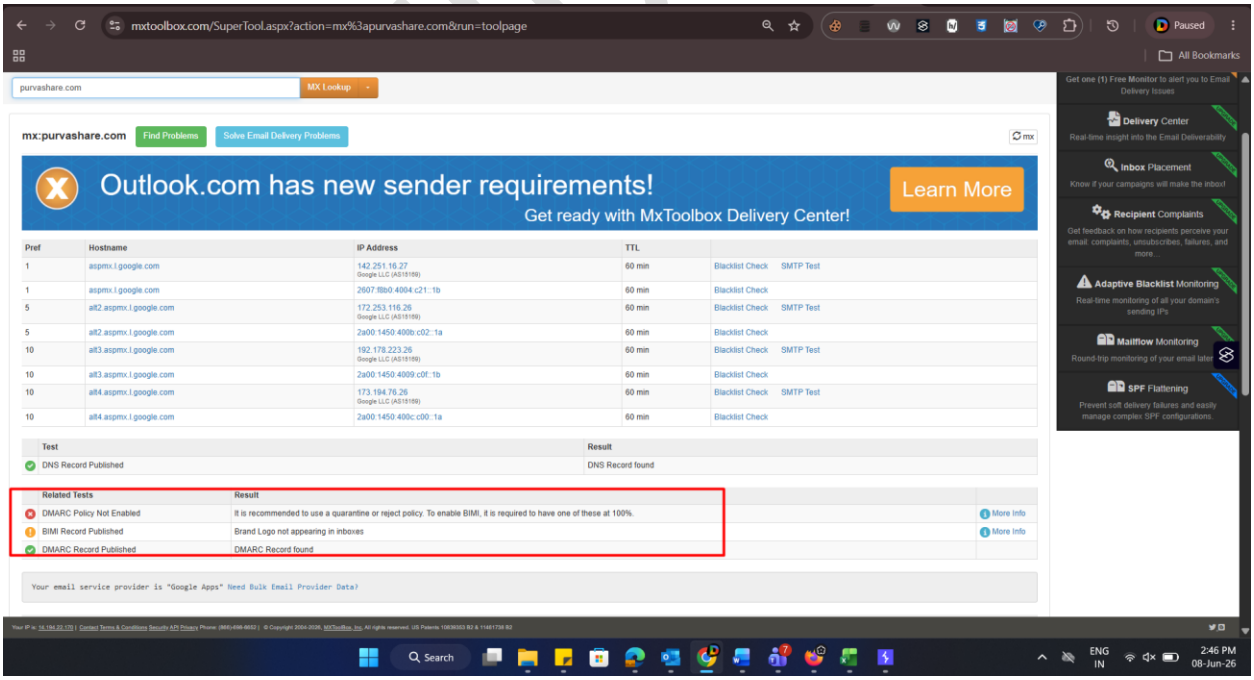


Fig. 1.4

Status: Open



2. No Rate Limit

Affected URL: https://uat-evoting.purvashare.com/accounts/forgot-password

It is observed that the application does not implement rate limiting on the OTP verification functionality. Multiple invalid OTP requests can be sent continuously using automated tools such as Burp Suite Intruder, and upon submitting a valid OTP in a subsequent request, the application accepts the OTP and redirects the user to the password reset screen without restricting the number of attempts.

Step I: Capture the OTP verification request and send multiple invalid OTP values using an automated tool (e.g., Burp Suite Intruder).
Step II: Submit the valid OTP among the requests and observe that the application accepts it without enforcing any rate limiting or account lockout, resulting in successful access to the password reset screen.

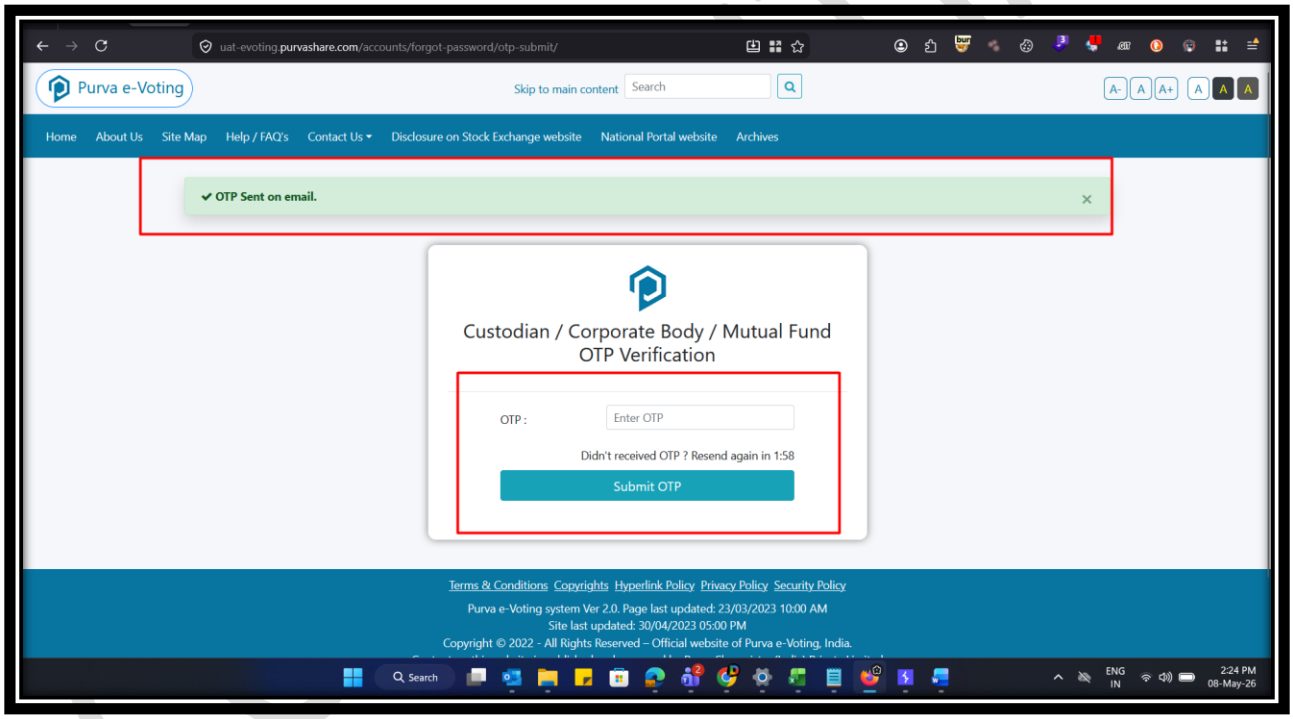


Fig. 2.1

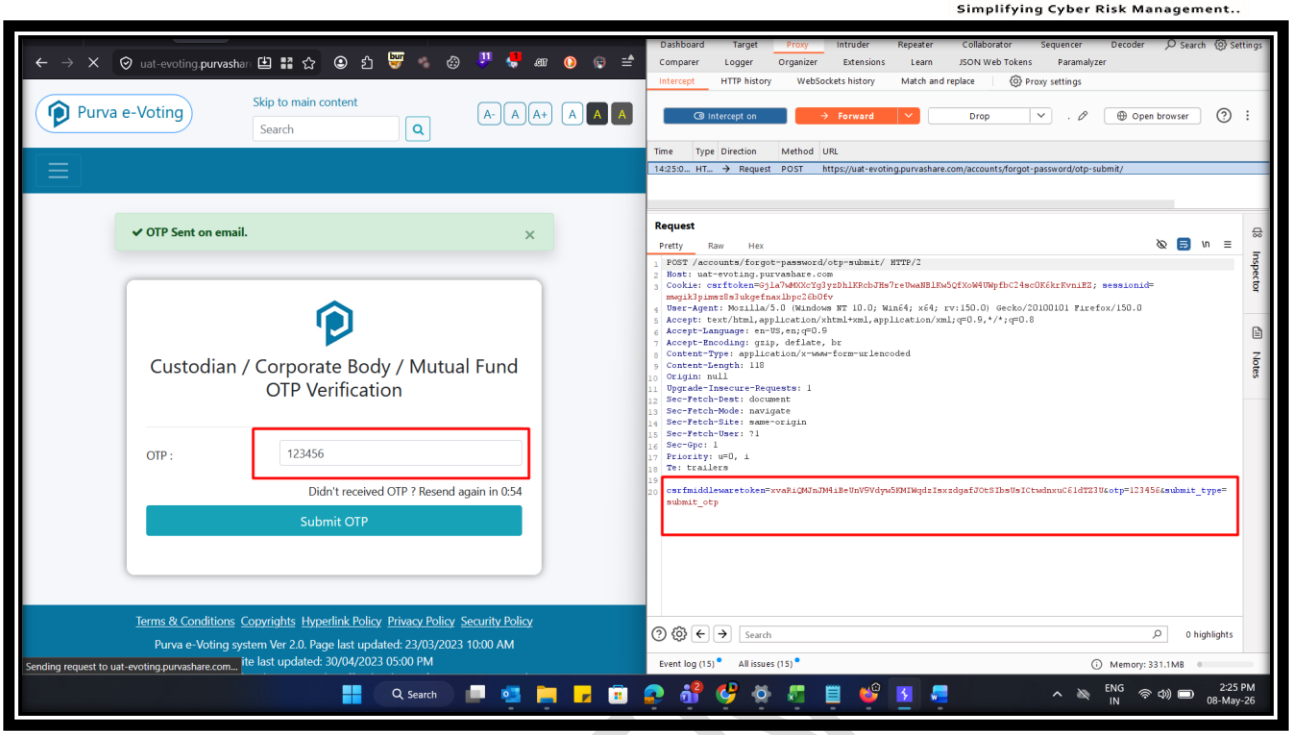

Purva e-Voting
Skip to main content
Search
OTP Sent on email.
Custodian / Corporate Body / Mutual Fund
OTP Verification
OTP :
123456
Didn't received OTP ? Resend again in 0:54
Submit OTP
Terms & Conditions Copyrights Hyperlink Policy Privacy Policy Security Policy
Purva e-Voting system Ver 2.0. Page last updated: 23/03/2023 10:00 AM
Sending request to uat-evoting.purvashare.com...
Request
POST /accounts/forgot-password/otp-submit/ HTTP/2
Host: uat-evoting.purvashare.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 118
Origin: null
csrfmiddlewaretoken=xvaRiQMJnJM4iBeUnV9Vdyw5KMIWqdzIsxzdgafJOtSIbsUsICtwdnxuC6ldTZ3U&otp=123456&submit_type=submit_otp

