shangano gwebu

  gshangano@gmail.com

1gov pentest report

**DOCUMENT PROPERTIES**

**Name of tester:** Shangano Gwebu

**Company tested**: Botswana Government

**Application tested**: 1gov

**Approved by**: Hackathon

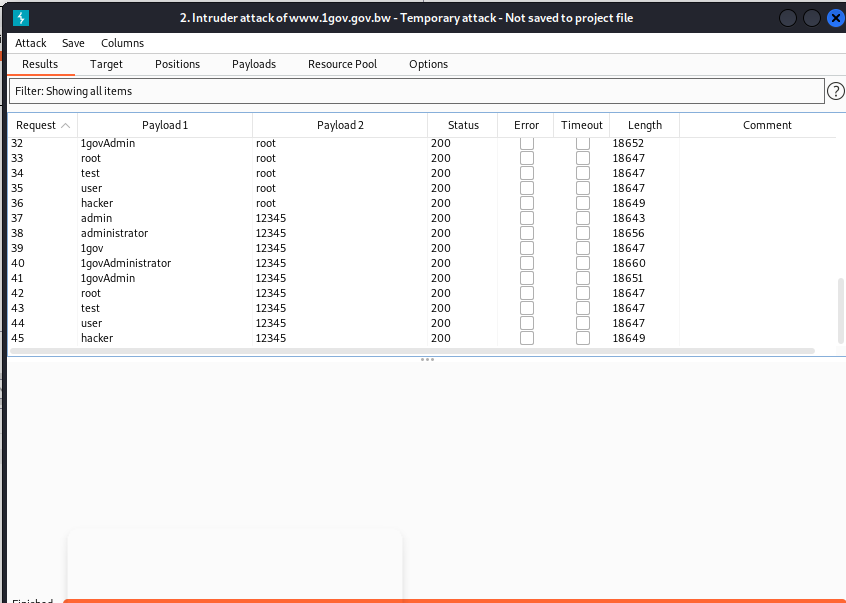
Time: 5 days

PROJECT OBJECTIVE

* After finding the vulnerabilities discovered in the pen test the company will now be able to make the web app more secure

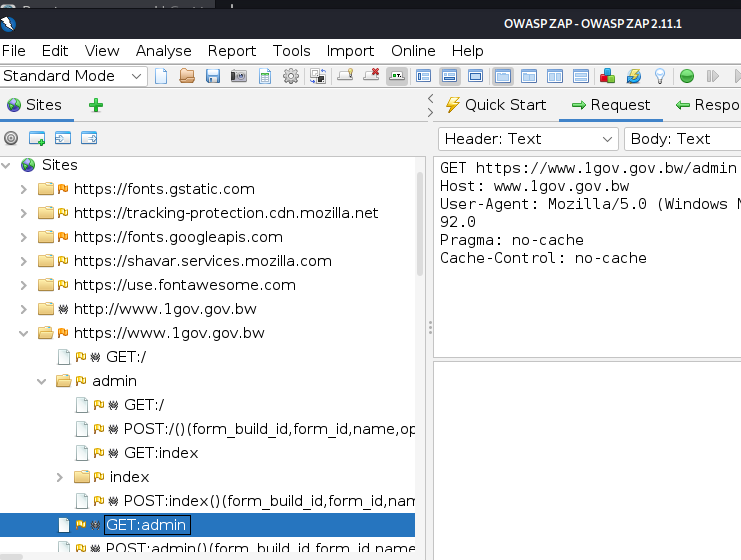
DETAILED FINDINDS

The first attempt was to try and brute force the log in form with common passwords using Burp suite. Because of time only few written passwords and usernames where entered below is the image showing the process



