Penetration Test Preparation

Information Security Office (ISO)

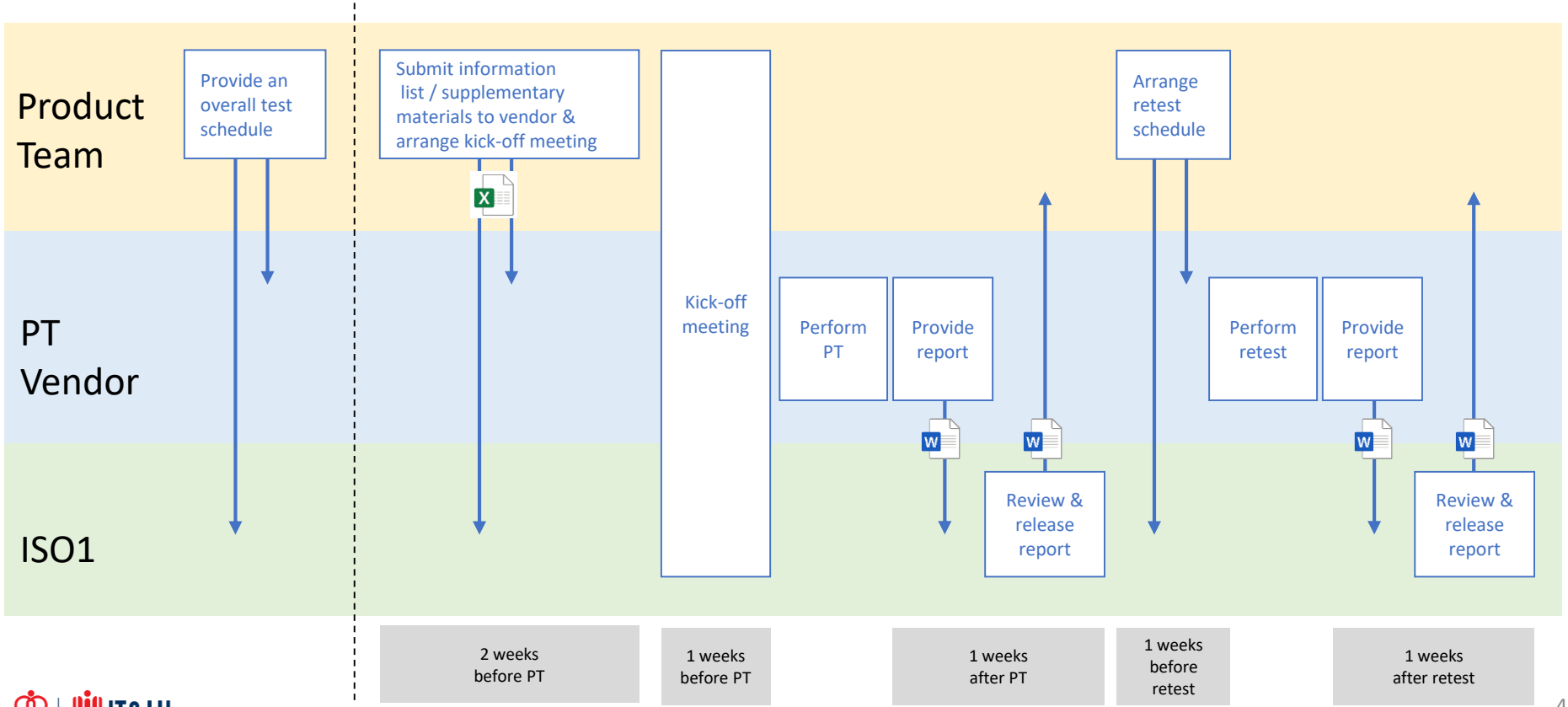
IT&HI Division

Content

- Introducing of Penetration Test (PT)
- Workflow
- PT Preparation
- PT Report and Findings Remediation

Introducing of Penetration Test

Workflow


Product Team
PT Vendor
ISO1
Provide an overall test schedule
Submit information list / supplementary materials to vendor & arrange kick-off meeting
Kick-off meeting
Perform PT
Provide report
Review & release report
Arrange retest schedule
Perform retest
Provide report
Review & release report
2 weeks before PT
1 weeks before PT
1 weeks after PT
1 weeks before retest
1 weeks after retest

Information List (Checklist) (Input by product team)

Information List:

Information	Response
Contact person (name, phone and email)	
Project Name	
Project Description	
System Type (Web App / Mobile App / Infrastructure)	
Login required?	
User roles (e.g. Approver, CMS admin)	
Architecture (On-premise / Private Cloud / Public Cloud)	
For public cloud, specify vendor platform (e.g. AWS)	
Required cloud configuration review?	
Contain API call?	
Entry URLs	
Other hidden URLs	
Testing location (onsite/remote)	
Available testing period	
Available testing time window	

Other Preparation Items (Checklist) (Input by product team)

Others preparation items:

- System architecture diagram – High level
- User guide/manual
- API specifications
- Application testing accounts (2 accounts per user roles)
- Cloud IAM accounts for cloud configuration review (read-only account)
- IP whitelist arrangement for PT vendor to access the target

Kick-off Meeting

- Application briefing
- Test preparation
- Test schedule

Findings Report

2. Summary of Findings

The tables below provide an overview of the findings and their remedial status which should be read in conjunction with the remaining parts of this report. The risk rating does not represent any conclusion on / assessment of the overall effectiveness or adequacy of HA 's security management process. Risk rating definitions are agreed with HA.

