CyberSmith SECURE

Coforge-CAG-WAP-2025

Coforge

Web Application VAPT

Coforge CAG- preoios

Disclaimer

All information contained in this document is confidential and proprietary to CyberSmithSECURE and Reproduction, disclosure or use of any information contained in this document by photographic, electronic or any other means, in whole or part, for any reason other than for the purpose of operations is strictly prohibited without written consent.

Limitations on Disclosure and Use

This document contains sensitive and confidential information concerning vulnerabilities of target applications. CyberSmithSECURE recommends that special precautions be taken to protect the confidentiality of the information contained in this report.

While the VAPT Team is confident that the major security vulnerabilities of the target applications have been identified, there can be no assurance that an assessment of this nature will identify all possible security exposures. Additionally, the findings and recommendations presented in this document are based on the technologies and known threats as of the date of this report. As technologies and risks change over time, the vulnerabilities and the recommendations associated with the target applications may also change.

Table of Content

RISK LEVEL & DESCRIPTION

The below vulnerability ranging risk pattern indicates the ratings of the vulnerability according to their respective CVSS3.1 Score.

Critical

The Critical risk level Immediate measures must be taken to reduce these risks and mitigate hazards. These vulnerabilities can allow attackers to take complete control of your web applications and web servers. In exploiting this type of vulnerability, attackers could carry out a range of malicious acts including. Stealing information (for example, user data) Tricking your users into supplying them with sensitive information (for example, credit card details).Defacing your website

High

The high-risk level indicates maximum risk associated with a specific vulnerability instance. Such vulnerability may enable an attacker to successfully exploit the underlying application and its data and partially or completely to compromise the application and its data to modify application behaviour to become other than its original intended purpose. The vulnerability marked as "High Risk" is recommended to be handled with utmost priority.

Medium

The medium risk level indicates considerable risk associated with a specific vulnerability instance. Such vulnerability may enable an attacker to exploit the underlying application and its data to a particular level so that the attacker can gain low level information about the application. Such information can be used by an attacker to craft more specific attacks based on the information collected.

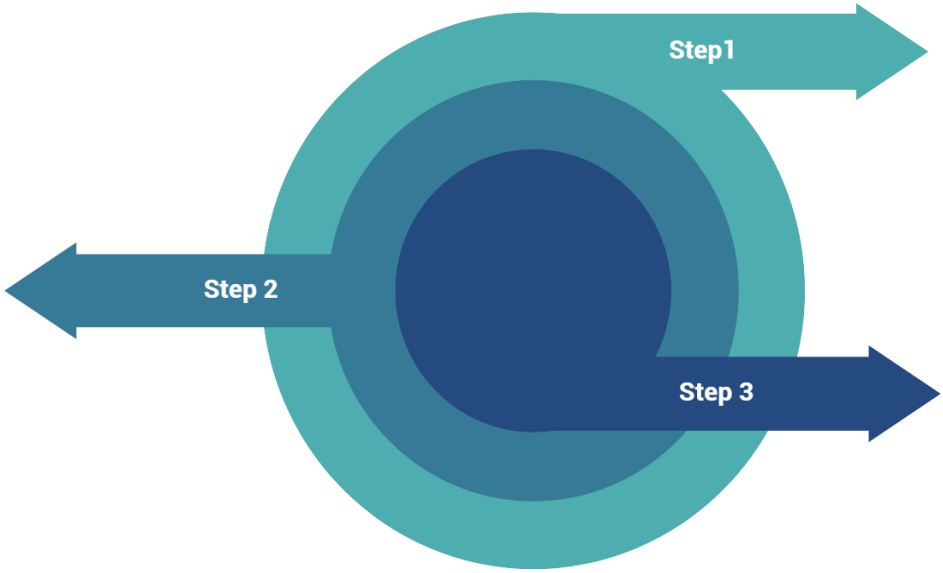
Low

The low risk level indicates lowest risk associated with a specific vulnerability instance. Such vulnerability may allow an attacker to gain some information about the application which was not intended to be known otherwise. The attacker may not have exploiting techniques available at that instance based on the information revealed by the system.

Informational

The recommended risk level indicates that some functionality or component is missing best practices implementation in the application. Such vulnerability may not have a risk associated with it currently, but it may become vulnerability in future due to change in application or due to exploiting techniques evolution or policy/legal requirements. The vulnerability mitigation depends upon owner's discretion; however, it is recommended to be mitigated if it not in line with the policy or law.

SCAN Type



Safe Checks

Essential measures in VAPT engagements that help to ensure that the assessment is conducted in a controlled and secure manner.

SANS Top 25

Lists the most dangerous software errors of the Common Weakness Enumeration (CWE) list that have been found in your web application

OWASP Top 10

Regularly-updated report outlining security concerns for web application security, focusing on the 10 most critical risks

Assessment Scope	The application security assessment is done: Grey-Box Penetration Testing
Assessment Date	The security vulnerabilities were reported for the following quarter on: 31st July 2025 to September 2025
Assessment Note	The Scope of the Assessment only focuses on the Web Application Coforge CAG.

List of Tools.

Scanning

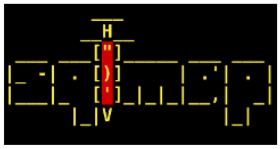




Enumeration



Expoloitation



Automation



Overall Findings

Pentest-ground Risk Assessment Analysis of the Entire Framework

Sr. No.	Hostname	Instant purpose	VAPT Status	Critical	High	Medium	Low	Informational	Total
1.	https://preoios.cag.gov.in/	Web App	Completed	0	8	9	8	0	25
Overall Findings				0	8	9	8	0	25

Test Case

Sr. No.	Test Case	Status
1	Business Logic Testing	Completed
2	Service Disruption Analysis	Completed
3	OWASP Top 10	Completed
4	Framework Based Vulnerability	Completed
5	Database Pentest	Completed

Vulnerabilities Found

https://preoios.cag.gov.in/

Sr.no	Vulnerability Name	Vulnerability Risk Type
1	Client-Side Authorization bypass leads to unauthorized malicious file upload - Audit Product	High
l2	Malicious File Upload -	
3	BAC - Client-Side Authorization bypass - search roles	
4	Malicious File Upload - Receipt Attachments	
5	BAC - Client-Side Authorization bypass - Receipts roles	
6	BAC - Client-Side Authorization bypass - search assessee for the report	
7	BAC - Client-Side Authorization bypass - select observations for report	
8	BAC - Client-Side Authorization bypass - update assessee details	
9	No Rate Limit on Login - Login	Medium
10	PII Disclosure in MyWorkReport Response	
11	PII Disclosure in Download My Graduation List Response	
12	PII Disclosure in Generate Offline Application Security Code Response	
13	PII Disclosure in Go to Send Items Response	
14	PII Disclosure in My Contribution Response	
15	PII Disclosure in MyEvents Response	
16	PII Disclosure in Profile Picture Response	
17	PII Disclosure in SendToListDashboard Response	
18	Error Based User Enumeration on Password Reset Page	Low
19	Concurrent Logins	
20	Text injection on error Page	
21	Missing Custom Error Page Leads to Server Version Disclosure	

22	Weak Content Security Policy	
23	Strict Transport Security Header Missing	
24	Overly Permissive Access-Control-Allow-Methods	
25	Unrestricted Access to Oracle Login Page via Directory Enumeration	

001	Client-Side Authorization bypass leads to unauthorized malicious file upload- Audit Product
URL	https://preoios.cag.gov.in/

Vulnerable Parameters: /

CVSS: 8.8- CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Severity: High

Vulnerability Description:

Client-side authorization bypass allows attackers to upload malicious files (e.g., web shells) to the audit product server by tampering with requests. Weak server-side validation enables remote code execution or data breaches. Mitigate with robust server-side checks, file type validation, and deny-by-default access policies.

Impact:

It can lead to the following impacts:

- Remote Code Execution: Malicious files like web shells enable attackers to execute arbitrary code, compromising the entire server.
- Data Breaches: Unauthorized file uploads expose sensitive audit data, leading to confidentiality violations and regulatory penalties.
- System Compromise: Malware can disrupt audit operations, causing downtime, financial loss, and reputational damage.
- Privilege Escalation: Attackers gain unauthorized access to administrative functions, enabling further exploitation of the system.

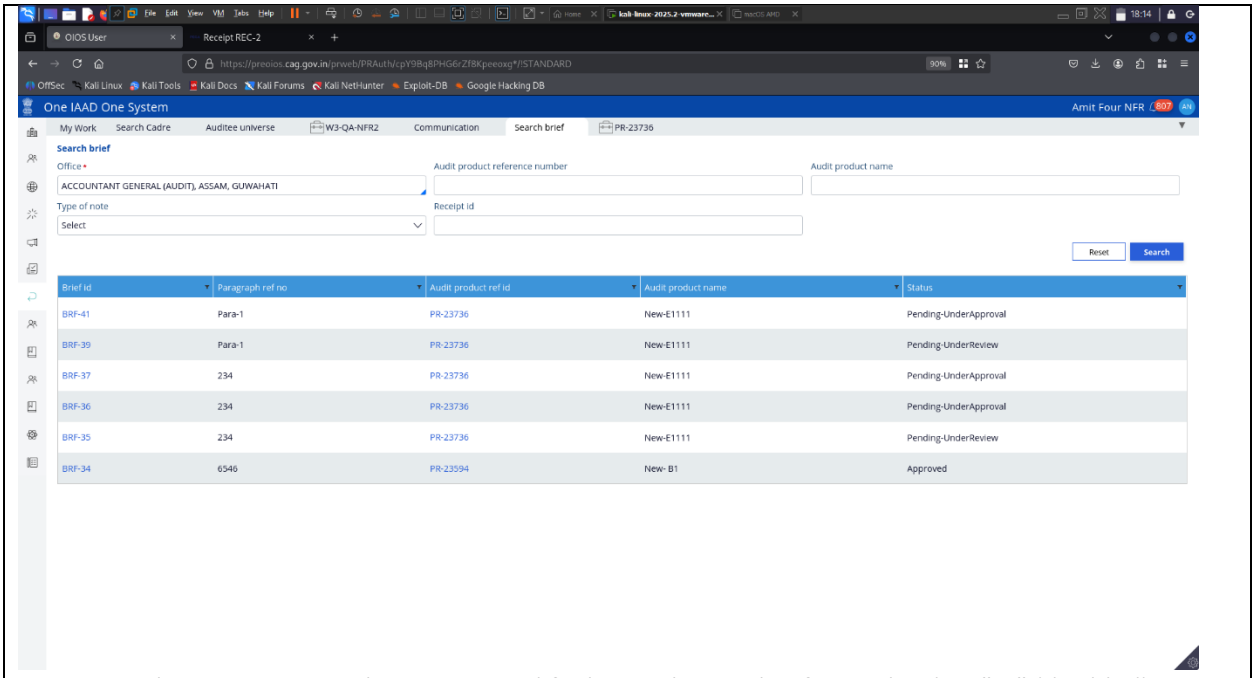
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

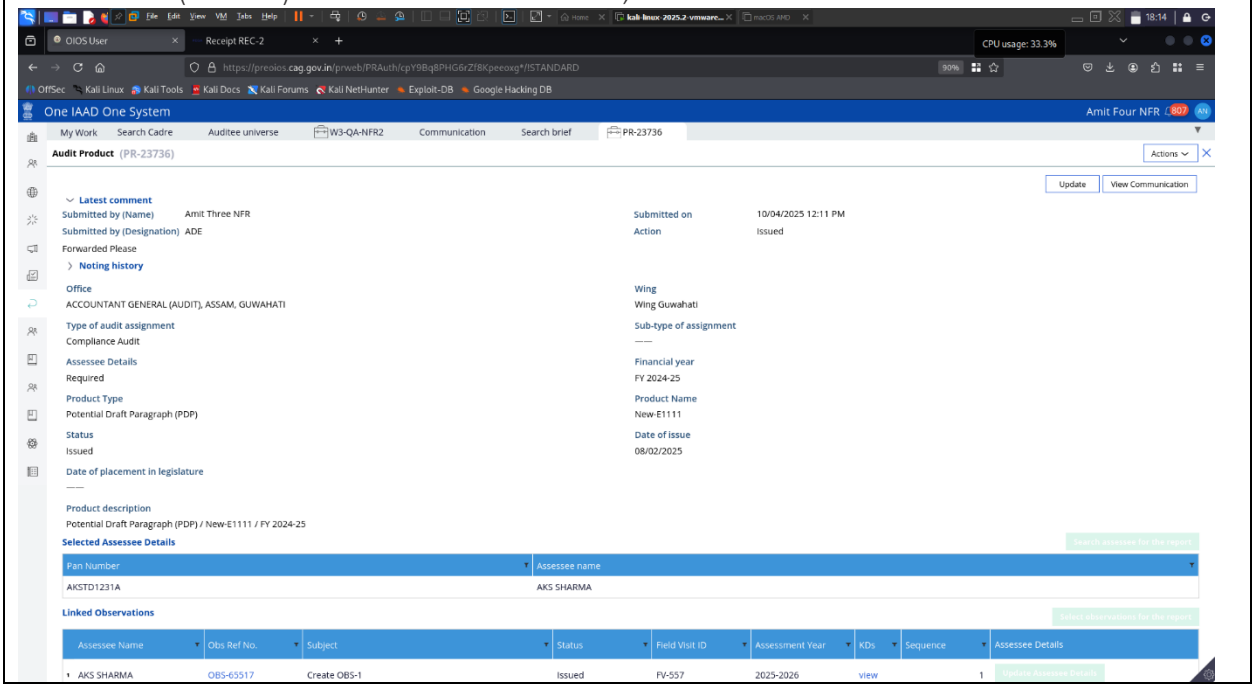
- Implement robust server-side authorization to validate all file upload requests, ensuring only authorized users can initiate uploads securely.
- Enforce strict file type validation using whitelists and scan content with antivirus tools to block malicious files effectively.
- Store uploads in non-executable directories with deny-by-default access policies to prevent unauthorized execution or access to files.
- Maintain comprehensive audit logs and real-time monitoring to detect and respond to suspicious upload attempts promptly.

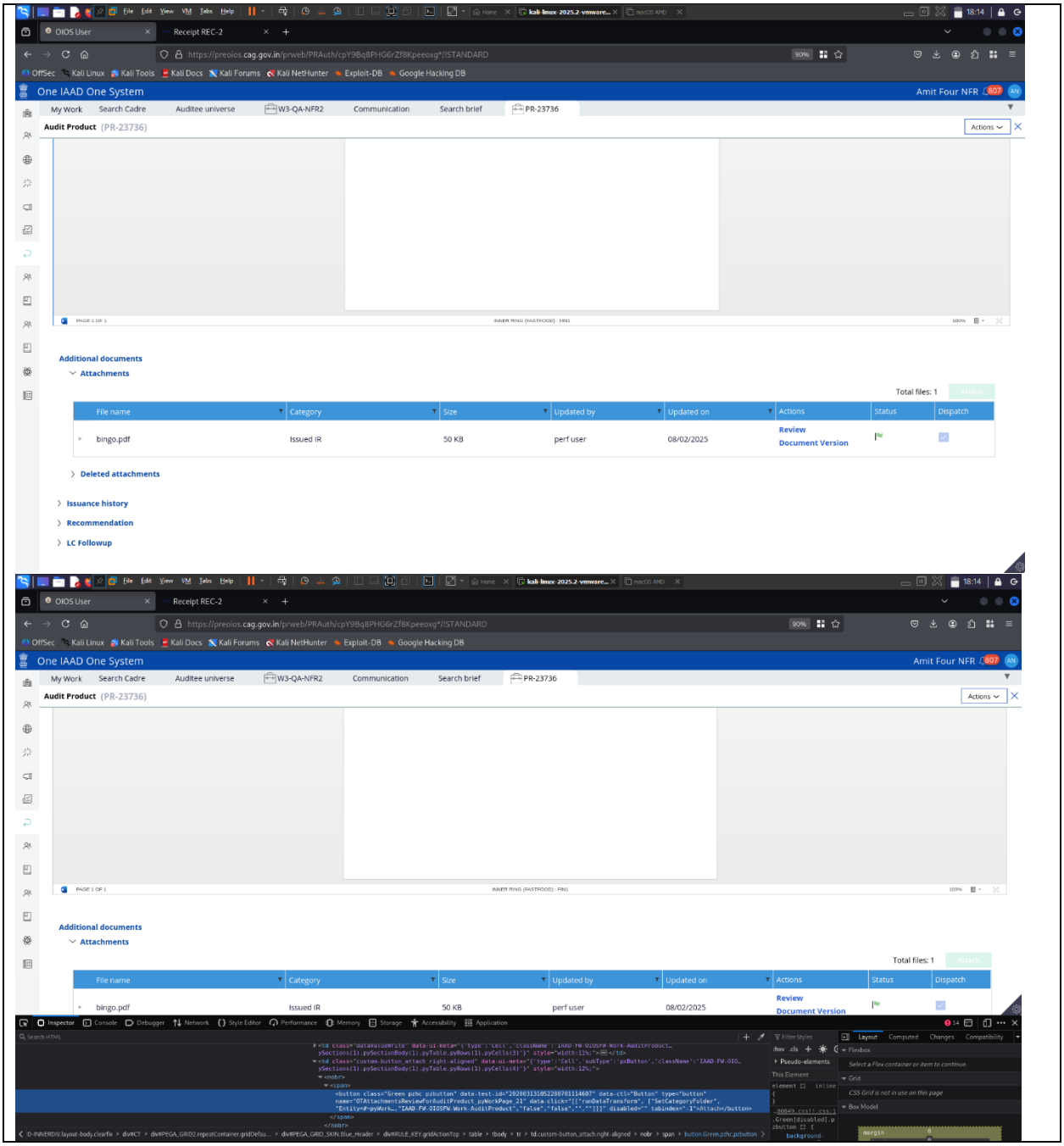
Proof of Concept:

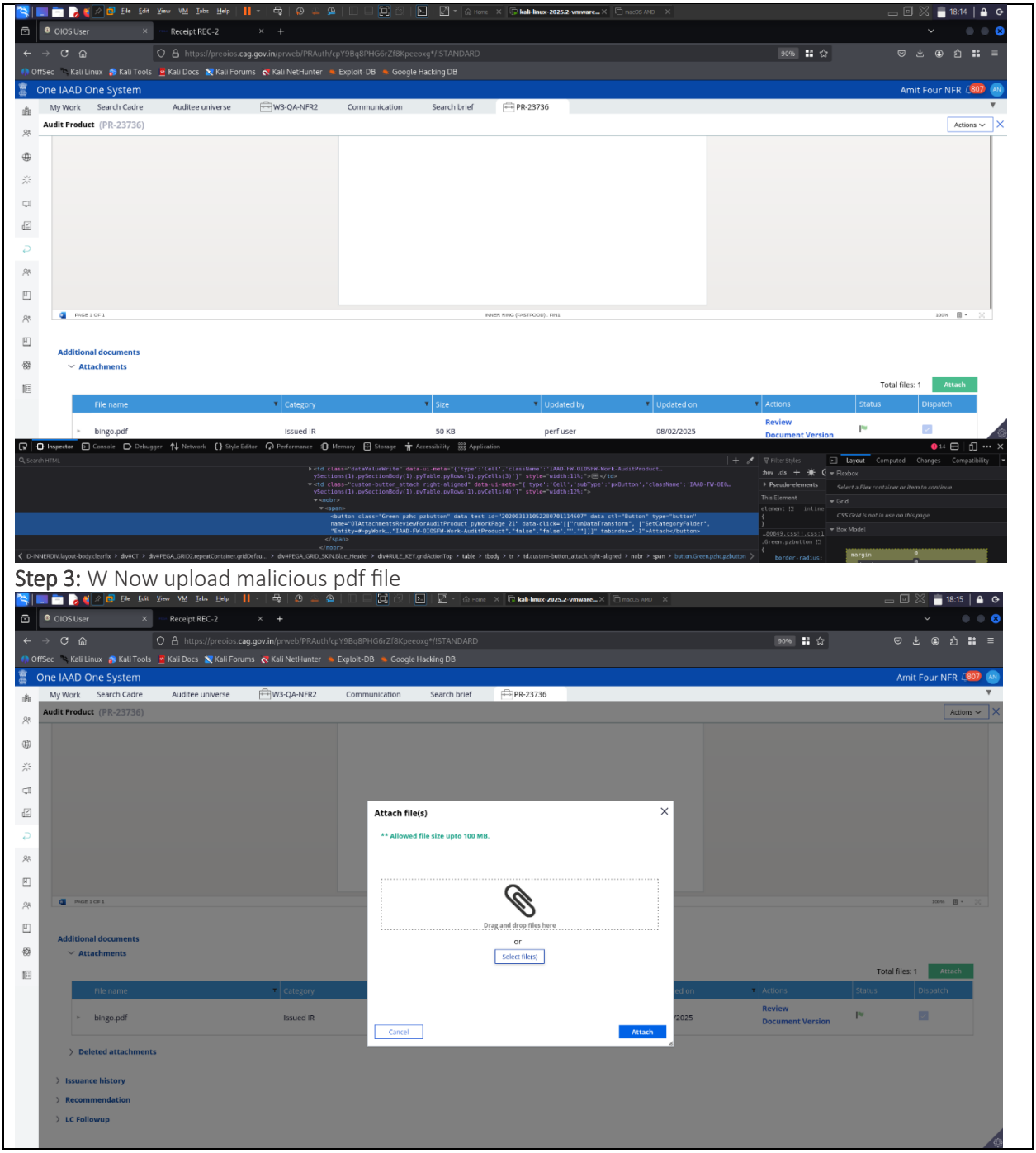
Step 1: Open the application and navigate to the Search brief > Audit Product ref id > section where the “Attach” button is disabled.



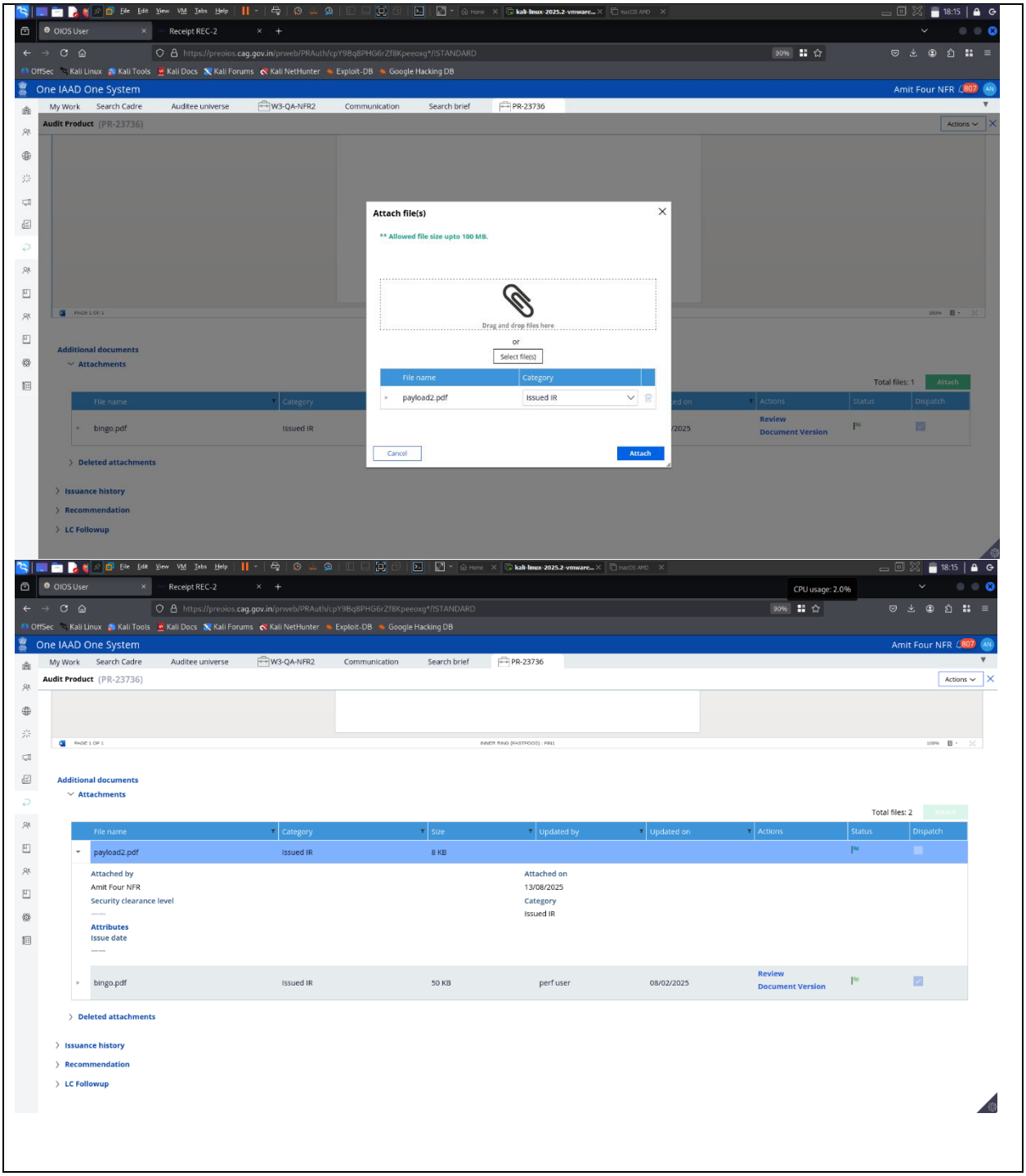
Step 2: Use browser Inspect Element → modify the attribute value from tabindex="-1" (disabled) to tabindex="1" (enabled). The button becomes active, and the restricted feature is now accessible.




One IAAD One System
Amit Four NFR
My Work
Search Cadre
Auditee universe
W3-QA-NFR2
Communication
Search brief
PR-23736
Audit Product (PR-23736)
Actions
Additional documents
Attachments
Total files: 1
File name
Category
Size
Updated by
Updated on
Actions
Status
Dispatch
bingo.pdf
Issued IR
50 KB
perf user
08/02/2025
Review
Document Version
Deleted attachments
Issuance history
Recommendation
LC Followup



Step 3: W Now upload malicious pdf file


One IAAD One System
Amit Four NFR
Audit Product (PR-23736)
Attach file(s)
** Allowed file size upto 100 MB.
Drag and drop files here
or
Select file(s)
File name
Category
payload2.pdf
Issued IR
Cancel
Attach
Additional documents
Attachments
bingo.pdf
Issued IR
Deleted attachments
Issuance history
Recommendation
LC Followup
CPU usage: 2.0%
Total files: 2
Size
Updated by
Updated on
Actions
Status
Dispatch
8 KB
Attached by
Amit Four NFR
Attached on
13/08/2025
Security clearance level
Category
Issued IR
Attributes
Issue date
50 KB
perf user
08/02/2025
Review
Document Version

002	Malicious File Upload
URL	https://preoios.cag.gov.in/

Vulnerable Parameters: /

CVSS: 8.8- CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Severity: High

Vulnerability Description:

Malicious file upload flaws let attackers upload harmful files (scripts, malware) due to poor validation of extensions or MIME types. Executable files can lead to server compromise or data theft. Prevent with server-side content scanning, whitelisting safe formats, and storing uploads outside the web root.

Impact:

It can lead to the following impacts:

- Server Compromise: Executable files can grant attackers full control, allowing data manipulation or system disruption.
- Data Theft: Malicious scripts extract sensitive user data, leading to privacy breaches and financial losses.
- Malware Spread: Infected files spread malware to users or systems, causing widespread operational and security issues.
- Compliance Violations: Unauthorized uploads breach regulatory standards, risking fines and legal consequences.

