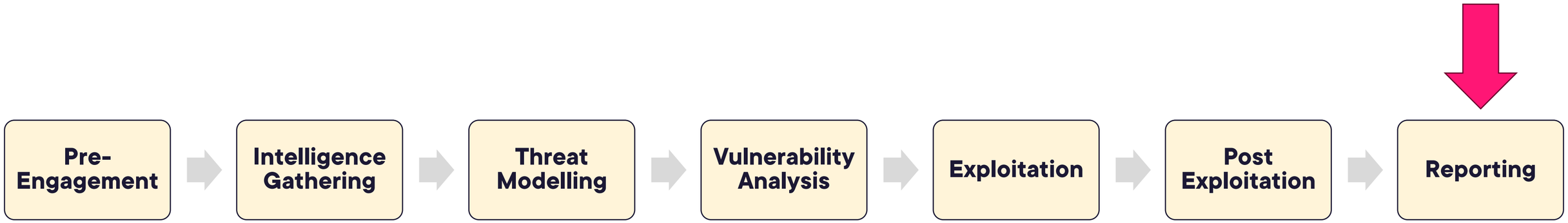
Reporting

Ricardo Reimao, OSCP, CISSP
Cybersecurity Consultant

Pentest Process – Reporting Phase



What Makes a Good Report?

Reporting is as important as the test itself

- Clients see the final report

Grammar and conciseness

Formatting and alignment

Review multiple times before sending to the client

- Peer reviews

Report Templates

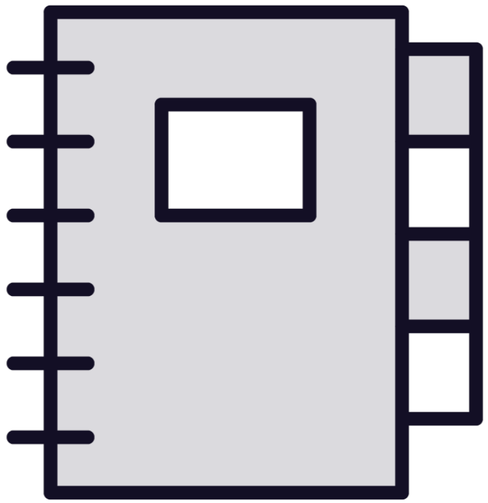
Each company has their pentest template

Understand your template and ensure it has all the required sections

- Review previous reports

Reports are usually delivered in PDF

Ethical and Legal Considerations



Always keep ethics and legal in mind during reporting

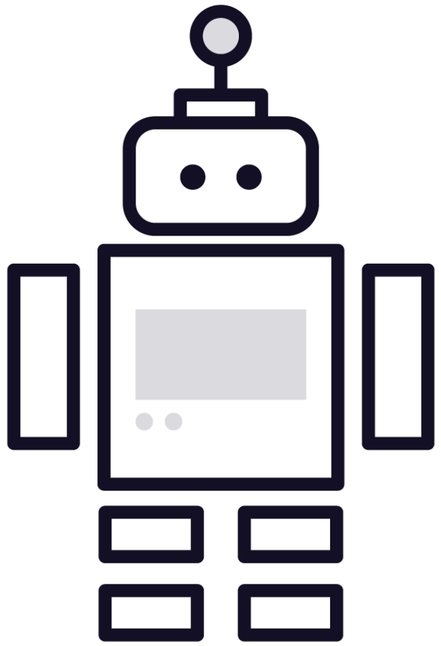
Obfuscate sensitive information

- Passwords, social security numbers

Do not make accusations or assumptions

Submit your report for internal QA

Artificial Intelligence (AI)



Each company have their own policy on the use of AI

Helps on report writing

- Does not replace a human

Never copy and paste AI-generated text

- Always review the content and write in your own words

Never submit sensitive information on AI platforms

Report Contents

The Report Structure

- Cover
- Table of Contents
- Change Tracking
- Executive Summary
- Project Scope
- Methodology
- Attack Narrative
- Findings and Recommendations
- Conclusion
- Appendix