Application Penetration Test

ID	Finding	Risk Rating	Status
3.1.1	Client-side Desync	High	Fixed
3.1.2	Improper Error Handling in Search Page	High	Fixed
3.2.1	Unnecessary / insecurity port open in the server	Medium	Not Fixed
3.2.2	Insecure Transport	Medium	Not Fixed
3.3.1	Vulnerable JavaScript Dependency	Low	Not Fixed
3.3.2	Client-side HTTP Parameter Pollution	Low	Not Fixed

Cloud Configuration Review

ID	Finding	Risk Rating	Status
4.1.1	Client-side Desync	High	Fixed
4.1.2	Improper Error Handling in Search Page	High	Fixed
4.2.1	Unnecessary / insecurity port open in the server	Medium	Not Fixed
4.2.2	Insecure Transport	Medium	Not Fixed
4.3.1	Vulnerable JavaScript Dependency	Low	Not Fixed
4.3.2	Client-side HTTP Parameter Pollution	Low	Not Fixed

Findings Report

3. Detailed Results for Application Penetration Test

3.1 High Risk Findings

3.1.1 Client-side Desync

Risk Level	High
Consequence	Major
Likelihood	Likely
OWASP Top Ten	A04:2021-Insecure Design
Affected	xxxxxxxxx/Content/uploads/docs/HUbRcnTbd7725773.pdf

Details

The server may be vulnerable to client-side desync attacks. A POST request was sent to the path '/Content/uploads/docs/HUbRcnTbd7725773.pdf' with a second request inside the body. The server responded before the request body was sent and did not close the connection, which may have lead to the smuggled request being interpreted as the next request. To verify this finding, review the response to 'Request 2'.

Client-side desync (CSD) vulnerabilities occur when a web server fails to correctly process the Content-Length of POST requests. By exploiting this behavior, an attacker can force a victim's browser to desynchronize its connection with the website, typically leading to XSS.

Advisory | Request 1 | Response 1 | Request 2 | Response 2 | Path to issue

Pretty | Raw | Hex | Render

```
1  HTTP/1.1 400 Bad Request
2  Content-Type: text/html; charset=us-ascii
3  Server: Microsoft-HTTPAPI/2.0
4  Date: Mon, 26 Aug 2024 05:02:14 GMT
5  Connection: close
6  Content-Length: 326
7
8  <!DOCTYPE HTML PUBLIC "-//[redacted]
9  <HTML>
     <HEAD>
       <TITLE>
         Bad Request
       </TITLE>
10     <META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii">
     </HEAD>
11   <BODY>
       <h2>
         Bad Request - Invalid Verb
       </h2>
12     <hr>
       <p>
         HTTP Error 400. The request verb is invalid.
       </p>
13   </BODY>
   </HTML>
```

Recommendation

We recommend that you can resolve this vulnerability by patching the server so that it either processes POST requests correctly, or closes the connection after handling them. You could also disable connection reuse entirely, but this may reduce performance. You can also resolve this issue by enabling HTTP/2.

Findings Report

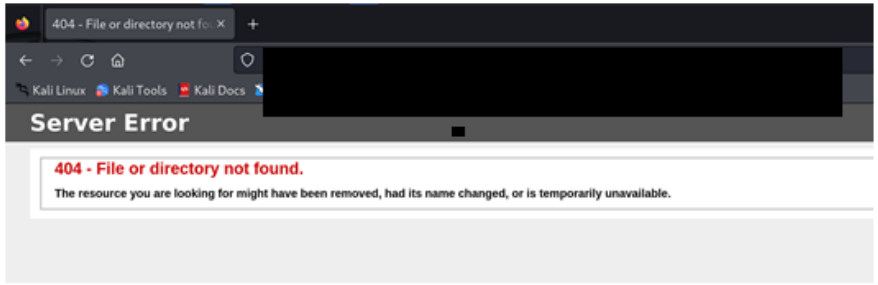
Verification Status

Fixed

Verification Observation

(2024-10-21)

The affected URL has been removed.



Release Report

Dear [redacted]

The penetration test for [redacted] has been completed.
Below is a finding summary and please kindly review the attached report for details.

Penetration Test Finding

Finding ID	Finding	Risk Level	Remediation Due Date	Comment
1	Lacking of API rate limit for the eFeedback Form Submission	Medium	28 May 2024	
2	Improper input validation on Phone Number Parameter[Parameter:tel]	Medium	28 May 2024	
3	No Back End Validation of Comment Field[Parameter:commentl]	Low	28 Aug 2024	

For remediation timeline requirement for each risk level, please refer to HA Guidelines for Vulnerability Management Process [link]
Please kindly let us know when the remediation is completed, we will arrange verification test accordingly.

Thank you.
Best Regards,

Thank you