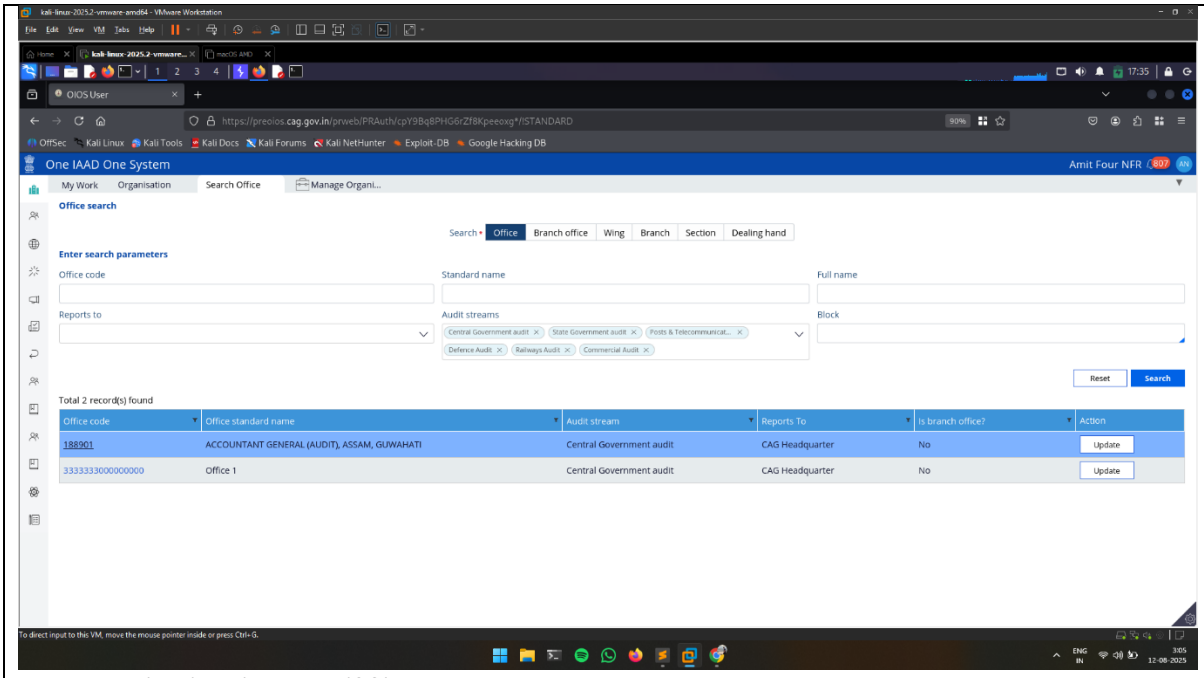
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

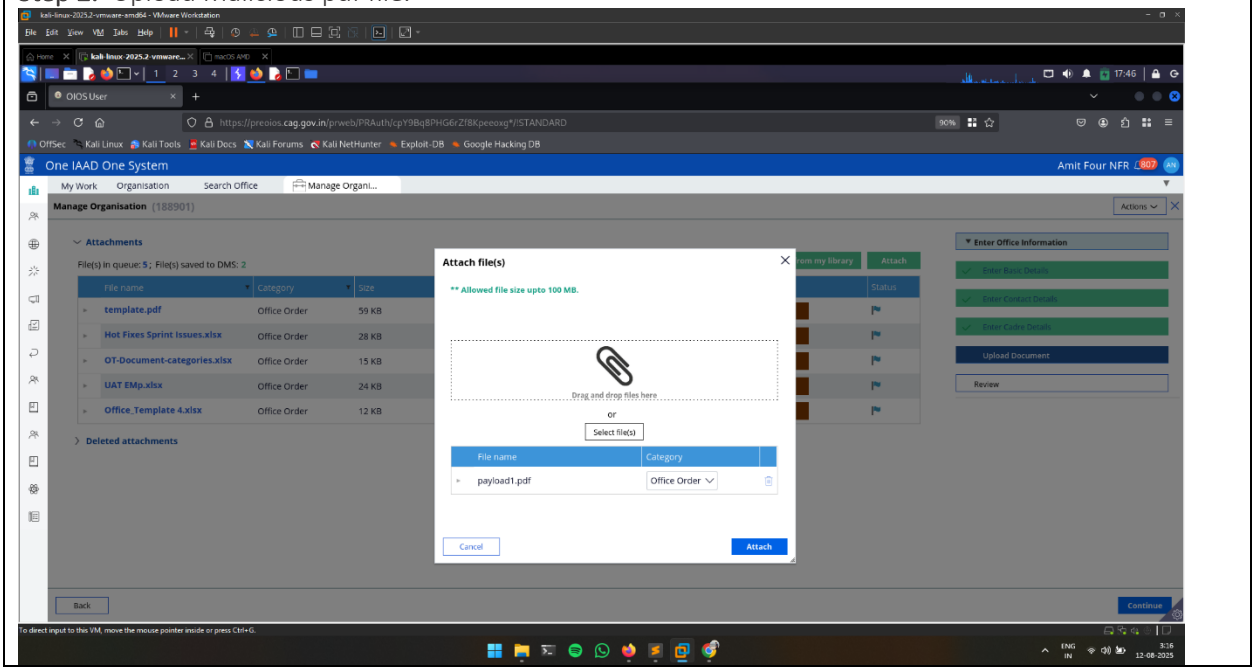
- Enforce server-side validation of file extensions and MIME types using strict whitelists to allow only safe file formats.
- Implement antivirus scanning for all uploaded files before storage to detect and block malware or harmful scripts effectively.
- Store files in isolated, non-web-accessible directories with randomized names to prevent direct access or execution risks.
- Apply file size limits and rate limiting to mitigate abuse, alongside logging to track upload patterns for anomalies.

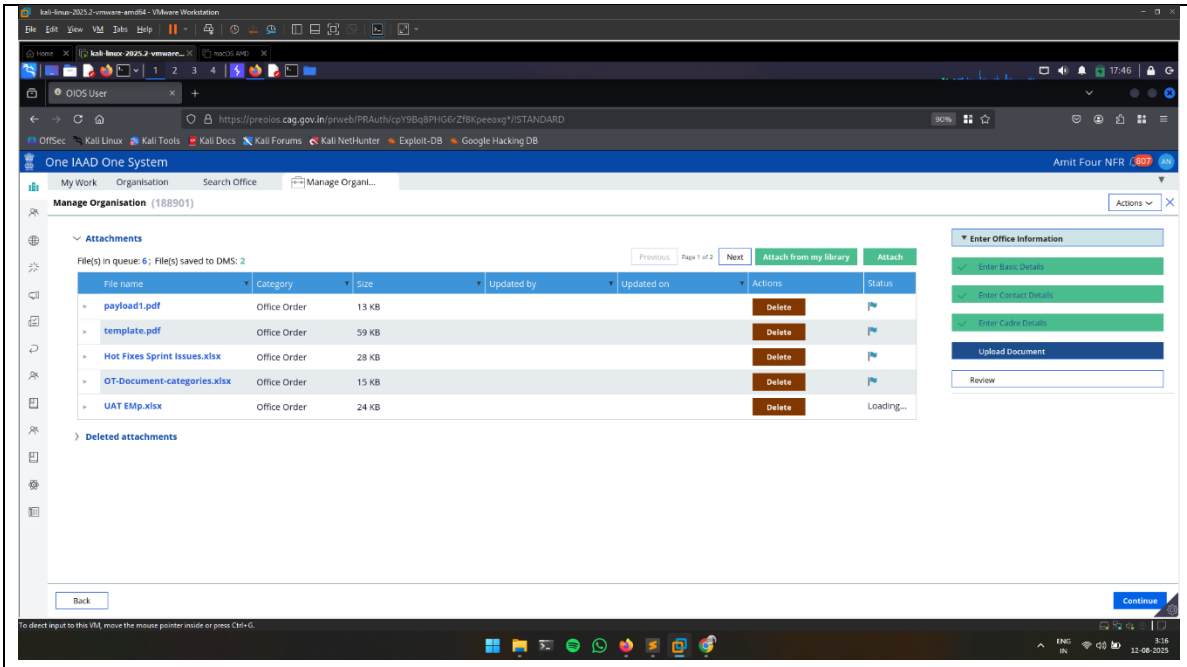
Proof of Concept:

Step 1: Open the application and navigate to the Search Office > Manage Organization section



Step 2: Upload Malicious pdf file.




One IAAD One System
Amit Four NFR
My Work
Organisation
Search Office
Manage Organi...
Manage Organisation (188901)
Actions
Attachments
File(s) in queue: 6 ; File(s) saved to DMS: 2
Previous
Next
Attach from my library
Attach
File name
Category
Size
Updated by
Updated on
Actions
Status
payload1.pdf
Office Order
13 KB
Delete
template.pdf
Office Order
59 KB
Delete
Hot Fixes Sprint Issues.xlsx
Office Order
28 KB
Delete
OT-Document-categories.xlsx
Office Order
15 KB
Delete
UAT EMp.xlsx
Office Order
24 KB
Delete
Loading...
Deleted attachments
Enter Office Information
Enter Basic Details
Enter Contact Details
Enter Cadre Details
Upload Document
Review
Back
Continue

003	BAC- Client-Side Authorization bypass- search roles
URL	https://preoios.cag.gov.in/

Vulnerable Parameters: /

CVSS: 8.1- CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Severity: High

Vulnerability Description:

Client-side role checks for searching roles are bypassable via request tampering, granting unauthorized access to sensitive role data. This risks privilege escalation or data leaks. Fix by enforcing server-side role-based access control (RBAC), validating user permissions, and logging access attempts to detect anomalies.

Impact:

It can lead to the following impacts:

- Privilege Escalation: Attackers access restricted roles, gaining unauthorized control over sensitive system functions.
- Data Exposure: Sensitive role data leaks, compromising user privacy and organizational security.
- System Misuse: Unauthorized role access enables fraudulent activities, disrupting operations and trust.
- Compliance Risks: Breaches in role access violate regulatory standards, leading to penalties.

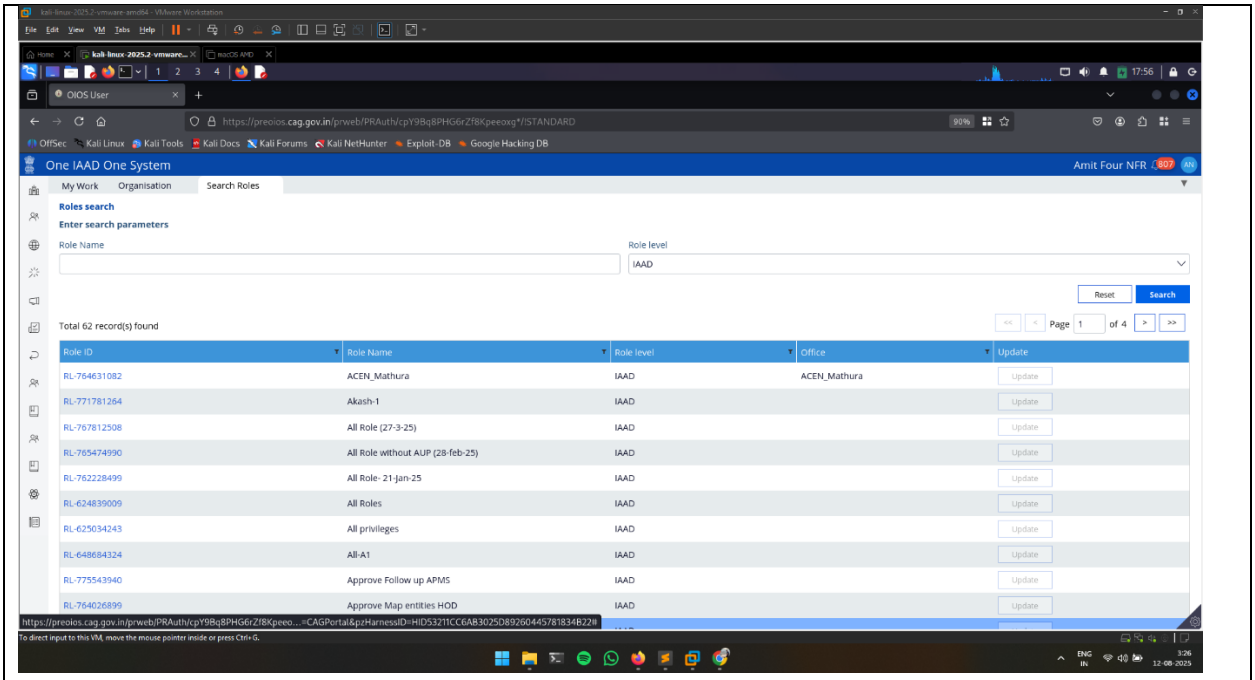
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

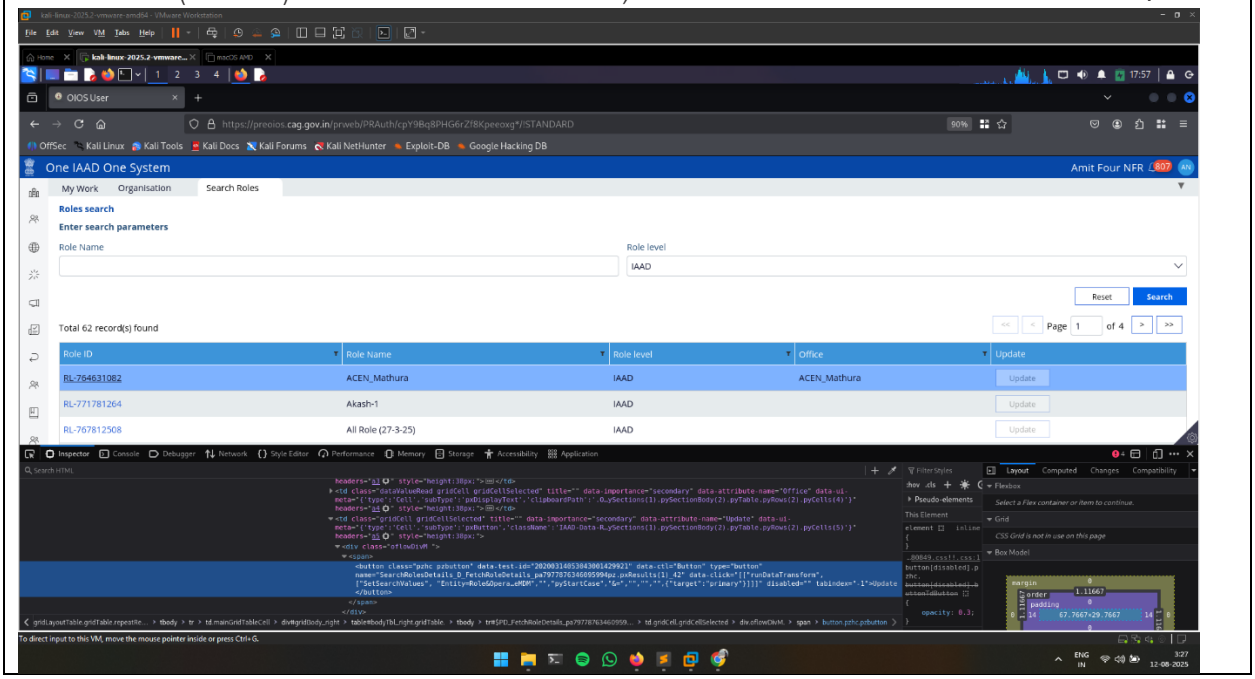
- Enforce server-side role-based access control (RBAC) to validate user permissions for role searches, preventing unauthorized data access.
- Use secure session tokens and encrypted channels to protect requests from tampering or interception during role searches.
- Implement detailed audit logging to track all search attempts, enabling detection of unauthorized access or suspicious behavior.
- Parameterize search queries to prevent injection attacks, ensuring only authorized role data is accessible to users.

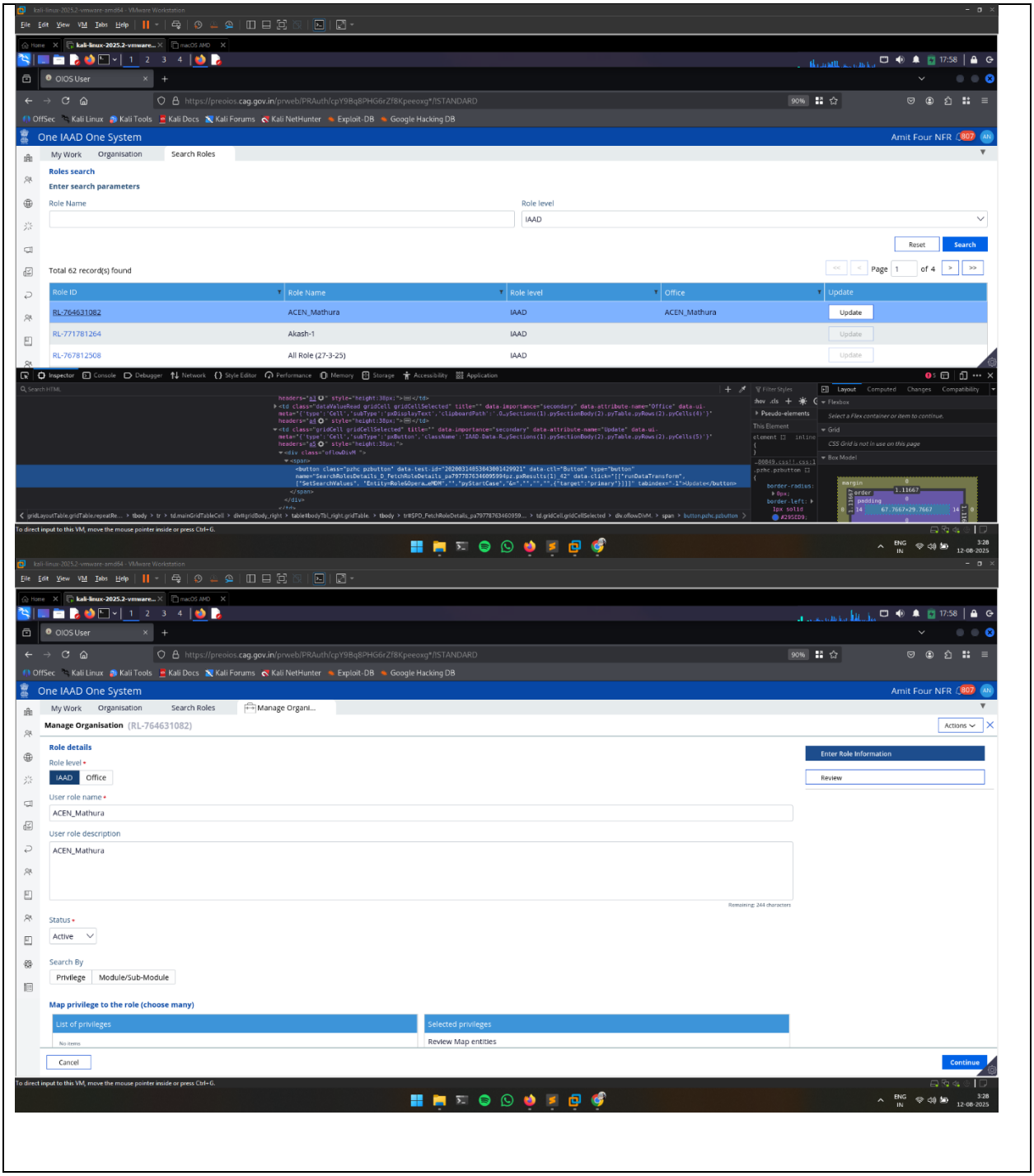
Proof of Concept:

Step 1: Open the application and navigate to the Search roles section where the “Update” button is disabled.



Step 2: Use browser Inspect Element → modify the attribute value from tabindex="-1" (disabled) to tabindex="1" (enabled). The button becomes active, and the restricted feature is now accessible.




One IAAD One System
Amit Four NFR
My Work
Organisation
Search Roles
Roles search
Enter search parameters
Role Name
Role level
IAAD
Reset
Search
Total 62 record(s) found
Role ID
Role Name
Role level
Office
Update
RL-764631082
ACEN_Mathura
IAAD
ACEN_Mathura
RL-771781264
Akash-1
IAAD
RL-767812508
All Role (27-3-25)
IAAD
Manage Organisation (RL-764631082)
Actions
Role details
Role level
IAAD
Office
User role name
ACEN_Mathura
User role description
ACEN_Mathura
Enter Role Information
Review
Status
Active
Search By
Privilege
Module/Sub-Module
Map privilege to the role (choose many)
List of privileges
Selected privileges
Review Map entities
Cancel
Continue

004	Malicious File Upload- Receipt Attachments
URL	https://preoios.cag.gov.in/

Vulnerable Parameters: /

CVSS: 8.8- CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Severity: High

Vulnerability Description:

Weak validation in receipt attachments allows uploading disguised malicious files (e.g., scripts as PDFs). This risks malware execution, data theft, or system compromise. Secure with server-side content scanning, whitelisting file types, random file renaming, and antivirus checks before storage or retrieval.

Impact:

It can lead to the following impacts:

- Malware Execution: Disguised scripts execute on servers or user devices, compromising systems and data.
- Financial Fraud: Malicious files manipulate receipt data, enabling fraudulent transactions or theft.
- Data Breaches: Sensitive financial details leak, causing privacy violations and reputational harm.
- Operational Disruption: Malware disrupts receipt processing, leading to delays and financial losses.

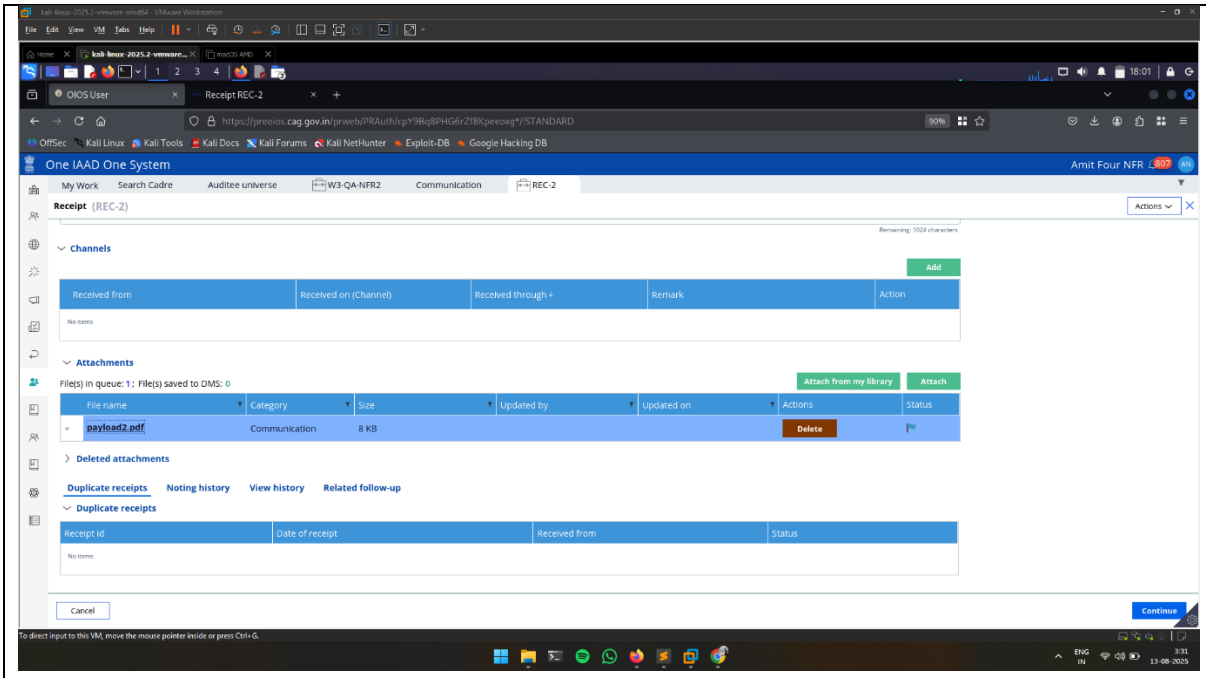
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

- Validate uploaded receipt attachments server-side with strict MIME type checks and whitelists to allow only safe formats.
- Integrate antivirus scanning for attachments before storage or retrieval to block disguised scripts or malware effectively.
- Store files in isolated, non-executable directories with random naming to prevent unauthorized access or execution risks.
- Enforce file size limits and monitor upload patterns, logging all attempts to detect and respond to anomalies.

Proof of Concept:

Step 1: We can observe that we are able to upload malicious pdf file.


One IAAD One System
Amit Four NFR
My Work
Search Cadre
Auditee universe
W3-QA-NFR2
Communication
REC-2
Receipt (REC-2)
Actions
Channels
Add
Received from
Received on (Channel)
Received through
Remark
Action
No items
Attachments
File(s) in queue: 1 ; File(s) saved to DMS: 0
Attach from my library
Attach
File name
Category
Size
Updated by
Updated on
Actions
Status
payload2.pdf
Communication
8 KB
Delete
Deleted attachments
Duplicate receipts
Noting history
View history
Related follow-up
Duplicate receipts
Receipt id
Date of receipt
Received from
Status
No items
Cancel
Continue

005	BAC- Client-Side Authorization bypass- Receipts roles
URL	https://preoios.cag.gov.in/

Vulnerable Parameters: /

CVSS: 8.1- CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Severity: High

Vulnerability Description:

Client-side receipt role checks can be bypassed by altering requests, allowing unauthorized access or modification of receipts. This risks financial fraud or data breaches. Mitigate with server-side RBAC, secure session management, and audit logs to ensure only authorized users access receipt functionalities.

Impact:

It can lead to the following impacts:

- Financial Fraud: Unauthorized receipt access enables manipulation, leading to monetary losses or fraudulent transactions.
- Data Leakage: Sensitive receipt data exposure compromises user privacy and organizational trust.
- Operational Disruption: Unauthorized modifications delay financial processes, impacting business operations.
- Regulatory Non-compliance: Breaches in access controls violate financial regulations, risking penalties.

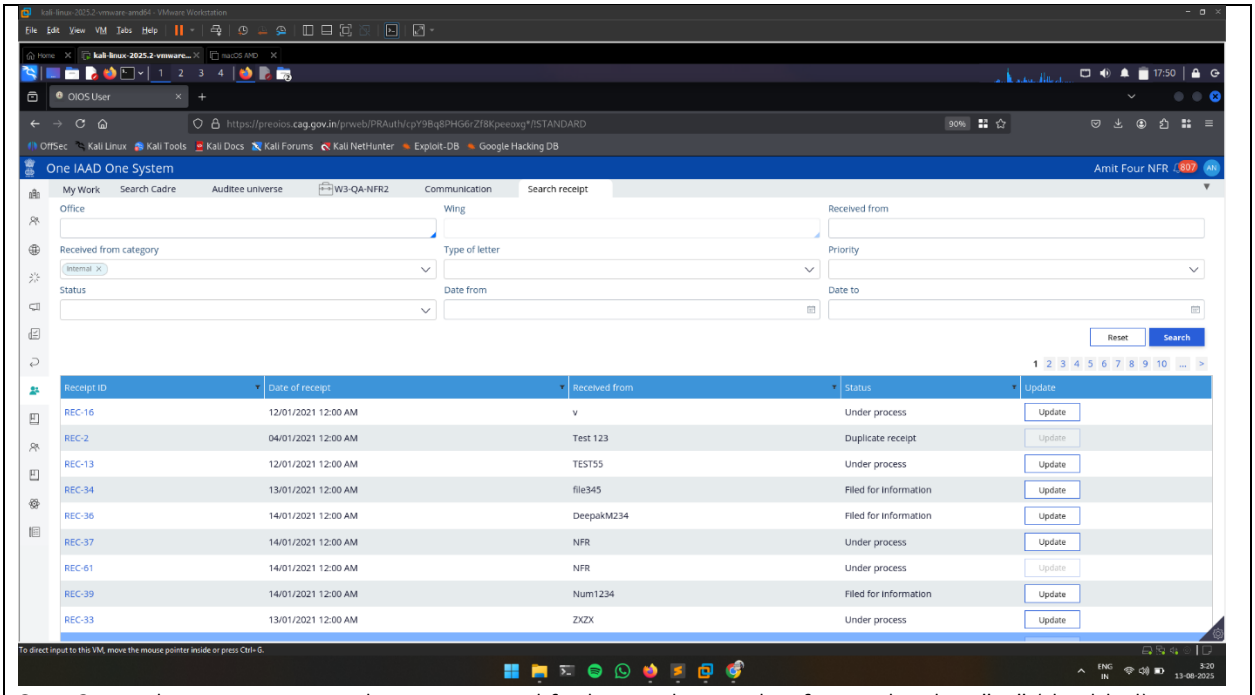
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

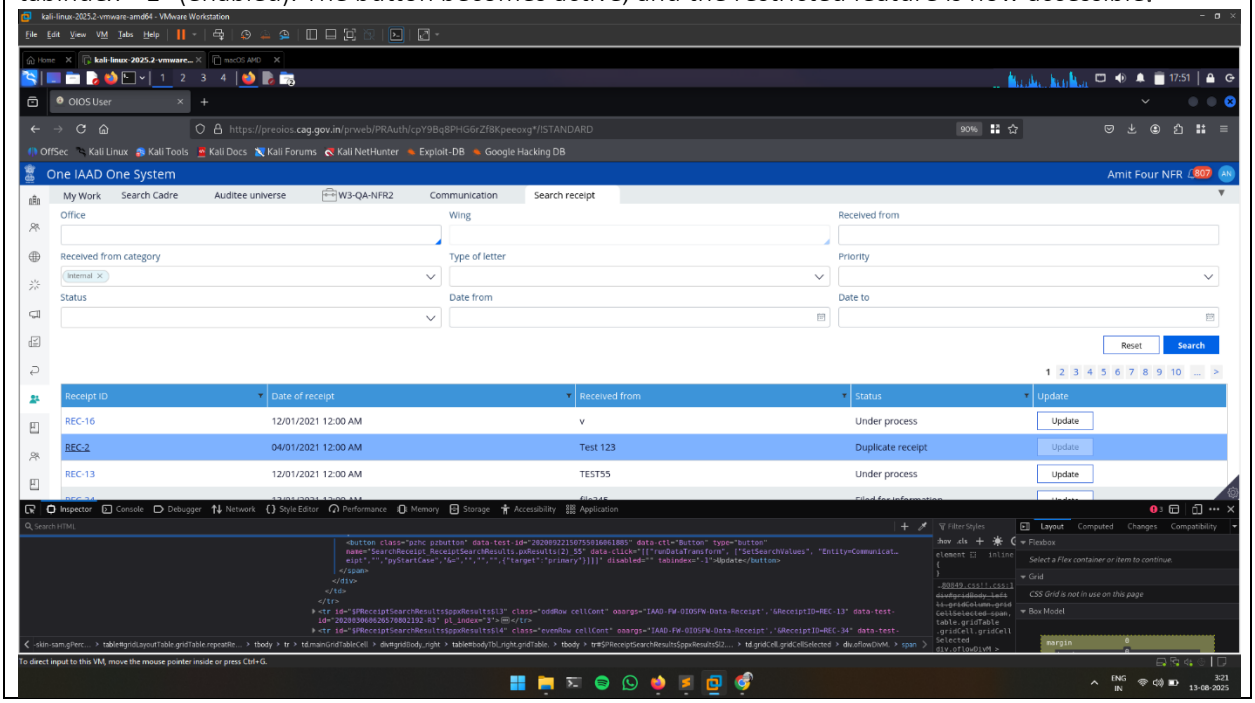
- Implement server-side RBAC to restrict receipt access and modifications to authorized users, preventing unauthorized tampering or access.
- Use secure session management with encrypted tokens to ensure requests are validated against user roles securely.
- Maintain detailed audit logs for all receipt-related actions to track access and detect unauthorized attempts promptly.
- Require multi-factor authentication for sensitive receipt operations to add an additional layer of security against fraud.

