Homologation Penetration Testing Guide

Sopra Steria Benelux

Homologation SEPA Request-to-Pay (SRTP) Scheme

Abstract	The present questionnaire should be completed by applicants starting the SEPA Request-to-Pay (SRTP) scheme homologation process
Document reference	SSB-SRTP-14
Issue	1.0 - Final
Date of Issue	04/08/2023
Produced by	Sopra Steria Benelux
Verified by	European Payments Council
Circulation	Public information

Table of Contents

1. General description

As part of the SRTP scheme homologation, penetration testing will be executed by the Homologation Body. This test is a special type of penetration test. Its goal is to determine, as main part of the entire homologation process, if the applicant or the technical solution provider (TSP) succeeds the homologation. This decision depends on the number and severity of the vulnerabilities at the end of the test.

Once a vulnerability with medium, high or critical severity has been identified, the applicant or TSP will be informed via the agreed communication channel. When the vulnerabilities lead to test failure and consequently the homologation, the Homologation Body will discuss with the applicant or TSP on how to further proceed. If the vulnerability can be re-tested successfully before the end of the penetration test, it will be reported as “Resolved” and does not have a negative impact on the final decision.

As priority will be given to a maximum of time for executing tests, a basic report will list the vulnerabilities detected, severity and status. This report will mention the conclusion “Pass” or “Fail”. A “Fail” for penetration testing will result in a “Fail” of the entire homologation process. The adherence process to the SRTP scheme can only proceed after a successful re-test at an additional cost.

2. External Black Box Penetration Test

Our approach for this penetration testing assessment will be “black-box” executed from the internet, meaning that our team of penetration testers will not have any prior knowledge about the topology/architecture of the network, technologies utilized, critical systems/applications or any other information about the in-scope systems.

Our methodology in penetration testing assessment consists of a cyclical process, involving a methodical approach to vulnerability identification and exploitation. Unlike other penetration tests or vulnerability assessments, where the aim is to report only the potential vulnerabilities within a system or network, our methodology involves focusing on the main identified weaknesses and their exploitation to verify and highlight their impact. The path of a penetration test may vary depending on the nature of the targets and the vulnerabilities that are identified. Our team of penetration testers follows a phased approach, in a repetitive manner, to achieve the objectives for a given engagement.

An overview of the phases that are being followed in every homologation penetration testing assessment, conducted by Sopra Steria is provided below:

1. Mapping the attack surface

We will work to accurately map the in-scope target networks and systems, to understand potential vulnerabilities and their impact. Then we will identify and categorize ‘live’ (i.e. responding) hosts, determine what services they expose, and fingerprint operating systems and installed software versions. This initial phase will allow us to create a detail-rich list of targets which may offer a route into the network.

2. Identifying potential vulnerabilities

During this phase we will utilize automated vulnerability scanning tools to rapidly appraise the target systems, identify potential security misconfigurations, missing patches, or vulnerable services, which could allow us to gain a foothold within a target system. Manual penetration testing will also be applied to discover new vulnerabilities.

3. Verifying and exploiting vulnerabilities

Using the same tools and techniques as a malicious threat actor, we will explore and manually verify any identified vulnerabilities, where appropriate vulnerabilities will be exploited to gain further access to the network or target systems. Custom exploit code may be developed, or publicly accessible exploits used to help assess a specific vulnerability.

The penetration testing assessment of information systems will be focusing on the identification of security weaknesses and vulnerabilities that will lead our team to get unauthorized access to critical systems of internet facing network. To achieve this objective, we will perform several attacks against the in-scope systems, following a prioritized execution of tests, as described in the below table.

Type of Test	Description of Tests	Test Priority
Exploitation of vulnerable services/ Operating Systems	In-scope systems will be tested for all known security vulnerabilities (CVEs) and misconfigurations, that may affect any of their services or Operating Systems, as of the day that this testing takes place. Our automated tools and manual testing allow us to be certain that any known vulnerability on in-scope assets will be identified.	Very High
Identity & Authentication Weakness Exploitation	Any identified services, such as databases, login pages, remote access protocols, protected by authentication mechanism will be subject to several password attacks (dictionary, password spraying, brute-force, credential staffing).	High
Web application attacks	Web applications in the external network will be also the target of our team during this penetration test, it is possible that they can assist in the compromise of systems and access to sensitive data. In case where our team believes that a web application can provide such opportunity to further compromise the network, they will be subject to web attacks, such as SQLi, XXE, XSS, CSRF or other technology-specific attacks.	High