Fig. 2.2

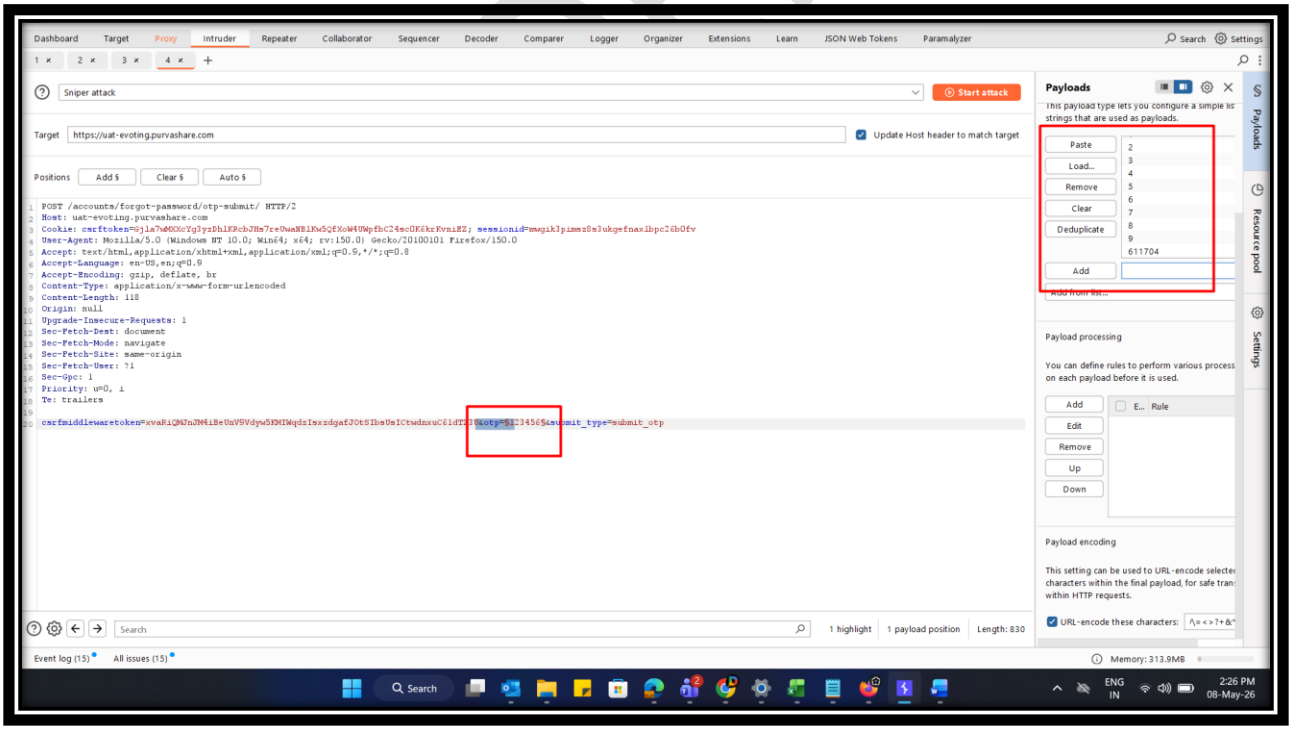

Sniper attack
Start attack
Target https://uat-evoting.purvashare.com
Update Host header to match target
Positions
Payloads
Payload processing
Payload encoding
POST /accounts/forgot-password/otp-submit/ HTTP/2
Host: uat-evoting.purvashare.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 118
Origin: null
csrfmiddlewaretoken=xvaRiQMJnJM4iBeUnV9Vdyw5KMIWqdzIsxzdgafJOtSIbsUsICtwdnxuC6ldTZ3U&otp=§123456§&submit_type=submit_otp

Fig. 2.3

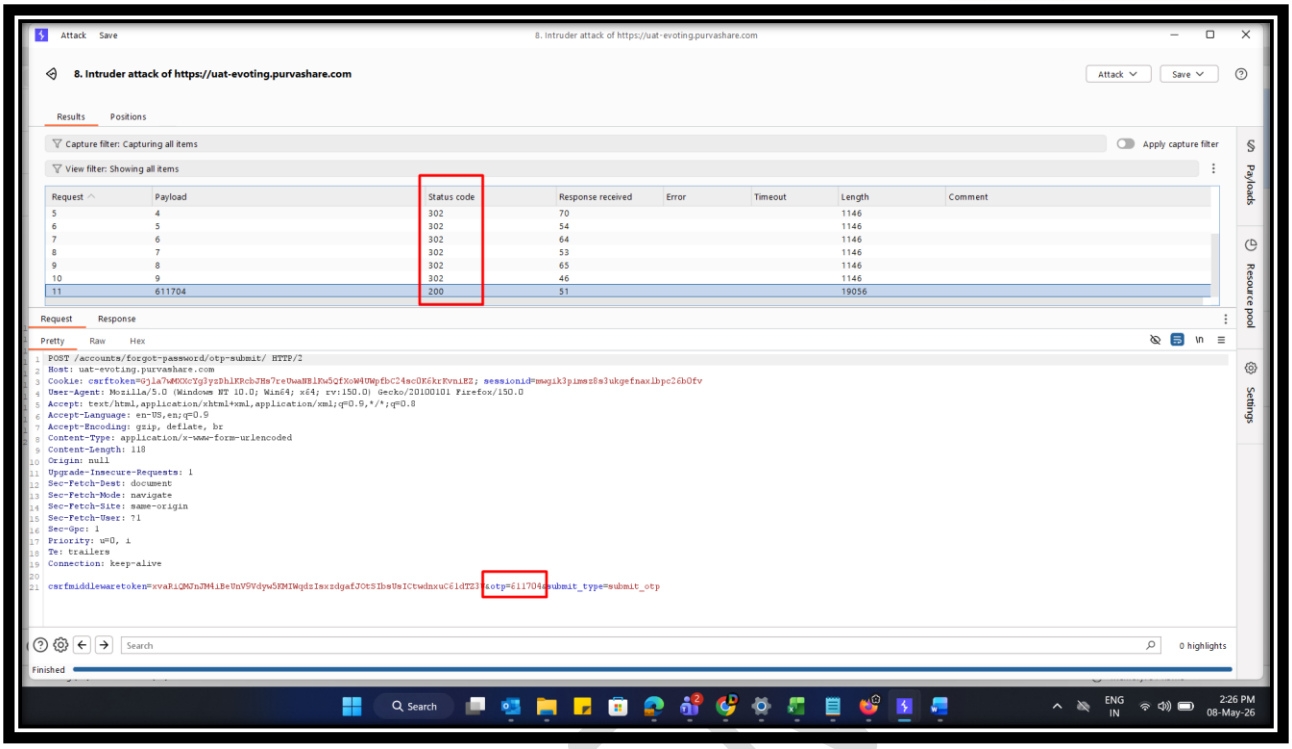

8. Intruder attack of https://uat-evoting.purvashare.com
Attack
Save
Results
Positions
Capture filter: Capturing all items
View filter: Showing all items
Request
Payload
Status code
Response received
Error
Timeout
Length
Comment
5 4 302 70 1146
6 5 302 54 1146
7 6 302 64 1146
8 7 302 53 1146
9 8 302 65 1146
10 9 302 46 1146
11 611704 200 51 19056
Request
Response
Pretty
Raw
Hex
POST /accounts/forgot-password/otp-submit/ HTTP/2
Host: uat-evoting.purvashare.com
Cookie: csrftoken=0jla7wMXXcYg3yzDhlKRcbJHs7reUwaNBlKw5QfXoW4UWpfbC24mcUE6krFvnLEZ; sessionid=mwgik3pimwz8s3ukgefnaxlbpc26hOfv
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:150.0) Gecko/20100101 Firefox/150.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 118
Origin: null
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Sec-Gpc: 1
Priority: u=0, i
Te: trailers
Connection: keep-alive
csrfmiddlewaretoken=xvaRiQMJnJM4iBeUnV9Vdyw5KMIWqdzIsxzdgafJOtSIbsUsICtwdnxuC6ldTZ3&otp=611704&submit_type=submit_otp
Search
0 highlights
Finished
Search
ENG
IN
2:26 PM
08-May-26

