

|  |
| --- |
| **PHILIPS-SCOE** |
| **XDS 2023-2**  **Intake ID=2764**  **Security Assessment – Statement of Work** |
|  |

**Document Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| Name of the document: SCoE Security Assessment SoW for XDS 2023-2 | | |  |
| Document Version: 1.0 | Document ID: | PRHC/C40/SVN/3037 |
| Author: Sai Praneetha Bhaskaruni, Harshal V |
| Reviewed by: Shabana Bagum | Effective Date: | 18-Oct-2023 |

**Document History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Author | Section | Changes |
| 0.1 | 18-Oct-2023 | Sai Praneetha Bhaskaruni, Harshal Kukade | Complete | Initial Draft |
| 1.0 | 18-Oct-2023 | Shabana Bagum | Complete | Addition and review |

Table of Contents

[**Objective** 4](#_Toc148535514)

[**Scope** 5](#_Toc148535515)

[**Out of Scope** 5](#_Toc148535516)

[**Precautions** 6](#_Toc148535517)

[**Testing logistics** 6](#_Toc148535518)

[**Pre-conditions to be met** 7](#_Toc148535519)

[**Test Suspension criteria** 7](#_Toc148535520)

[**Test Type** 8](#_Toc148535521)

[**Tools used** 8](#_Toc148535522)

[**Testing timeframe** 9](#_Toc148535523)

[**Additional Points of Kick-off Call** 9](#_Toc148535524)

## **Objective**

* Test objectives for this assessment is to find security vulnerabilities, which includes Identification of vulnerabilities, analyze them, and suggest possible mitigations.
* Reporting the vulnerabilities along with the severity ratings
* No penetration testing or exploitation to be done without prior permission. Meanwhile POC could be made to reproduce the issue for better understanding of the vulnerability.
* Report will be delivered after completion of the security assessment.

## **Scope**

**Web Application Testing: XDS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type | Scope of Assessment | | | |
| Web Application | XDS 2023-2 | URL | Admin url:  <https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/admin>    Viewer url:  <https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/viewer>    Audit url:  <https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/audit>  Image upload url:  <https://ec2-3-71-200-223.eu-central-1.compute.amazonaws.com/imageupload> | |
| Version | 2023-2 | |
| Environment | Test | |
| User Roles | root | Credentials available |

## **Out of Scope**

Below Mentioned items are out of scope for the current security assessment:

* Source Code Review
* Stress test (DDOS)

## **Precautions**

* Testing on productions systems is not recommended.
* For Network production system security testing, please refer to the Network Security testing for Production SoW (sent separately – if applicable)
* For application security testing on a production system, Automated scanning and DoS is strictly not allowed unless the BU request for an automated scan.
* Ask the BU to back up the database/application and settings if a scanning must be done on a production system so that if something goes wrong, it can be backed up.
* It is recommended not to perform any other testing (functional testing, stress testing etc.) during the security testing.
* Prior permission should be taken from the third party, to avoid any possible contractual violations from reverse engineering of application.

## **Testing logistics**

Connection through VPN

Accessible from PGN

Public access

VM installed in SCoE lab

Installer sent to SCoE

Physical system sent to SCoE

## **Pre-conditions to be met**

Relevant Product/application documentation provided

Product installation and Setup done

Application accessible

Demo and sample data given

Approvals required for testing

Product under test should have all functionality working as per design

Product Security Risk Assessment to be submitted before testing (if available)

Secure code analysis (e.g Fortify) report to be submitted

Static binary analysis (e.g Blackduck) to be submitted

## **Test Suspension criteria**

Testing may be suspended for a single functional area or the entire system, if any of the following condition arises: -

* Explicitly asked by the BIU.
* If defects of the systems negatively affect testing further functionality.
* If any of the preconditions mentioned in above section are not met.

## **Test Type**

Manual testing

Automated testing

Manual + Automated testing

Black box

Gray box

## **Tools used**

|  |  |
| --- | --- |
| Web application | Burp Suite Pro, ZAP, Nmap, Wappalyzer |

## **Testing timeframe**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Task Name | Duration | Start Date\* | End Date\* | Dependencies | Responsible person |
| Testing | 5 Days | 19-Oct-2023 | 26-Oct-2023 | Test environment should be up and running | Sai Praneetha Bhaskaruni, Harshal Kukade |
| Report preparation and delivery | 2 Days | 27-Oct-2023 | 30-Oct-2023 | Testing should be completed | Sai Praneetha Bhaskaruni, Harshal Kukade |

\*The proposed timeline is subject to the continuous environment readiness and its dependencies. The report delivery date might get extended in case of any roadblocks in the availability of the testing environment or systems.

## **Additional Points of Kick-off Call**

* Note: 24th Oct is holiday.