As the size of the applicant's environment can vary, it is not feasible to execute all tests for larger environments. Therefore, the category of the applicant's environment is first determined. For each category different kind of tests are executed. There are 3 categories recognized by the homologation penetration test: small, medium, and large. The assignment to the category depends on the number of systems that need to be tested, open ports, services exposed and the complexity of those services. The category of the applicant's environment is determined at the beginning of the homologation penetration

test. A hybrid approach is also possible; for example, we can perform the penetration test by using the large category approach, combined with the small category approach for the most critical systems identified by the applicant.

Type of Test	Description of Tests	Categories	Priority for the category
Application hosting platform and technologies	A minimal attack surface, and well-maintained applications and application servers, are key defenses against web application attacks. The application server will be assessed to ensure that only those protocols required for hosting of the application are exposed, and that all exposed services are configured securely and in accordance with established good practice. Where possible the Operating System's likely version and patch level will be assessed. Requests to, and responses from, the application server will be checked to ensure that they implement modern security controls designed to protect application users and data.	Small	Medium
		Medium	Medium
		Large	High
Data Exposure	Consultants will look at the methods being used to protect data being transmitted between the application server and the user's browser. Where deployed, the TLS configuration will be reviewed to ensure that the chosen protocols and ciphers are robust and sufficient to protect user data. TLS certificates will be examined to ensure that they are trusted and provide the necessary assurance for end users. Content exposed by the application or its server (for example web pages, directory listings, server banners, error messages) will be reviewed to ensure that it does not provide an attacker with information about the application or its hosting environment which could assist them in targeting their attacks against the platform.	Small	Medium
		Medium	Medium
		Large	High
Access Control & Authentication	The application will be tested from an unauthenticated perspective to ensure that an anonymous attacker cannot bypass or otherwise subvert the authentication mechanism. Attempts will be made to enumerate valid usernames, and to conduct brute force attacks against the login functionality. Authenticated testing will only be conducted if anonymous user can register a new user in the web application. Consultants will then look at elements including session management and storage, password rules and quality, and password recovery functions.	Small	High
		Medium	Medium
		Large	Low

	If applicable authenticated testing will also be conducted from multiple user accounts – consultants will ensure that application enforced segregation of data or functionality (for example according to a user's role, or to some business unit restriction) cannot be bypassed. Consultants will attempt to bypass restrictions on user permissions, and to gain access to administrative functions with 'standard' user accounts.		
User Input Validation	An injection vulnerability could be used to run commands on the underlying web server, bypass authentication controls, or access sensitive data, and will often lead to a complete compromise of the application. Scripting and injection vulnerabilities are often amongst the most serious encountered during web application security testing. Scripting vulnerabilities such as Cross-Site Scripting (XSS) or Cross-Site Request Forgery (CSRF) could allow an attacker to cause malicious script to run within a user's web browser – the effect of this could be the theft of sensitive data, defacement of the application, or unauthorized access to the user's session.	Small	Very high
		Medium	Medium
		Large	Low

It must be noted that Denial-of-Service and Man-in-The-Middle attacks will be avoided during the assessment, due to high probability of having a disruptive effect on the services in the network. In case identified weaknesses can be exploited by MiTM and DoS attacks, our team will assess the actual impact and will attempt to exploit given vulnerabilities in a controlled manner, where the stakeholders will be aware of and have already agreed to.

Fulfilment of success indicators will be proven by the supporting material that will be available in our final report, which is intended to provide a step-by-step walkthrough of the attacks performed and highlight the access levels that were obtained during the assessment. In our reports, technical walkthroughs are designed in a way that aims to enable an advanced computer user to follow the steps to replicate the attacks outlined.

Throughout the assessment, our team will perform all penetration testing activities from Sopra Steria designated machines and any workings (e.g. screenshots, security scans output) will be securely stored on them. In the final deliverable of the penetration testing assessment, our team will provide all necessary information (IP addresses of attacking machines, compromised systems, exploited vulnerabilities etc.) to stakeholders, so it is possible for them to trace the attacks and any other penetration testing activities originating by our machines.

