Intrusion Test Procedure

RESTRICTED DISTRIBUTION: ACCOR TEAMS, 3RD PARTY VENDORS

Version Status

This version of this document is currently:

	In Progress
	In Review
	Published
	In Test
⇒	**Tested/Applicable**

Document History

Version	Author	Reviewers	Date	Milestone
1.5	J. Ettinger	A.Treps	27 October 2014	Includes PCI DSS scoping details
1.6		P. Auré	3 March 2016	Annual review: typography / minor modifications
1.7		P. Auré	9 March 2017	Annual review
1.8		P. Auré	14 March 2018	Annual review
1.9		P. Auré	29 March 2019	Annual review
2.0	K. Locati	A. Treps	04 Feb 2021	Annual update, split test procedure & test policy
2.1		B. MADER	10 April 2022	Annual review
2.2		B. MADER	3 March 2023	Annual review
2.3		F.REGNIER	22 March 2024	Update for PCI V4 reference + orga changes + Defect Dojo planning

Projected Review Date:

(= 12 months after publication)

Table of Contents

1 Introduction

1.1 Purpose of this document

The goal of this document is to clearly define the intrusion test procedure followed by Accor Security Team.

It should be shared with third party vendors.

1.2 Sources

Accor intrusion test procedure is based on industry standards such as:

- OWASP testing guide
- NIST SP 800-115
- PCI DSS v3.2.1 requirements

2 Before the test

2.1 Required documents

Detailed list of required documents to be prepared by the Accor project owner is documented in Accor Intrusion Test policy.
Below is the information required from third party vendors (SaaS or vendor hosted applications, web agency, etc.). You can use the "questionnaire" template at the end of this procedure to share this information.

- Signed agreement (see template on the last page of this procedure)

- IP range / URLs of the application to test

- Testing data
    - User accounts & passwords with different level of privilege (admin, user, guest) and scope of rights (accor users VS testCompany users, or hotel 1 users VS hotel 2 users)
    - Test datasets when applicable (If an API is involved, e.g postman or swagger)

- Architecture / network diagrams / description of the main use cases by user types / illustrations of connections with Accor systems: *the goal is not to get de detailed vision of the systems internals, but to identify all the entry points, including those used for back-office users, system administration, new releases or patches deployment, etc.*

- Any existing user or administration guide

- Vendor contact email and telephone number for communication during the assessment

2.2 Performance / Denial of service

Tests are non-destructive neither are intended to generate high load on the system. Our team will never engage in activities which may lead to a denial of service of the target application.

However, if for some reason the target becomes unstable or unreachable during the test, we will immediately notify the vendor and work towards a solution to the issue.

If any test may lead to availability issues, it is preferable that the vendor also provides us with pre-production access in order to avoid any risk associated with that particular test (pre-prod should however be iso-prod).

2.3 Source IP address

Tests will be performed from these IP addresses:

- 195.137.181.0/24 (AccorHotels's range)
- 91.208.9.0/24 (AccorHotels's range)
- 64.39.96.0/20 (Qualys automated scanner)

3 Execution of security tests

3.1 General information

When executing a penetration test, the tester and vendor shall be able to communicate quickly so as to report any incident or issue with the test.

Any severe vulnerability will be reported immediately to the vendor. If exploitation may put the information system at risk, we would refrain from exploiting the vulnerability before collecting vendor consent and additional guidelines. Please note such exploitation may be required to confirm the vulnerability isn't a false positive and to evaluate associated risks.

3.2 Reconnaissance

The security team gathers relevant information from a variety of publicly available sources by combining the results of manual and automated intelligence gathering, using tools such as search engines (Google, duckduckgo, archive.org, shodan), DNS history (dnsdumpster), public databases (haveibeenpwned, breachcompilation, openbugbounty), etc.

The information gathering stage is described as "passive" as it does not interfere with the target systems.

We then proceed with mapping application functionality, use cases, enumerating technologies and open ports using a variety of tools such as nmap, Burp Suite, dirbuster, qualys, etc.

3.3 Threat modelling

During this phase, the security team defines attack scenarios based on the previously collected information.

This phase identifies potential avenues of exploitation and attack against the target that could potentially be exploited by malicious users and intruders. It guides the manual testing that will be performed by the security team.

3.4 Vulnerability identification

Based upon the results of the previous steps, we then search for potential vulnerabilities on the target.

By using a mix of automated (web application scanners such as Burp Suite), and manual testing (replaying and tampering with application requests), we search for common security issues. Then, the security team manually plays out the attack scenario to identify more complex vulnerabilities such as authentication, authorization or business logic flaws.