Executive Summary

A summary of the tests written for the business audience

- Avoid technical terms
- Explain the business impact of a potential attacker

Do not include every single finding

- Instead, a high level of what was found

Ideal length is one page

Project Scope

Defines what was tested during the engagement

- Assets
- Assessment type

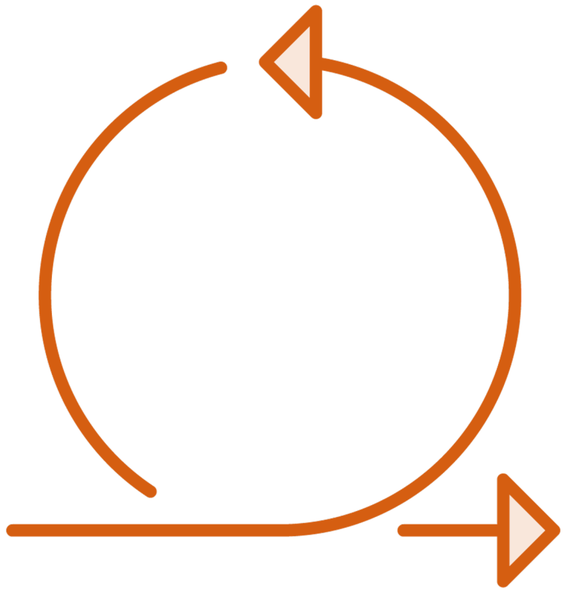
Should be exactly what was defined on the SOW

- Might include assets found during the engagement

Might also include the out-of-scope items

Newly identified assets

Methodology



Defines the approach used during the tests

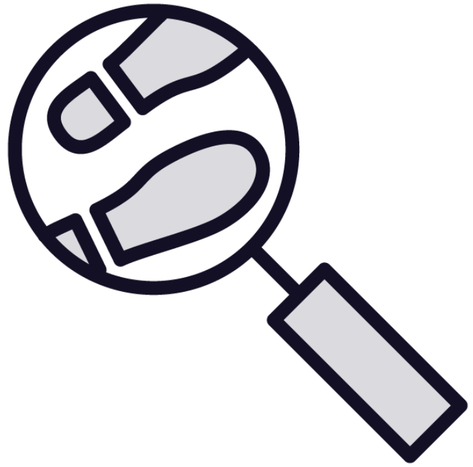
Should follow the phases of the test

- Reconnaissance, vulnerability identification, etc.

Should include some of the main tools and techniques used

Mention any compliance frameworks followed

Testing Narrative



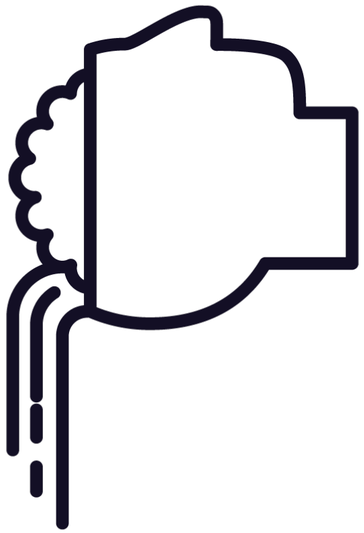
The step-by-step of the tests

Includes screenshots of the main test attempts

- Include even tests that were not successful

Should be written in a narrative/story format

Findings and Recommendations



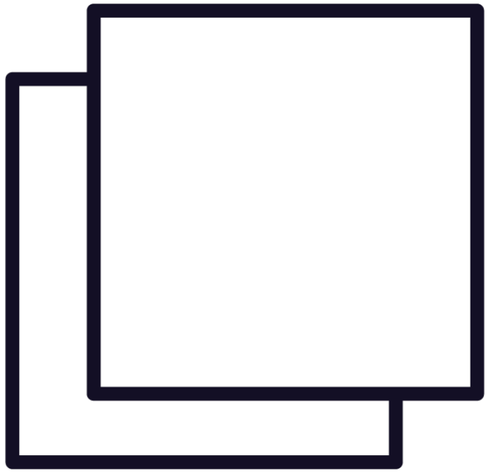
The main section for the technical audience

Contains the list of identified vulnerabilities with their details and how to remediate them

