00x?? Test plan - Example - hackxpert.com/pentest

0. Document revision history

Version	Revisor	Date

1. Goal of the document

[Write down what you are trying to achieve with this document]

In this document we will describe the testing strategy including but not limited to:

- The features to be tested
- The methodology
- The roles and responsibilities
- The entry and exit criteria for testing

2. Who is this document for

[Write down the intended readers of the document in this section, this can be brief]

This document has been created to inform the security representative at "The XSS Rat" and the CEO of how testing will be conducted.

3. Project description

[Describe what the product you are testing does. What it's functionalities are and who it's intended audience is briefly.]

The project is a webshop that is partially completed intended to sell merchandise. Mock payments can be made but no action is taken such as reducing stock. The project is intended for the fans of the owner of the website and is a B2C website.

4. Testing objectives

[Write down what you want to achieve with testing. This can be brief and can be similar for most of your clients but make sure it's adapted to every client.]

The objective of security testing of the product is to:

- define security goals through understanding security requirements of the applications;
- identify any potential security threats;
- Validate that the security controls operate as expected;
- eliminate the impact of security issues on the safety and integrity of the product;
- guarantee that the product will function correctly under malicious attacks;

5. Roles and responbilities

[Will the tester be operating alone? Who is to sign off on what document?]

Project lead	- Oversee all documentation is complete and signed - Initiate contact - Receive debriefing	info@thexssrat.com
Tester	- Will test the application - Will create a detailed report - Will create a debriefing video	Your contact here

6. Scope

6.1 In scope

[Mention the domains that are in scope or a wildcard. Could also be IP adresses or applications on any other device.]

- hackxpert.com/pentest

6.2 Out of scope

[Mention anything explicitly out of scope]

- Port scanning is out of scope
- mail.hackxpert.com is out of scope

7. Testing methodology

[Outline what tests you will be doing on what sections of the scope]

We will be following the OWASP top 10 methodology by taking the following steps:

- Testing for excessive logging
- ...

7.1 Testing entry criteria

[List anything you need before you can start testing]

- The domain needs to be shared with the tester
- VPN access needs to be working
- The site needs to be online
- Test plan needs to be signed off on

7.2 Exit criteria

[Define when testing is done]

- All above mentioned tests have been executed on the complete scope
- The ...

8. Results/Deliverables

[Define what you will give to the client to exit the testing]

- A complete test report has been delivered
- A debriefing video has been delivered
- A sign-off slip has been approved and signed off on

9. Tools

[Define any tools you will be using]

- Nmap
- Nikto
- ...
- Burp suite

10. Glossary

[If you've used words that are not common knowledge, define them here.]

- OWASP top 10 = The ***OWASP Top 10*** is a standard awareness document for developers and web application security.

- ...

11. Sign off

This document needs to be signed by both parties before testing can commence.

This constitutes a contract of engagement.

Signed:_____
Name: _____
Title: _____
Date: _____
RECIPIENT (The XSS Rat)
Signed:_____
Name: The XSS Rat (Wesley Thijs)
Title: President / Security Engineer
Date: _____