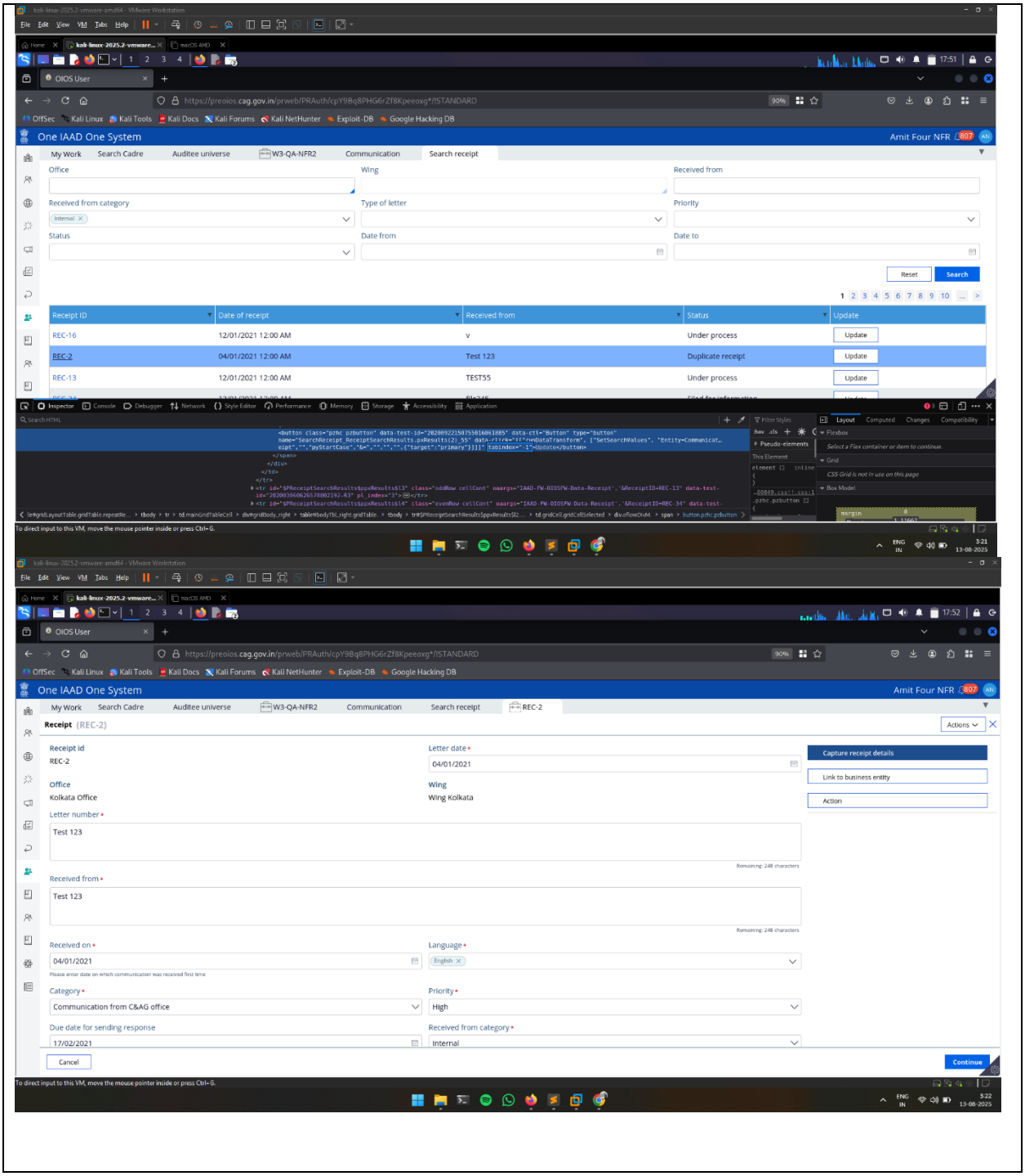
Proof of Concept:

Step 1: Open the application and navigate to the Search receipt section where the “Update” button is disabled.



Step 2: Use browser Inspect Element → modify the attribute value from tabindex="-1" (disabled) to tabindex="1" (enabled). The button becomes active, and the restricted feature is now accessible.




One IAAD One System
Amit Four NFR
My Work
Search Cadre
Auditee universe
W3-QA-NFR2
Communication
Search receipt
Office
Wing
Received from
Received from category
Type of letter
Priority
Status
Date from
Date to
Reset
Search
Receipt ID
Date of receipt
Received from
Status
Update
REC-16
12/01/2021 12:00 AM
v
Under process
REC-2
04/01/2021 12:00 AM
Test 123
Duplicate receipt
REC-13
12/01/2021 12:00 AM
TEST55
Under process
One IAAD One System
Amit Four NFR
REC-2
Receipt (REC-2)
Actions
Receipt id
REC-2
Letter date
04/01/2021
Capture receipt details
Link to business entity
Action
Office
Kolkata Office
Wing
Wing Kolkata
Letter number
Test 123
Received from
Test 123
Received on
04/01/2021
Language
English
Category
Communication from C&AG office
Priority
High
Due date for sending response
17/02/2021
Received from category
Internal
Cancel
Continue

006	BAC- Client-Side Authorization bypass- search assessee for the report
URL	https://preoios.cag.gov.in/

Vulnerable Parameters: /

CVSS: 8.1- CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Severity: High

Vulnerability Description:

Client-side bypass in assessee search allows unauthorized access to sensitive taxpayer data via tampered requests. This risks data leakage or compliance issues. Prevent with server-side RBAC, parameterized queries, and audit logs to validate and track search requests against user permissions.

Impact:

It can lead to the following impacts:

- Data Leakage: Unauthorized access to assessee data exposes sensitive financial or personal information.
- Compliance Violations: Breaches in taxpayer data access risk non-compliance with tax regulations, leading to fines.
- Fraud Risk: Exposed assessee details enable targeted fraud or identity theft.
- Reputational Damage: Data leaks erode trust in the organization's security practices.

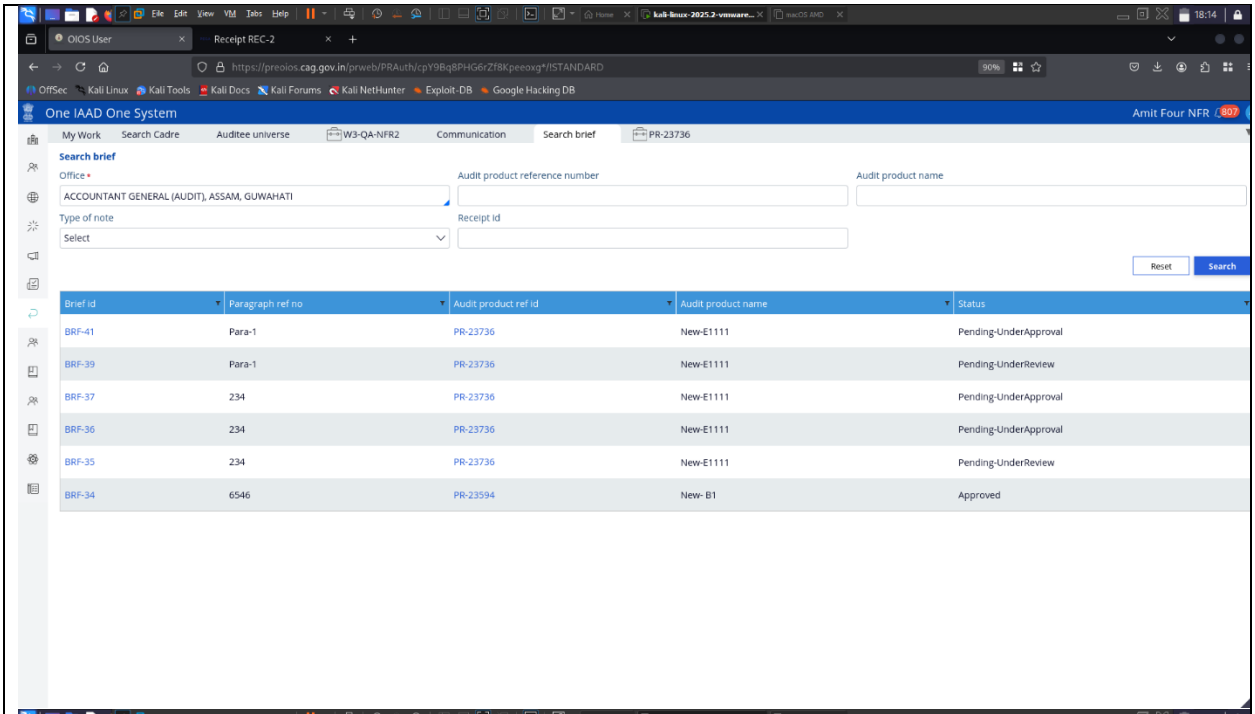
Recommendation:

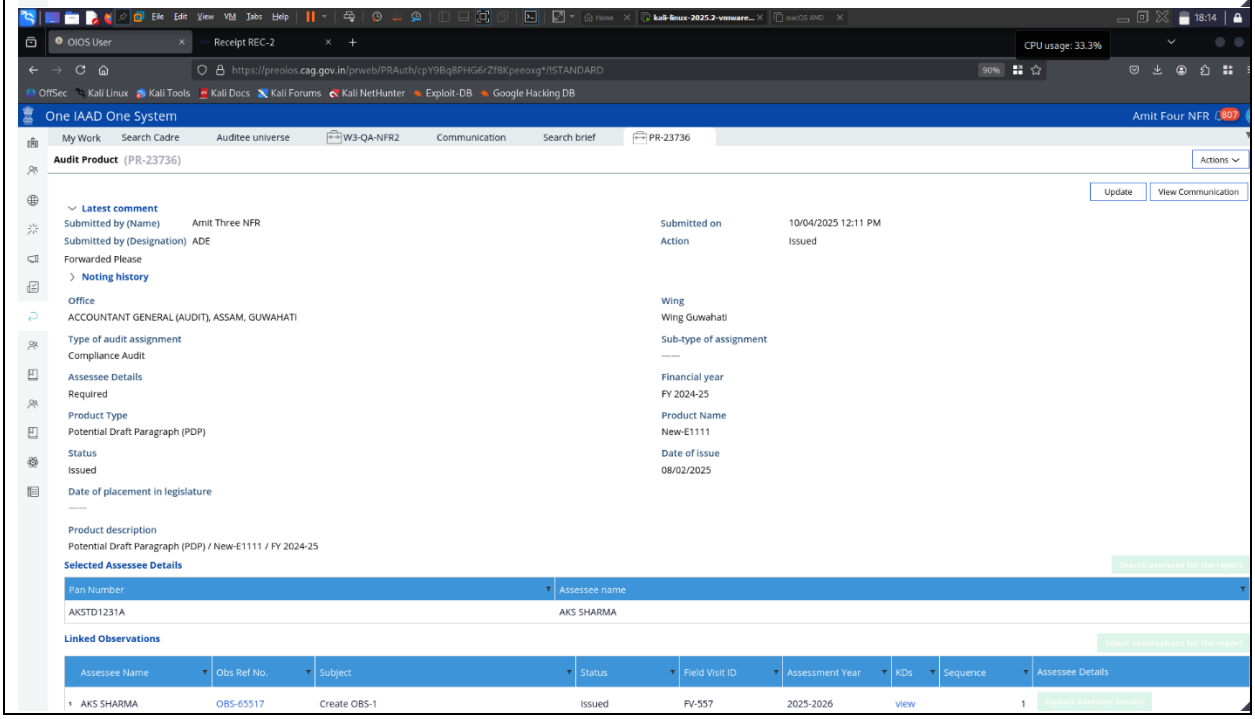
We recommend the following security measures to mitigate the vulnerability:

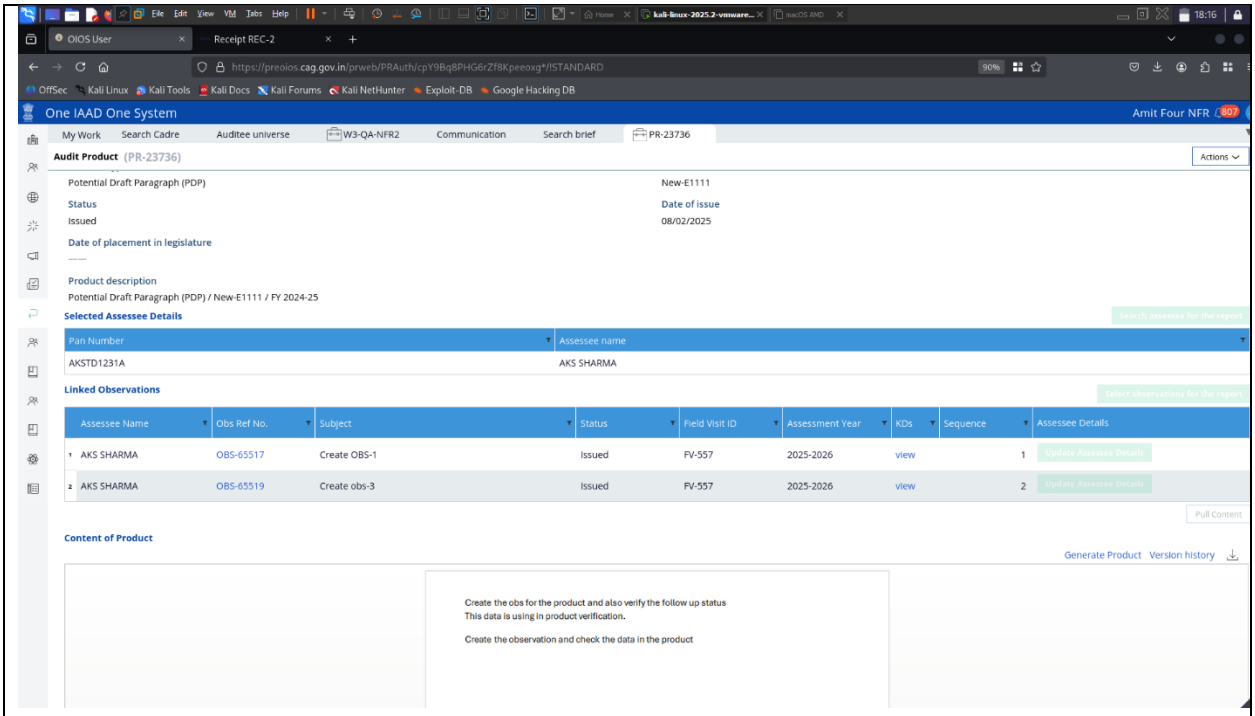
- Enforce server-side RBAC to restrict assessee search access, ensuring only authorized users can query sensitive taxpayer data.
- Use parameterized queries and input validation to prevent injection and ensure searches align with user permissions.
- Implement audit logs to track all search requests, enabling monitoring and detection of unauthorized access attempts.
- Apply data masking for sensitive search results, ensuring only permitted data is displayed based on user roles.

Proof of Concept:

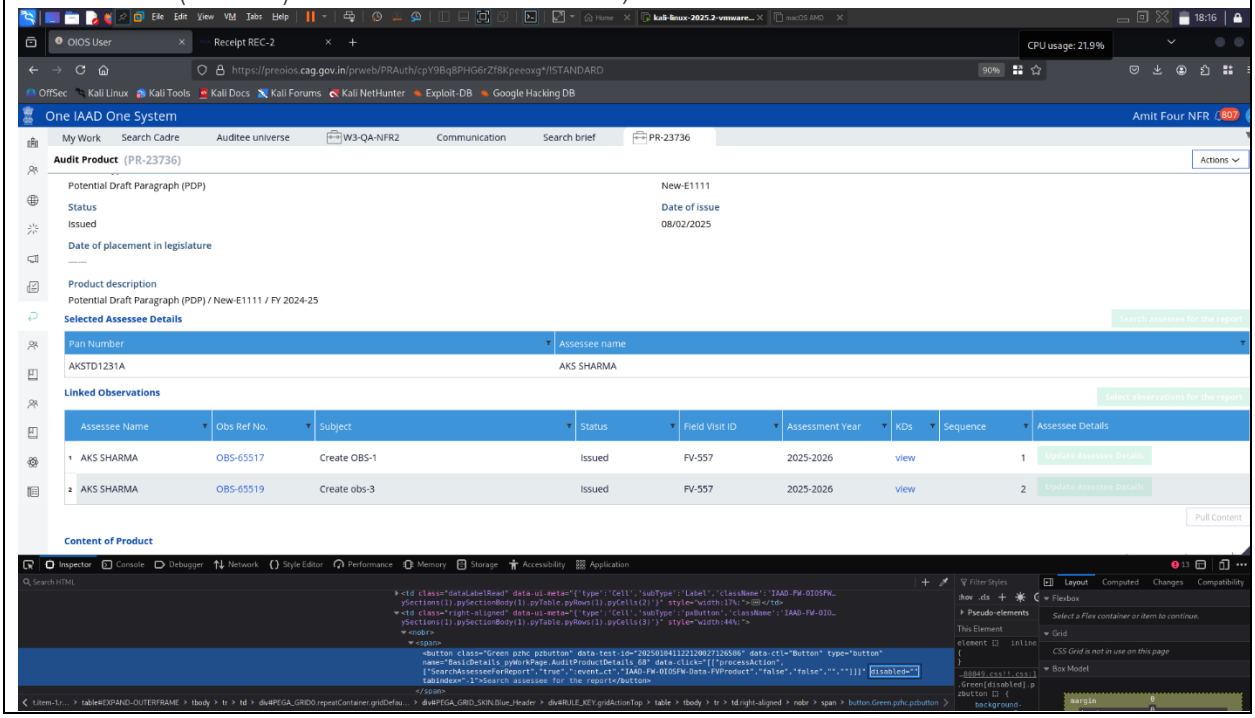
Step 1: Open the application and navigate to the Search brief > Audit Product ref id > section where the "Search assessee for the report" button is disabled.

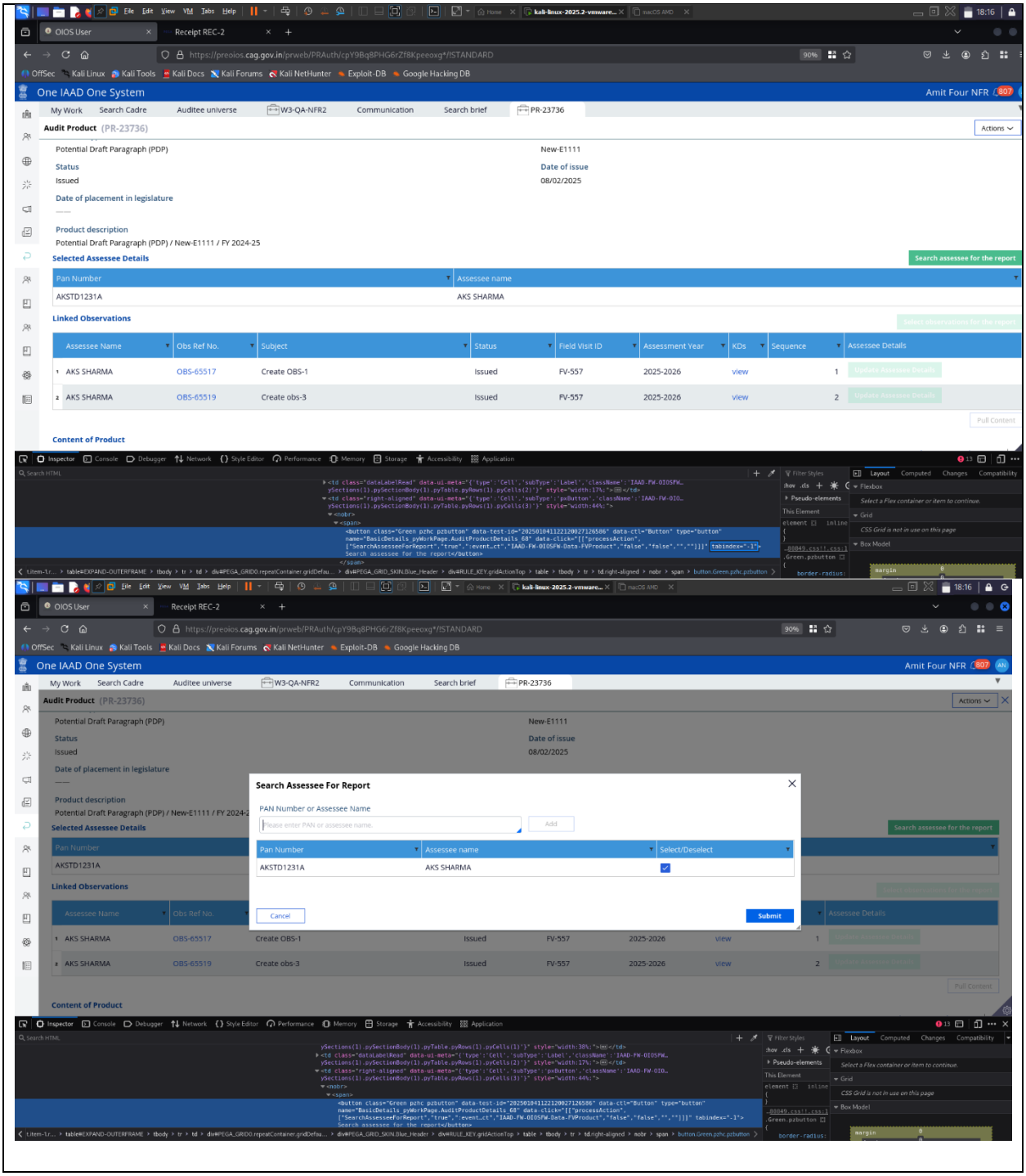

OIOS User
Receipt REC-2
https://preoios.cag.gov.in/prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!STANDARD
One IAAD One System
Amit Four NFR
My Work
Search Cadre
Auditee universe
W3-QA-NFR2
Communication
Search brief
PR-23736
Search brief
Office
ACCOUNTANT GENERAL (AUDIT), ASSAM, GUWAHATI
Audit product reference number
Audit product name
Type of note
Select
Receipt id
Reset
Search
Brief id
Paragraph ref no
Audit product ref id
Audit product name
Status
BRF-41
Para-1
PR-23736
New-E1111
Pending-UnderApproval
BRF-39
Para-1
PR-23736
New-E1111
Pending-UnderReview
BRF-37
234
PR-23736
New-E1111
Pending-UnderApproval
BRF-36
234
PR-23736
New-E1111
Pending-UnderApproval
BRF-35
234
PR-23736
New-E1111
Pending-UnderReview
BRF-34
6546
PR-23594
New- B1
Approved


CPU usage: 33.3%
OIOS User
Receipt REC-2
https://preoios.cag.gov.in/prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!STANDARD
One IAAD One System
Amit Four NFR
My Work
Search Cadre
Auditee universe
W3-QA-NFR2
Communication
Search brief
PR-23736
Audit Product (PR-23736)
Actions
Update
View Communication
Latest comment
Submitted by (Name) Amit Three NFR
Submitted by (Designation) ADE
Submitted on 10/04/2025 12:11 PM
Action Issued
Forwarded Please
Noting history
Office
ACCOUNTANT GENERAL (AUDIT), ASSAM, GUWAHATI
Wing
Wing Guwahati
Type of audit assignment
Compliance Audit
Sub-type of assignment
Assessee Details
Required
Financial year
FY 2024-25
Product Type
Potential Draft Paragraph (PDP)
Product Name
New-E1111
Status
Issued
Date of issue
08/02/2025
Date of placement in legislature
Product description
Potential Draft Paragraph (PDP) / New-E1111 / FY 2024-25
Selected Assessee Details
Pan Number
Assessee name
AKSTD1231A
AKS SHARMA
Linked Observations
Assessee Name
Obs Ref No.
Subject
Status
Field Visit ID
Assessment Year
KDs
Sequence
Assessee Details
1 AKS SHARMA
OBS-65517
Create OBS-1
Issued
FV-557
2025-2026
view
1



Step 2: Use browser Inspect Element → modify the attribute value from tabindex="-1" (disabled) to tabindex="1" (enabled). The button becomes active, and the restricted feature is now accessible.




One IAAD One System
Amit Four NFR
My Work
Search Cadre
Auditee universe
W3-QA-NFR2
Communication
Search brief
PR-23736
Audit Product (PR-23736)
Actions
Potential Draft Paragraph (PDP)
New-E1111
Status
Issued
Date of issue
08/02/2025
Date of placement in legislature
Product description
Potential Draft Paragraph (PDP) / New-E1111 / FY 2024-25
Selected Assessee Details
Search assessee for the report
Pan Number
Assessee name
AKSTD1231A
AKS SHARMA
Linked Observations
Assessee Name
Obs Ref No.
Subject
Status
Field Visit ID
Assessment Year
KDs
Sequence
Assessee Details
AKS SHARMA
OBS-65517
Create OBS-1
Issued
FV-557
2025-2026
view
1
AKS SHARMA
OBS-65519
Create obs-3
Issued
FV-557
2025-2026
view
2
Content of Product
Search Assessee For Report
PAN Number or Assessee Name
Please enter PAN or assessee name.
Add
Select/Deselect
Cancel
Submit

007	BAC- Client-Side Authorization bypass- select observations for report
URL	https://preoios.cag.gov.in/

Vulnerable Parameters: /

CVSS: 8.1- CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Severity: High

Vulnerability Description:

Bypassing client-side controls for selecting report observations allows unauthorized data inclusion, risking inaccurate reports or data exposure. Fix by enforcing server-side authorization, validating observation selections against user roles, and using secure APIs to ensure only permitted data is accessed.

Impact:

It can lead to the following impacts:

- Inaccurate Reports: Unauthorized observation selection leads to false reporting, impacting decision-making.
- Data Exposure: Sensitive observation data leaks, compromising confidentiality and trust.
- Compliance Issues: Manipulated reports violate audit standards, risking regulatory penalties.
- Operational Errors: Incorrect data inclusion disrupts audit processes, causing delays.