3.5 Vulnerability analysis

If a vulnerability is found, we will then try to manually exploit it to assess associated risk and avoid reporting any false positive, using tools such as publicly available exploits (exploitdb, Metasploit) or custom scripts.

Should the vulnerability put the application and system at high risk, it will immediately be reported to the previously defined vendor contacts. If exploitation may but the system at risk, we will evaluate with the vendor as previously stated.

3.6 Note: during the test

Unless instructed to do so by Accor Security team, or specifically agreed, the application owner/vendor should not try to fix the detected vulnerabilities in real time as it might:

- Perturbate the test itself
- Generate production or security issues due to lack of QA on these changes

IP addresses used for the security test should not be manually blocked neither generate incident response during the agreed timeframe for the test. However, security team remains available to confirm if any alert is related to the test in progress.

4 Reporting and follow-up after testing

4.1 Reporting

At the end of testing activities, a report will be generated and delivered to the project team. This report should go through our review process which implies a delay of approximately 7 days after testing.

The report shall include an executive summary summarizing the pentest results, global risk level evaluation and main issues found, if any.

The report will also contain a detailed section about each security issue, with:

- **Reference**
- **Severity** level associated with the vulnerability defined as follows:
  - **Low**: there is no immediate risk for the system with this vulnerability. If that vulnerability might seem unimportant by itself, combined with one or several others it could lead to the compromise of the whole system.
  - **Medium**: the vulnerability is not dangerous by itself but gives a way to exploit other vulnerabilities.
  - **Critical**: a part or a functionality of the system can be compromised.
  - **Severe**: the whole application, database, system or network is under control of the attacker.
- Affected **assets**
- Identified **risks** if exploited
- **Type** according to OWASP classification
- **Description** and exploitation steps
- Recommended **mitigations**

Please note that the report is confidential and should not be transferred to any party not involved in the project.

In addition to the report, we will send an action plan spreadsheet to be completed by the project owner with actions undertaken to fix identified vulnerabilities.

The Agenda and the list of realized pentests are also made available in the defect dojo application for compliance followup.
Defect Dojo allows the compliance team to follow mandatory pentests in the PCI Scope.

An optional debrief call can be set up after the test in order to answer any questions related to the report.

4.2 Follow-up

Once the vendor has defined corrective actions, the spreadsheet should be returned to the security team for evaluation. If the proposed fixes are approved, then the vendor may proceed with executing the action plan.

After all vulnerabilities have been fixed, a quick retest should be planned with the security team so as to confirm identified vulnerabilities have been fixed. Usually, one working day is sufficient to perform the restest.

In case of major updates, the project team should contact the security team to evaluate whether any subsequent penetration test may be required.

5 Test scope

5.1 Global scope

The penetration test should look at all entry points to the system or application, including back-office or administration interfaces.

5.2 Type of tests

The penetration test is performed to detect and propose remediation actions on all the project layer:

- Infrastructure: through network-layer penetration testing activities including components that support network functions as well as operating systems. Identified vulnerabilities might be related to firewall or network device misconfiguration, lack of hardening, or missing security updates.

- Application-layer: test includes at a minimum, vulnerabilities listed in OWASP Top 10 and PCI-DSS Requirement 6.5

- Organizational aspects: by checking existence of user access management procedures, compliance attestation when applicable, and more globally checking Accor procedure “security in project” has been followed. These aspects are under Accor project team responsibility, **the penetration test is not an audit of the third-party vendor internal procedures**.

6 Pentest agreement letter

Your details

Accor IT security
Attn Ludovic COURGNAUD
Accor
82 Rue Henry Farman
92130 Issy-les-Moulineaux,

Place, date

Subject: Penetration test agreement

I, Name, position, hereby authorize the Accor security team to proceed with an external penetration test on Provider systems as described in AccorHotels intrusion testing procedure.

The purpose of this test is to determine if Accor information managed by Provider is safe from anonymous attackers and other Provider customers. These tests will be of non-destructive nature and the Accor team will not attempt any denial of service attack.

Vendor Signature

7 Questionnaire

7.1 URLs / IP

7.2 List of testing accounts + passwords (example below, at least 2 differents privilege level & 2 different scope of rights)

- Scope 1 / Role Admin
- Scope 1 / Role user
- Scope 2 / Role Admin

7.3 Testing data (test cases to simulate all business features / postman or swagger for APIs, etc.)

7.4 General documentation

7.4.1 Who are the users of this service (including special users of charge of the service administration / moderation / API management / etc)

7.4.2 Please illustrate the main use cases, if possible as a workflow description including technical elements (applications, servers) involved.

7.4.3 Please describe how this service will be integrated with Accor systems.

7.4.4 Network diagram

7.4.5 User guide

7.4.6 Administration guide

7.5 Contact (phone number / e-mail)