Fig. 2.4

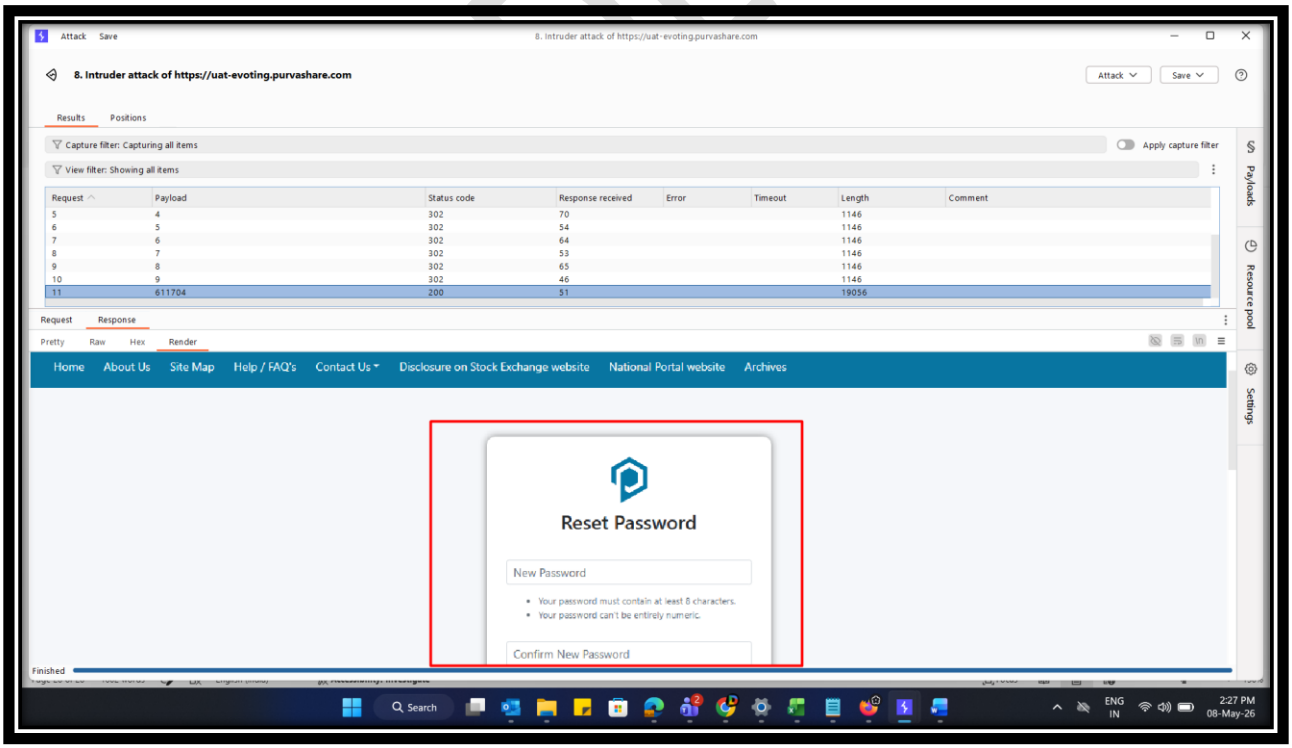
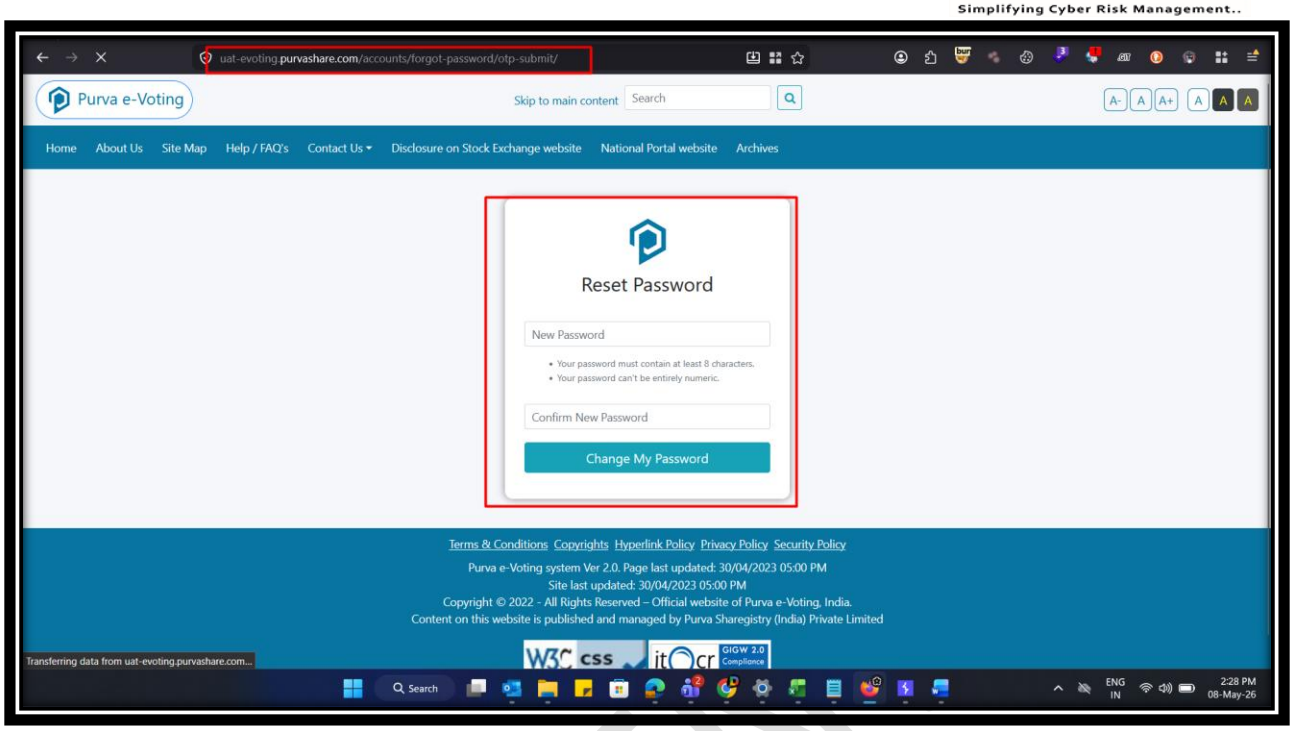
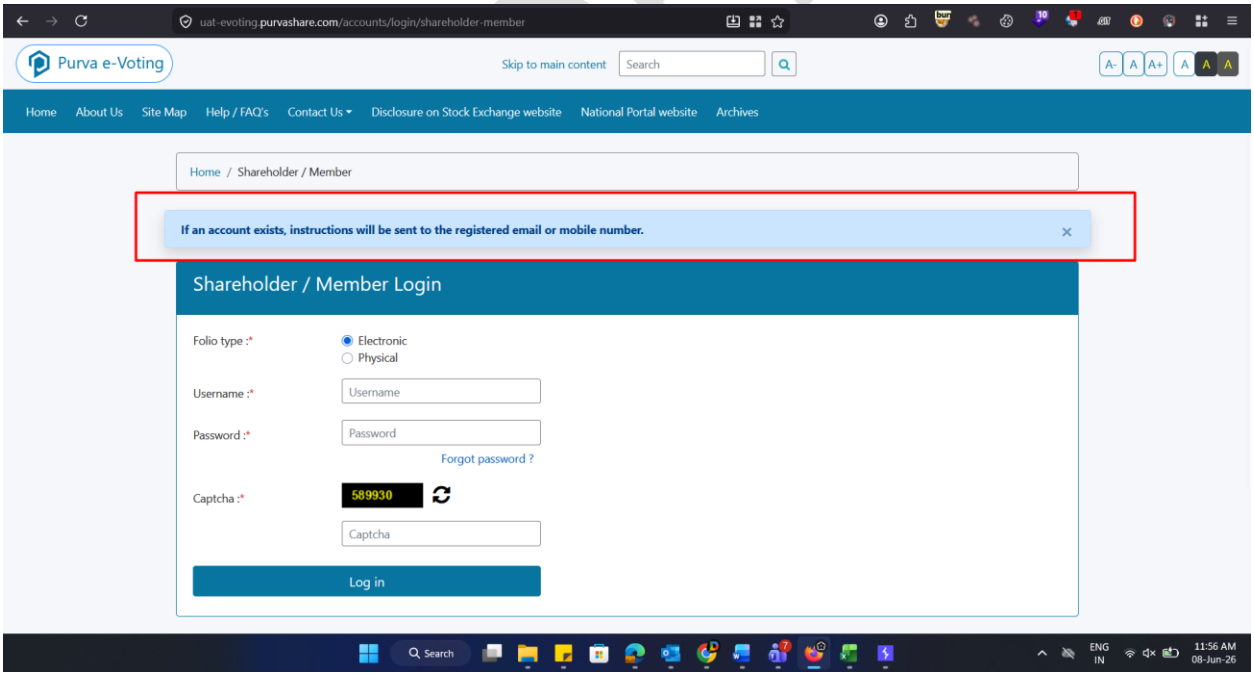
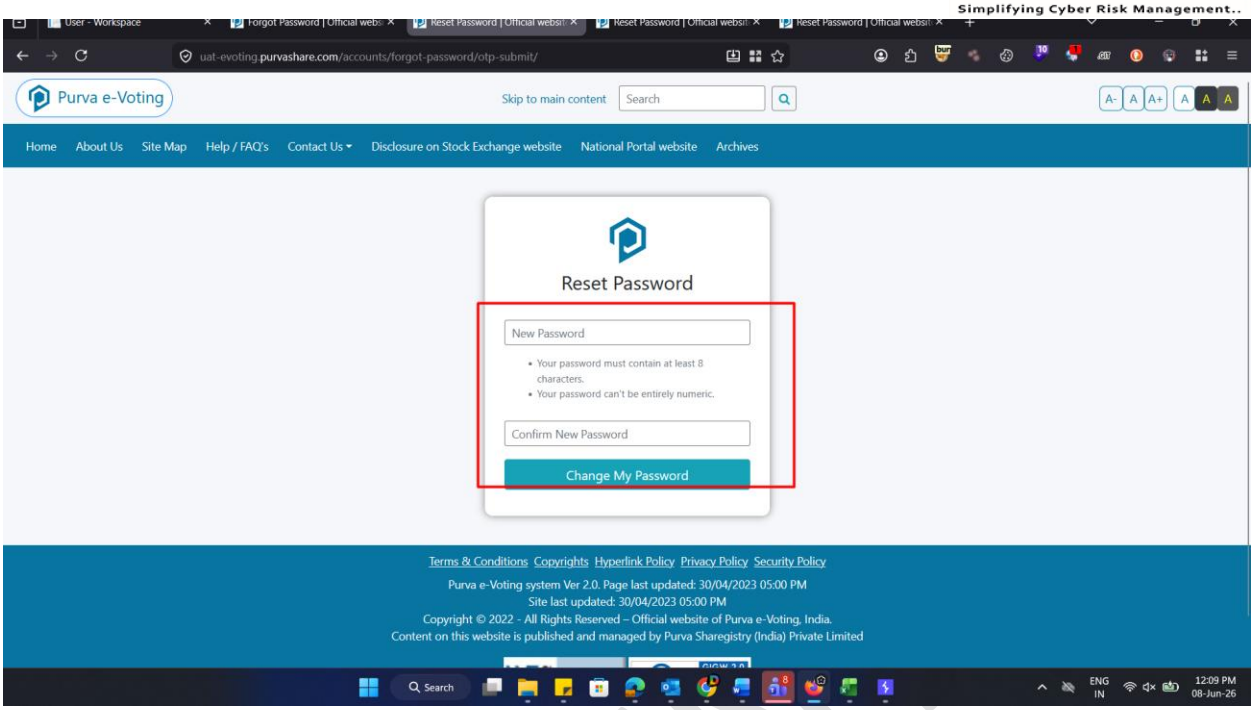

8. Intruder attack of https://uat-evoting.purvashare.com
Attack
Save
Results
Positions
Capture filter: Capturing all items
View filter: Showing all items
Request
Payload
Status code
Response received
Error
Timeout
Length
Comment
5 4 302 70 1146
6 5 302 54 1146
7 6 302 64 1146
8 7 302 53 1146
9 8 302 65 1146
10 9 302 46 1146
11 611704 200 51 19056
Request
Response
Pretty
Raw
Hex
Render
Home
About Us
Site Map
Help / FAQ's
Contact Us
Disclosure on Stock Exchange website
National Portal website
Archives
Reset Password
New Password
Your password must contain at least 8 characters.
Your password can't be entirely numeric.
Confirm New Password
Finished
Search
ENG
IN
2:27 PM
08-May-26

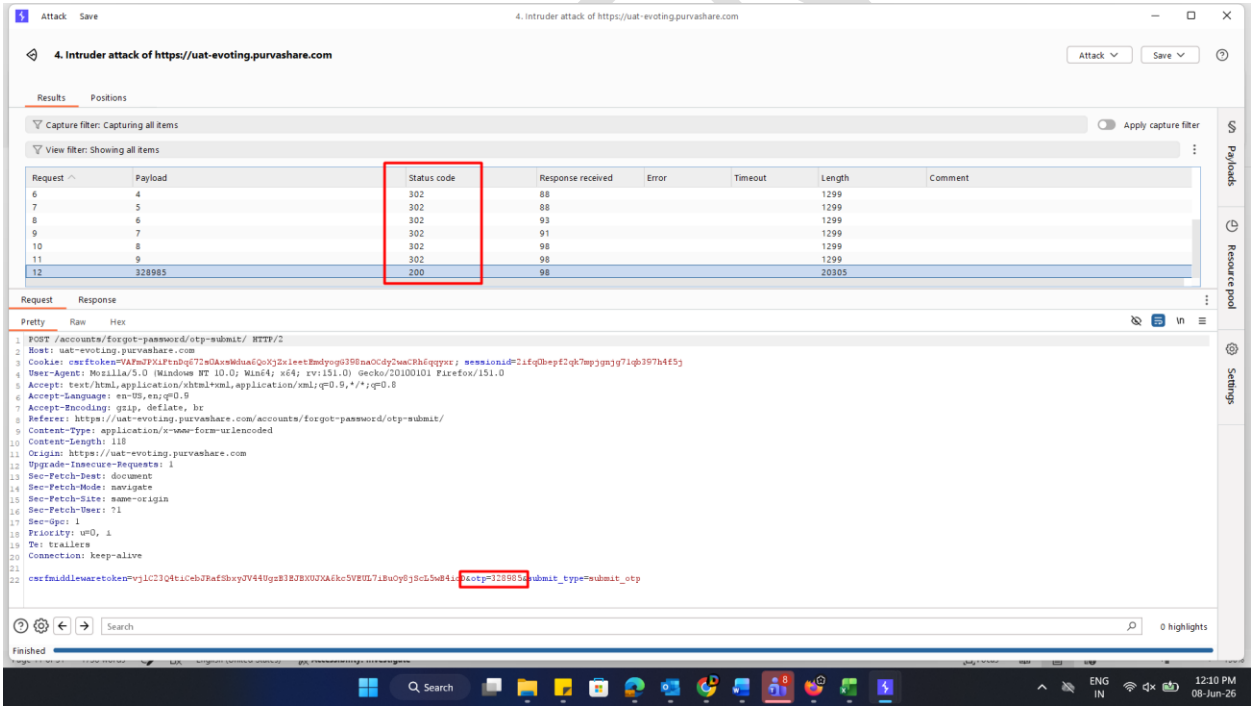
Fig. 2.5


uat-evoting.purvashare.com/accounts/forgot-password/otp-submit/
Purva e-Voting
Skip to main content
Search
Home
About Us
Site Map
Help / FAQ's
Contact Us
Disclosure on Stock Exchange website
National Portal website
Archives
Reset Password
New Password
• Your password must contain at least 8 characters.
• Your password can't be entirely numeric.
Confirm New Password
Change My Password
Terms & Conditions
Copyrights
Hyperlink Policy
Privacy Policy
Security Policy
Purva e-Voting system Ver 2.0. Page last updated: 30/04/2023 05:00 PM
Site last updated: 30/04/2023 05:00 PM
Copyright © 2022 - All Rights Reserved – Official website of Purva e-Voting, India.
Content on this website is published and managed by Purva Sharegistry (India) Private Limited
Transferring data from uat-evoting.purvashare.com...
Search
ENG
IN
2:28 PM
08-May-26