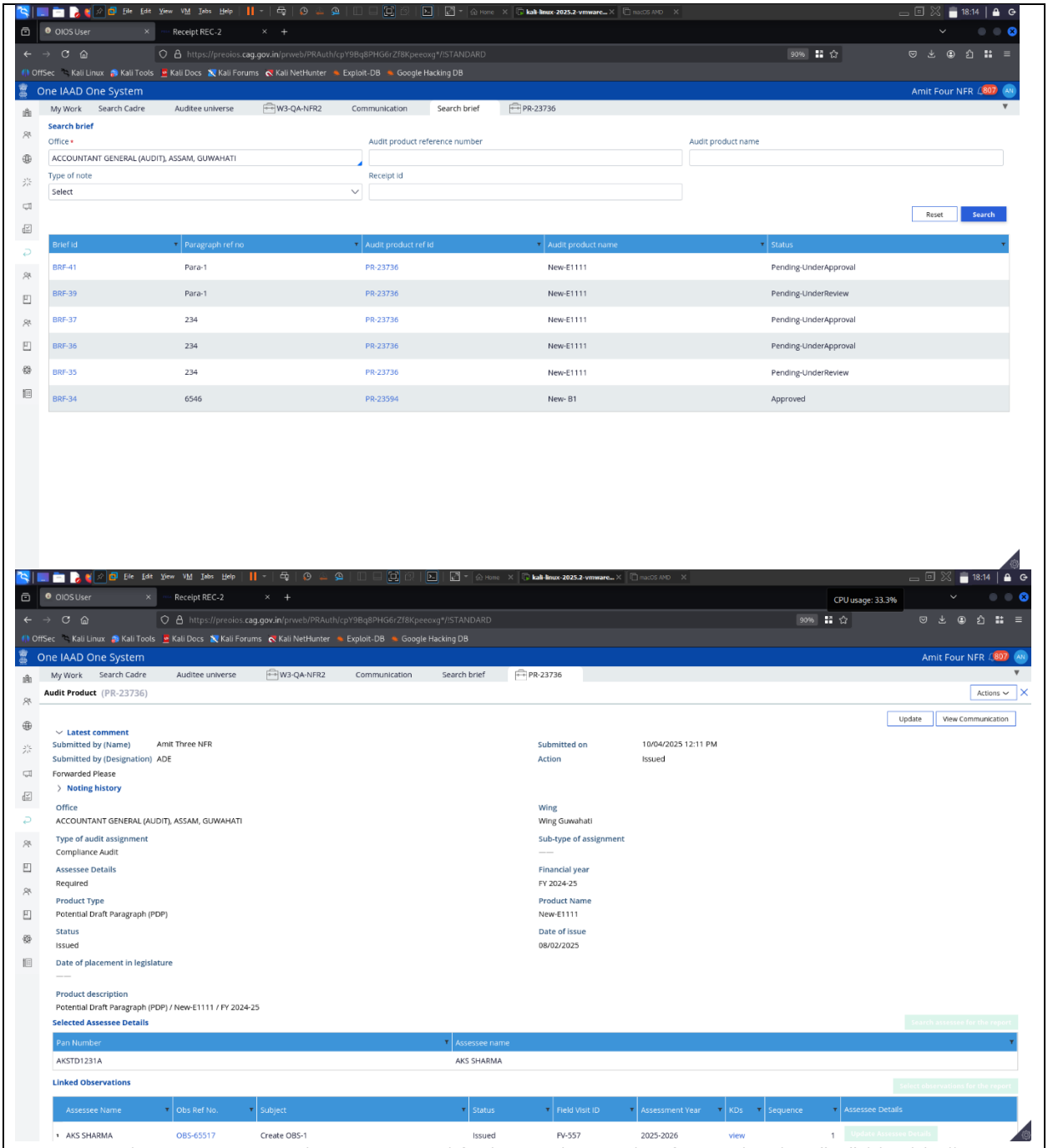
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

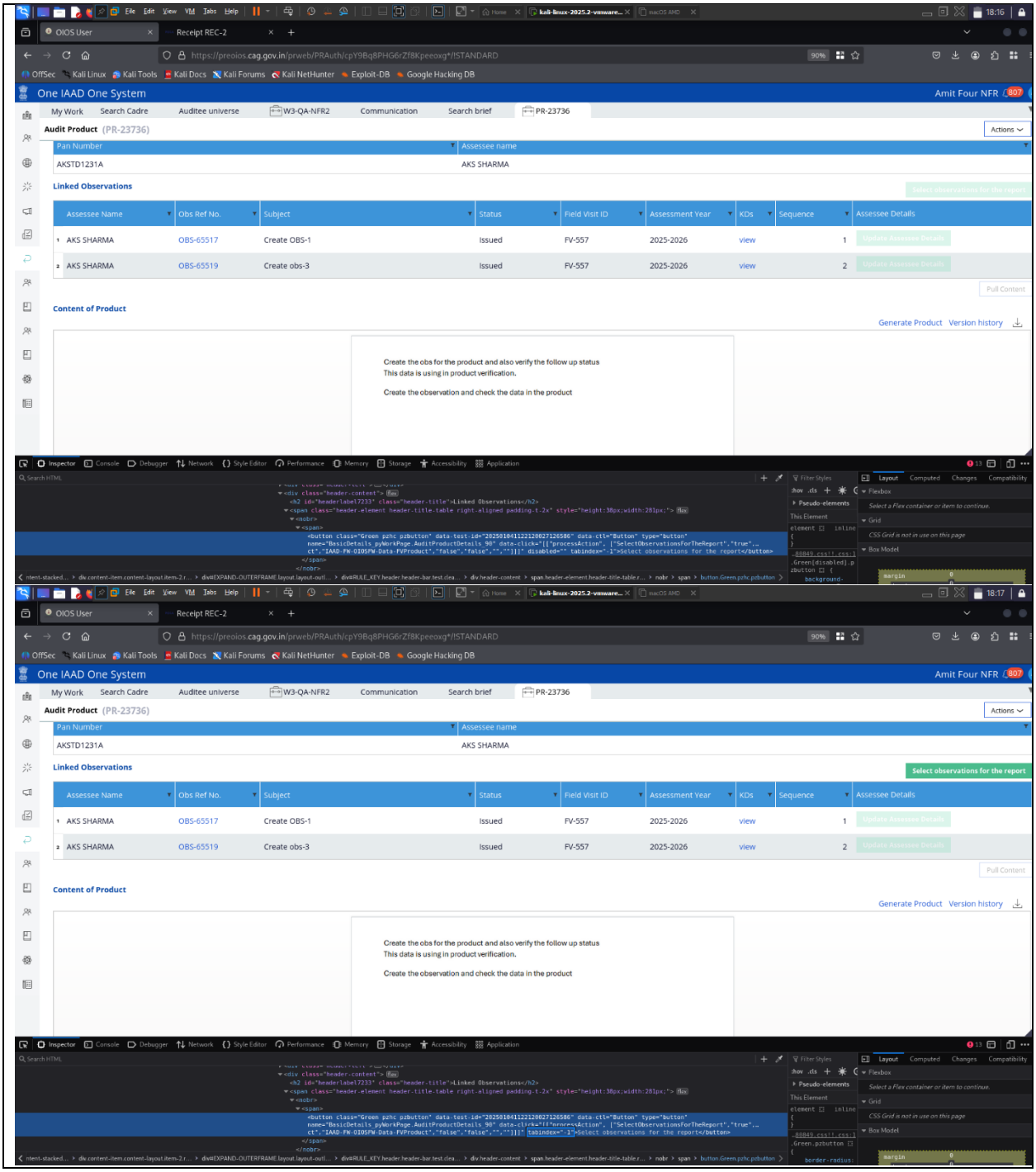
- Enforce server-side authorization to validate observation selections, ensuring only authorized users can include data in reports.
- Use secure APIs with role-based checks to restrict data access, preventing unauthorized inclusions in report generation.
- Maintain audit logs to track observation selections, enabling detection of unauthorized or suspicious report modifications.
- Apply least privilege principles, ensuring users can only access and select data relevant to their assigned roles.

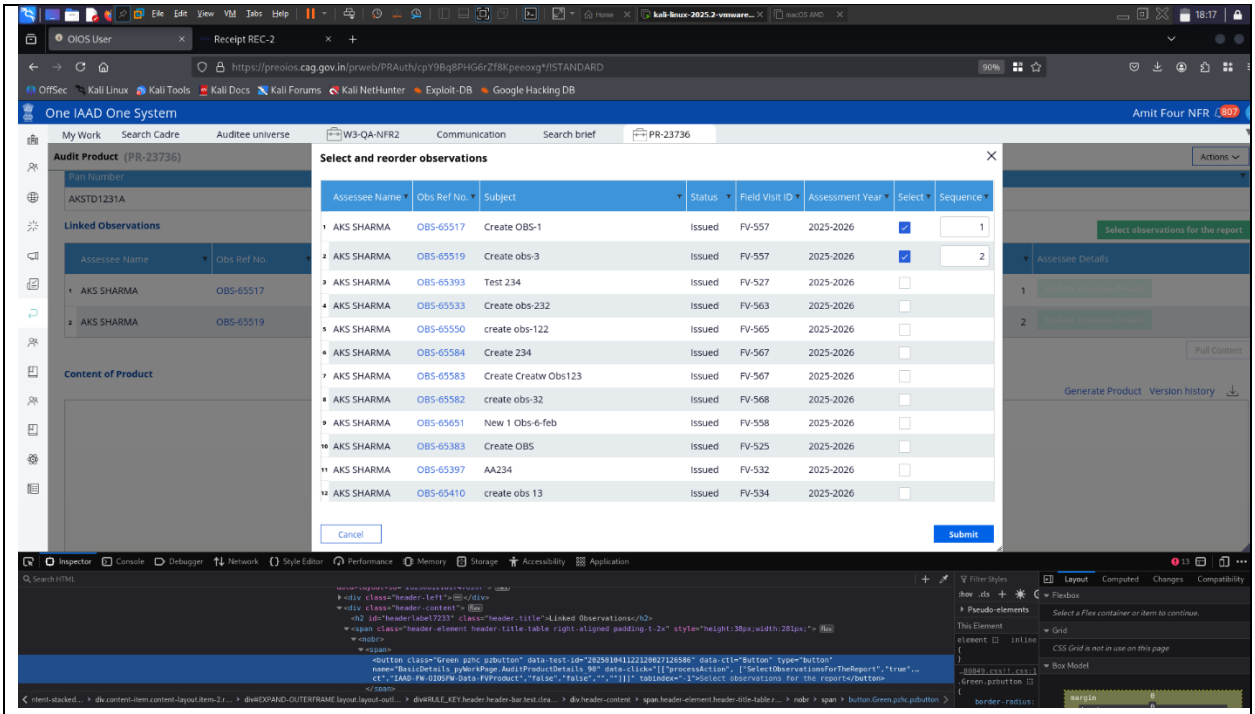
Proof of Concept:

Step 1: Open the application and navigate to the Search brief > Audit Product ref id > section where the “Select Observation for Report” button is disabled.



Step 2: Use browser Inspect Element → modify the attribute value from tabindex="-1" (disabled) to tabindex="1" (enabled). The button becomes active, and the restricted feature is now accessible.


One IAAD One System
Amit Four NFR
My Work
Search Cadre
Auditee universe
W3-QA-NFR2
Communication
Search brief
PR-23736
Audit Product (PR-23736)
Actions
Pan Number
Assessee name
AKSTD1231A
AKS SHARMA
Linked Observations
Select observations for the report
Assessee Name
Obs Ref No.
Subject
Status
Field Visit ID
Assessment Year
KDs
Sequence
Assessee Details
AKS SHARMA
OBS-65517
Create OBS-1
Issued
FV-557
2025-2026
view
1
AKS SHARMA
OBS-65519
Create obs-3
Issued
FV-557
2025-2026
view
2
Content of Product
Generate Product
Version history
Create the obs for the product and also verify the follow up status
This data is using in product verification.
Create the observation and check the data in the product


One IAAD One System
Amit Four NFR
Audit Product (PR-23736)
Select and reorder observations
Assessee Name
Obs Ref No.
Subject
Status
Field Visit ID
Assessment Year
Select
Sequence
AKS SHARMA OBS-65517 Create OBS-1 Issued FV-557 2025-2026
AKS SHARMA OBS-65519 Create obs-3 Issued FV-557 2025-2026
AKS SHARMA OBS-65393 Test 234 Issued FV-527 2025-2026
AKS SHARMA OBS-65533 Create obs-232 Issued FV-563 2025-2026
AKS SHARMA OBS-65550 create obs-122 Issued FV-565 2025-2026
AKS SHARMA OBS-65584 Create 234 Issued FV-567 2025-2026
AKS SHARMA OBS-65583 Create Creatw Obs123 Issued FV-567 2025-2026
AKS SHARMA OBS-65582 create obs-32 Issued FV-568 2025-2026
AKS SHARMA OBS-65651 New 1 Obs-6-feb Issued FV-558 2025-2026
AKS SHARMA OBS-65383 Create OBS Issued FV-525 2025-2026
AKS SHARMA OBS-65397 AA234 Issued FV-532 2025-2026
AKS SHARMA OBS-65410 create obs 13 Issued FV-534 2025-2026
Cancel
Submit

008	BAC- Client-Side Authorization bypass- update assessee details
URL	https://preoios.cag.gov.in/

Vulnerable Parameters: /

CVSS: 8.1- CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Severity: High

Vulnerability Description:

Client-side bypass enables unauthorized updates to assessee details via request tampering, risking fraud or data corruption. Secure with server-side RBAC, input validation, audit trails, and multi-factor confirmation for sensitive changes to prevent unauthorized modifications in regulated systems.

Impact:

It can lead to the following impacts:

- Enables unauthorized data tampering, risking fraud or privacy violations, compromising sensitive assessee details and violating GDPR compliance requirements.
- Facilitates data corruption, undermining system integrity, leading to inaccurate reports and potential legal issues in regulated environments.
- Exposes PII to unauthorized access, increasing identity theft risks, eroding user trust, and impacting organizational reputation significantly.
- Allows privilege escalation, enabling attackers to modify critical data, disrupting operations and causing non-compliance with ISO 27001 standards.

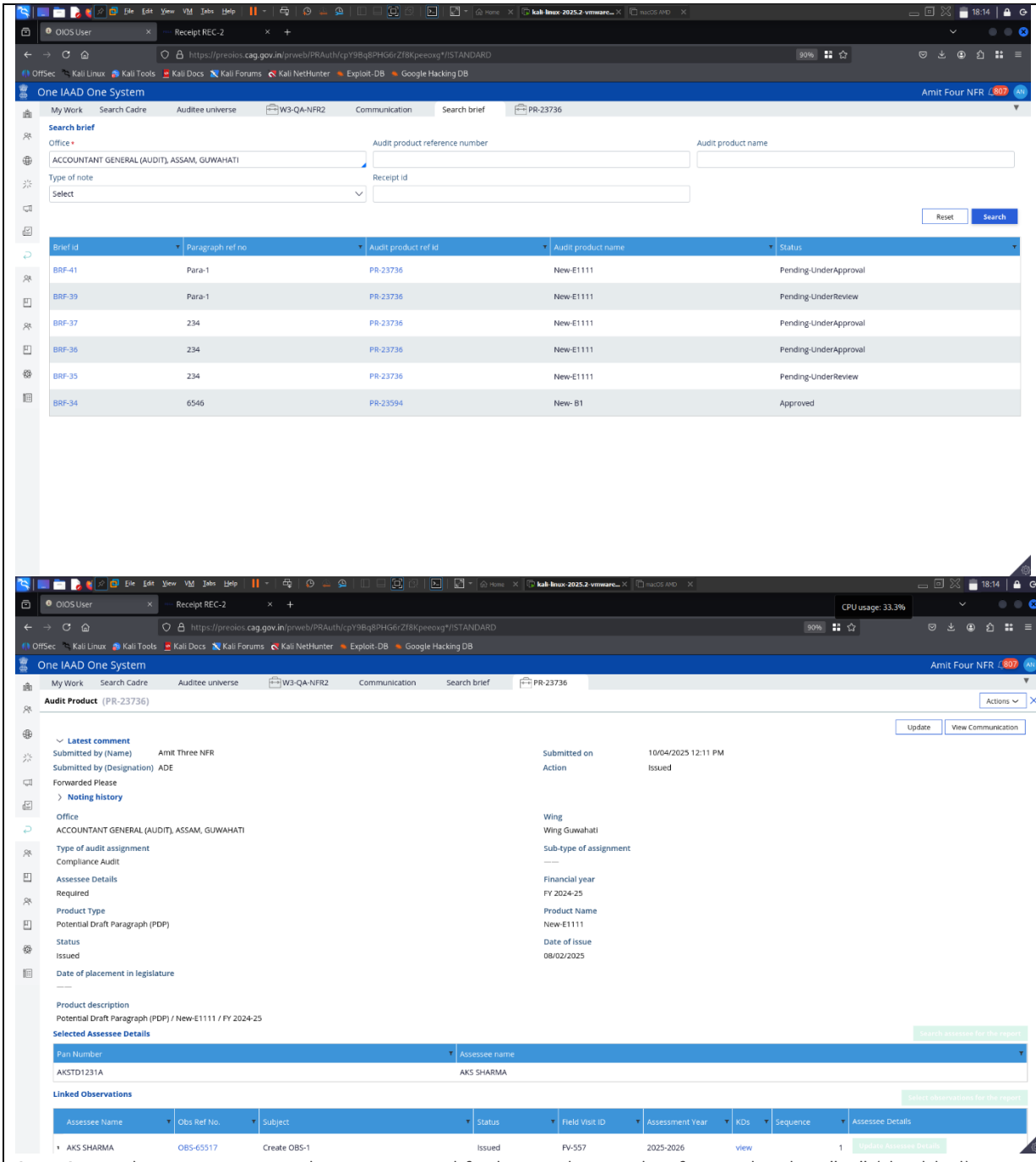
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

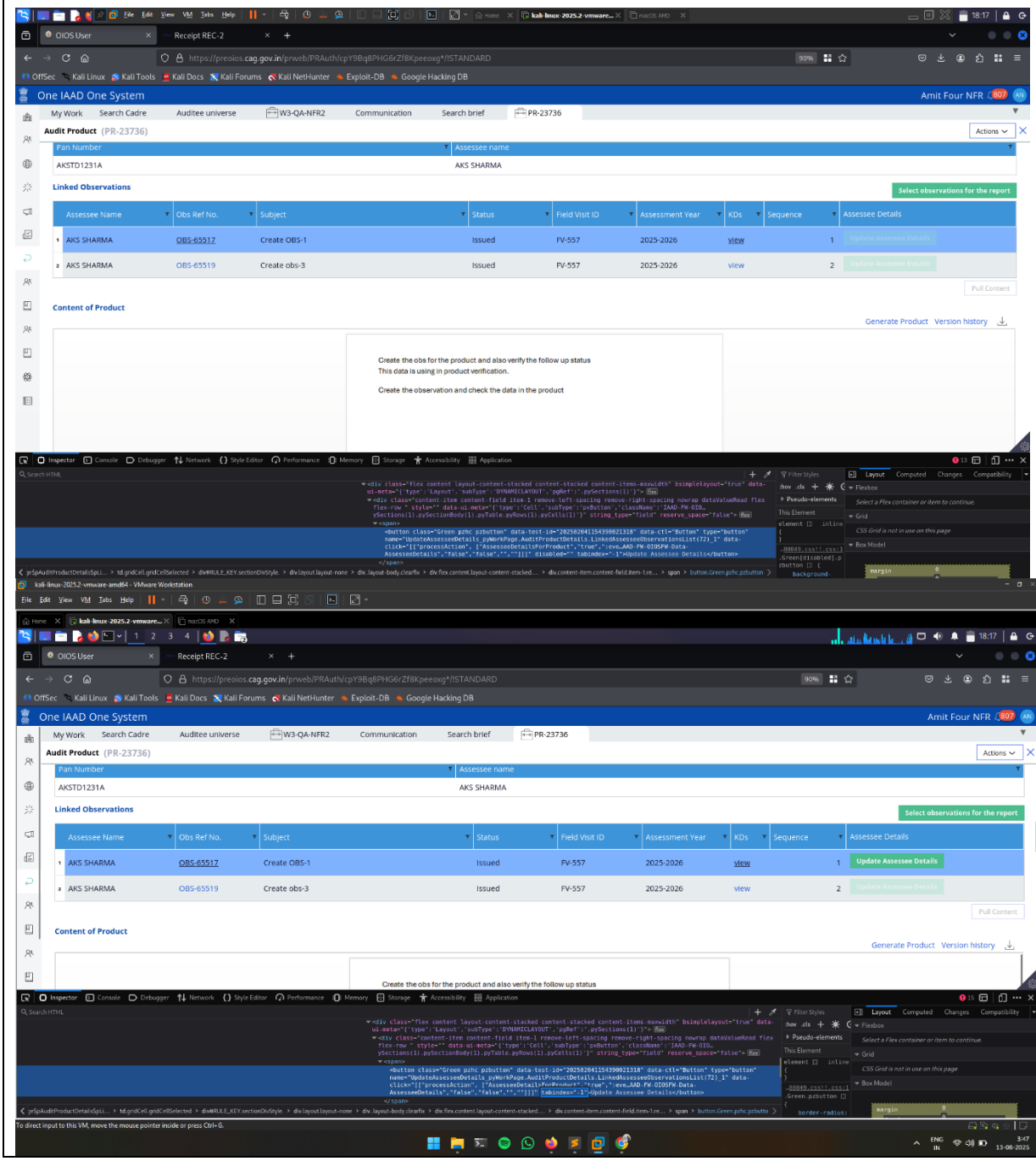
- Implement server-side RBAC and input validation to restrict assessee detail updates to authorized users, preventing fraud.
- Require multi-factor confirmation for sensitive updates to ensure only verified users can modify critical data securely.
- Maintain audit trails with before-after logs to track changes, enabling detection and rollback of unauthorized modifications.
- Use secure session management with encrypted tokens to prevent request tampering during assessee detail update processes.

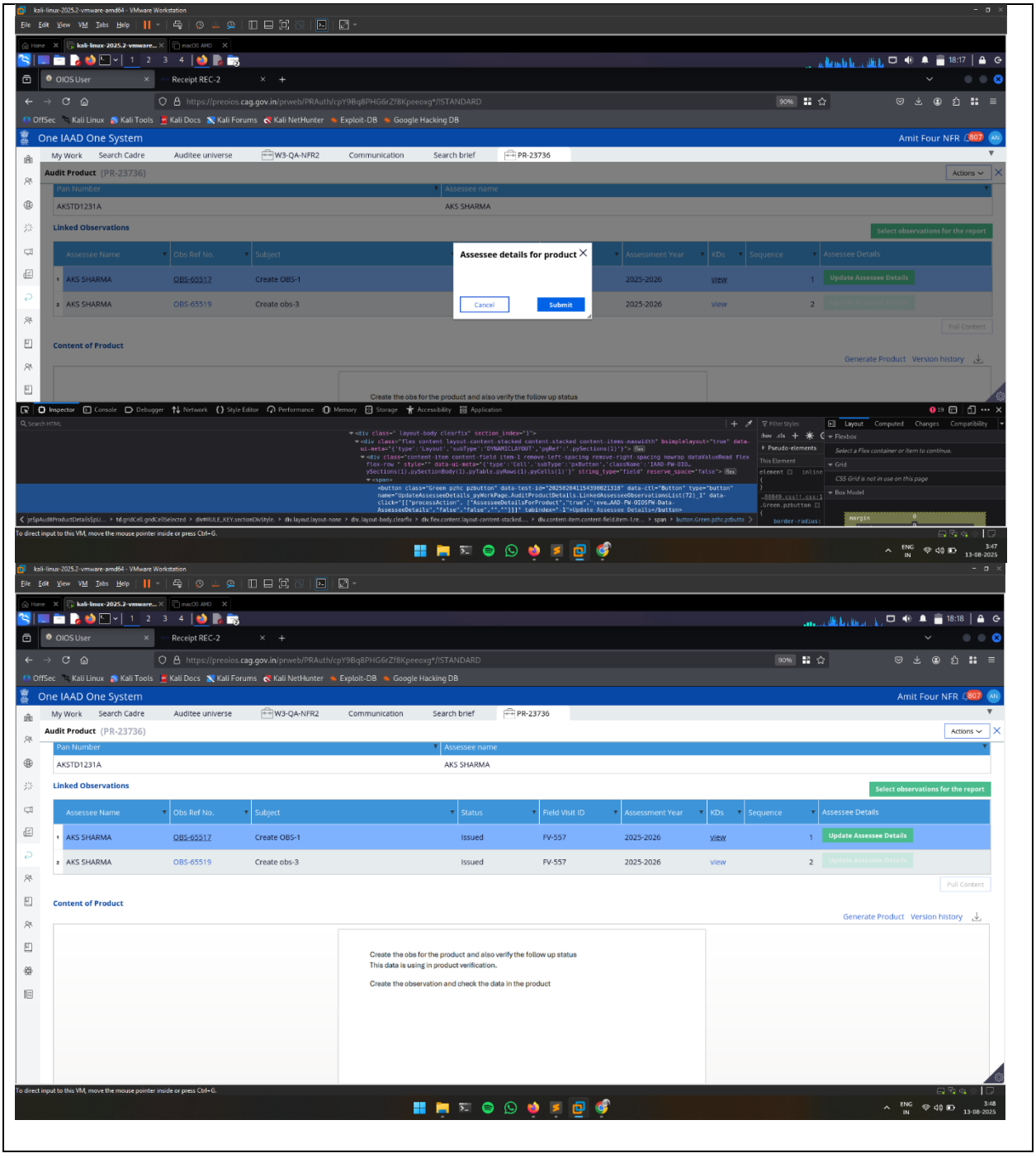
Proof of Concept:

Step 1: Open the application and navigate to the Search brief > Audit Product ref id > section where the “Update Assessee Details” button is disabled.



Step 2: Use browser Inspect Element → modify the attribute value from tabindex="-1" (disabled) to tabindex="1" (enabled). The button becomes active, and the restricted feature is now accessible.


One IAAD One System
Amit Four NFR
Audit Product (PR-23736)
Pan Number
Assessee name
AKSTD1231A
AKS SHARMA
Linked Observations
Select observations for the report
Assessee Name
Obs Ref No.
Subject
Status
Field Visit ID
Assessment Year
KDs
Sequence
Assessee Details
AKS SHARMA
OBS-65517
Create OBS-1
Issued
FV-557
2025-2026
view
1
Update Assessee Details
AKS SHARMA
OBS-65519
Create obs-3
Issued
FV-557
2025-2026
view
2
Update Assessee Details
Content of Product
Generate Product
Version history
Create the obs for the product and also verify the follow up status
This data is using in product verification.
Create the observation and check the data in the product


One IAAD One System
Amit Four NFR
Audit Product (PR-23736)
Pan Number
AKSTD1231A
Assessee name
AKS SHARMA
Linked Observations
Assessee Name
Obs Ref No.
Subject
Assessee details for product
Cancel
Submit
Assessment Year
KDs
Sequence
Assessee Details
AKS SHARMA
OBS-65517
Create OBS-1
2025-2026
view
Update Assessee Details
OBS-65519
Create obs-3
Content of Product
Generate Product
Version history
Create the obs for the product and also verify the follow up status
One IAAD One System
Amit Four NFR
Audit Product (PR-23736)
Pan Number
AKSTD1231A
Assessee name
AKS SHARMA
Linked Observations
Select observations for the report
Assessee Name
Obs Ref No.
Subject
Status
Field Visit ID
Assessment Year
KDs
Sequence
Assessee Details
AKS SHARMA
OBS-65517
Create OBS-1
Issued
FV-557
2025-2026
view
Update Assessee Details
OBS-65519
Create obs-3
Content of Product
Generate Product
Version history
Create the obs for the product and also verify the follow up status
This data is using in product verification.
Create the observation and check the data in the product

009	No Rate Limit on Login- Login
URL	https://preoios.cag.gov.in/

Vulnerable Parameter: /

CVSS: 6.5- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L

Severity: Medium

Vulnerability Description:

Absence of rate limiting on login endpoints allows attackers to perform brute force attacks, guessing credentials rapidly. This risks unauthorized access, account compromise, or denial-of-service. Mitigate with rate limiting, CAPTCHA, and account lockout mechanisms after repeated failed attempts to deter automated attacks and protect user accounts.

Impact:

It can lead to the following impacts:

- Enables brute force attacks, compromising user accounts and sensitive data.
- Risks denial-of-service, overwhelming servers and disrupting legitimate user access.
- Facilitates credential stuffing, escalating unauthorized access across systems.
- Erodes user trust, damaging organizational reputation and compliance status.