Should be concise and easy to understand

Writing Findings

Findings Best Practices



Usually aggregated by vulnerability type

- Example: Default credentials

Describes what it is, which servers are affected, and details of the exploitation

Might include external references

What to Include in Each Finding

- Name of the vulnerability
- Priority
- Assets impacted
- CVE (if applicable)
- CVSS Score (if applicable)
- Description of vulnerability
- Exploitation
- External references
- Sensitive data found (if applicable)
- Evidence of exploitation

Assessing the Business Impact

Describe the impact that a real attacker would cause if exploited

Understand what an attacker could do and what kind of data they could access

Globomantics example:

“The SQL Injection vulnerability allows an attacker full control of the Globomantics Mail database.
An attacker could impact the confidentiality, availability and integrity of the database.
The database contains sensitive data such as cleartext passwords and email communications of all employees.”

Risk Scoring

Impact	×	Likelihood	=	Risk
- Real attack impact - Data sensitiveness - Affected assets		- How easy to exploit - Exploit availability - External vs. internal - Cyber trends		Critical High Medium Low

Unauthenticated SQL Injection

Priority: HIGH

Affected Assets:
mail.globomantics.com

Description:
During the tests it was observed an SQL Injection vulnerability on the ‘username’ parameter on the login.aspx page. Since the DB user has admin access, it was possible to retrieve the entire Globomantics database. […]

For more information on SQL Injection:
https://owasp.org/www-community/attacks/SQL_Injection

Exploitation:
Using a scape character (‘) it was possible to inject SQL statements into the application workflow. We were able to retrieve the entire Globomantics database, including clear text passwords

Evidences: [...]

Findings

A concise description of what was found and where it was found

Things to include:

- Name of the vulnerability
- Priority
- Assets impacted
- CVE (if applicable)
- CVSS Score (if applicable)
- Description of finding
- Exploitation
- External references
- Sensitive data found (if applicable)
- Evidence of exploitation

```
Unauthenticated SQL Injection

[…]

Recommendations:

To prevent SQL injections it is recommended
that:
- All fields use parametrized queries
(prepared statements).
- Prefer using stored procedures
- All input is validated using allow-lists
- All user input is escaped at server-level

To minimize the impact of an SQL Injection
exploitation, it is also recommended that
the database user only has the minimum
required access. In this case, it is
recommended that the user only has read
access to the required fields in the
database.

For more information about SQL injections,
consult:
https://cheatsheetseries.owasp.org/cheatshee
ts/SQL_Injection_Prevention_Cheat_Sheet.html

It is also recommended that user passwords
are not stored in clear text, instead, they
should be stored in their hash+salt values.
```

Recommendations

Writing meaningful and concise recommendations for the technical team

Research the latest techniques to prevent a vulnerability

Things to include:

- High level description of recommendation
- Step-by-step (if applicable)
- External references

Globomantics SQL Injection Vulnerability

Vulnerability	**Unauthenticated SQL Injection**
Priority	**HIGH**
Impacted Assets	**mail.globomantics.com**
CVE | CVSS	**N/A**
Description	During the tests it was observed an SQL Injection vulnerability on the ‘username’ parameter on the login.aspx page. Since the DB user has admin access, it was possible to retrieve the entire Globomantics database. [...] For more information on SQL Injection: https://owasp.org/www-community/attacks/SQL_Injection
Exploitation	Using a scape character (‘) it was possible to inject SQL statements into the application workflow. We were able to retrieve the entire Globomantics database, including clear text passwords
Business Impact	The SQL Injection vulnerability allows an attacker to have full control of the Globomantics Mail database. An attacker could impact the confidentiality, availability and integrity of the database. The database contains sensitive data such as cleartext passwords and email communications of all employees.
Recommendations	To prevent SQL injections it is recommended that: - All fields use parametrized queries (prepared statements). - Prefer using stored procedures - All input is validated using allow-lists - All user input is escaped at server-level To minimize the impact of an SQL Injection exploitation, it is also recommended that the database user only has the minimum required access. In this case, it is recommended that the user only has read access to the required fields in the database. For more information about SQL injections, consult: https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html It is also recommended that user passwords are not stored in clear text, instead, they should be stored in their hash values

Up Next:

Remediations and Recommendations