Status: Open


uat-evoting.purvashare.com/accounts/login/shareholder-member
Purva e-Voting
Skip to main content
Search
Home
About Us
Site Map
Help / FAQ's
Contact Us
Disclosure on Stock Exchange website
National Portal website
Archives
Home / Shareholder / Member
If an account exists, instructions will be sent to the registered email or mobile number.
Shareholder / Member Login
Folio type :*
Electronic
Physical
Username :*
Username
Password :*
Password
Forgot password ?
Captcha :*
589930
Captcha
Log in
Search
ENG
IN
11:56 AM
08-Jun-26


uat-evoting.purvashare.com/accounts/forgot-password/otp-submit/
Purva e-Voting
Skip to main content
Search
Home
About Us
Site Map
Help / FAQ's
Contact Us
Disclosure on Stock Exchange website
National Portal website
Archives
Reset Password
New Password
Your password must contain at least 8 characters.
Your password can't be entirely numeric.
Confirm New Password
Change My Password
Terms & Conditions
Copyrights
Hyperlink Policy
Privacy Policy
Security Policy
Purva e-Voting system Ver 2.0. Page last updated: 30/04/2023 05:00 PM
Site last updated: 30/04/2023 05:00 PM
Copyright © 2022 - All Rights Reserved – Official website of Purva e-Voting, India.
Content on this website is published and managed by Purva Sharegistry (India) Private Limited


4. Intruder attack of https://uat-evoting.purvashare.com
Attack
Save
Results
Positions
Capture filter: Capturing all items
View filter: Showing all items
Request
Payload
Status code
Response received
Error
Timeout
Length
Comment
Request
Response
Pretty
Raw
Hex
POST /accounts/forgot-password/otp-submit/ HTTP/2
Host: uat-evoting.purvashare.com
Finished

3. End-of-life Nginx Version in Use

Affected URL: https://uat-evoting.purvashare.com

It is observed that the application is using an outdated/end-of-life version of the Nginx web server. End-of-life software versions no longer receive security updates, bug fixes, or vendor support, which may expose the server to publicly known vulnerabilities and security weaknesses.

Step I: Identify the nginx version from the server response headers using Burp Suite or browser developer tools.
Step II: Verify the identified version on the EOL website and observe that it is unsupported. (Refer to Fig. 6.1 & 6.2)

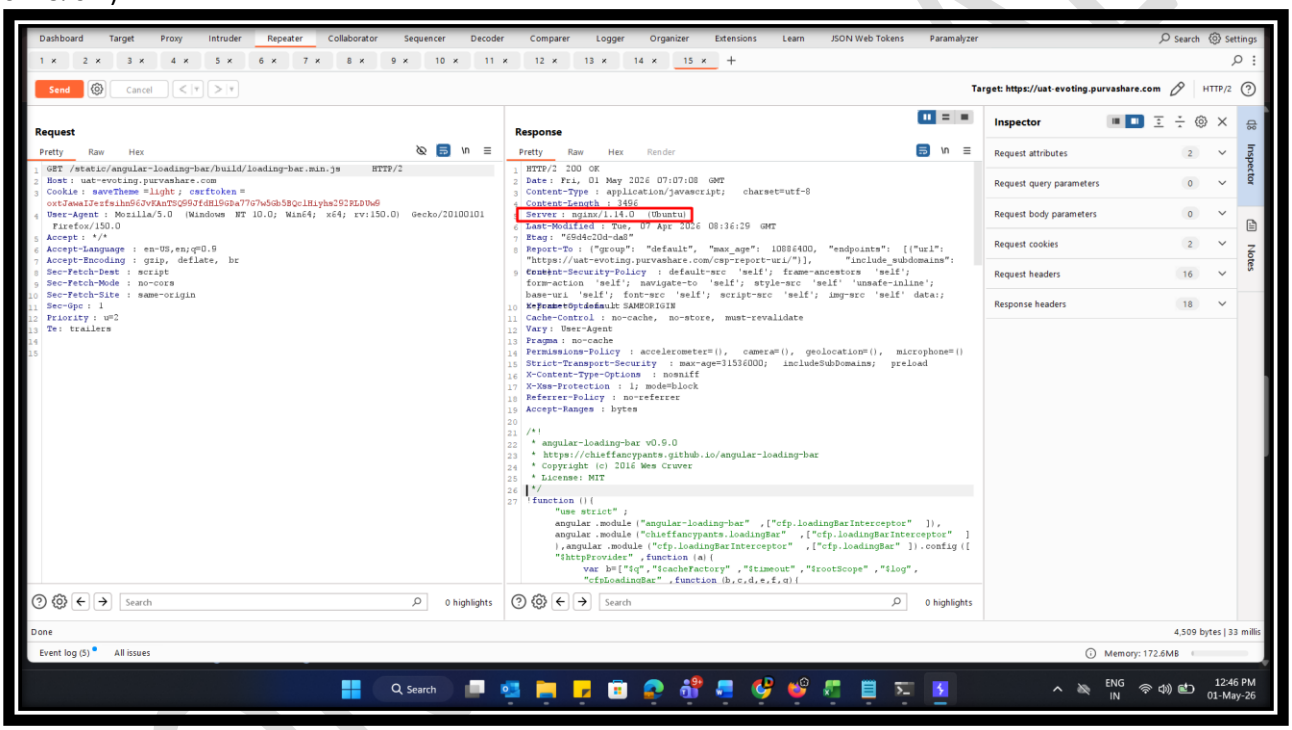


Fig. 3.1

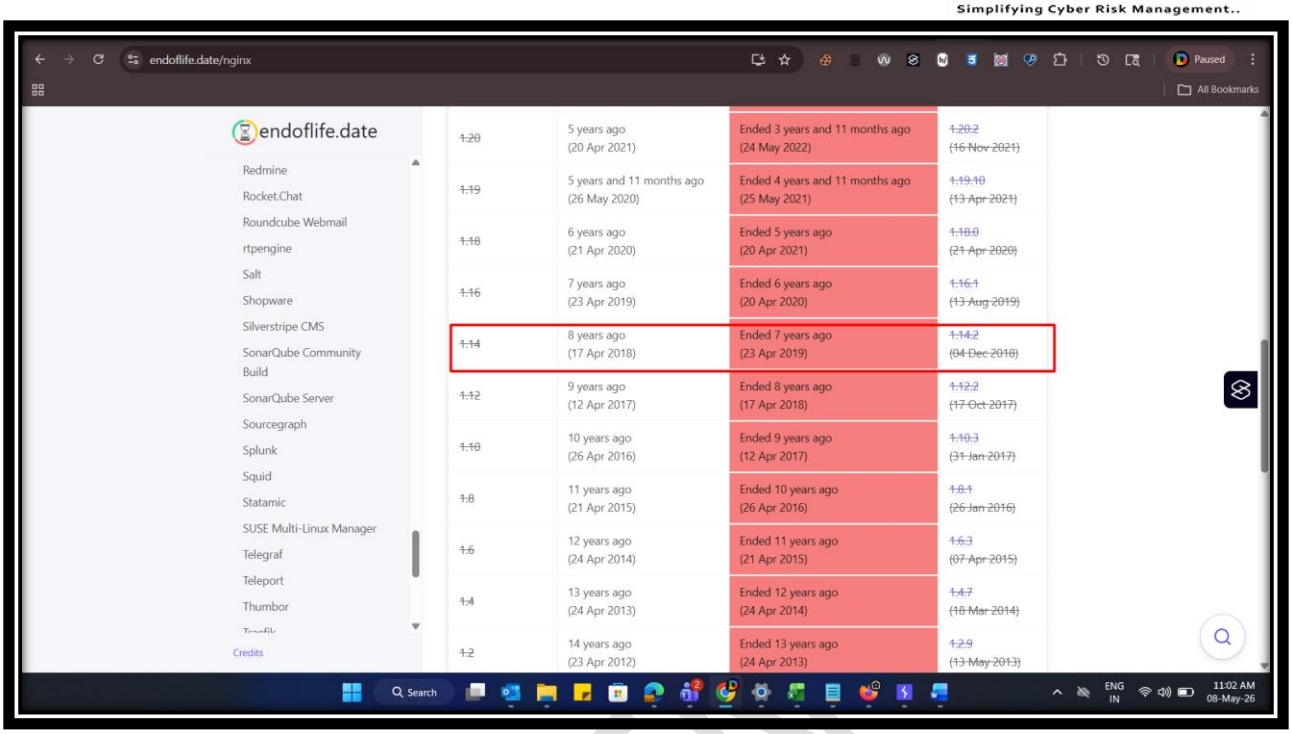
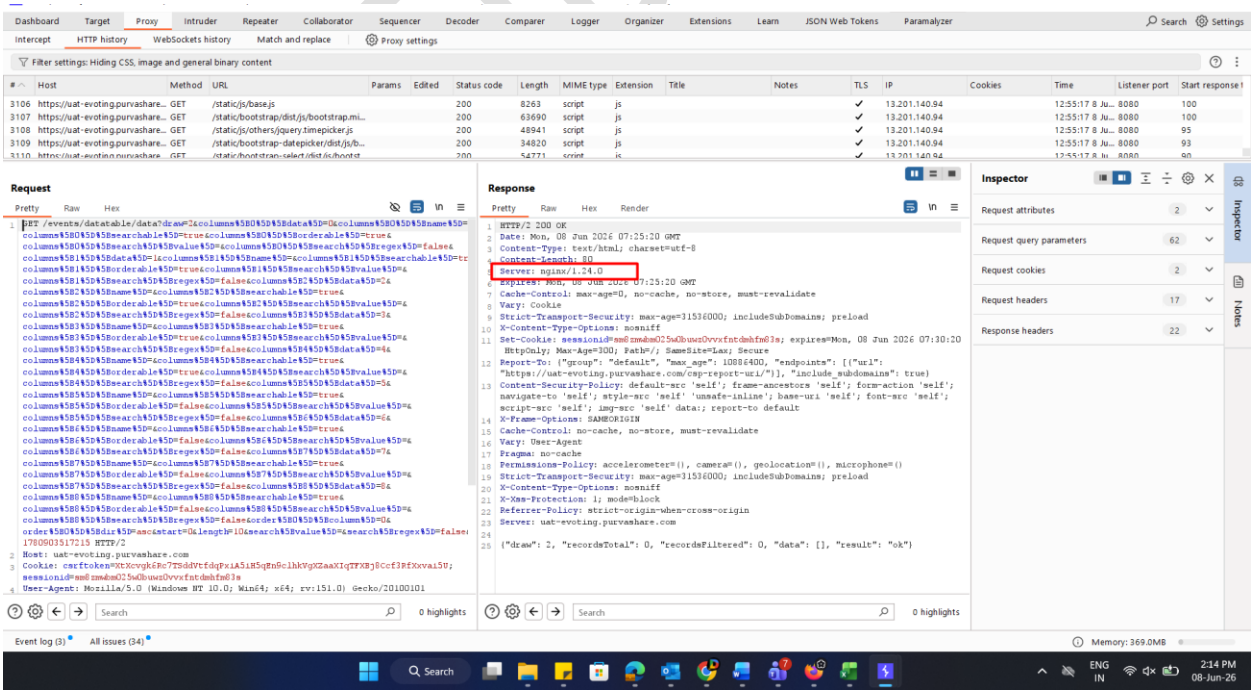
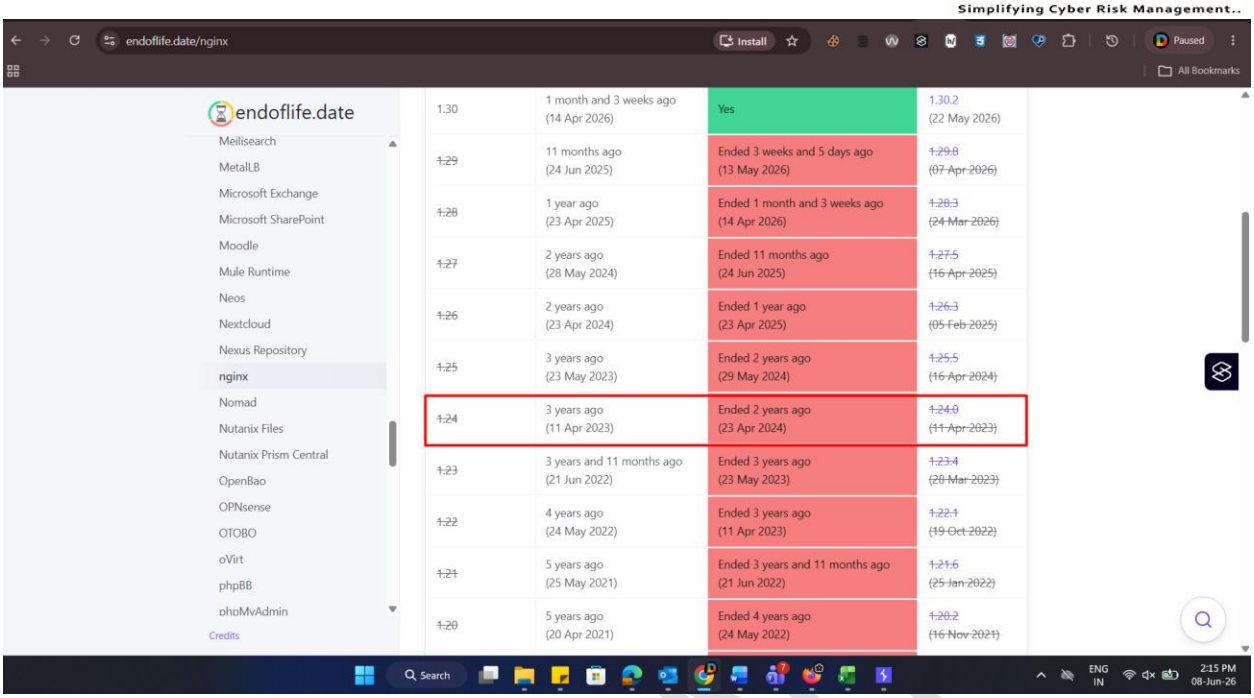