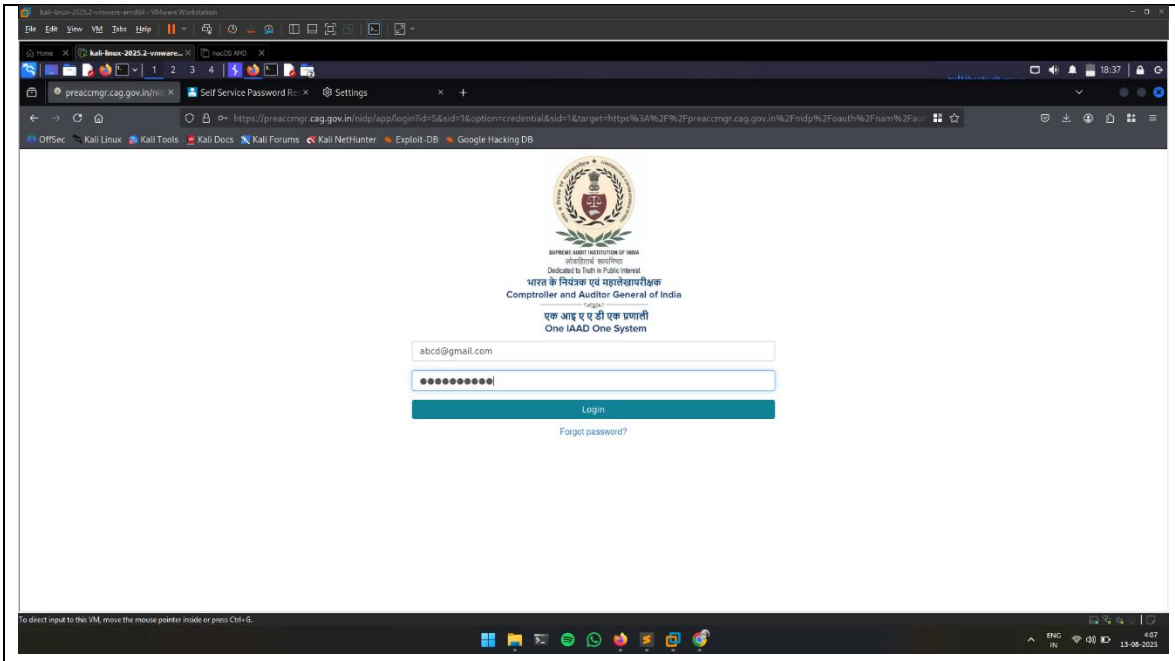
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

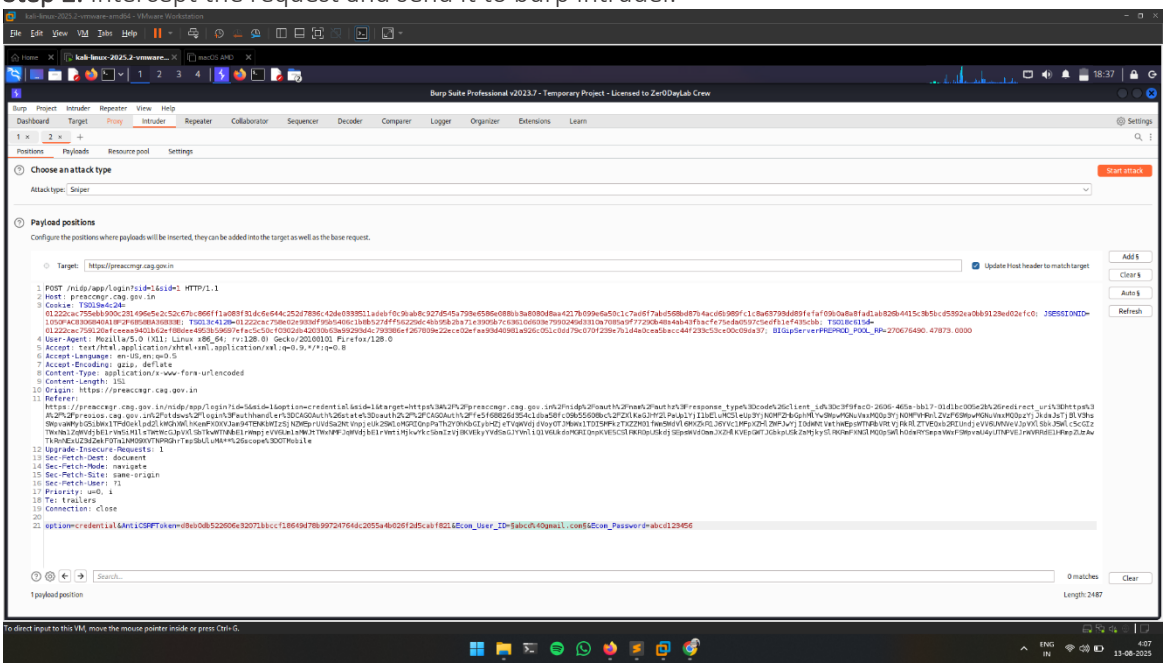
- Apply rate limiting to login endpoints (5-10 attempts/minute) per OWASP to block brute-force attacks and protect against unauthorized access or DoS.
- Add CAPTCHA after failed logins, per NIST SP 800-63B, to deter automated bots and enhance security against credential guessing attacks.
- Implement account lockout after 5-10 failed attempts, per PCI DSS, suspending access for 30 minutes to prevent unauthorized access and notify users.
- Monitor login attempts with ISO 27001-compliant tools, logging anomalies and integrating with SIEM for real-time threat detection and response.

Proof of Concept:

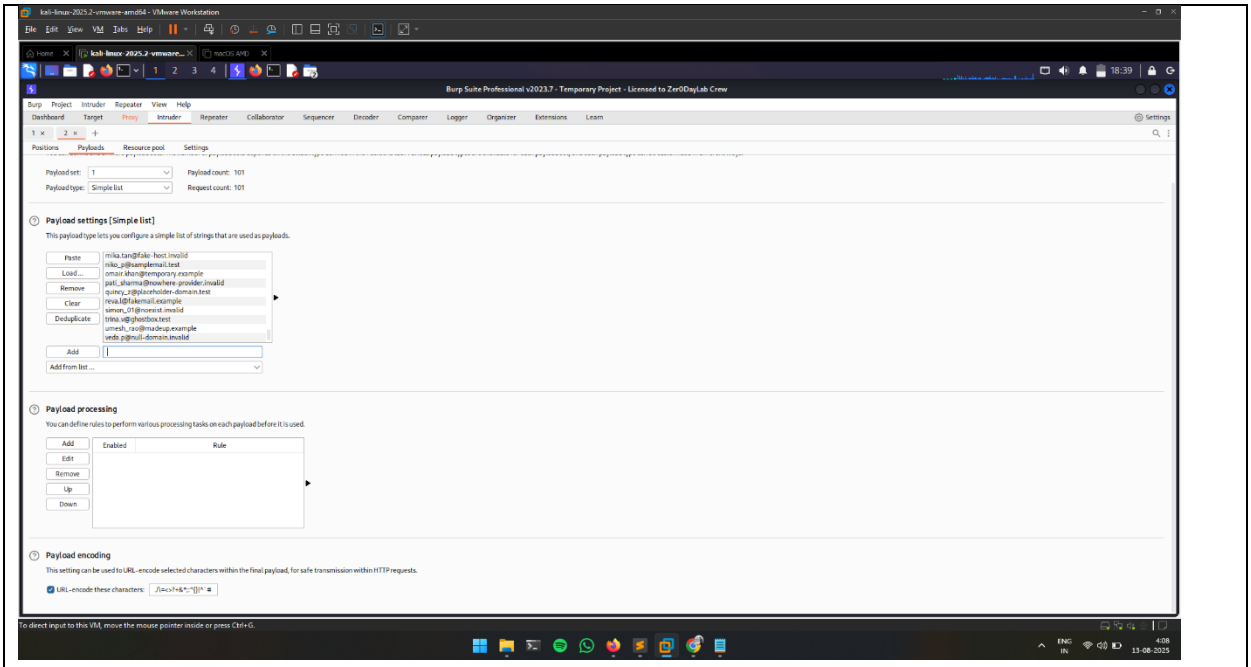
Step 1: Enter email and password on input parameters and send the request.



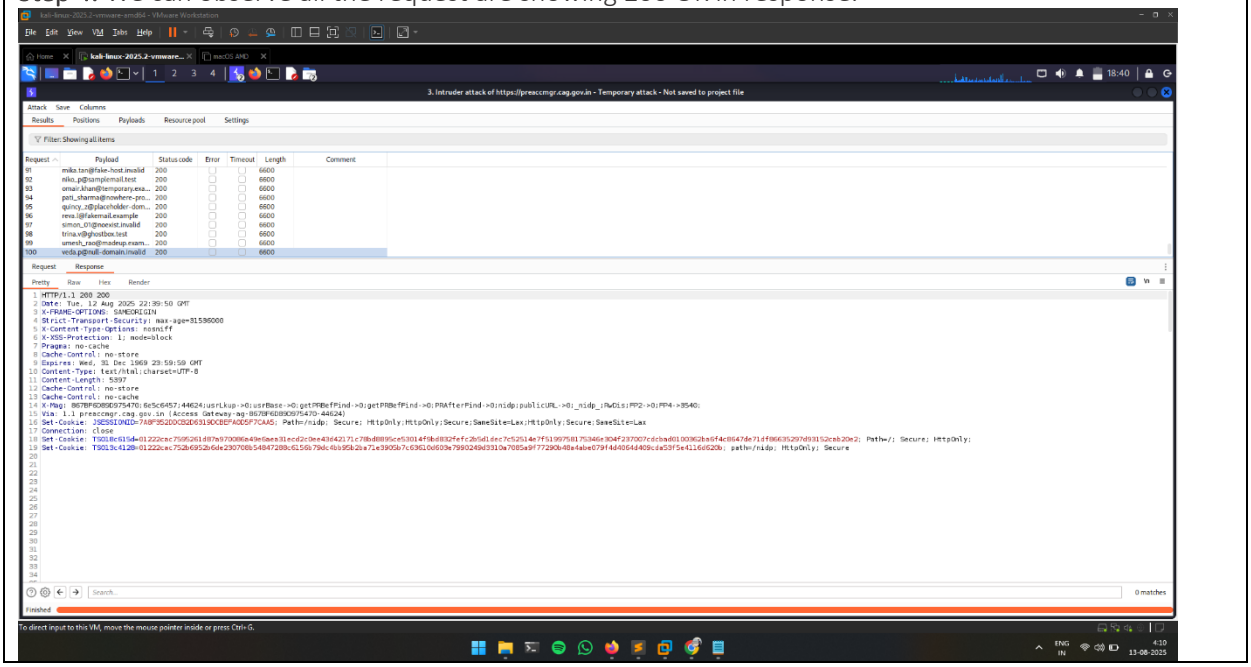
Step 2: Intercept the request and send it to burp intruder.

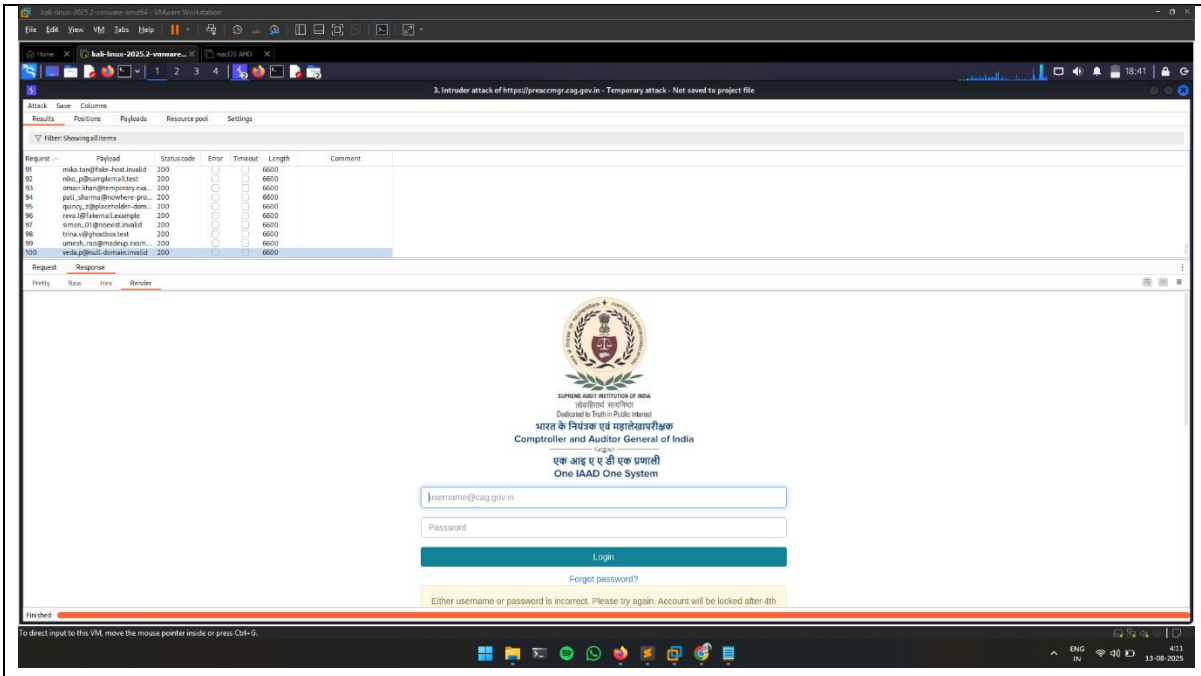


Step 3: Set the payload for multiple request and start the attack.



Step 4: We can observe all the request are showing 200 OK in response.




3. Intruder attack of https://preaccmgr.cag.gov.in - Temporary attack - Not saved to project file
Request
Response
SUPREME AUDIT INSTITUTION OF INDIA
Dedicated to Truth in Public Interest
भारत के नियंत्रक एवं महालेखापरीक्षक
Comptroller and Auditor General of India
एक आइ ए ए डी एक प्रणाली
One IAAD One System
username@cag.gov.in
Password
Login
Forgot password?
Either username or password is incorrect. Please try again. Account will be locked after 4th
Finished

010	PII Disclosure in MyWorkReport Response
URL	https://preoios.cag.gov.in/

Vulnerable Parameter: /

CVSS: 6.5- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Severity: Medium

Vulnerability Description:

MyWorkReport response exposes sensitive PII (e.g., names, addresses) due to improper data filtering. This risks identity theft or data breaches. Attackers can intercept responses to steal information. Mitigate with server-side data minimization, encryption of sensitive fields, and access controls to ensure only authorized users receive relevant PII in responses.

Impact:

It can lead to the following impacts:

- Exposes names and addresses, enabling identity theft and targeted attacks.
- Risks regulatory fines for violating data protection laws like GDPR.
- Facilitates social engineering by providing attackers with sensitive PII.
- Undermines user trust, leading to reputational damage and potential lawsuits.

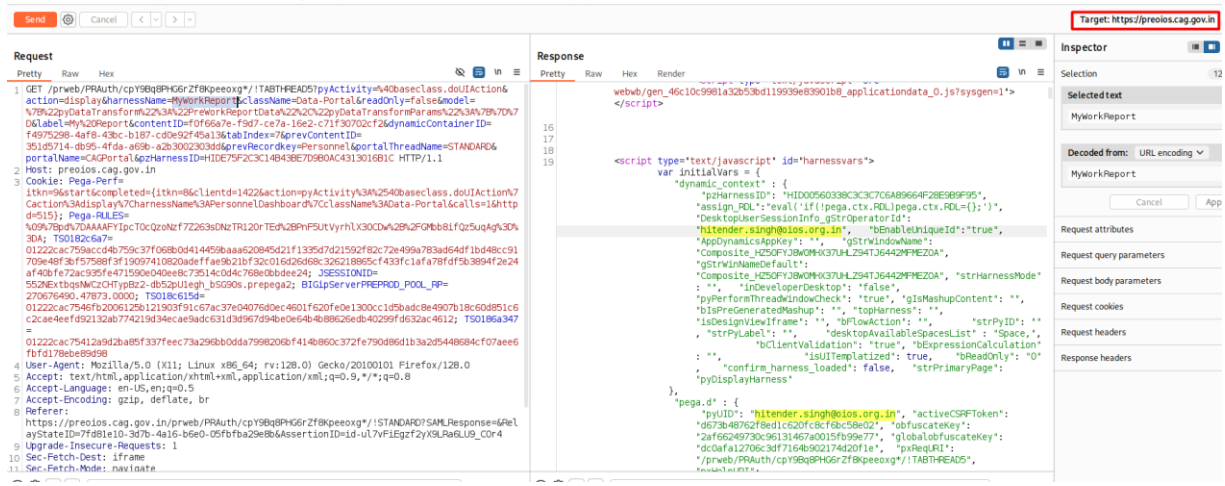
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

- Minimize PII in responses via server-side filtering, per GDPR, excluding sensitive data like addresses to reduce risks of interception and data breaches.
- Encrypt PII in transit with TLS 1.3, per NIST SP 800-52, ensuring confidentiality and preventing attackers from accessing names or addresses.
- Enforce RBAC per OWASP ASVS, restricting PII access to authorized users and logging requests for audit and compliance purposes.
- Conduct regular scans and penetration tests, per ISO 27001, to identify and fix PII leakage vulnerabilities in MyWorkReport endpoints.

Proof of Concept:

Step 1: Observe in the API response that sensitive PII such as the user's email (hitender.singh@ioios.org.in) is disclosed in the pyUID field.



011	PII Disclosure in Download My Graduation List Response
URL	https://preoios.cag.gov.in/

Vulnerable Parameter: /

CVSS: 6.5- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Severity: Medium

Vulnerability Description:

Download My Graduation List response leaks PII (e.g., student names, IDs) due to unfiltered data exposure. This risks privacy violations or data misuse. Attackers can access sensitive information via intercepted responses. Fix with server-side data sanitization, role-based access controls, and encryption to limit PII exposure to authorized users only.

Impact:

It can lead to the following impacts:

- Leaks student names and IDs, risking privacy violations and data misuse.
- Enables identity theft, impacting students' personal and financial security.
- Violates compliance with education data regulations like FERPA.
- Damages institutional reputation, reducing trust among students and stakeholders.

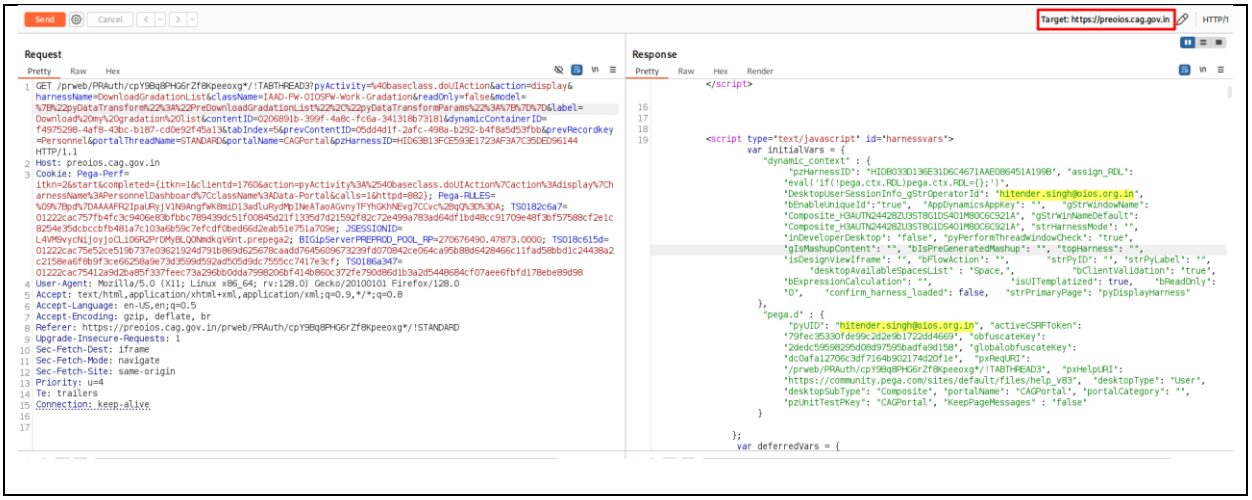
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

- Sanitize downloaded data server-side, per OWASP, redacting PII like student IDs to prevent privacy violations during file access or transmission.
- Encrypt downloads with FIPS 140-2 standards, ensuring PII is secure and only accessible to authenticated users with valid decryption keys.
- Apply RBAC per NIST SP 800-53, limiting download access to authorized roles and logging all requests for security audits.
- Require MFA for downloads, per PCI DSS 8.3, adding verification to ensure only legitimate users access sensitive graduation lists.

Proof of Concept:

Step 1: Observe in the API response that sensitive PII such as the user's email (hitender.singh@ioios.org.in) is disclosed in the pyUID field.


Send
Cancel
Target: https://preoios.cag.gov.in
HTTP/1
Request
Pretty
Raw
Hex
GET /prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!TABTHREAD3?pyActivity=%40baseclass.doUIAction&action=display&harnessName=DownloadGradationList&className=IAAD-FW-OIOSFW-Work-Gradation&readOnly=false&model=%7B%22pyDataTransform%22%3A%22PreDownloadGradationList%22%2C%22pyDataTransformParams%22%3A%7B%7D%7D&label=Download%20my%20gradation%20list&contentID=0206891b-399f-4a8c-fc6a-341318b73181&dynamicContainerID=f4975298-4af8-43bc-b187-cd0e92f45a13&tabIndex=5&prevContentID=05dd4d1f-2afc-498a-b292-b4f8a5d53fbb&prevRecordkey=Personnel&portalThreadName=STANDARD&portalName=CAGPortal&pzHarnessID=HID63B13FCE593E1723AF3A7C35DED96144
HTTP/1.1
Host: preoios.cag.gov.in
Cookie: Pega-Perf=
itkn=2&start&completed={itkn=1&clientd=1760&action=pyActivity%3A%2540baseclass.doUIAction%7Caction%3Adisplay%7CharnessName%3APersonnelDashboard%7CclassName%3AData-Portal&calls=1&httpd=882}; Pega-RULES=
%09%7Bpd%7DAAAAFR2IpaURyjVlN9AngfwK8miDI3adluRydMpINeATaoAGvnyTFYhGKhNEvg7CCvc%2Bq%3D%3DA; TS0182c6a7=
01222cac757fb4fc3c9406e83bfbbc78943 9dc51f00845d21f1335d7d2159 2f82c72e499a783ad64df1bd48cc91709e48f3bf57588cf2e1c8254e35dcbccbfb481a7c103a6b59c7efcdf0bed66d2eab51e751a709e; JSESSIONID=
L4VM9vycNijoyjoCL106R2PrDMy8LQQNmdkqV6Nt.prepega2; BIGipServerPREPRCD_POOL_RP=270676490.47873.0000; TS018c615d=
01222cac75e52ce519b737e03621924d791b869d625678caadd7645609673239fd070842ce064ca95b80d6428466c11fad58bbd1c24438a2c2158ea6f8b9f3ce66258a9e73d3599d592ad505d9dc7555cc7417e3cf; TS0186a347=
01222cac75412a9d2ba85f337feec73a296bb0dda7998206bf414b860c372fe790d86d1b3a2d5448684cf07aee6fbfd178ebe89d98
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
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
Referer: https://preoios.cag.gov.in/prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!STANDARD
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Priority: u=4
Te: trailers
Connection: keep-alive
Response
Pretty
Raw
Hex
Render
</script>
<script type="text/javascript" id="harnessvars">
var initialVars = {
"dynamic_context" : {
"pzHarnessID": "HIDB033D136E31D6C4671AAE0B6451A199B", "assign_RDL":
'eval('if('pega.ctx.RDL)pega.ctx.RDL={};')',
'DesktopUserSessionInfo_gStrOperatorId': 'hitender.singh@oios.org.in',
'bEnableUniqueId':"true", "AppDynamicsAppKey": "", "gStrWindowName":
'Composite_H3AUTN24428ZU3ST8G1DS4O1M8OC6C921A', "gStrWinNameDefault":
'Composite_H3AUTN24428ZU3ST8G1DS4O1M8OC6C921A', "strHarnessMode": "",
'inDeveloperDesktop': 'false', "pyPerformThreadWindowCheck": 'true',
'gIsMashupContent': "", "bIsPreGeneratedMashup": "", "topHarness": "",
'isDesignViewIframe': "", "bFlowAction': "", "strPyID": "", "strPyLabel": "",
"desktopAvailableSpacesList" : "Space,", "bClientValidation": 'true',
'bExpressionCalculation': "", "isUITemplatized": true, "bReadOnly":
"0", "confirm_harness_loaded": false, "strPrimaryPage": "pyDisplayHarness"
},
"pega.d" : {
"pyUID": "hitender.singh@oios.org.in", "activeCSRFToken":
'79fec35330fde96c2d2e9b172 2dd4669', "obfuscateKey":
'2dedc59598295d08d97595badfa9d158', "globalobfuscateKey":
'dc0afa12706c3df7164b902174d2 0f1e', "pxReqURI":
'/prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!TABTHREAD3', "pxHelpURI":
'https://community.pega.com/sites/default/files/help_v83", "desktopType": "User",
'desktopSubType': "Composite", "portalName": "CAGPortal", "portalCategory": "",
'pzUnitTestPKey": "CAGPortal", "KeepPageMessages" : 'false'
}
};
var deferredVars = {

012	PII Disclosure in Generate Offline Application Security Code Response
URL	https://preoios.cag.gov.in/

Vulnerable Parameter: /

CVSS: 6.5- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Severity: Medium

Vulnerability Description:

Generate Offline Application Security Code response exposes PII (e.g., user IDs, contact details) without proper filtering. This risks data leakage or unauthorized access. Attackers can exploit intercepted responses. Mitigate with server-side PII minimization, encryption of sensitive data, and strict access controls to ensure only authorized users receive necessary information.

Impact:

It can lead to the following impacts:

- Exposes user IDs and contacts, risking unauthorized access and fraud.
- Facilitates data breaches, leading to potential regulatory penalties.
- Enables targeted phishing attacks using leaked sensitive information.
  Undermines system trust, causing user disengagement and reputational harm.

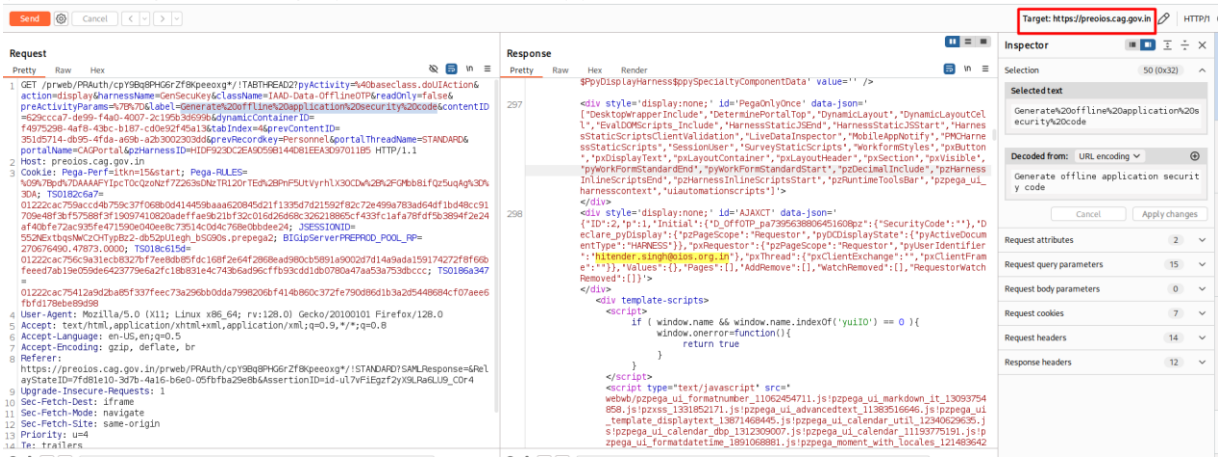
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

- Filter PII server-side, per HIPAA, excluding contact details from responses to minimize leakage risks during security code generation processes.
- Encrypt responses with HTTPS and HSTS, per OWASP, protecting user IDs from interception during transmission over unsecured networks.
- Enforce strict access controls, per ISO 27001, limiting code generation to authenticated users and logging for forensic analysis.
- Use secure coding practices, per OWASP SAMM, with static analysis to detect and fix PII exposure in response generation.

Proof of Concept:

Step 1: Observe in the API response that sensitive PII such as the user's email (hitender.singh@ioios.org.in) is disclosed in the pyUID field.



013	PII Disclosure in Go to Send Items Response
URL	https://preoios.cag.gov.in/

Vulnerable Parameter: /

CVSS: 6.5- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Severity: Medium

Vulnerability Description:

Go to Send Items response leaks PII (e.g., recipient details, addresses) due to inadequate data filtering. This risks privacy breaches or data theft. Attackers can intercept responses to access sensitive information. Prevent with server-side data sanitization, encryption, and role-based access controls to restrict PII exposure to authorized users only.

Impact:

It can lead to the following impacts:

- Leaks recipient details, enabling privacy breaches and data theft.
- Risks regulatory non-compliance with data protection laws like CCPA.
- Facilitates social engineering attacks using exposed PII.
- Damages organizational credibility, leading to loss of user confidence.

