

1gov pen-testing plan

Shangano Gwebu



June 29, 2022

Contents

[PENETRATION TESTIG GOALS 1](#_Toc107598570)

[APPROACH 1](#_Toc107598571)

[PENETRATION TESTING WAYS 1](#_Toc107598572)

[TOOLS USED 2](#_Toc107598573)

[ROLES AND RESPONSIBILITIES: 2](#_Toc107598574)

[Methodology 3](#_Toc107598575)

[Rules of Engagement Worksheet: 4](#_Toc107598576)

# PENETRATION TESTING GOALS

* To ensure that the system is secure
* To identify weakness in the code
* Identify the risk
* Find vulnerabilities

# APPROACH

This is going to be a white box test. Penetration testing will be done on the 1GOV platform. Testing will be conducted on a period of 5 days, starting from 29/06/2022 to 03/07/2022. Two operating systems will be used in this testing process, which are kali-Linux and Windows 11. Most of the code inspection to find vulnerabilities will be done in windows operating system. Another method which will be included will be to use the google hacking database which a powerful site provided by google which enables users to find vulnerabilities in some databases that exist on google. Kali Linux will be used to run some of the complex commands that works best in that operating system.

# PENETRATION TESTING WAYS

Penetration will be done in 2 ways which are manually and automatically

**1.manually**: using the procedures developed for a particular application and type of threat

2 automatically using:

* web application vulnerability scanners,
* binary analysis tools,
* proxy tools.

Some of the main attacks that will be carried out include the following

* Cross site scripting;
* SQL injection;
* Server misconfiguration;
* Form manipulation;
* Cookies poisoning;
* Platforms vulnerabilities;
* Weak session management;
* Buffer overflows;
* Command injection.

## TOOLS USED

Burp suite:

Burp Suite is an integrated platform and graphical tool for performing security testing of web applications, it supports the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

OWASP:

Owasp zap is an open source web application security scanner. This tool is used to find vulnerabilities

**Testing Objectives**

The objective of security testing of the product is to:

• define security goals through understanding security requirements of the applications;

• identify the 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;

## ROLES AND RESPONSIBILITIES:

|  |  |  |
| --- | --- | --- |
| Role | Responsibility | Contact-Info |
| Team-Leader | • Test process setting up and adjusting  • Security test plan creation  • Test strategy authoring  • Test activities tracking  • Giving conclusion about the quality | gshangano@gmail.com |
| Test-designer | • Security models creation  • Test cases and test suites creation and updating | gshangano@gmail.com |
| Test -Engineer | Running test cases  • Defects authoring  • Test results analysis  • Test reports creation |  |

# Methodology

**1.Dependencies:** This is the part where third party modules will be tested which includes code, libraries etc. The main aim of this process is to verify whether:

* An application has vulnerabilities of (3-rd part) components it uses;
* Modules that provide security services fail;
* There are security vulnerabilities in the file system;
* There are security vulnerabilities in the registry

**2.Client-side testing:** In this type of testing I will be focusing on the user interface. In order to try and break through the security I will try enter input sequences like**:**

Escape characters;

• Long strings;

• Parts of some code in a programming language;

• Incorrect input values;

• Testing for error handling;

• Perform cross site scripting.

**3.Exposed implementation vulnerabilities (implementation testing):** This is the testing used to find vulnerabilities that are caused by the implementation phase. These vulnerabilities may exist because:

* Developers who develop only their modules could unintentionally reveal data: for example, incorrect validation;
* • Time-of-check-to-time-of-use issues.

# Rules of Engagement Worksheet:

**Penetration Testing Team Contact Information:**

Primary Contact: \_\_\_\_\_\_\_\_\_\_\_\_Shangano Gwebu

Mobile Phone: \_\_\_\_\_\_\_\_\_\_\_\_76223626\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Pager: \_\_\_\_\_\_\_\_\_\_\_None\_\_\_\_\_\_\_\_\_\_\_

Secondary Contact: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Lebogang Gwebu\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mobile Phone: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_77490230\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Pager: \_\_\_\_\_\_\_None\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Target Organization Contact Information:**

Primary Contact: Government of Botswana

"Daily Debriefing" Time/Location: \_\_\_\_Microsoft teams\_ 10:00-10:30 am

Start Date of Penetration Test: \_\_\_\_\_\_\_\_\_\_\_\_29/06/2022\_\_\_\_\_\_\_

End Date of Penetration Test: \_\_\_03/07/2022\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Testing Occurs at Following Times: \_\_\_\_\_24hrs\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Will test be announced to target personnel: \_\_\_\_yes\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Will target organization shun IP addresses of attack systems: \_\_NO\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Does target organization's network have automatic shunning capabilities that might disrupt access in unforeseen ways (i.e. create a denial-of-service condition), and if so, what steps will be taken to mitigate the risk: \_\_\_\_\_\_\_NO\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Would the shunning of attack systems conclude the test: \_\_\_\_\_\_\_\_YES\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

IP addresses of penetration testing team's attack systems: \_\_\_\_\_\_\_\_\_Not to be displayed\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Type of test: White Box testing \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the policy regarding viewing data (including potentially sensitive/confidential data) on compromised hosts: \_\_\_Data accessed by the tester will not be revealed anyhow to the public, the data will only be viewed by testers and will be documented only to show the organizations where the application is vulnerable.

Will target personnel observe the testing team: \_\_\_\_\_\_YES\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Head of Penetration Testing Team \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date If necessary, signatures of individual testers: \_\_\_\_\_\_\_\_\_\_\_\_\_29/06/2022\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature \_\_\_\_S.Gwebu\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_