Fig. 3.2

Status: Open

Note: Nginx 1.24 is EOL version.





CONFIDENTIAL

4. Credentials in Cleartext

Affected URL: https://uat-evoting.purvashare.com/

It is observed that the username and password are transmitted in clear text within the request payload. The credentials are visible in plain text when intercepted using tools like Burp Suite, indicating the lack of proper encryption.

Step I: Log in to the application and intercept the authentication request using a proxy tool (e.g., Burp Suite) or browser developer tools.

Step II: Observe that the credentials (username and password) are transmitted in cleartext within the request instead of being securely encrypted. (Refer to Fig. 7.1 & 7.2)

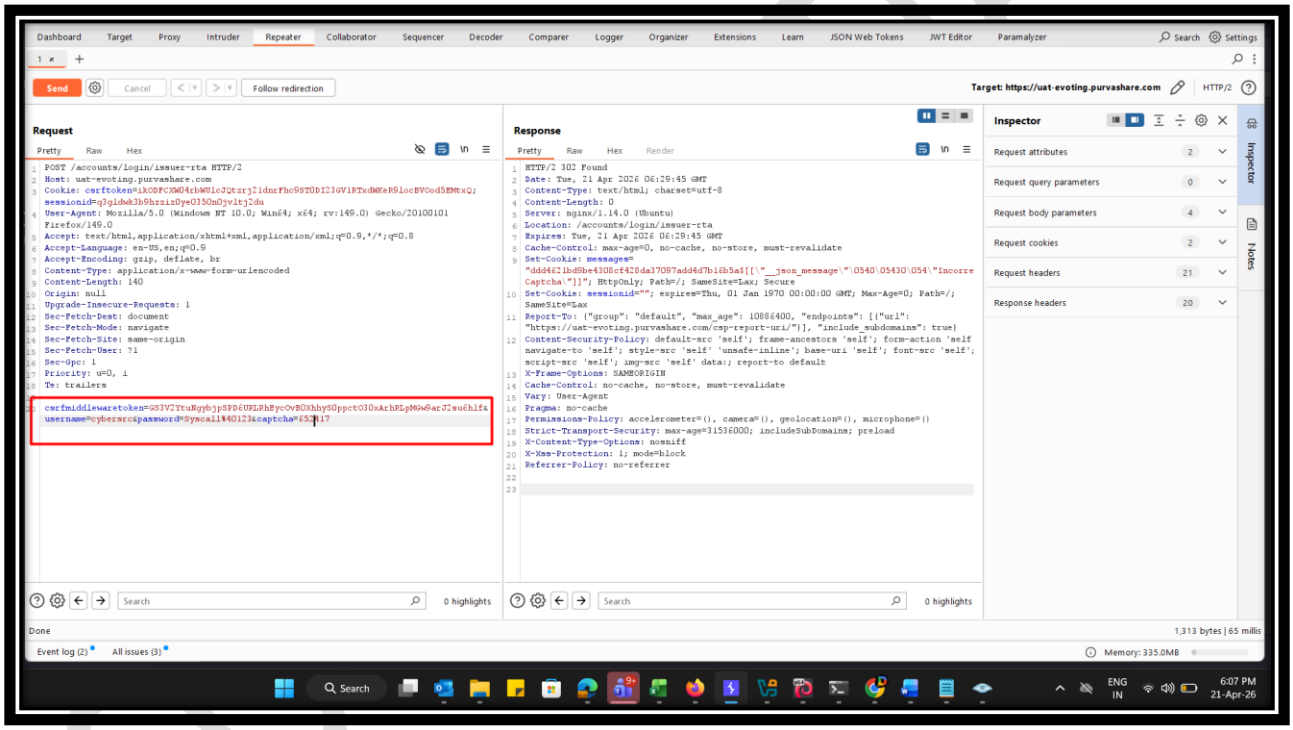


Fig. 4.1

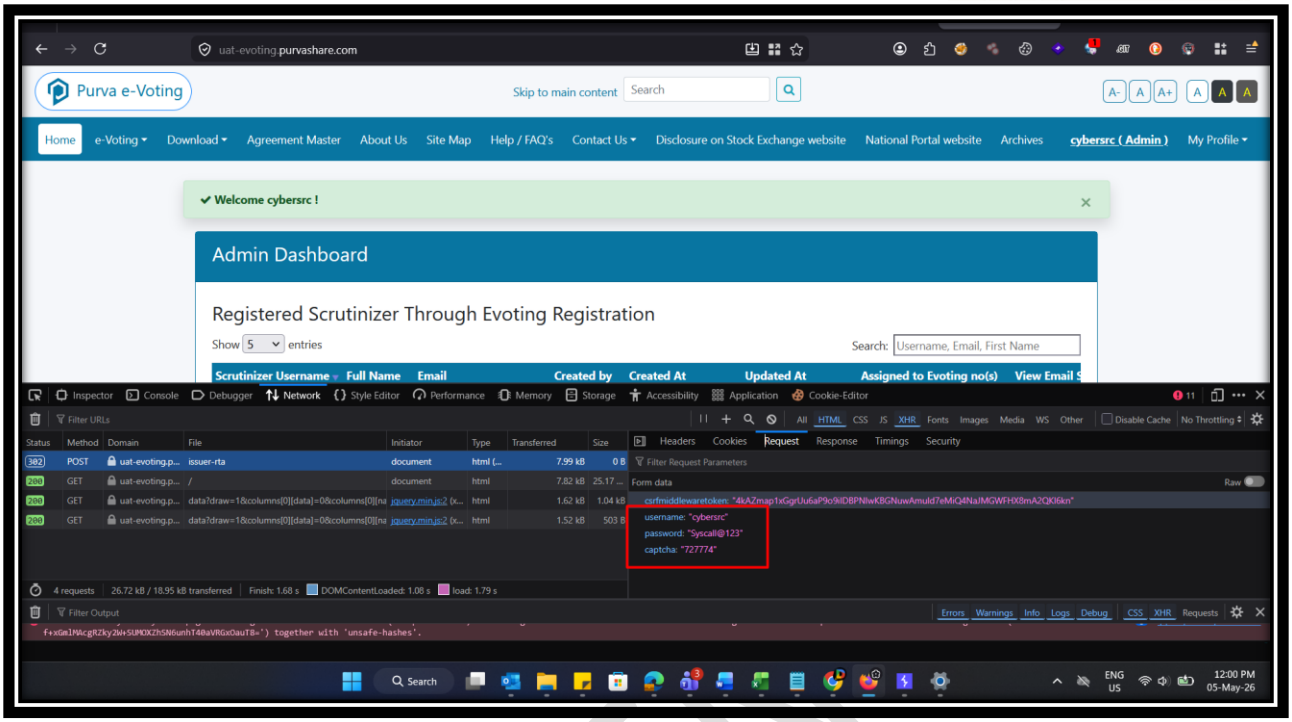
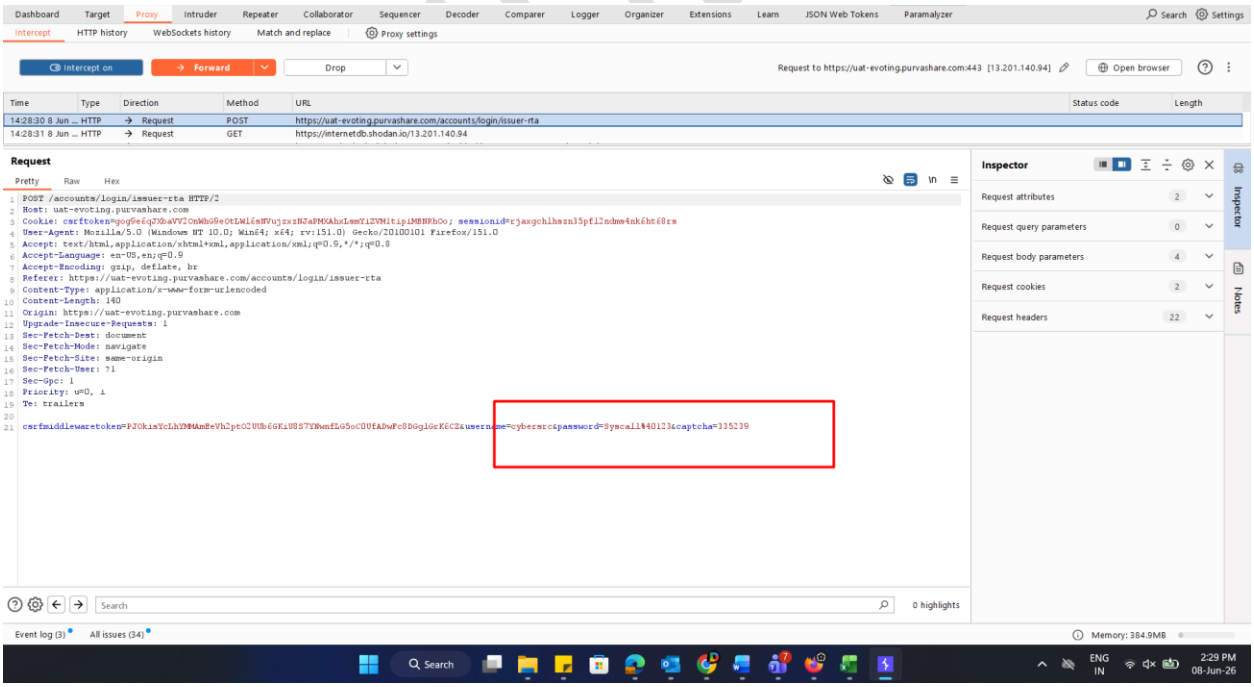
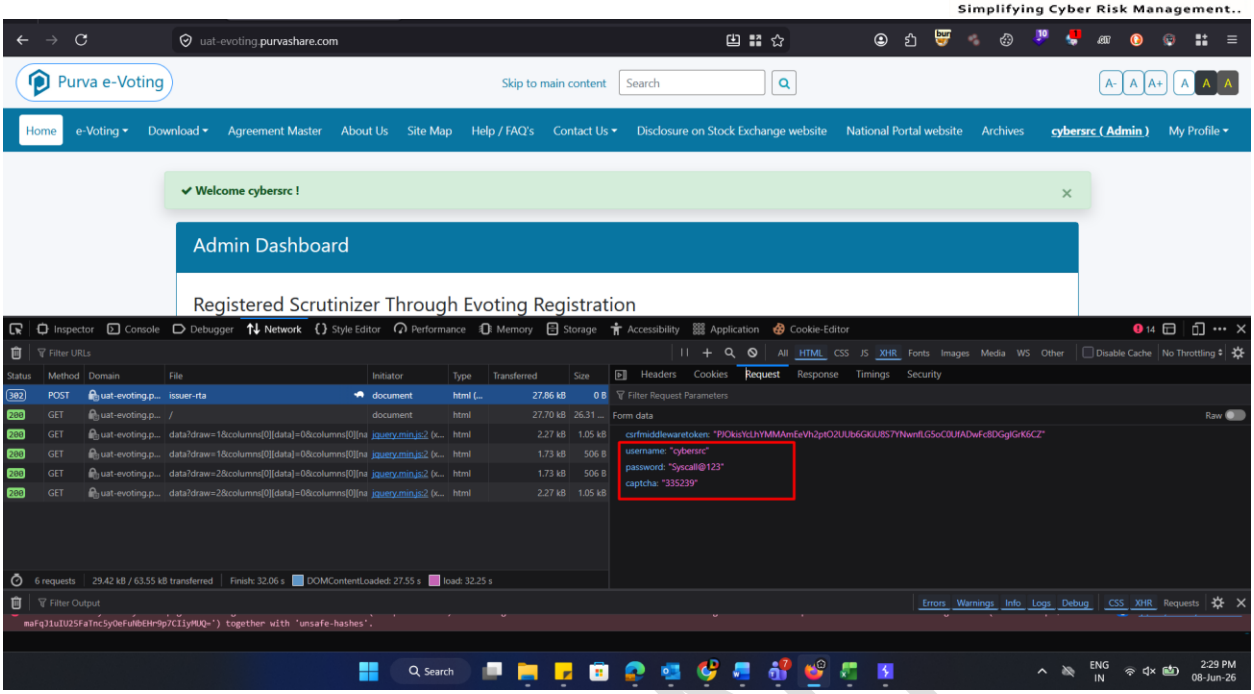