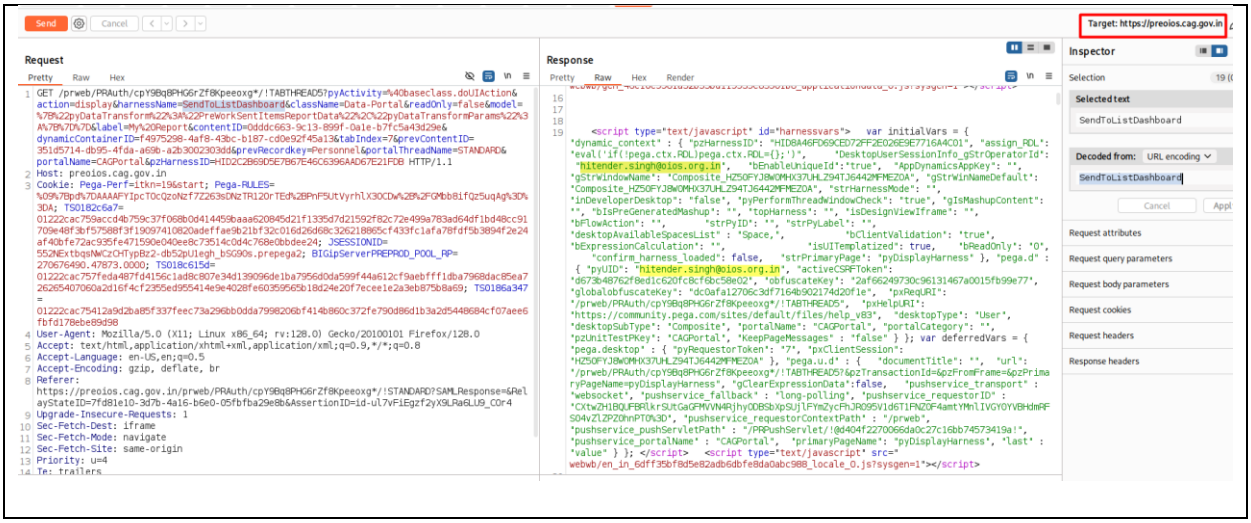
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

- Sanitize responses server-side, per GDPR, removing excess PII like addresses to prevent privacy breaches during data transmission or interception.
- Encrypt data with TLS 1.3, per NIST, securing recipient details from unauthorized access during send item response generation.
- Implement RBAC, per OWASP ASVS, restricting PII to authorized users and maintaining audit logs for compliance and monitoring.
- Perform privacy impact assessments, per ISO 27701, to evaluate and mitigate PII exposure risks in send item workflows.

Proof of Concept:

Step 1: Observe in the API response that sensitive PII such as the user's email (hitender.singh@ioios.org.in) is disclosed in the pyUID field.


Send
Cancel
Target: https://preoios.cag.gov.in
Request
Pretty
Raw
Hex
GET /prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!TABTHREAD5?pyActivity=%40baseclass.doUIAction&action=display&harnessName=SendToListDashboard&className=Data-Portal&readOnly=false&model=%7B%22pyDataTransform%22%3A%22PreWorkSentItemsReportData%22%2C%22pyDataTransformParams%22%3A%7B%7D%7D&label=My%20Report&contentID=0ddddc663-9c13-899f-0a1e-b7fc5a43d29e&dynamicContainerID=f4975298-4af8-42bc-b187-cd0e92f45a1&tabIndex=7&prevContentID=351d5714-db95-4fda-a69b-a2b3002303dd&prevRecordkey=Personnel&portalThreadName=STANDARD&portalName=CAGPortal&pzHarnessID=HID2C2B69D5E7B67E46C6396AAD67E21FDB HTTP/1.1
Host: preoios.cag.gov.in
Cookie: Pega-Perf=itkn=19&start; Pega-RULES=%05%7BpdhJDAAAAFYIpcTOcQzoNzf7Z263sDNzTR12OrTEd%2BPnF5UtVyrhlX30CDw%2B%2FGMbb8ifQz5uqAg%3D%3DA; TS0182c6a7=01222cac759accd4b759c37f068b0d414459baaa620845d21f1335d7d21592f82c72e499a783ad64df1bd48cc91709e48f3bf57588f3f1909741082Oadeffae9b21bf32c016d26d68c326218865cf433fc1afa78fdf5b3894f2e24af40bfe72ac935fe471590e040ee8c73514c0d4c768e0bbdee24; JSESSIONID=552NExtbqsNWCzCHTypBz2-db52pUiegh_bSG9Os.prepega2; BIGipServerPREPROD_POOL_RP=270676490.47873.0000; TS018c615d=01222cac757feda487fd4156c1ad8c807e34d139096de1ba7956d0da599f44a612cf9aebfff1dba7968dac85ea726265407060a2d16f4cf2355ed955414e9e4028fe60359565b18d24e20f7ecee1e2a3eb875b8a69; TS0186a347=01222cac75412a9d2ba85f337feec73a296bb0dda7998206bf414b860c372fe790d86d1b3a2d5448684cf07aee6fbfd178ebe89d98
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
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
Referer: https://preoios.cag.gov.in/prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!STANDARD?SAMLResponse=&RelayStateID=7fd81e10-3d7b-4a16-b6e0-05fbfba29e8b&AssertionID=id-ul7VF1Egzf2yX9LRa6LU9_C0r4
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Priority: u=4
Te: trailers
Response
Pretty
Raw
Hex
Render
<script type="text/javascript" id="harnessvars"> var initialVars = {
"dynamic_context" : { "pzHarnessID": "HID8A46FD69CED72FF2E026E9E7716A4C01", "assign_RDL":
"eval('if(!pega.ctx.RDL)pega.ctx.RDL={};')", "DesktopUserSessionInfo_gStrOperatorId":
"hitender.singh@oios.org.in", "bEnableUniqueId":"true", "AppDynamicsAppKey": "",
"gStrWindowName": "Composite_HZ5OFYJ8WOMHX37UHLZ94TJ6442MFMEZOA", "gStrWinNameDefault":
"Composite_HZ5OFYJ8WOMHX37UHLZ94TJ6442MFMEZOA", "strHarnessMode": "",
"inDeveloperDesktop": "false", "pyPerformThreadWindowCheck": "true", "gIsMashupContent":
"", "bIsPreGeneratedMashup": "", "topHarness": "", "isDesignViewIframe": "",
"bFlowAction": "", "strPyID": "", "strPyLabel": "",
"desktopAvailableSpacesList" : "Space,", "bClientValidation": "true",
"bExpressionCalculation": "", "isUITemplatized": true, "bReadOnly": "0",
"confirm_harness_loaded": false, "strPrimaryPage": "pyDisplayHarness" }, "pega.d" :
{ "pyUID": "hitender.singh@oios.org.in", "activeCSRFToken":
"d673b48762f8ed1c620fc8cf6bc58e02", "obfuscateKey": "2af66249730c96131467a0015fb99e77",
"globalobfuscateKey": "dc0afa12706c3df7164b902174d20f1e", "pxReqURI":
"/prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!TABTHREAD5", "pxHelpURI":
"https://community.pega.com/sites/default/files/help_v83", "desktopType": "User",
"desktopSubType": "Composite", "portalName": "CAGPortal", "portalCategory": "",
"pzUnitTestPKey": "CAGPortal", "keepPageMessages" : "false" } }; var deferredVars = {
"pega.desktop" : { "pyRequestorToken": "7", "pxClientSession":
"HZ5OFYJ8WOMHX37UHLZ94TJ6442MFMEZOA" }, "pega.u.d" : { "documentTitle": "", "url":
"/prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!TABTHREAD5?&pzTransactionId=&pzFromFrame=&pzPrimaryPageName=pyDisplayHarness", "gClearExpressionData":false, "pushservice_transport" :
"websocket", "pushservice_fallback" : "long-polling", "pushservice_requestorID" :
"CXtw2H1BQLFBRlkrSLttGaGFMVVM4HjhyCOBSbXpSUjlFYmZycFhJRG95V1d6T1FNZGF4amtYMnlIVGYOYVBHdmRFSO4V2lZPZOhnPTQ%3D", "pushservice_requestorContextPath" : "/prweb",
"pushservice_pushServletPath" : "/PRPushServlet/!@d404f2270066da0c27c16bb74573419a!",
"pushservice_portalName" : "CAGPortal", "primaryPageName": "pyDisplayHarness", "last" :
"value" } }; </script> <script type="text/javascript" src="
webwb/en_in_6dff35bf8d5e82adb6dbfe8da0abc988_locale_0.js?sysgen=1"></script>
Inspector
Selection
Selected text
SendToListDashboard
Decoded from: URL encoding
SendToListDashboard
Cancel
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers

014	PII Disclosure in My Contribution Response
URL	https://preoios.cag.gov.in/

Vulnerable Parameter: /

CVSS: 6.5- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Severity: Medium

Vulnerability Description:

My Contribution response exposes PII (e.g., contributor names, financial details) due to poor data filtering. This risks privacy violations or fraud. Attackers can steal sensitive data via intercepted responses. Mitigate with server-side data minimization, encryption of sensitive fields, and access controls to ensure only authorized users access relevant PII.

Impact:

It can lead to the following impacts:

- Exposes contributor names and financial details, risking fraud.
- Violates data protection regulations, incurring legal and financial penalties.
- Enables targeted scams using leaked sensitive financial information.
- Erodes trust, harming organizational reputation and user engagement.

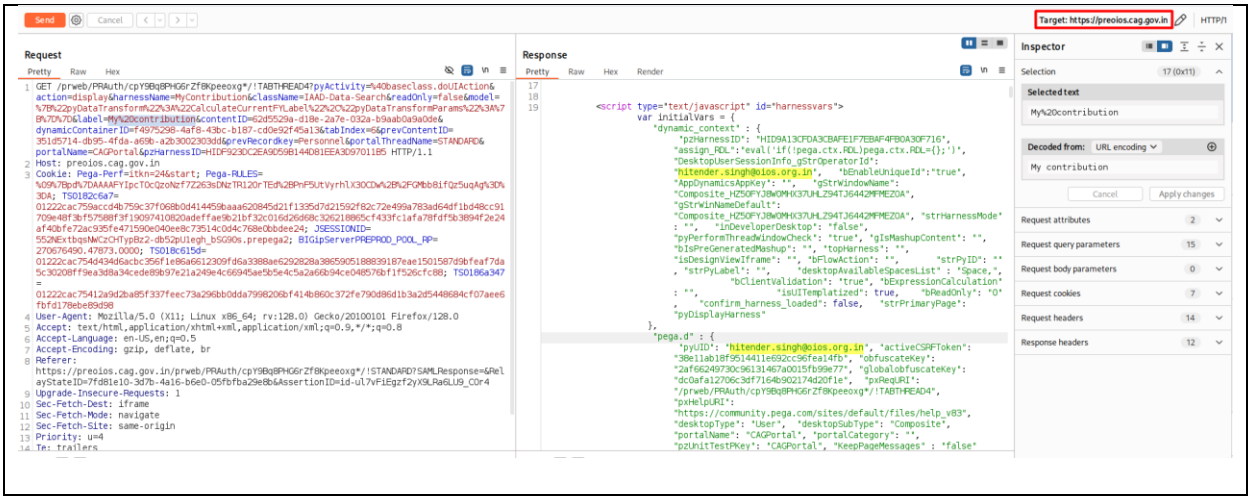
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

- Filter PII like financial details server-side, per PCI DSS, to prevent fraud and limit exposure in contribution response data.
- Encrypt sensitive fields with AES, per FIPS 197, protecting contributor names during API responses and ensuring data confidentiality.
- Use ABAC, per NIST SP 800-162, tailoring PII access based on user attributes and logging for compliance and audits.
- Adopt OWASP Cheat Sheet practices, including input validation to eliminate PII leaks in contribution response endpoints.

Proof of Concept:

Step 1: Observe in the API response that sensitive PII such as the user's email (hitender.singh@ioios.org.in) is disclosed in the pyUID field.


Send
Cancel
Target: https://preoios.cag.gov.in
HTTP/1
Request
Pretty
Raw
Hex
GET /prweb/PRAuth/cpY9BqBPHG6rZf8Kpeeoxg*/!TABTHREAD4?pyActivity=%40baseclass.doUIAction&action=display&harnessName=MyContribution&className=IAAD-Data-Search&readOnly=false&model=%7B%22pyDataTransform%22%3A%22CalculateCurrentFYLabel%22%2C%22pyDataTransformParams%22%3A%7B%7D%7D&label=My%20contribution&contentID=62d5529a-d18e-2a7e-032a-b9aab0a9a0de&dynamicContainerID=f4975298-4af8-43bc-b187-cd0e92f45a13&tabIndex=6&prevContentID=351d5714-db95-4fda-a65b-a2b3002303d1&prevRecordKey=Personnel&portalThreadName=STANDARD&portalName=CAGPortal&pzHarnessID=HIDF923DC2EA9D59B144D81EEA3D97011B5 HTTP/1.1
Host: preoios.cag.gov.in
Cookie: Pega-Perf=itkn=24&start; Pega-RULES=%09%7Bpd%7DAAAAFYIpcTOcQzoNzf7Z263sDNzTR12OrTEd%2BPnF5UtVyrhlX3OCDw%2B%2FGMbb8ifQz5uqAg%3D%3DA; TS018c6a7=01222cac759accd4b759c37f068b0d414459baaa620845d21f1335d7d21592f82c72e499a783ad64df1bd48cc91709e48f3bf57588f3f1909741082 0adeffae9b21bf32c016d26d68c326218865cf433fc1afa78fdf5b3894f2e24af40bfe72ac935fe471590e040ee8c73514c0d4c768e0bbdee24; JSESSIONID=552NExtbqsNWCzOHTypB2-db52pUiegh_bSG9Os.prepega2; BIGipServerPREPROD_POOL_RP=270676490.47873.0000; TS018c615d=01222cac754d434d6acbc356f1e86a6612309fd6a3388ae6292828a3865905188839187eae1501587d9bfeaf7da5c30208ff9ea3d8a34cede89b97e21a249e4c66945ae5b5e4c5a2a66b94ce048576bf1f526cfc88; TS0186a347=01222cac75412a9d2ba85f337feec73a296bb0dda7998206bf414b860c372fe790d86d1b3a2d5488684cf07aee6fbfd178ebe89d98
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
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
Referer: https://preoios.cag.gov.in/prweb/PRAuth/cpY9BqBPHG6rZf8Kpeeoxg*/!STANDARD?SAMLResponse=&RelayStateID=7fd81e10-3d7b-4a16-b6e0-05fbfba29e8b&AssertionID=id-ul7vFiEgzf2yXSLRa6LU9_COr4
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Priority: u=4
Te: trailers
Response
Pretty
Raw
Hex
Render
<script type="text/javascript" id="harnessvars">
var initialVars = {
"dynamic_context" : {
"pzHarnessID": "HID9A13CFDA3CBAFE1F7EBAF4FB0A30F716",
"assign_RDL":"eval('if(!pega.ctx.RDL)pega.ctx.RDL={};')",
"DesktopUserSessionInfo_gStrOperatorId":
"hitender.singh@oios.org.in", "bEnableUniqueId":"true",
"AppDynamicsAppKey": "", "gStrWindowName":
"Composite_HZ5OFYJ8WOMHX37UHLZ94TJ6442MFMEZOA",
"gStrWinNameDefault":
"Composite_HZ5OFYJ8WOMHX37UHLZ94TJ6442MFMEZOA", "strHarnessMode"
: "", "inDeveloperDesktop": "false",
"pyPerformThreadWindowCheck": "true", "gIsMashupContent": "",
"bIsPreGeneratedMashup": "", "topHarness": "",
"isDesignViewIframe": "", "bFlowAction": "", "strPyID": ""
, "strPyLabel": "", "desktopAvailableSpacesList" : "Space,",
"bClientValidation": "true", "bExpressionCalculation"
: "", "isUITemplatized": true, "bReadOnly": "0"
, "confirm_harness_loaded": false, "strPrimaryPage":
"pyDisplayHarness"
},
"pega.d" : {
"pyUID": "hitender.singh@oios.org.in", "activeCSRFToken":
"38e11ab18f9514411e692cc96fea14fb", "obfuscateKey":
"2af66249730c96131467a0015fb99e77", "globalobfuscateKey":
"dc0afa12706c3df7164b902174d20f1e", "pxReqURI":
"/prweb/PRAuth/cpY9BqBPHG6rZf8Kpeeoxg*/!TABTHREAD4",
"pxHelpURI":
"https://community.pega.com/sites/default/files/help_v83",
"desktopType": "User", "desktopSubType": "Composite",
"portalName": "CAGPortal", "portalCategory": "",
"pzUnitTestPKey": "CAGPortal", "keepPageMessages" : "false"
Inspector
Selection
17 (0x11)
Selected text
My%20contribution
Decoded from:
URL encoding
My contribution
Cancel
Apply changes
Request attributes
2
Request query parameters
15
Request body parameters
0
Request cookies
7
Request headers
14
Response headers
12

015	PII Disclosure in MyEvents Response
URL	https://preoios.cag.gov.in/

Vulnerable Parameter: /

CVSS: 6.5- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Severity: Medium

Vulnerability Description:

MyEvents response leaks PII (e.g., attendee names, contact details) due to unfiltered data exposure. This risks privacy breaches or data misuse. Attackers can intercept responses to steal information. Fix with server-side PII sanitization, encryption, and role-based access controls to limit exposure of sensitive data to authorized users only.

Impact:

It can lead to the following impacts:

- Leaks attendee names and contacts, risking privacy breaches.
- Enables phishing or social engineering with exposed PII.
- Violates data protection laws, leading to regulatory fines.
- Damages event organizer credibility, reducing user trust and participation.

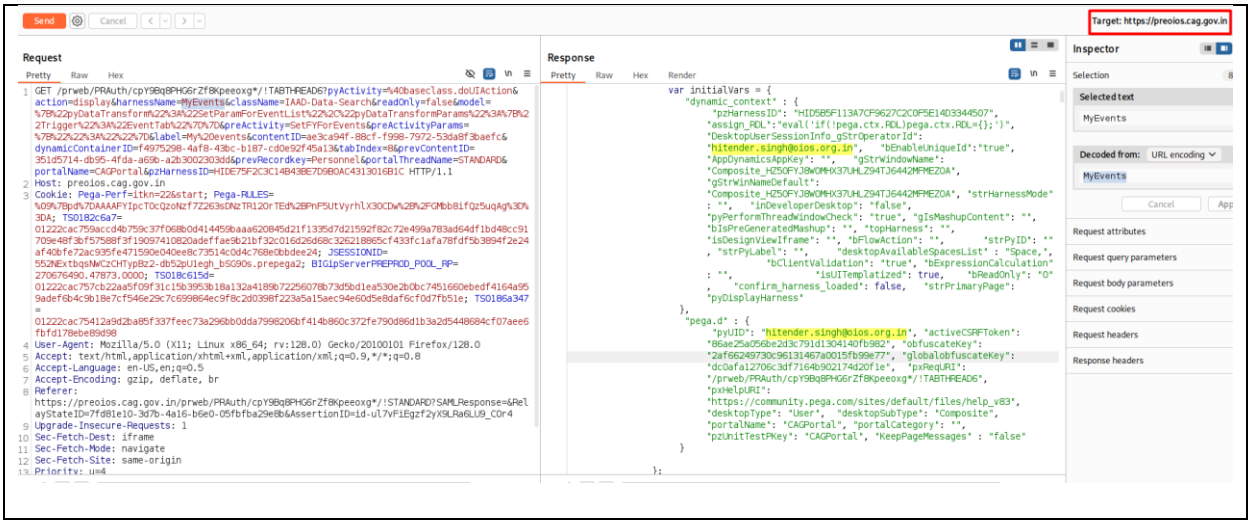
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

- Anonymize attendee PII server-side, per OWASP, masking contact details in responses to prevent privacy breaches while retaining event data.
- Encrypt responses with ISO 27018-compliant protocols, securing PII during transmission and preventing unauthorized access to event data.
- Enforce session-based access controls, per NIST, limiting PII to event organizers and logging access for audit purposes.
- Scan responses regularly with GDPR-compliant tools, assessing and mitigating PII exposure in MyEvents response workflows.

Proof of Concept:

Step 1: Observe in the API response that sensitive PII such as the user's email (hitender.singh@ioios.org.in) is disclosed in the pyUID field.


Send
Cancel
Target: https://preoios.cag.gov.in
Request
Pretty
Raw
Hex
GET /prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!TABTHREAD6?pyActivity=%40baseclass.doUIAction&action=display&harnessName=MyEvents&className=IAAD-Data-Search&readOnly=false&model=%7B%22pyDataTransform%22%3A%22SetParamForEventList%22%2C%22pyDataTransformParams%22%3A%7B%22Trigger%22%3A%22EventTabh%22%7D%7D&preActivity=SetTVForEvents&preActivityParams=%7B%22%22%3A%22%22%7D&label=My%20events&contentID=ae3ca94f-88cf-f998-7972-53da8f3baefc&dynamicContainerID=f4975298-4af8-43bc-b187-cd0e92f45a13&tabIndex=8&prevContentID=351d5714-db95-4fda-a69b-a2b3002303dd&prevRecordkey=Personnel&portalThreadName=STANDARD&portalName=CAGPortal&pzHarnessID=HIDE75F2C3C14B43BE7D9B0AC4313016B1C HTTP/1.1
Host: preoios.cag.gov.in
Cookie: Pega-Perf-itkn=22&start; Pega-RULES=%09%7Bpd%7DAAAAFYIpcTOcQzoNzf7Z263sDNzTR12OrTEd%2BPnF5UtVyrhlX3OCDw%2B%2FGMbb8ifQz5uqAg%3D%3DA; TS0182c6a7=01222cac759accd4b759c37f068b0d414459baaa620845d21f1335d7d21592f82c72e499a783ad64df1bd48cc91709e48f3bf57588f3f1909741082oadeffae9b21bf32c016d26d68c32621886 5cf433fc1afa78fdf5b3894f2e24af40bfe72ac9355fe471590e040ee8c73514c0d4c768e0bbdee24; JSESSIONID=552NExtbqsNWCzCHTypBz2-db52pU1egh_bSG9Os.prepega2; BIGipServerPREPROD_POOL_RP=270676490.47873.0000; TS018c615d=01222cac757cb22aa5f09f31c15b3953b18a132a4189b72256078b73d5bd1ea530e2b0bc7451660ebedf4164a959adef6b4c9b18e7cf546e29c7c699864ec9f8c2d0398f223a5a15aec94e60d5e8daf6cf0d7fb51e; TS0186a347=01222cac75412a9d2ba85f337feec73a296bb0dda7998206bf414b860c372fe790d86d1b3a2d5448684cf07aee6fbfd178ebe89d98
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
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
Referer: https://preoios.cag.gov.in/prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!STANDARD?SAMLResponse=&RelayStateID=7fd81e10-3d7b-4a16-b6e0-05fbfba29e8b&AssertionID=id-ul7vFiEgzf2yX9LRa6LU9_COr4
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Priority: u=4
Response
Pretty
Raw
Hex
Render
var initialVars = {
"dynamic_context" : {
"pzHarnessID": "HID5B5F113A7CF9627C2C0F5E14D3344507",
'assign_RDL':"eval('if(!pega.ctx.RDL)pega.ctx.RDL={};')",
'DesktopUserSessionInfo_gStrOperatorId':
'hitender.singh@oios.org.in", "bEnableUniqueId":"true",
'AppDynamicsAppKey': "", "gStrWindowName':
'Composite_HZ5OFYJ8WOMHX37UHLZ94TJ6442MFMEZOA',
'gStrWinNameDefault':
'Composite_HZ5OFYJ8WOMHX37UHLZ94TJ6442MFMEZOA', "strHarnessMode": "", "inDeveloperDesktop": "false",
"pyPerformThreadWindowCheck": "true", "gIsMashupContent": "",
"bIsPreGeneratedMashup": "", "topHarness": "",
"isDesignViewIframe": "", "bFlowAction": "", "strPyID": "", "strPyLabel": "", "desktopAvailableSpacesList" : "Space,",
"bClientValidation": "true", "bExpressionCalculation": "", "isUITemplatized": true, "bReadOnly": "0",
"confirm_harness_loaded": false, "strPrimaryPage":
"pyDisplayHarness"
},
"pega.d" : {
"pyUID": "hitender.singh@oios.org.in", "activeCSRFToken":
"86ae25a056be2d3c791d1304140fb982", "obfuscateKey":
"2af66249730c96131467a0015fb99e77", "globalobfuscateKey":
"dc0afa12706c3df7164b902174d20f1e", "pxReqURI":
"/prweb/PRAuth/cpY9BqBPHG6rZf8Kpeeoxg*/!TABTHREAD6",
"pxHelpURI":
'https://community.pega.com/sites/default/files/help_v83',
"desktopType": "User", "desktopSubType": "Composite",
"portalName": "CAGPortal", "portalCategory": "",
"pzUnitTestPKey": "CAGPortal", "KeepPageMessages" : "false"
}
};
Inspector
Selection
Selected text
MyEvents
Decoded from: URL encoding
MyEvents
Cancel
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers

016	PII Disclosure in Profile Picture Response
URL	https://preoios.cag.gov.in/

Vulnerable Parameter: /

CVSS: 6.5- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Severity: Medium

Vulnerability Description:

Profile Picture response exposes PII (e.g., user IDs, names) due to improper data handling. This risks privacy violations or identity theft. Attackers can access sensitive data via intercepted responses. Mitigate with server-side data minimization, encryption of metadata, and strict access controls to ensure only authorized users receive profile-related information.

Impact:

It can lead to the following impacts:

- Exposes user IDs and names, risking identity theft.
- Facilitates targeted attacks using intercepted profile-related PII.
- Violates privacy regulations, incurring compliance penalties and fines.
- Undermines user trust, damaging organizational reputation and loyalty.
- PII Disclosure in SendToListDashboard Response

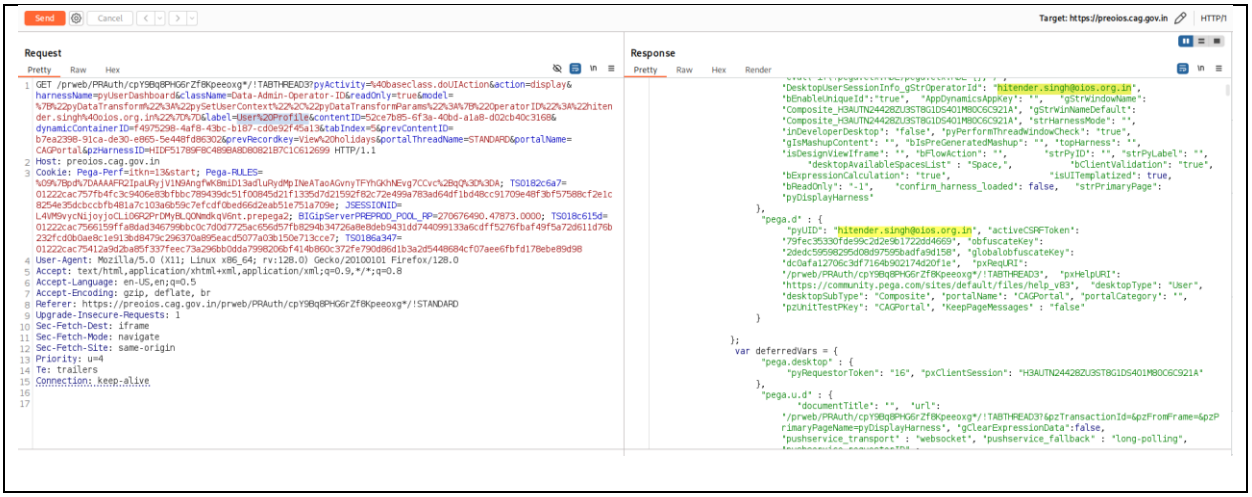
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

- Minimize PII like user IDs server-side, per GDPR, excluding sensitive metadata from profile picture responses to reduce privacy risks.
- Encrypt metadata with TLS 1.3, per NIST, protecting profile data during transmission and preventing interception by unauthorized parties.
- Apply strict access controls, per OWASP ASVS, limiting profile data to authenticated users and logging access for audits.
- Conduct vulnerability scans, per ISO 27001, to identify and patch PII leaks in profile picture response handling.

Proof of Concept:

Step 1: Observe in the API response that sensitive PII such as the user's email (hitender.singh@ioios.org.in) is disclosed in the pyUID field.