We will use reasonable care to execute our work in a way which seeks to minimize the risk of causing damage. Nonetheless, during the execution of our attempts to simulate what a real cyber attacker would do, there is a risk that we may cause disruption or damage to those systems or third-party systems and the information contained therein. The applicant is aware of this risk and authorizes Sopra Steria to perform the tests described herein.

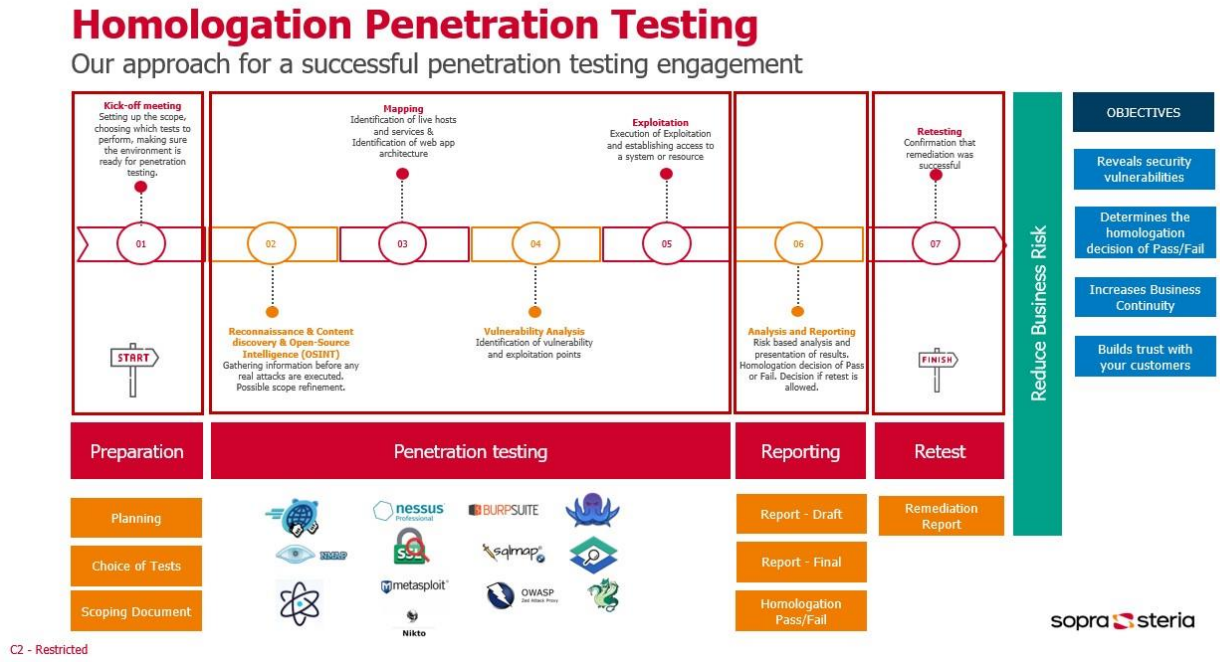
3. Starting conditions for penetration testing

Before starting the penetration tests, some basic conditions must be fulfilled. These conditions are evaluated during the penetration test kick-off meeting.

- The environment on which the penetration test is going to be performed needs to be representative of the applicant's production environment.
- A single Point Of Contact (SPOC) on the applicant's side needs to be provided and available to the penetration tester and to the project manager on Sopra Steria side during the time of penetration test. The SPOC needs to be able to support Sopra Steria from management and technical side. If one SPOC cannot fulfil both management and technical side, the SPOC needs to fulfil at least management side. This SPOC can appoint another technical SPOC which covers the technical side of the penetration test.
- The applicant is required to provide technical support to the penetration tester throughout the duration of the penetration testing process. This support includes ensuring availability in case the target scope becomes unavailable or experiences service degradation. Additionally, it encompasses situations where the penetration tester may encounter blocks or restrictions due to their actions.
- The main focus of the homologation penetration test is the web API using the RTP scheme and the web server(s) of the applicant. It is not meant to be a full-blown penetration test. If we encounter any other clients like mobile application, thick client etc that are using these APIs and are important to penetration test, we could include them in the homologation penetration test on best effort basis.
- The target applications running on the target scope need to be fully functional and reachable during the penetration test.
- There should be no changes (nor deployments) being made on the target scope during the time of the penetration test.
- In case the applicant wishes Sopra Steria to use only specific IP addresses for penetration testing, the applicant can provide Sopra Steria with VPN access. Otherwise, IP addresses used by Sopra Steria will be communicated before the start of the penetration test. In rare cases when those IP addresses change during the penetration test, the applicant will be informed.
- In case a security solution (like IPS or WAF) would be aggressively blocking the automated scans, Sopra Steria will request to make an exception for their IP addresses used in penetration testing.
- A penetration test of the applicant's solution needs to be performed before the homologation penetration test takes place. The penetration test must not be older than one year. At least grey-box level penetration test is recommended.
- There needs to be a legal contract between the applicant and Sopra Steria before the beginning of the penetration test which allows the penetration testing. This contract will also cover responsibilities on both sides.