Fig. 4.2

Status: Open





CONFIDENTIAL

5. Outdated and vulnerable Components in Use

Affected URL: https://uat-evoting.purvashare.com/

It is observed that the application is using outdated and potentially vulnerable third-party components, including jQuery version 3.6.0, DataTables version 1.10.23, Nginx version 1.14.0, and Bootstrap version 4.3.1. These versions are no longer up to date and may contain known security vulnerabilities, missing security patches, and lack support for modern security mechanisms. The use of such outdated components increases the risk of exploitation, including but not limited to cross-site scripting (XSS), security misconfigurations, and exposure to publicly known vulnerabilities.

Step I: Access the application and analyze it using browser developer tools or technology fingerprinting tools (e.g., Retire.js, Wappalyzer) to identify outdated and vulnerable components in use.(Refer to Fig. 8.1 to 8.4)

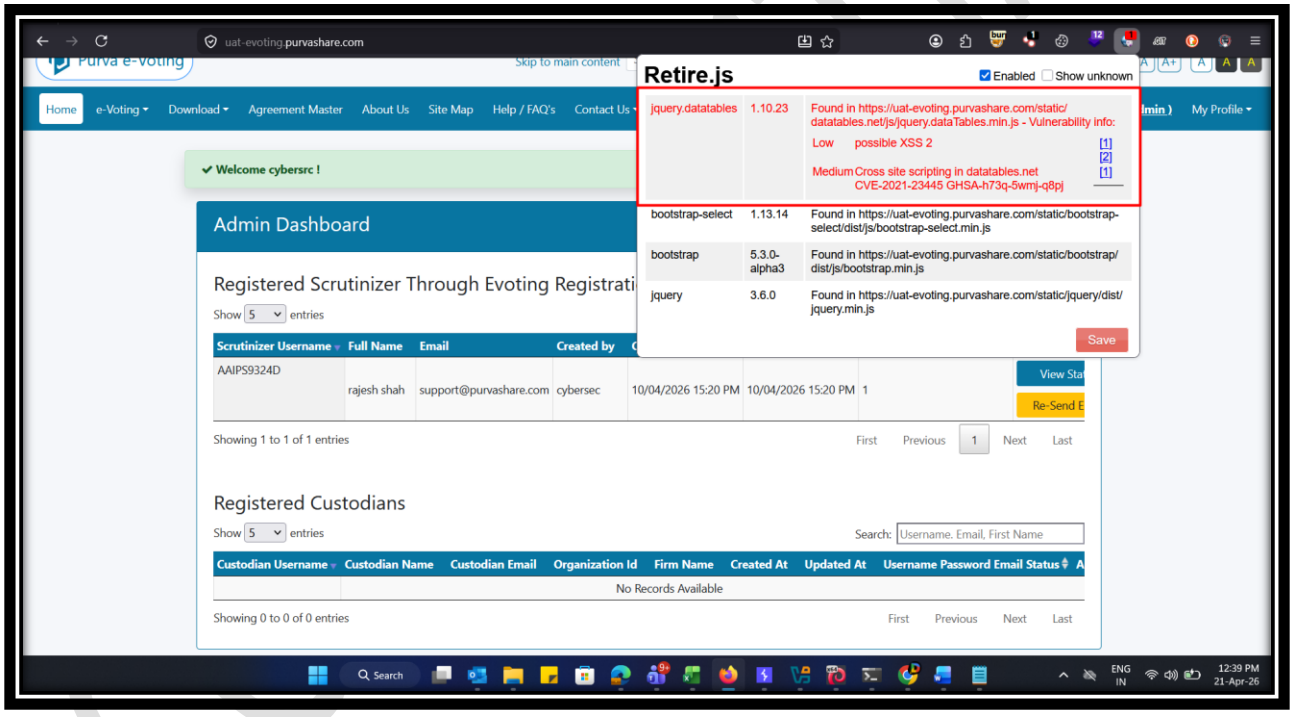


Fig. 5.1

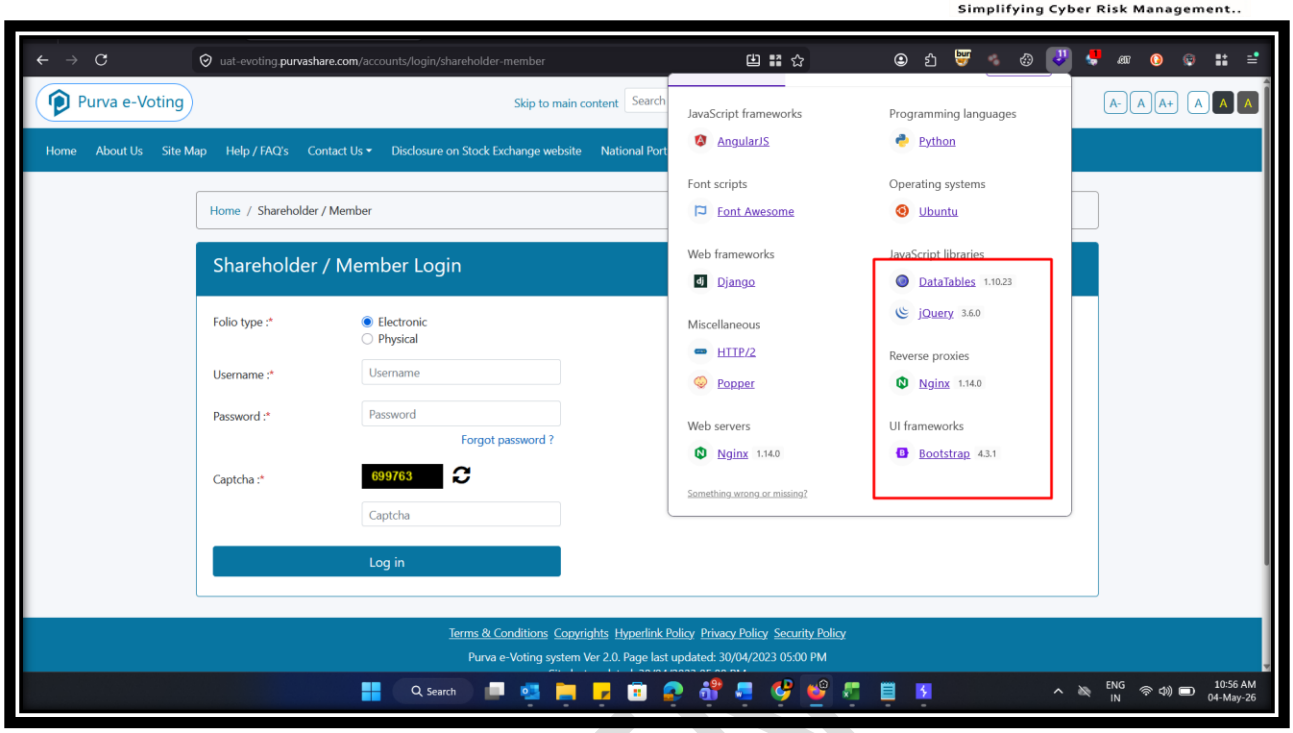

uat-evoting.purvashare.com/accounts/login/shareholder-member
Purva e-Voting
Skip to main content
Search
Home
About Us
Site Map
Help / FAQ's
Contact Us
Disclosure on Stock Exchange website
National Port
Home / Shareholder / Member
Shareholder / Member Login
Folio type :*
Electronic
Physical
Username :*
Username
Password :*
Password
Forgot password ?
Captcha :*
699763
Captcha
Log in
JavaScript frameworks
AngularJS
Programming languages
Python
Font scripts
Font Awesome
Operating systems
Ubuntu
Web frameworks
Django
JavaScript libraries
DataTables 1.10.23
jQuery 3.6.0
Miscellaneous
HTTP/2
Popper
Reverse proxies
Nginx 1.14.0
Web servers
Nginx 1.14.0
UI frameworks
Bootstrap 4.3.1
Something wrong or missing?
Terms & Conditions
Copyrights
Hyperlink Policy
Privacy Policy
Security Policy
Purva e-Voting system Ver 2.0. Page last updated: 30/04/2023 05:00 PM
Search
ENG
IN
10:56 AM
04-May-26