Send
Cancel
Target: https://preoios.cag.gov.in
HTTP/1
Request
Pretty
Raw
Hex
GET /prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!TABTHREAD3?pyActivity=%40baseclass.doUIAction&action=display&harnessName=pyUserDashboard&className=Data-Admin-Operator-ID&readOnly=true&model=%7B%22pyDataTransform%22%3A%22pySetUserContext%22%2C%22pyDataTransformParams%22%3A%7B%22OperatorID%22%3A%22hitender.singh%40oios.org.in%22%7D%7D&label=User%20Profile&contentID=52ce7b85-6f3a-40bd-a1a8-d02cb40c3168&dynamicContainerID=f4975298-4af8-43bc-b187-cd0e92f45a13&tabIndex=5&prevContentID=b7ea2398-91ca-de30-e885-5e448fd08302&prevRecordKey=View%20Holidays&portalThreadName=STANDARD&portalName=CAGPortal&pzHarnessID=HIDF51789F8C489BA8D80821B7C1C612699 HTTP/1.1
Host: preoios.cag.gov.in
Cookie: Pega-Perf=itkn=13&start; Pega-RULES=%09%78pd%7DAAAAFR2ipaUFyjVlN9AngfwK0miD13adluRydMpINeATaoAGvnyTFYhGKhNEvg7CCvc%2BqQ%3D%3DA; TSD182c6a7=01222cac757fb4fc3c9406e83bfbbc7894396dc51f00845d21f1335d7d21592f82c72e499a783ad64df1bd48cc91709e48f3bf57588cf2e1c8254e35dcbccbfb481a7c103a6b59c7efcdf0bed66d2eab51e751a709e; JSESSIONID=L4VM9vycNijoyjoCLi06R2PrDMyBLQONmdkqV6nt.prepega2; BIGipServerPREPROD_POOL_RP=270676490.47873.0000; TSD18c615d=01222cac7566159ffa80dad346796bbc0c7d0d7725ac656d57fb8294b34726a8e8deb9431dd744099133a6cdff5276fbaf49f5a72d611d76b232fcd0b0ae8c1e913bd8479c296370a895eacd5077a03b150e713cce7; TSD186a347=01222cac75412a9d2ba85f337feec73a296bb0dda7998206bf414b860c372fe790d86d1b3a2d5448684cf07aee6fbfd178ebe89d98
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
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
Referer: https://preoios.cag.gov.in/prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!STANDARD
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Priority: u=4
Te: trailers
Connection: keep-alive
Response
Pretty
Raw
Hex
Render
'DesktopUserSessionInfo_gStrOperatorId': "hitender.singh@oios.org.in",
'bEnableUniqueId':"true", "AppDynamicsAppKey": "", "gStrWindowName":
'Composite_H3AUTN24428ZU3ST8G1DS4O1M80C6C921A', 'gStrWinNameDefault':
'Composite_H3AUTN24428ZU3ST8G1DS4O1M80C6C921A', 'strHarnessMode': "",
'inDeveloperDesktop': 'false', 'pyPerformThreadWindowCheck': 'true',
'gIsMashupContent': "", 'bIsPreGeneratedMashup': "", 'topHarness': "",
'isDesignViewIframe': "", 'bFlowAction': "", 'strPyID': "", 'strPyLabel': "",
'desktopAvailableSpacesList' : 'Space,', 'bClientValidation': "true",
'bExpressionCalculation': "true", 'isUITemplatized': true,
'bReadOnly': "-1", 'confirm_harness_loaded': false, 'strPrimaryPage':
'pyDisplayHarness'
},
"pega.d" : {
"pyUID": "hitender.singh@oios.org.in", "activeCSRFToken":
'79fec3533Ofde99c2d2e9b1722dd4669', 'obfuscateKey':
'2dedc59598295d08d95759b8adfa9d158', 'globalobfuscateKey':
'dc0afa12706c3df7164b902174d20f1e', "pxReqURI":
'/prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!TABTHREAD3', "pxHelpURI":
'https://community.pega.com/sites/default/files/help_v83', "desktopType": "User",
'desktopSubType': "Composite", "portalName": "CAGPortal", "portalCategory": "",
'pzUnitTestPKey': "CAGPortal", 'keepPageMessages' : 'false'
}
};
var deferredVars = {
"pega.desktop" : {
"pyRequestorToken": "16", "pxClientSession": "H3AUTN24428ZU3ST8G1DS4O1M80C6C921A"
},
"pega.u.d" : {
"documentTitle": "", "url":
'/prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!TABTHREAD3?&pzTransactionId=&pzFromFrame=&pzPrimaryPageName=pyDisplayHarness', 'gClearExpressionData':false,
'pushservice_transport' : 'websocket', 'pushservice_fallback' : 'long-polling',

017	PII Disclosure in SendToListDashboard Response
URL	https://preoios.cag.gov.in/

Vulnerable Parameter: /

CVSS: 6.5- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Severity: Medium

Vulnerability Description:

SendToListDashboard response leaks PII (e.g., user details, addresses) due to inadequate filtering. This risks data breaches or unauthorized access. Attackers can exploit intercepted responses to steal sensitive information. Prevent with server-side data sanitization, encryption, and role-based access controls to restrict PII exposure to authorized users only.

Impact:

It can lead to the following impacts:

- Leaks user details and addresses, enabling data theft.
- Risks regulatory fines for non-compliance with data protection laws.
- Facilitates phishing attacks using exposed sensitive information.
- Erodes user confidence, harming organizational reputation and engagement.

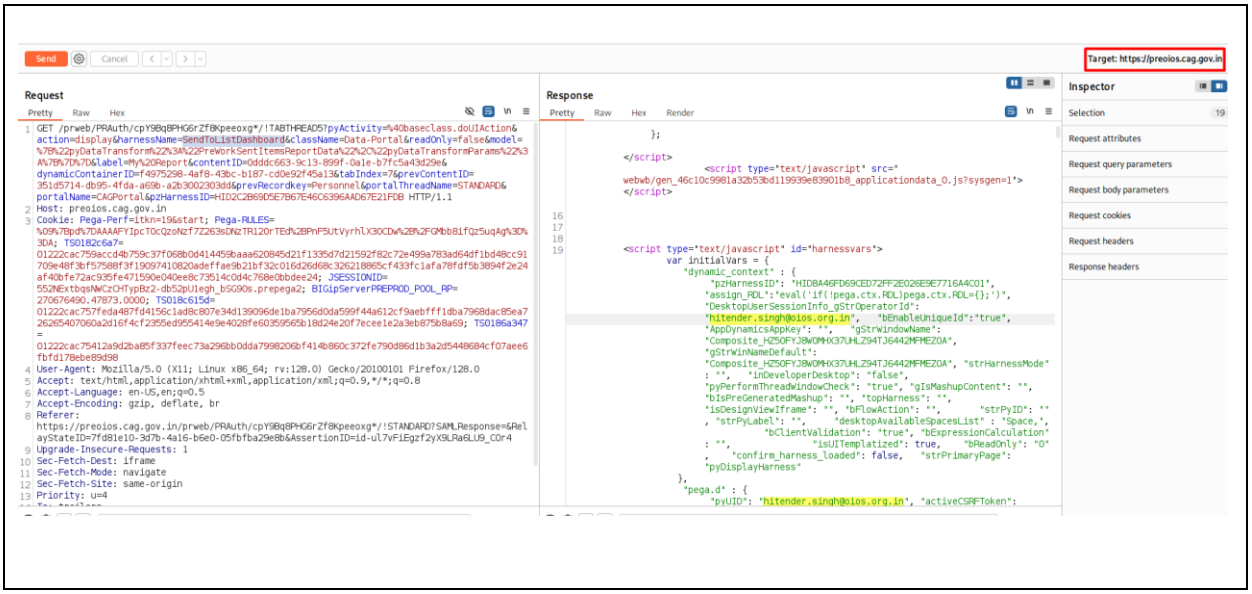
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

- Sanitize PII server-side, per GDPR, removing addresses from dashboard responses to prevent data breaches during transmission or interception.
- Encrypt responses with HTTPS, per OWASP, securing user details from unauthorized access during dashboard data retrieval processes.
- Implement RBAC, per NIST SP 800-53, restricting PII to authorized users and logging requests for compliance and monitoring.
- Perform regular testing, per ISO 27701, to assess and mitigate PII exposure risks in SendToListDashboard response workflows.

Proof of Concept:

Step 1: Observe in the API response that sensitive PII such as the user's email (hitender.singh@ioios.org.in) is disclosed in the pyUID field.


Send
Cancel
Target: https://preoios.cag.gov.in
Request
Pretty
Raw
Hex
GET /prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!TABTHREAD57pyActivity=%40baseclass.doUIAction&action=display&harnessName=SendToListDashboard&className=Data-Portal&readOnly=false&model=%7B%22pyDataTransform%22%3A%22PreWorkSentItemsReportData%22%2C%22pyDataTransformParams%22%3A%7B%7D%7D&label=My%20Report&contentID=0dddc663-9c13-899f-0a1e-b7fc5a43d29e&dynamicContainerID=f4975298-4af8-43bc-b187-cd0e92f45a13&tabIndex=7&prevContentID=351d5714-db95-4fda-a69b-a2b3002303dd&prevRecordkey=Personnel&portalThreadName=STANDARD&portalName=CAGPortal&pzHarnessID=HID2C2B69D5E7B67E46C6396AAD67E21FDB HTTP/1.1
Host: preoios.cag.gov.in
Cookie: Pega-Perf=itkn=19&start; Pega-RULES=%09%7Bpd%7DAAAAFYIpcTOcQzoNzf7Z263sDNzTR12OrTEd%2BPnF5UtVyrhlX3OCDw%2B%2FGMbb8ifQz5uqAg%3D%3DA; TS0182c6a7=01222cac759accd4b759c37f068b0d414459baaa620845d21f1335d7d21592f82c72e499a783ad64df1bd48cc91709e48f3bf57508f3f1909741082Oadeffae9b21bf32c016d26d69c32621080Scf433fc1afa78fdf5b3894f2e24af40bfe72ac935fe471590e040ee8c73514c0d4c768e0bbdee24; JSESSIONID=552NExtbqsNWCzCHTypBz2-db52pUlegh_bSG9Os.prepega2; BIGipServerPREPROD_POOL_RP=270676490.47873.0000; TS018c615d=01222cac757feda487fd4156c1ad8c807e34d139096de1ba7956d0da599f44a612cf9aebfff1dba7968dac85ea72626540706Oa2d16f4cf2355ed955414e9e4028fe60359565b18d24e20f7eceele2a3eb875b8a69; TS0186a347=01222cac75412a9d2ba85f337feec73a296bb0dda7998206bf414b860c372fe790d86d1b3a2d5448684cf07aee6fbfd178ebe89d98
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
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
Referer: https://preoios.cag.gov.in/prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!STANDARD?SAMLResponse=&RelayStateID=7fd81e10-3d7b-4a16-b6e0-05fbfba29e8b&AssertionID=id-ul7vFiEgzf2yX9LRaGLU9_COr4
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Priority: u=4
Response
Pretty
Raw
Hex
Render
};
</script>
<script type="text/javascript" src="
webwb/gen_46c10c9981a32b53bd119939e83901b8_applicationdata_0.js?sysgen=1">
</script>
<script type="text/javascript" id="harnessvars">
var initialVars = {
"dynamic_context" : {
"pzHarnessID": "HID8A46FD69CED72FF2E026E9E7716A4C01",
"assign_RDL":"eval('if(!pega.ctx.RDL)pega.ctx.RDL={};')",
"DesktopUserSessionInfo_gStrOperatorId":
"hitender.singh@oios.org.in", "bEnableUniqueId":"true",
"AppDynamicsAppKey": "", "gStrWindowName":
"Composite_HZ5OFYJ8W0MHX37UHLZ94TJ6442MFMEZOA",
"gStrWinNameDefault":
"Composite_HZ5OFYJ8W0MHX37UHLZ94TJ6442MFMEZOA", "strHarnessMode"
: "", "inDeveloperDesktop": "false",
"pyPerformThreadWindowCheck": "true", "gIsMashupContent": "",
"bIsPreGeneratedMashup": "", "topHarness": "",
"isDesignViewIframe": "", "bFlowAction": "", "strPyID": ""
, "strPyLabel": "", "desktopAvailableSpacesList" : "Space,",
"bClientValidation": "true", "bExpressionCalculation"
: "", "isUITemplatized": true, "bReadOnly": "O"
, "confirm_harness_loaded": false, "strPrimaryPage":
"pyDisplayHarness"
},
"pega.d" : {
"pyUID": "hitender.singh@oios.org.in", "activeCSRFToken":
Inspector
Selection
19
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers

018	Error Based User Enumeration on Password Reset Page
URL:	https://preoios.cag.gov.in/

Vulnerable Parameter: /

CVSS: 4.3- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Severity: Low

Vulnerability Description:

The password reset page reveals user existence through distinct error messages for valid versus invalid usernames, enabling attackers to enumerate valid accounts. This risks targeted phishing or brute-force attacks. Mitigate by standardizing error messages, implementing rate limiting, and adding CAPTCHA to deter automated enumeration, ensuring compliance with OWASP and GDPR guidelines for user privacy protection.

Impact:

It can lead to the following impacts:

- Enables attackers to identify valid accounts, increasing risks of targeted phishing campaigns exploiting user data, violating GDPR privacy requirements.
- Facilitates brute-force attacks, potentially compromising accounts and leading to unauthorized access or data breaches, impacting user trust.
- Exposes system to automated enumeration, overwhelming servers and causing denial-of-service, disrupting legitimate user access and operations.
- Undermines compliance with OWASP and ISO 27001, risking legal penalties and reputational damage due to poor privacy practices.

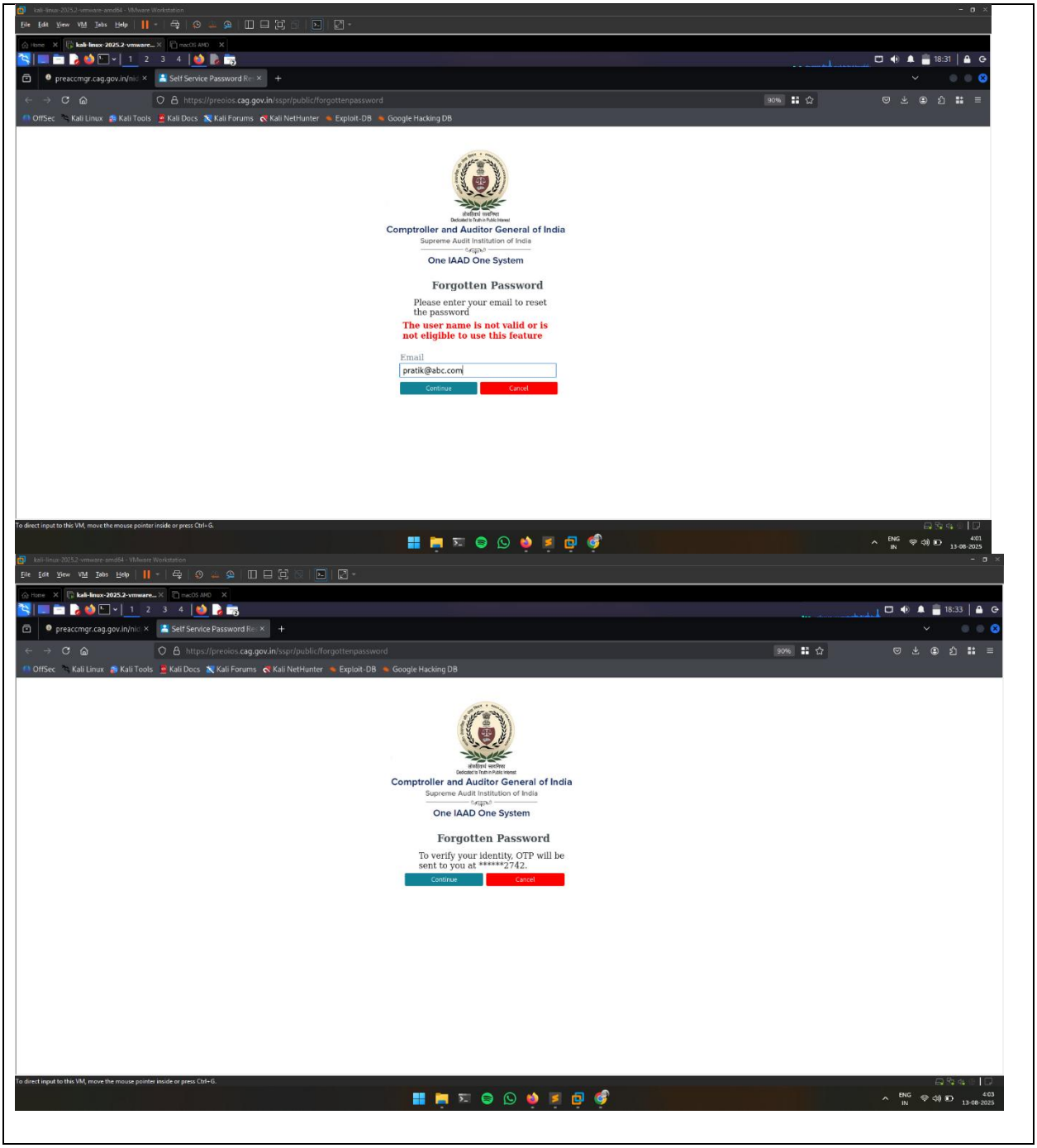
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

- Standardize error messages for valid and invalid usernames per OWASP guidelines, ensuring no user existence is revealed, reducing phishing and brute-force risks while maintaining GDPR compliance for privacy protection.
- Implement rate limiting on password reset requests (e.g., 5 attempts/minute) per NIST SP 800-63B, throttling automated enumeration attempts and integrating with SIEM for real-time monitoring of suspicious activity.
- Add CAPTCHA challenges after repeated failed attempts, following OWASP recommendations, to deter bots and prevent automated enumeration, enhancing security and protecting user accounts from targeted attacks.
- Conduct regular audits and penetration testing per ISO 27001, identifying and fixing enumeration vulnerabilities in password reset workflows to ensure robust privacy and security controls.

Proof of Concept:

Step 1: We can observe that the error message is showing whether the username is valid or not.


Comptroller and Auditor General of India
Supreme Audit Institution of India
One IAAD One System
Forgotten Password
Please enter your email to reset the password
The user name is not valid or is not eligible to use this feature
Email
pratik@abc.com
Continue
Cancel
Comptroller and Auditor General of India
Supreme Audit Institution of India
One IAAD One System
Forgotten Password
To verify your identity, OTP will be sent to you at ******2742.
Continue
Cancel

019	Concurrent Logins
URL:	https://preoios.cag.gov.in/

Vulnerable Parameter: /

CVSS: 4.3- CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L

Severity: Low

Vulnerability Description:

Concurrent logins allow multiple simultaneous sessions with the same credentials, risking unauthorized access if credentials are compromised. Attackers can exploit shared accounts, leading to data breaches or session hijacking. Mitigate by enforcing single-session policies, implementing session timeouts, and using device fingerprinting per NIST SP 800-63B to detect and block suspicious concurrent access, enhancing account security.

Impact:

It can lead to the following impacts:

- Allows unauthorized access via stolen credentials, leading to data breaches, financial loss, or sensitive information exposure, violating user privacy.
- Increases session hijacking risks, enabling attackers to impersonate users, manipulate data, or disrupt services, impacting system integrity.
- Complicates audit trails, hindering detection of malicious activities, and violating NIST SP 800-63B security standards for session management.
- Erodes user trust, as concurrent logins may expose shared accounts to misuse, leading to reputational and operational damage.

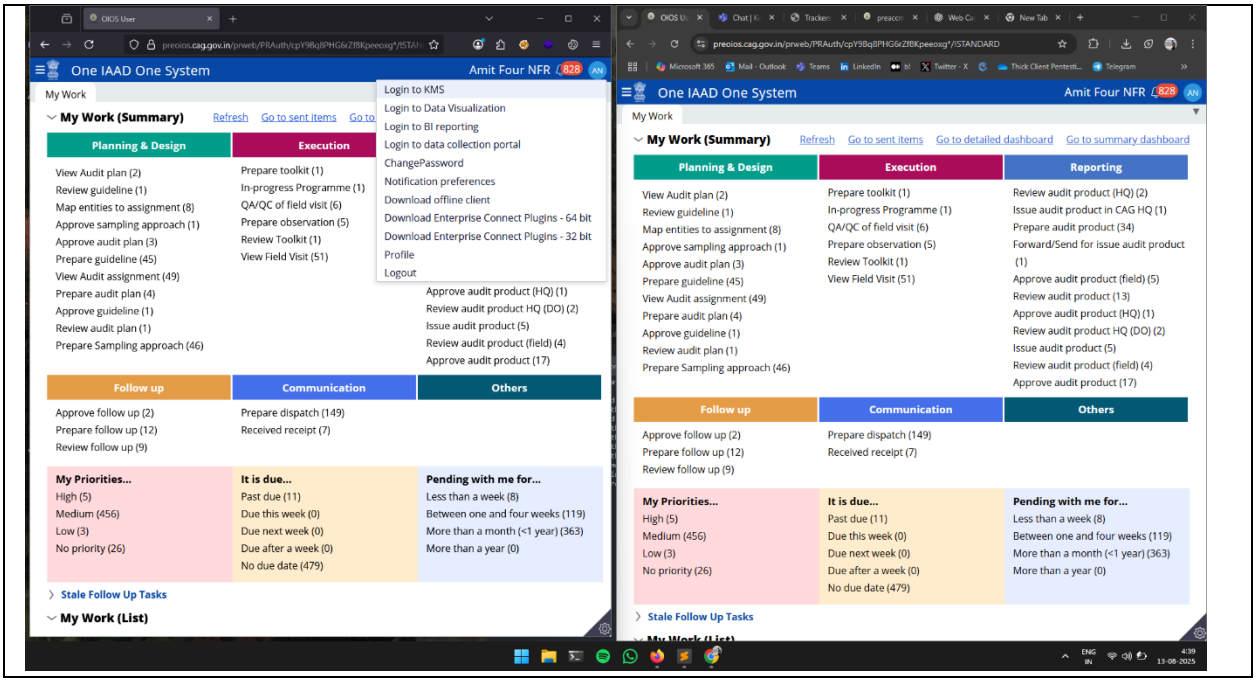
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

- Enforce single-session policies per NIST SP 800-63B, invalidating previous sessions upon new login to prevent unauthorized access and reduce risks of session hijacking or data breaches.
- Implement session timeouts (e.g., 15 minutes of inactivity) per OWASP guidelines, automatically terminating idle sessions to minimize exposure from compromised credentials and enhance account security.
- Use device fingerprinting and behavioral analysis, aligned with ISO 27001, to detect and block suspicious concurrent logins, logging anomalies for forensic investigation and compliance auditing.
- Deploy multi-factor authentication (MFA) per PCI DSS 8.3, adding an extra verification layer to ensure only legitimate users access accounts, mitigating risks of shared credential misuse.

Proof of Concept:

Step 1: Outdated


One IAAD One System
Amit Four NFR
My Work
My Work (Summary)
Refresh
Go to sent items
Planning & Design
Execution
Reporting
Follow up
Communication
Others
Login to KMS
Login to Data Visualization
Login to BI reporting
Login to data collection portal
ChangePassword
Notification preferences
Download offline client
Download Enterprise Connect Plugins - 64 bit
Download Enterprise Connect Plugins - 32 bit
Profile
Logout
My Priorities...
It is due...
Pending with me for...
Stale Follow Up Tasks
My Work (List)

020	Text injection on error Page
URL:	https://preoios.cag.gov.in/

Vulnerable Parameter: /

CVSS: 4.3- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

Severity: Low

Vulnerability Description:

Text injection on error pages allows attackers to inject malicious scripts or content via user inputs, risking cross-site scripting (XSS) attacks. This can lead to session theft or data compromise. Mitigate by sanitizing inputs, encoding outputs per OWASP guidelines, and implementing a robust Content Security Policy (CSP) to prevent script execution and protect users from malicious content.

Impact:

It can lead to the following impacts:

- Enables XSS attacks, allowing attackers to steal session cookies, compromising user accounts and sensitive data, breaching confidentiality.
- Facilitates malicious script execution, leading to unauthorized actions like data theft or user redirection, violating OWASP security guidelines.
- Risks defacement of error pages, degrading user experience and trust, and potentially exposing systems to further exploits.
- Increases vulnerability to client-side attacks, undermining GDPR compliance and risking legal consequences for data protection failures.

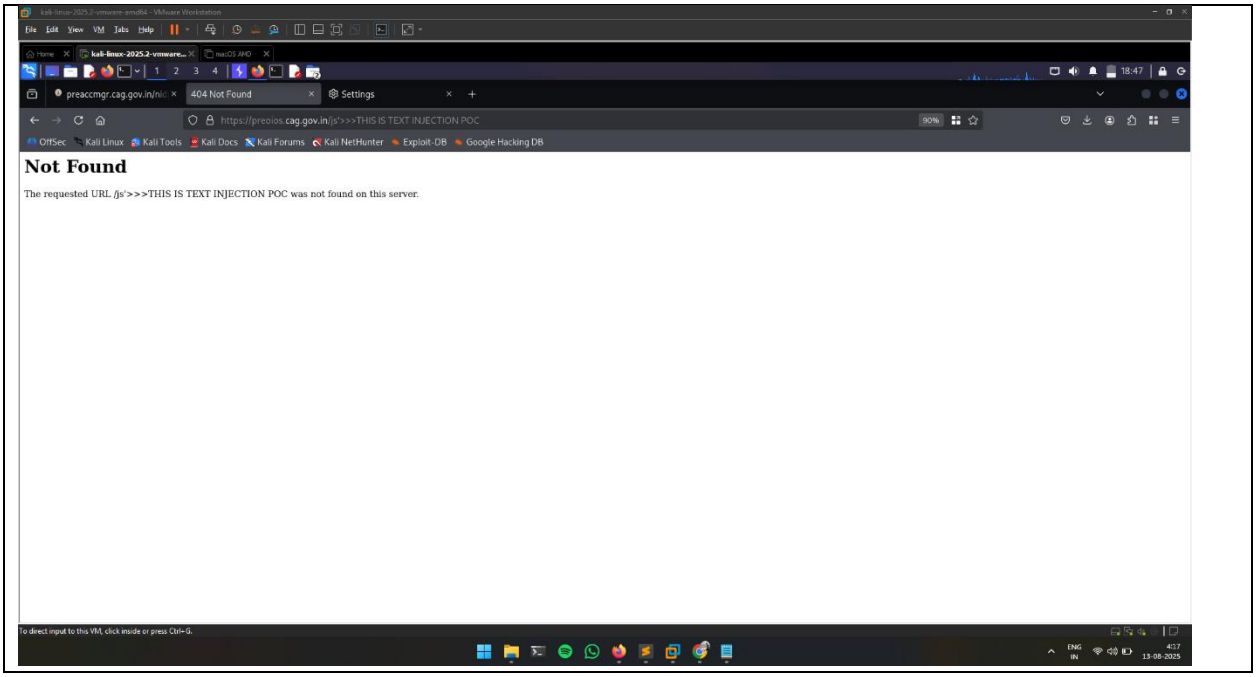
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

- Sanitize user inputs server-side using OWASP-recommended libraries (e.g., DOMPurify) to prevent XSS by removing malicious scripts, ensuring safe error page rendering and protecting user sessions.
- Encode all outputs on error pages per OWASP XSS Prevention Cheat Sheet, escaping special characters to block script execution and reduce risks of session theft or data compromise.
- Implement a strict Content Security Policy (CSP) per OWASP, restricting script sources to trusted domains, enforcing HTTPS, and preventing unauthorized code execution on error pages.
- Regularly test error page inputs with automated tools compliant with ISO 27001, identifying injection vulnerabilities and applying patches to maintain secure user interactions and compliance.

Proof of Concept:

Step 1: We can observe that we are able to inject script on error page.


404 Not Found
Settings
https://preciois.cag.gov.in/js'>>>THIS IS TEXT INJECTION POC
Not Found
The requested URL /js'>>>THIS IS TEXT INJECTION POC was not found on this server.

021	Missing Custom Error Page Leads to Server Version Disclosure
URL:	https://preoios.cag.gov.in/js

Vulnerable Parameter: /js

CVSS: 4.3- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Severity: Low

Vulnerability Description:

Without custom error pages, server errors expose version details, enabling attackers to exploit known vulnerabilities in specific server software. This risks targeted attacks like remote code execution. Mitigate by configuring custom error pages, disabling server banners, and following OWASP and NIST SP 800-53 guidelines to obscure server details and reduce attack surface exposure.

Impact:

It can lead to the following impacts:

- Exposes server software versions, enabling attackers to exploit known vulnerabilities, risking remote code execution or system compromise.
- Increases attack surface, as disclosed details guide targeted attacks, potentially leading to data breaches and operational disruptions.
- Violates OWASP and NIST SP 800-53 guidelines, risking non-compliance penalties and reputational damage due to poor security practices.
- Facilitates reconnaissance, allowing attackers to plan sophisticated attacks, compromising system integrity and user data security.

Recommendation:

We recommend the following security measures to mitigate the vulnerability:

- Configure custom error pages for all server responses per OWASP, suppressing version details and genericizing messages to prevent attackers from identifying exploitable software vulnerabilities.
- Disable server banners and headers exposing version information, following NIST SP 800-53 guidelines, to reduce attack surface and protect against targeted exploits like remote code execution.
- Implement logging and monitoring of error responses per ISO 27001, analyzing for unintended disclosures and integrating with SIEM to detect reconnaissance attempts and ensure compliance.
- Conduct periodic vulnerability scans and penetration tests, aligned with OWASP ASVS, to verify error page configurations and eliminate information leakage risks across all endpoints.