4. Homologation penetration test process

The homologation penetration test is performed during a fixed amount of time, 6 working days in total for execution, reporting and management. If an observed vulnerability is eligible to be re-tested and is successfully remediated before the end of the penetration test, it will be reported as “Resolved” and does not have a negative impact on the final decision. The following picture provides a high-level overview of the homologation penetration test:



High-level overview of homologation penetration testing process

The main steps of the process are described below:

4.1. Planning of the penetration test

Once the applicant or TSP applies for SRTP scheme homologation to the Homologation Body, a period of approximately 2 months at minimum should be considered for the start-up of penetration test. The tests should be done, in line with the full homologation process, within a period of six months after the identification of the applicant or TSP by the EPC.

The final planning will be in function of the readiness of the SRTP system for penetration tests and the availability of slots for testing at the homologation body. The lead assessor will align with the applicant or TSP and test team of the Homologation Body.

The final start of the tests depends on the respect of the starting conditions mentioned above.

4.2. Kick-off meeting

A kick-off meeting between the homologation body and the applicant will be organized before the start of the penetration test. During this meeting, Sopra Steria will explain the scope of the penetration test and the applicant may be requested to provide more insight about the scope (target servers and applications). The communication channel for the penetration test will be defined in this meeting.

Approach to penetration testing, category (small, medium, big) of the target is defined during this meeting. SPOC will be also appointed during the kick-off meeting on Sopra Steria side in order to immediately stop the penetration test if requested by the applicant.

4.3. Execution of penetration test

The black-box penetration test will be executed by a senior penetration tester. Following tasks are executed during the penetration test:

1. **Reconnaissance & OSINT collection**
   Gathering information before any real attacks are executed. Possible scope refinement.

2. **Mapping**
   Identification of live hosts and services and identification of web app architecture.

3. **Vulnerability analysis**
   Identification of vulnerability and exploitation points.

4. **Exploitation**
   Execution of exploitation and establishing unauthorized access to a system or resource.

4.4. Reporting results

Once the penetration test is done, all vulnerabilities are listed in a basic report. The template is attached. The report is transmitted to the Lead Assessor. The general conclusion becomes part of the overall homologation report. The Penetration Test report will be addressed to the applicant or technical solution provider.

The **resulting deliverable of the penetration testing assessment** is a report which is delivered to the applicant or technical solution provider after the completion of the penetration testing activities and will be finalized after any adjustments derived from customer's input. Our reports follow a pre-defined structure to ensure that both technical and non-technical audience can understand the risks reported with a given web application. An indicative structure for our penetration testing report is:

1. The first page contains basic information (like the title of the homologation penetration test, name of the client, date and security classification of the report).
2. Foreword briefly introduces what is the current document about (with client name and date).
3. Summary of vulnerabilities (summary table of all the found vulnerabilities).
4. Conclusion (decision of pass or fail, if retest is possible and short explanation of the decision)
5. Annex (Optional section)

The decision of pass or fail will be given in this report together with the decision if a retest is allowed or not for the applicant.

5. Fail and pass conditions

The following table summarizes when an applicant fails or passes a homologation penetration test:

CONDITION	RESULT	RETEST ALLOWED
1 or more **critical** severity vulnerabilities found	FAILED	NO
1 or more **high** severity vulnerabilities found	FAILED	YES
3 or more **medium** severity vulnerabilities found	FAILED	YES
1 or **2 medium** severity vulnerabilities found	PASSED*	YES
1 or more **low** severity vulnerabilities found	PASSED	N/A

* - it is however strongly recommended to fix all medium severity findings