Fig. 5.2

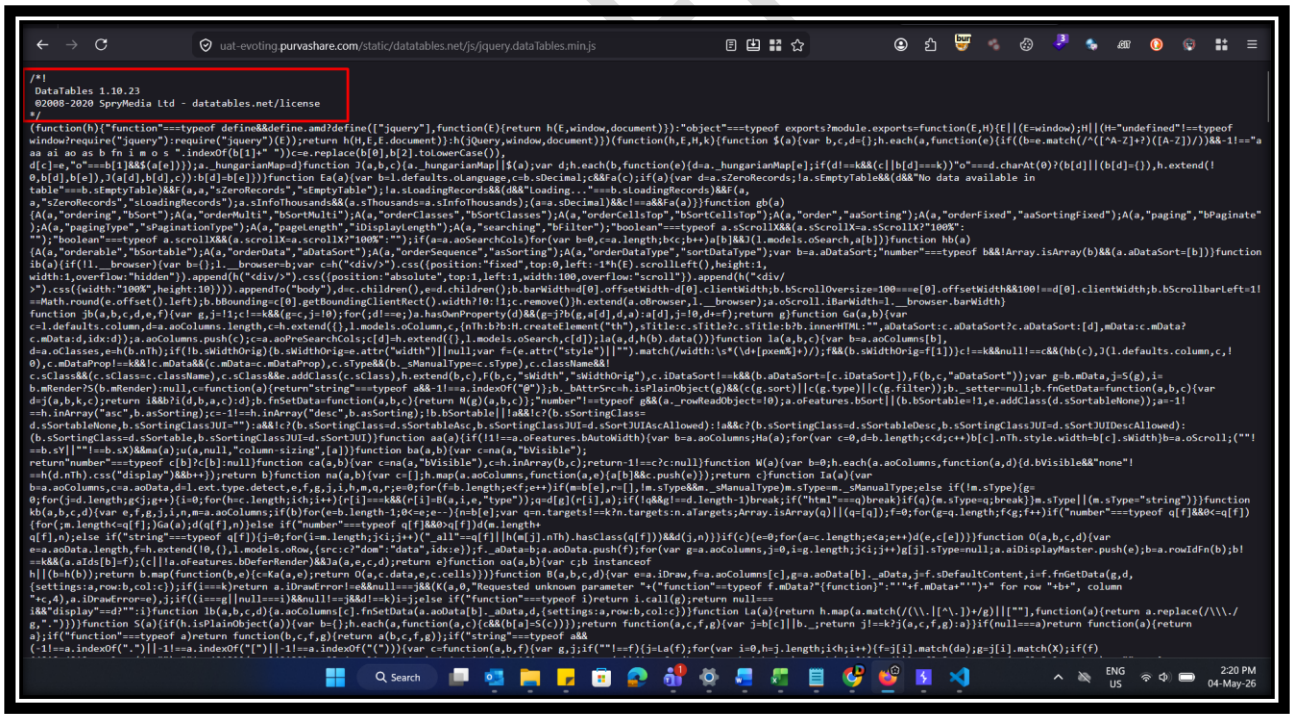

uat-evoting.purvashare.com/static/datatables.net/js/jquery.dataTables.min.js
/*!
DataTables 1.10.23
©2008-2020 SpryMedia Ltd - datatables.net/license
*/
Search
ENG
US
2:20 PM
04-May-26

Fig. 5.3

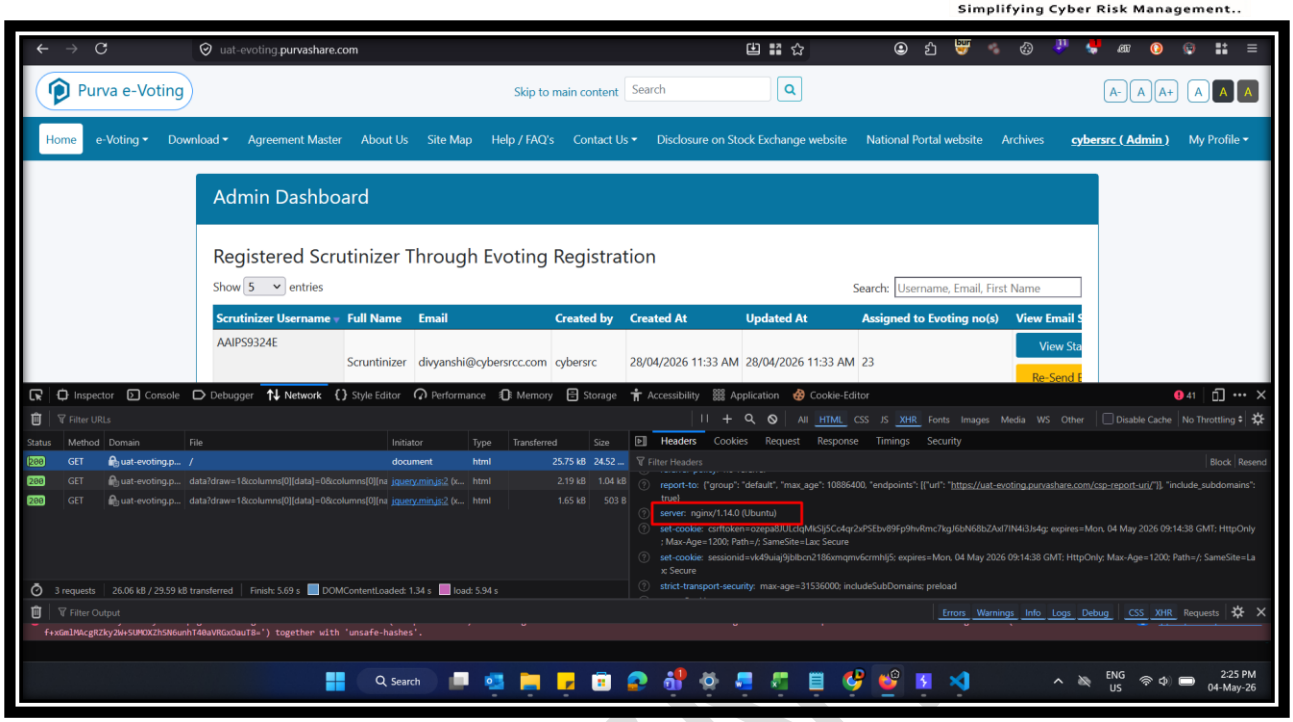
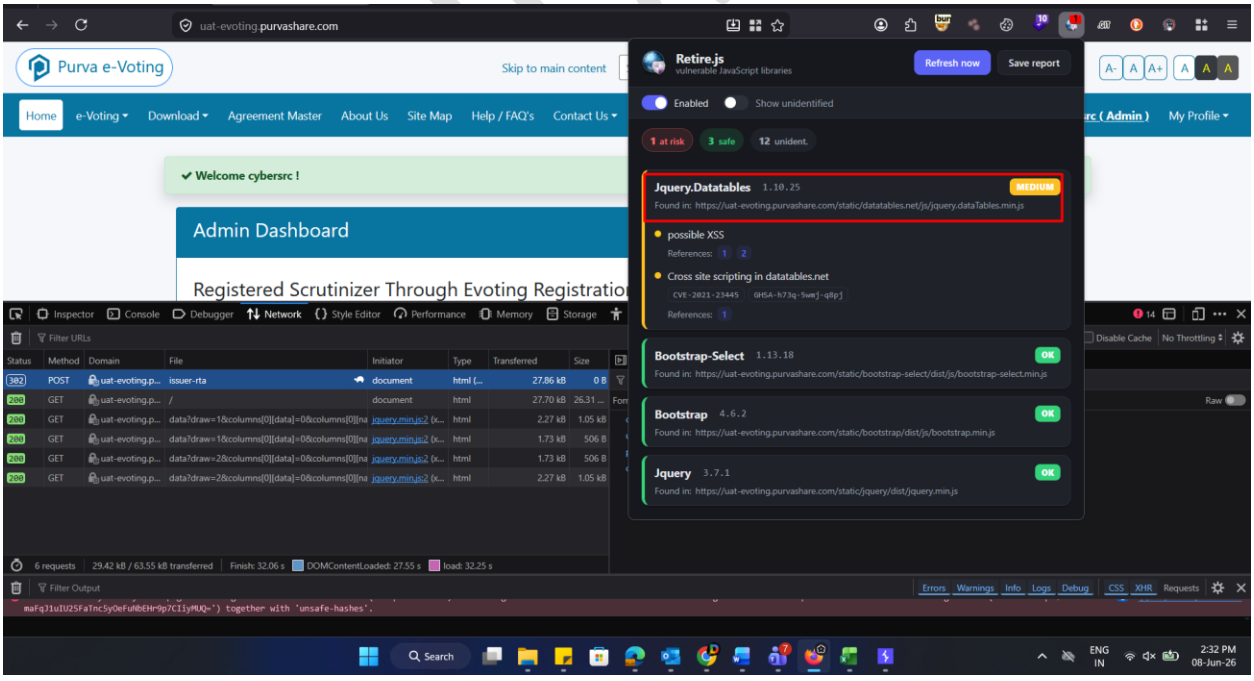
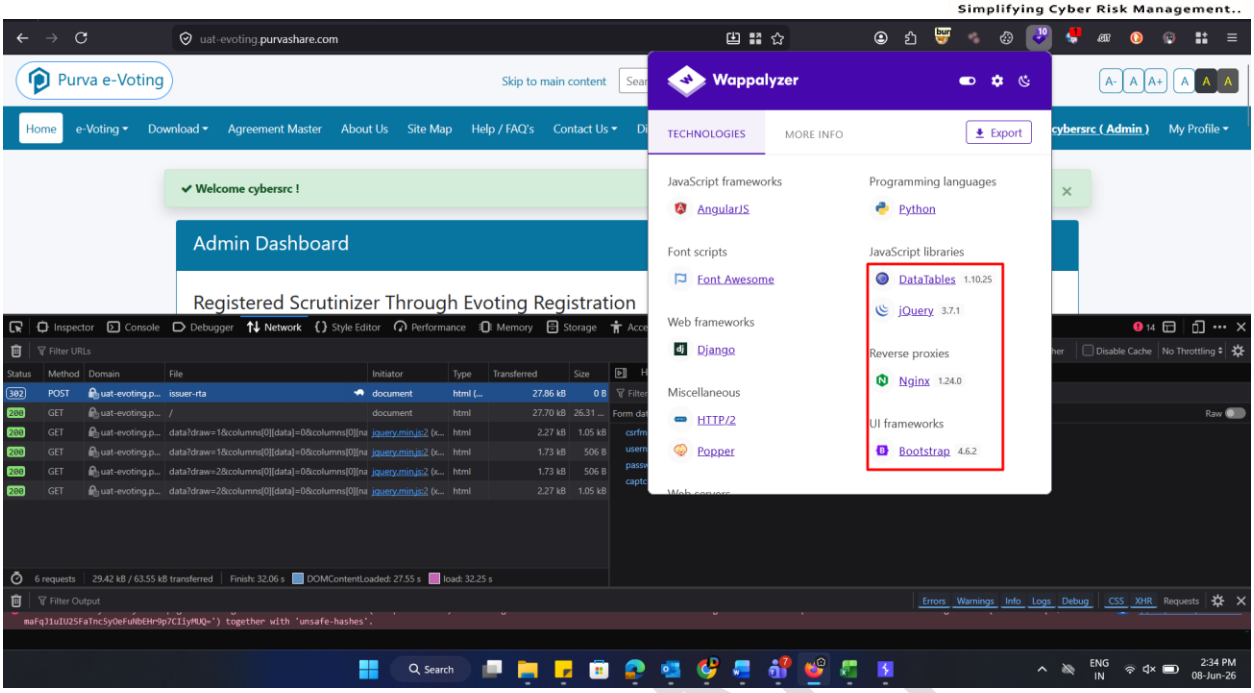


Fig. 5.4

Status: Open





CONFIDENTIAL

6. Server Version Disclosure

Affected URL: https://uat-evoting.purvashare.com/

It is observed that the application discloses the server version information in HTTP response headers, specifically revealing the use of Nginx version 1.14.0. This information disclosure allows an external user to identify the exact server software and version in use, which is outdated and may contain known vulnerabilities.