Proof of Concept:

Step 1: We


https://preoios.cag.gov.in/js/libs/jquery
li Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
404 Not Found
nginx

022	Weak Content Security Policy
URL:	https://preoios.cag.gov.in/

Vulnerable Parameter: /

CVSS: 4.3- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

Severity: Low

Vulnerability Description:

A weak Content Security Policy (CSP) fails to restrict resource loading, allowing malicious scripts or content to execute, risking XSS attacks or data theft. Mitigate by implementing a strict CSP per OWASP, limiting sources to trusted domains, enforcing HTTPS, and regularly auditing policy effectiveness to ensure robust protection against unauthorized script execution and client-side attacks.

Impact:

It can lead to the following impacts:

- Allows malicious script execution, enabling XSS attacks that steal user data or sessions, breaching confidentiality and GDPR compliance.
- Increases risk of unauthorized content loading, leading to data theft or user manipulation, undermining system security and trust.
- Fails to enforce HTTPS, risking data interception and protocol downgrade attacks, violating OWASP security recommendations.
- Exposes system to client-side vulnerabilities, complicating compliance with ISO 27001 and increasing legal and reputational risks.

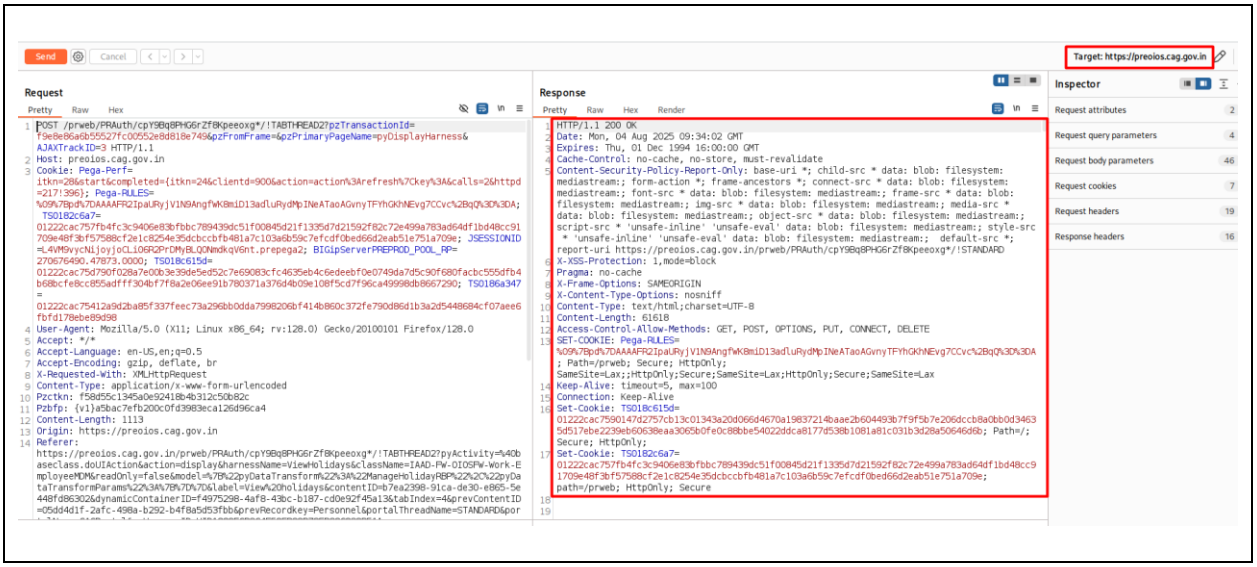
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

- Deploy a strict CSP per OWASP, limiting resource loading to trusted domains (e.g., 'self'), enforcing HTTPS, and blocking inline scripts to prevent XSS and data theft.
- Regularly audit CSP configurations using tools compliant with ISO 27001, ensuring policy effectiveness and updating directives to address new threats and maintain robust client-side security.
- Enforce HTTPS-only resources in CSP headers, per NIST SP 800-52, preventing mixed content vulnerabilities and ensuring secure data transmission across all web interactions.
- Educate developers on CSP best practices via OWASP guidelines, integrating secure coding reviews to prevent weak policies and ensure compliance with industry security standards.

Proof of Concept:

Step 1: Intercept any HTTPS request to https://preoios.cag.gov.in using Burp Suite and observe the response headers showing weak Content-Security-Policy (unsafe-inline, unsafe-eval)


Send
Cancel
Target: https://preoios.cag.gov.in
Request
Pretty Raw Hex
POST /prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!TABTHREAD2?pzTransactionId=
f9e8e86a6b55527fc00552e8d818e749&pzFromFrame=&pzPrimaryPageName=pyDisplayHarness&
AJAXTrackID=3 HTTP/1.1
Host: preoios.cag.gov.in
Cookie: Pega-Perf=
itkn=28&start&completed={itkn=24&clientd=900&action=action%3Arefresh%7Ckey%3A&calls=2&httpd
=217!396}; Pega-RULES=
%09%7Bpd%7DAAAAFR2IpaURyjV1N9AngfwKBmiD13adluRydMpINeATaoAGvnyTFYhGKhNEvg7CCvc%2BqQ%3D%3DA;
TS018Bc6a7=
01222cac757fb4fc3c9406e83bfbbc789439dc51f00845d21f1335d7d21592f82c72e499a783ad64df1bd48cc91
709e48f3bf57588cf2e1c8254e35dcbccbfb481a7c103a6b59c7efcdf0bed66d2eab51e751a709e; JSESSIONID
=L4VM9vycNiJoyjoCLiO6P2PrDMyBLQONmdkqV6Nt.prepega2; BIGipServerPREPROD_POOL_RP=
270676490.47873.0000; TS018c615d=
01222cac75d790f028a7e00b3e39de5ed52c7e69083cfc4635eb4c6edeebf0e0749da7d5c90f680facbc555dfb4
b68bcfe8cc855adfff304bf7f8a2e06ee91b780371a376d4b09e108f5cd7f96ca49998db8667290; TS0186a347
=
01222cac75412a9d2ba85f337feec73a296bb0dda7998206bf414b860c372fe790d86d1b3a2d5448684cf07aee6
fbfd178ebe89d98
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded
Pzctkn: f58d55c1345a0e92418b4b312c50b82c
Pzbfp: {v1}a5bac7efb200c0fd3983eca126d96ca4
Content-Length: 1113
Origin: https://preoios.cag.gov.in
Referer:
https://preoios.cag.gov.in/prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!TABTHREAD2?pyActivity=%40b
aseclass.doUIAction&action=display&harnessName=ViewHolidays&className=IAAD-FW-OIOSFW-Work-E
mployeeMDM&readOnly=false&model=%7B%22pyDataTransform%22%3A%22Manage+Holiday+RBP%22%2C%22pyDa
taTransformParams%22%3A%7B%7D%7D&label=View%20holidays&contentID=b7ea2398-91ca-de30-e865-5e
448fd86302&dynamicContainerID=f4975298-4af8-43bc-b187-cd0e92f45a13&tabIndex=4&prevContentID
=05dd4d1f-2afc-498a-b292-b4f8a5d53fbb&prevRecordkey=Personnel&portalThreadName=STANDARD&por
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Date: Mon, 04 Aug 2025 09:34:02 GMT
Expires: Thu, 01 Dec 1994 16:00:00 GMT
Cache-Control: no-cache, no-store, must-revalidate
Content-Security-Policy-Report-Only: base-uri *; child-src * data: blob: filesystem:
mediastream:; form-action *; frame-ancestors *; connect-src * data: blob: filesystem:
mediastream:; font-src * data: blob: filesystem: mediastream:; frame-src * data: blob:
filesystem: mediastream:; img-src * data: blob: filesystem: mediastream:; media-src *
data: blob: filesystem: mediastream:; object-src * data: blob: filesystem: mediastream:;
script-src * 'unsafe-inline' 'unsafe-eval' data: blob: filesystem: mediastream:; style-src
* 'unsafe-inline' 'unsafe-eval' data: blob: filesystem: mediastream:; default-src *;
report-uri https://preoios.cag.gov.in/prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!STANDARD
X-XSS-Protection: 1,mode=block
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Type: text/html;charset=UTF-8
Content-Length: 61618
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, CONNECT, DELETE
SET-COOKIE: Pega-RULES=
%09%7Bpd%7DAAAAFR2IpaURyjV1N9AngfwKBmiD13adluRydMpINeATaoAGvnyTFYhGKhNEvg7CCvc%2BqQ%3D%3DA
; Path=/prweb; Secure; HttpOnly;
SameSite=Lax;;HttpOnly;Secure;SameSite=Lax;HttpOnly;Secure;SameSite=Lax
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: TS018c615d=
01222cac7590147d2757cb13c01343a20d066d4670a19837214baae2b604493b7f9f5b7e206dccb8a0bb0d3463
5d517ebe2239eb60638eaa3065b0fe0c88bbe54022ddca8177d538b1081a81c031b3d28a50646d6b; Path=/;
Secure; HttpOnly;
Set-Cookie: TS0182c6a7=
01222cac757fb4fc3c9406e83bfbbc789439dc51f00845d21f1335d7d21592f82c72e499a783ad64df1bd48cc9
1709e48f3bf57588cf2e1c8254e35dcbccbfb481a7c103a6b59c7efcdf0bed66d2eab51e751a709e;
path=/prweb; HttpOnly; Secure
Inspector
Request attributes 2
Request query parameters 4
Request body parameters 46
Request cookies 7
Request headers 19
Response headers 16

023	Strict Transport Security Header Missing
URL:	https://preoios.cag.gov.in/

Vulnerable Parameter: /

CVSS: 4.3- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Severity: Low

Vulnerability Description:

Missing HTTP Strict Transport Security (HSTS) headers allows connections over unencrypted HTTP, risking man-in-the-middle attacks and data interception. Mitigate by enabling HSTS with a long max-age per OWASP and NIST SP 800-52, forcing HTTPS connections, including subdomains, and adding the site to HSTS preload lists to ensure secure communication and prevent protocol downgrade attacks.

Impact:

It can lead to the following impacts:

- Permits unencrypted HTTP connections, risking man-in-the-middle attacks and data interception, compromising user confidentiality and GDPR compliance.
- Enables protocol downgrade attacks, exposing sensitive data to eavesdropping, undermining system security and user trust.
- Increases vulnerability to session hijacking, allowing attackers to steal credentials or data, violating OWASP security standards.
- Risks non-compliance with NIST SP 800-52, leading to regulatory penalties and reputational damage for inadequate security measures.

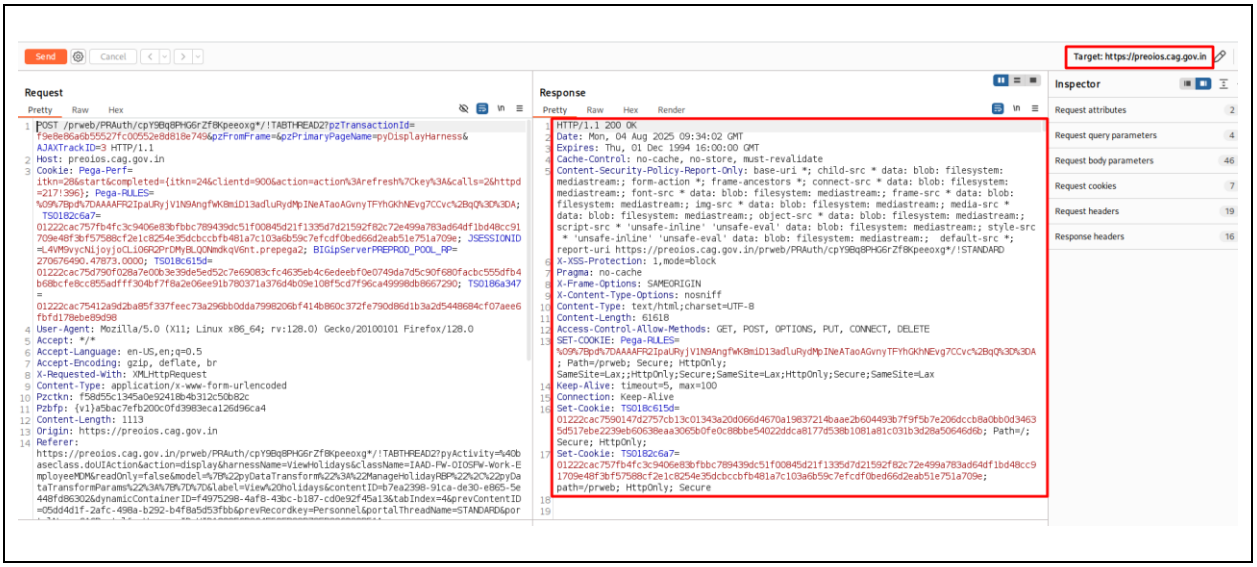
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

- an-in-the-middle attacks and data interception.
- Add the site to HSTS preload lists, per NIST SP 800-52, ensuring browsers enforce HTTPS, reducing risks of protocol downgrade attacks and enhancing user trust.
- Monitor HSTS compliance with automated tools per ISO 27001, logging non-HTTPS requests and alerting administrators to misconfigurations to maintain secure communication channels.
- Conduct penetration testing to verify HSTS enforcement, aligned with OWASP ASVS, identifying and fixing vulnerabilities that allow unencrypted connections to ensure robust security.

Proof of Concept:

Step 1: Intercept any HTTPS request to https://preoios.cag.gov.in using Burp Suite and observe the response headers showing missing HSTS.


Send
Cancel
Target: https://preoios.cag.gov.in
Request
Pretty Raw Hex
POST /prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!TABTHREAD2?pzTransactionId=
f9e8e86a6b55527fc00552e8d818e749&pzFromFrame=&pzPrimaryPageName=pyDisplayHarness&
AJAXTrackID=3 HTTP/1.1
Host: preoios.cag.gov.in
Cookie: Pega-Perf=
itkn=28&start&completed={itkn=24&clientd=900&action=action%3Arefresh%7Ckey%3A&calls=2&httpd
=217!396}; Pega-RULES=
%09%7Bpd%7DAAAAFR2IpaURyjV1N9AngfwKBmiD13adluRydMpINeATaoAGvnyTFYhGKhNEvg7CCvc%2BqQ%3D%3DA;
TS018Bc6a7=
01222cac757fb4fc3c9406e83bfbbc789439dc51f00845d21f1335d7d21592f82c72e499a783ad64df1bd48cc91
709e48f3bf57588cf2e1c8254e35dcbccbfb481a7c103a6b59c7efcdf0bed66d2eab51e751a709e; JSESSIONID
=L4VM9vycNiJoyjoCLiO6P2PrDMyBLQONmdkqV6Nt.prepega2; BIGipServerPREPROD_POOL_RP=
270676490.47873.0000; TS018c615d=
01222cac75d790f028a7e00b3e39de5ed52c7e69083cfc4635eb4c6edeebf0e0749da7d5c90f680facbc555dfb4
b68bcfe8cc855adfff304bf7f8a2e06ee91b780371a376d4b09e108f5cd7f96ca49998db8667290; TS0186a347
=
01222cac75412a9d2ba85f337feec73a296bb0dda7998206bf414b860c372fe790d86d1b3a2d5448684cf07aee6
fbfd178ebe89d98
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded
Pzctkn: f58d55c1345a0e92418b4b312c50b82c
Pzbfp: {v1}a5bac7efb200c0fd3983eca126d96ca4
Content-Length: 1113
Origin: https://preoios.cag.gov.in
Referer:
https://preoios.cag.gov.in/prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!TABTHREAD2?pyActivity=%40b
aseclass.doUIAction&action=display&harnessName=ViewHolidays&className=IAAD-FW-OIOSFW-Work-E
mployeeMDM&readOnly=false&model=%7B%22pyDataTransform%22%3A%22Manage+Holiday+RBP%22%2C%22pyDa
taTransformParams%22%3A%7B%7D%7D&label=View%20holidays&contentID=b7ea2398-91ca-de30-e865-5e
448fd86302&dynamicContainerID=f4975298-4af8-43bc-b187-cd0e92f45a13&tabIndex=4&prevContentID
=05dd4d1f-2afc-498a-b292-b4f8a5d53fbb&prevRecordkey=Personnel&portalThreadName=STANDARD&por
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Date: Mon, 04 Aug 2025 09:34:02 GMT
Expires: Thu, 01 Dec 1994 16:00:00 GMT
Cache-Control: no-cache, no-store, must-revalidate
Content-Security-Policy-Report-Only: base-uri *; child-src * data: blob: filesystem:
mediastream:; form-action *; frame-ancestors *; connect-src * data: blob: filesystem:
mediastream:; font-src * data: blob: filesystem: mediastream:; frame-src * data: blob:
filesystem: mediastream:; img-src * data: blob: filesystem: mediastream:; media-src *
data: blob: filesystem: mediastream:; object-src * data: blob: filesystem: mediastream:;
script-src * 'unsafe-inline' 'unsafe-eval' data: blob: filesystem: mediastream:; style-src
* 'unsafe-inline' 'unsafe-eval' data: blob: filesystem: mediastream:; default-src *;
report-uri https://preoios.cag.gov.in/prweb/PRAuth/cpY9Bq8PHG6rZf8Kpeeoxg*/!STANDARD
X-XSS-Protection: 1,mode=block
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Type: text/html;charset=UTF-8
Content-Length: 61618
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, CONNECT, DELETE
SET-COOKIE: Pega-RULES=
%09%7Bpd%7DAAAAFR2IpaURyjV1N9AngfwKBmiD13adluRydMpINeATaoAGvnyTFYhGKhNEvg7CCvc%2BqQ%3D%3DA
; Path=/prweb; Secure; HttpOnly;
SameSite=Lax;;HttpOnly;Secure;SameSite=Lax;HttpOnly;Secure;SameSite=Lax
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: TS018c615d=
01222cac7590147d2757cb13c01343a20d066d4670a19837214baae2b604493b7f9f5b7e206dccb8a0bb0d3463
5d517ebe2239eb60638eaa3065b0fe0c88bbe54022ddca8177d538b1081a81c031b3d28a50646d6b; Path=/;
Secure; HttpOnly;
Set-Cookie: TS0182c6a7=
01222cac757fb4fc3c9406e83bfbbc789439dc51f00845d21f1335d7d21592f82c72e499a783ad64df1bd48cc9
1709e48f3bf57588cf2e1c8254e35dcbccbfb481a7c103a6b59c7efcdf0bed66d2eab51e751a709e;
path=/prweb; HttpOnly; Secure
Inspector
Request attributes 2
Request query parameters 4
Request body parameters 46
Request cookies 7
Request headers 19
Response headers 16

024	Overly Permissive Access-Control-Allow-Methods
URL:	https://preoios.cag.gov.in/

Vulnerable Parameter: /

CVSS: 4.3- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Severity: Low

Vulnerability Description:

Overly permissive Access-Control-Allow-Methods headers allow excessive HTTP methods in CORS requests, risking unauthorized API access or data manipulation. This can lead to privilege escalation or data breaches. Mitigate by restricting methods to only necessary ones (e.g., GET, POST) per OWASP, validating origins, and auditing CORS policies to ensure compliance with secure API design standards.

Impact:

It can lead to the following impacts:

- Allows unauthorized API access via excessive HTTP methods, risking data manipulation or privilege escalation, breaching system integrity.
- Facilitates malicious CORS requests, potentially exposing sensitive data to untrusted origins, violating OWASP security guidelines.
- Increases attack surface, enabling attackers to exploit APIs, leading to data breaches and operational disruptions.
- Undermines compliance with secure API standards, risking legal penalties and reputational damage due to poor access controls.

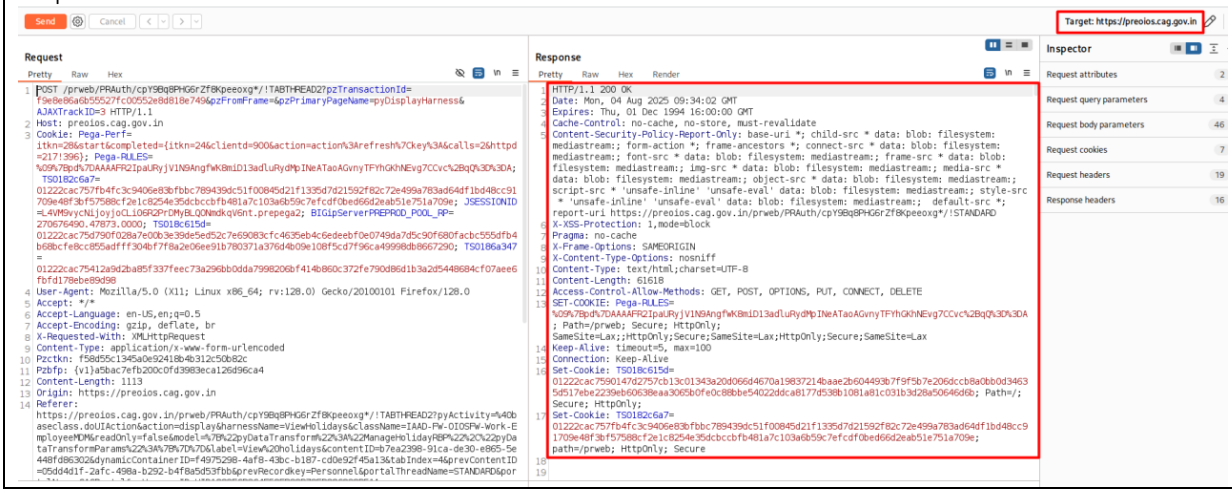
Recommendation:

We recommend the following security measures to mitigate the vulnerability:

- Restrict CORS Access-Control-Allow-Methods to essential HTTP methods (e.g., GET, POST) per OWASP, preventing unauthorized API access and reducing risks of data manipulation or escalation.
- Validate CORS origins server-side, following NIST SP 800-53, allowing only trusted domains and rejecting overly permissive configurations to ensure secure API interactions.
- Audit CORS policies regularly with tools compliant with ISO 27001, logging method requests and analyzing for anomalies to prevent exploitation and maintain compliance.
- Implement rate limiting on CORS-enabled endpoints, per OWASP API Security, throttling excessive requests to mitigate abuse and protect against unauthorized data access attempts.

Proof of Concept:

Step 1: Intercept any HTTPS request to https://preoios.cag.gov.in using Burp Suite and observe the response headers.



025	Unrestricted Access to Oracle Login Page via Directory Enumeration
URL:	https://preoios.cag.gov.in/bi-security-login/login-failed.jsp?msi=false&mt=false&redirect=L2FuYWx5dGljcy9zYXcuZGxsP2dldFByZXZpZXdJbWFnZSZwcmV2aWV3RmlsZVBhdGg9L2V0Yy9wYXNzd2QmaGFzaD0xX3VMT21UV3ViQm5NWWN3SnZNRllrdHQ3NklCOUVMRmJIOEktU2xrLTFBTEQzSm9mZ3gwcnZERXdGMjhQQ2tr&lang=en
Vulnerable Parameter: /bi-security-login/login-failed.jsp?msi=false&mt=false&redirect=L2FuYWx5dGljcy9zYXcuZGxsP2dldFByZXZpZXdJbWFnZSZwcmV2aWV3RmlsZVBhdGg9L2V0Yy9wYXNzd2QmaGFzaD0xX3VMT21UV3ViQm5NWWN3SnZNRllrdHQ3NklCOUVMRmJIOEktU2xrLTFBTEQzSm9mZ3gwcnZERXdGMjhQQ2tr&lang=en		
CVSS: 4.3- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
Severity: Low		

Vulnerability Description:

Unrestricted access to the Oracle login page through directory enumeration exposes sensitive endpoints, risking unauthorized access or brute-force attacks. Attackers can discover hidden paths to target systems. Mitigate by restricting directory access, implementing robots.txt, using strong authentication per OWASP, and deploying WAFs to block enumeration attempts, ensuring compliance with ISO 27001 security standards.

Impact:

It can lead to the following impacts:

- Exposes sensitive login endpoints, enabling brute-force attacks or unauthorized access, compromising system security and user accounts.
- Facilitates reconnaissance, allowing attackers to target Oracle systems, risking data breaches and operational disruptions.
- Violates OWASP and ISO 27001 standards, leading to compliance failures, legal penalties, and reputational damage.
- Increases phishing risks, as exposed login pages enable targeted attacks, undermining user trust and system integrity.

Recommendation:

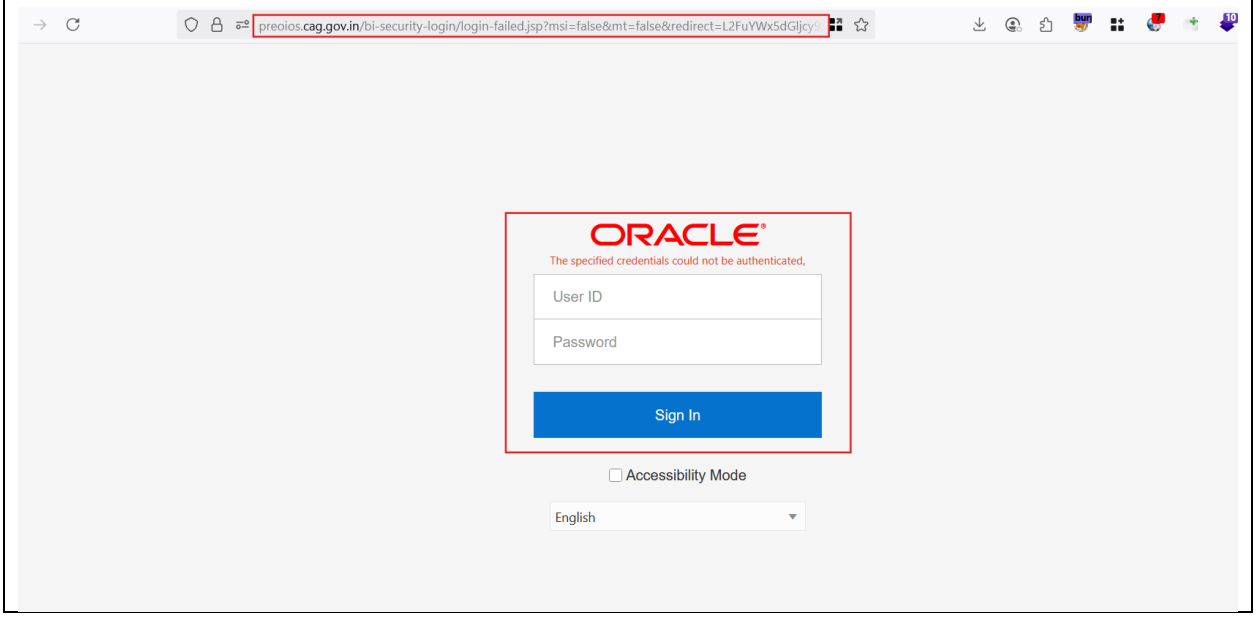
We recommend the following security measures to mitigate the vulnerability:

- Restrict directory access using server configurations (e.g., .htaccess) per OWASP, blocking enumeration attempts and preventing exposure of sensitive Oracle login endpoints to attackers.
- Implement robots.txt and security.txt per ISO 27001, guiding crawlers away from sensitive paths and providing secure reporting channels to reduce enumeration risks.
- Deploy strong authentication (e.g., MFA) on Oracle login pages, following NIST SP 800-63B, to prevent unauthorized access and protect against brute-force attacks.
- Use WAFs to block directory enumeration attempts, per OWASP ASVS, logging and analyzing suspicious requests to ensure compliance and maintain endpoint security.

Proof of Concept:

Step 1: Visit the url:

https://preoios.cag.gov.in/bi-security-login/login-failed.jsp?msi=false&mt=false&redirect=L2FuYWx5dGljcy9zYXcuZGxsP2dldFByZXZpZXdJbWFnZSZwcmV2aWV3RmlsZVBhdGg9L2V0Yy9wYXNzd2QmaGFzaD0xX3VMT21UV3ViQm5NWWN3SnZNRllrdHQ3NklCOUVMRmJIOEktU2xrLTFBTEQzSm9mZ3gwcnZERXdGMjhQQ2tr&lang=en .



SUMMARY OF FINDINGS & CONCLUSION:

Finally, it must be remembered that security is an ongoing process, and that this report will provide an idea of the current vulnerabilities we were able to detect. There is no guarantee that new vulnerabilities will not be found and exploited in the future.

The assessment was only possible because **joint support** & **coordination** from the **information security team of organization** for **sharing & coordinating** during the assessment period. It is advised to refer the **Technical Report** for understanding **in-depth of vulnerabilities** that were discovered **by technical team of CyberSmithSECURE Pvt. Ltd.**

The Security Researchers of the CyberSmithSECURE performed Vulnerability Testing. We jointly recommend that all suggested measures in this document be performed to ensure the overall security of the target website.

We thank internal Information Security team for their support & cooperation during the time of assessment.