Step I: Access the application and intercept any request using browser developer tools or a proxy tool (e.g., Burp Suite), then observe the response headers revealing the server version i.e, nginx version.(Refer to Fig. 9.1)

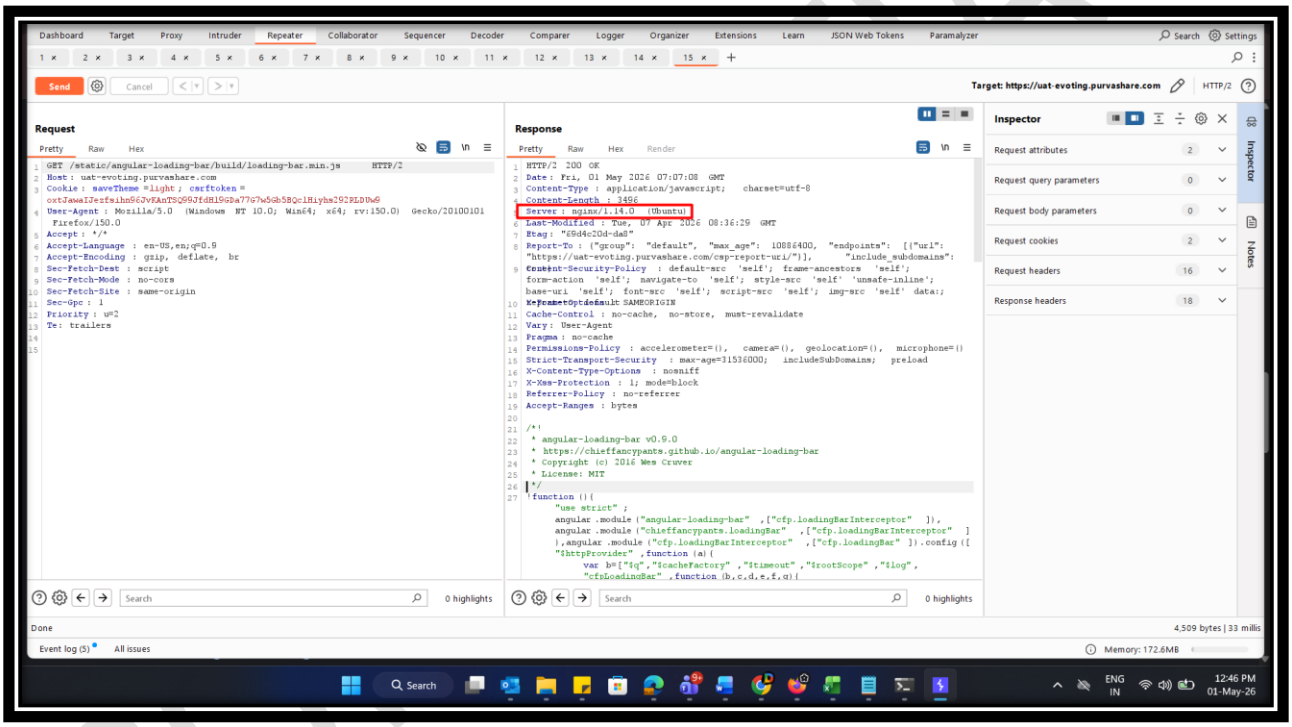
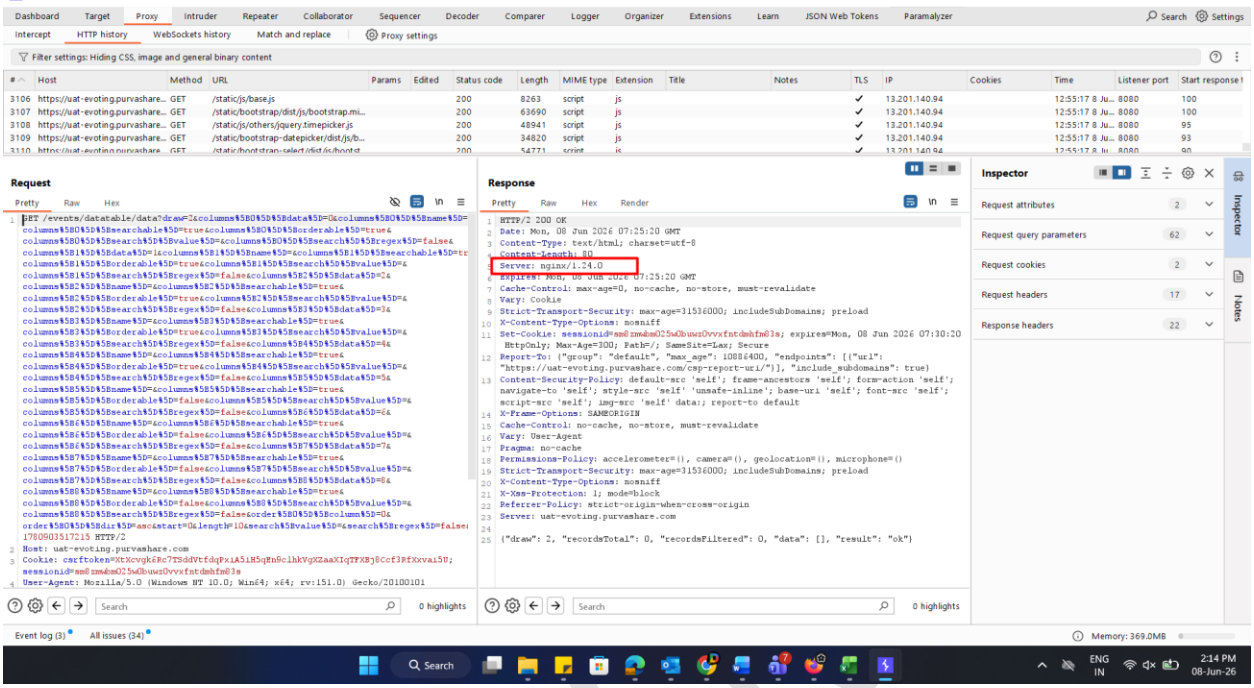


Fig. 6.1

Status: Open



CONFIDENTIAL

7. Cookie Path Set to Root

Affected URL: https://uat-evoting.purvashare.com

It is observed that the application sets the cookie path attribute to the root directory (/), making the cookie accessible across the entire application. This configuration allows the same cookie to be sent with requests to all paths within the domain, rather than restricting it to only the specific application context where it is required. Such a broad scope increases unnecessary exposure of sensitive session cookies.

Step I: Access the application and inspect the cookies using browser developer tools or a proxy tool (e.g., Burp Suite), then observe that the Path attribute of the cookie is set to "/", making it accessible across the entire application. (Refer to 11.1)

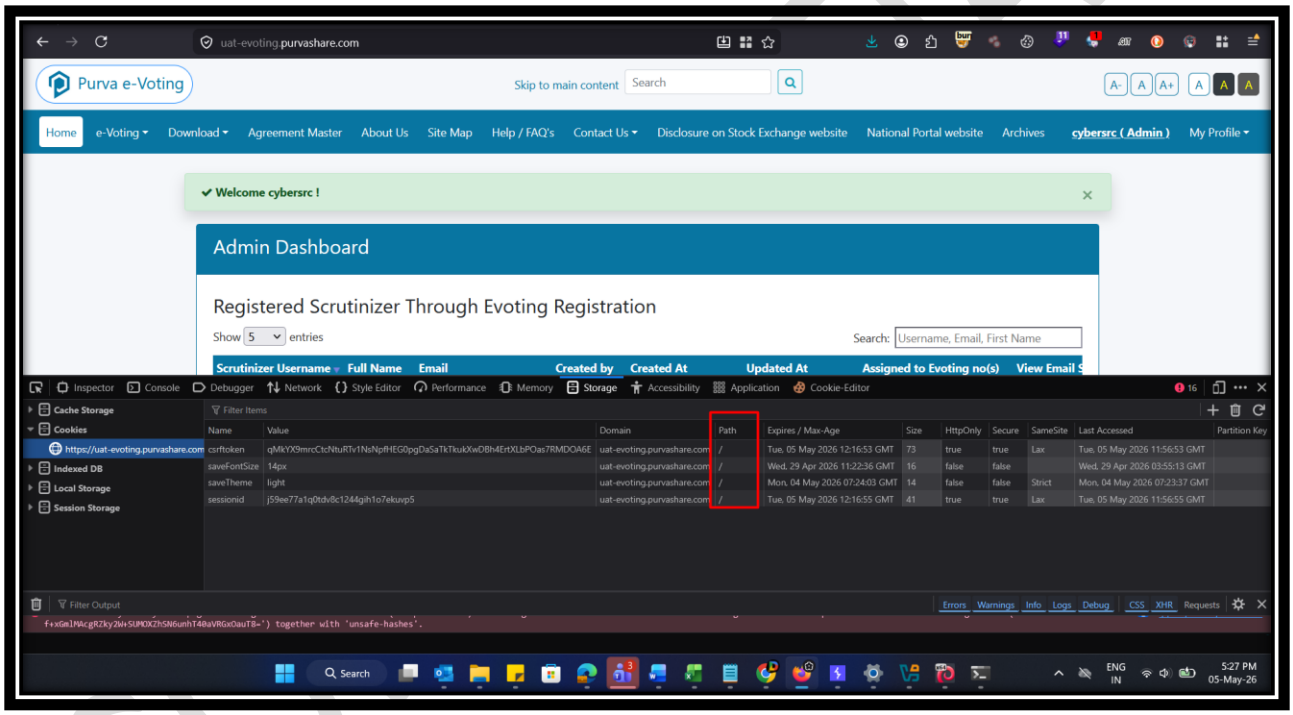
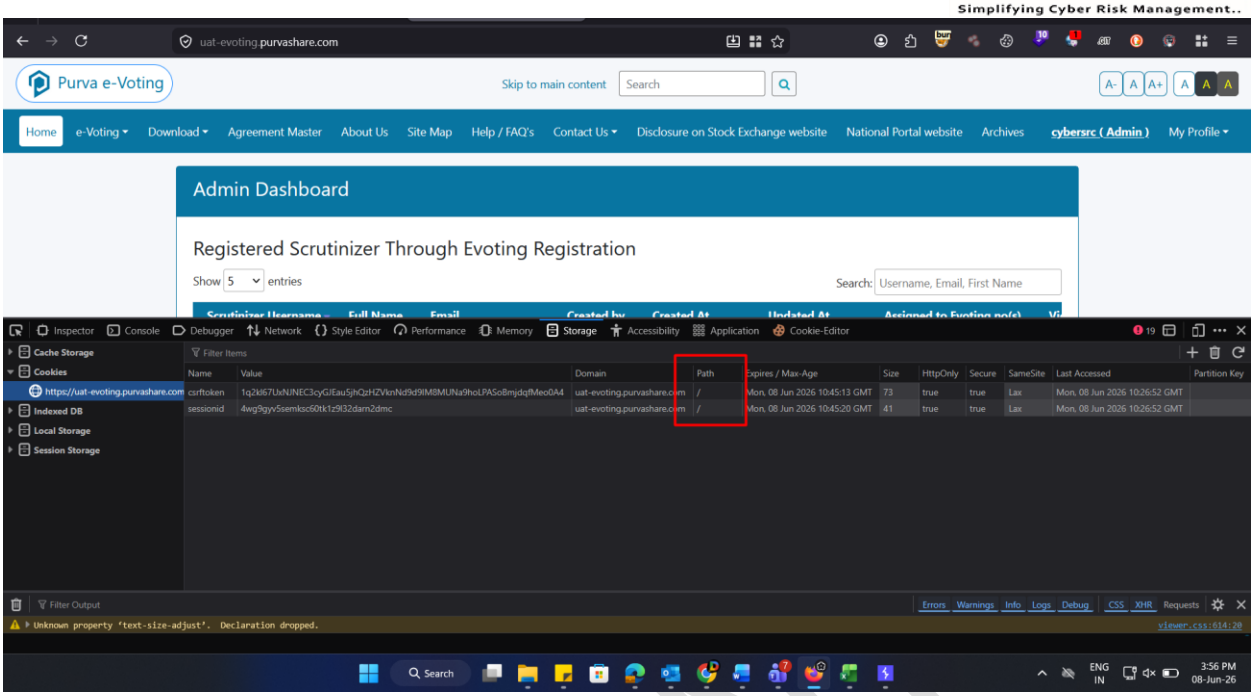


Fig. 7.1

Status: Open

CONFIDENTIAL



CONFIDENTIAL

CONFIDENTIAL