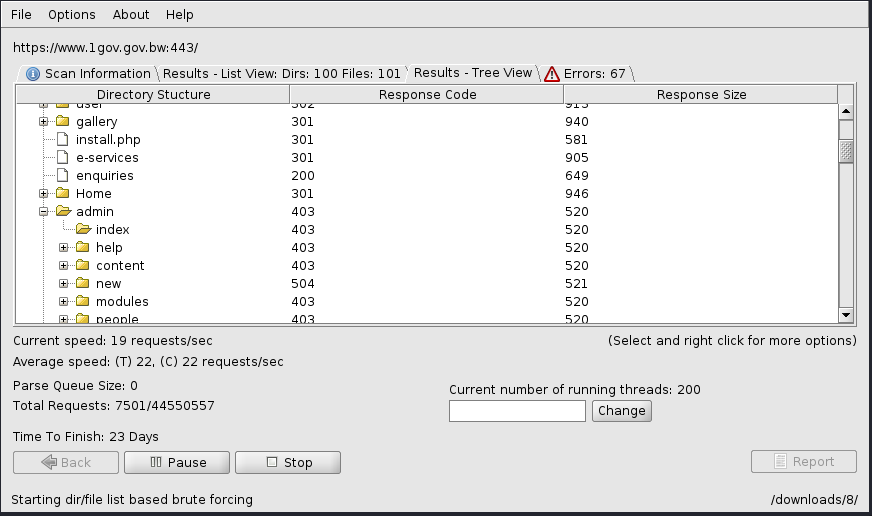
Burp suite came with different passwords combinations but all of them where not successful. Because of lesser time only written passwords where used not a list of different passwords.

2. The second Attempt was to find hidden files, eg admin login page. If an attacker can find the login page they will have a light or way in which they can escalate privileges. The tool used in this exercise was the OWASP ZAP. Below is the image of the result

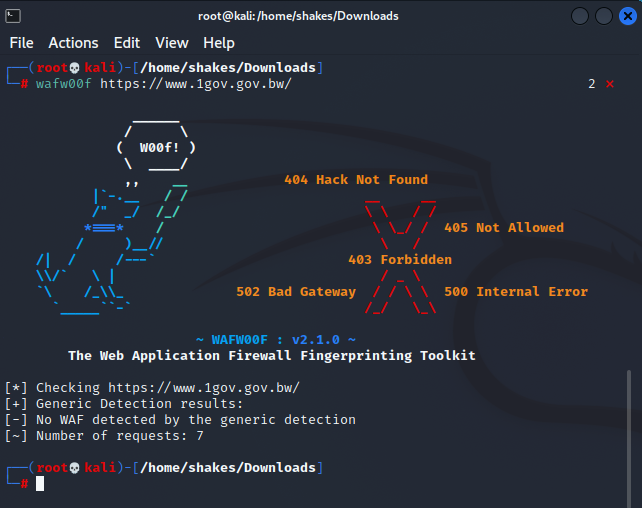


Admin page was found and this is big win when it comes to attackers because now they know where exactly to attack and escalate privileges

3.Dirbuster was another tool employed to help find hidden pages and some txt files that may lead exploitation of the website. The tool was successful and we also found the admin page file with some information in the web hierarchy. below is picture showing the finding



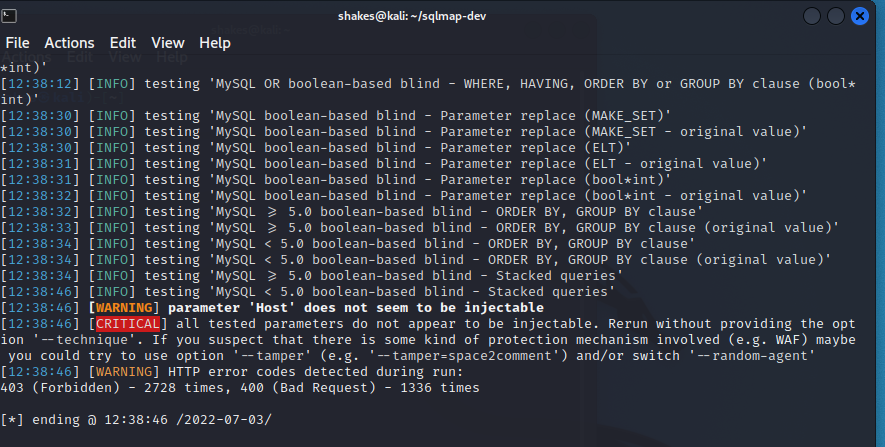
4. Waw00f is one of the most powerful tool that is used to detect whether the application contains the firewall or not. 1gov platform contains no firewall thus making the website vulnerable. If an application contains firewall it will help prevent 20% of the attacks but because it is not implemented here it makes the web application vulnerable. Below is the finding of waw00f



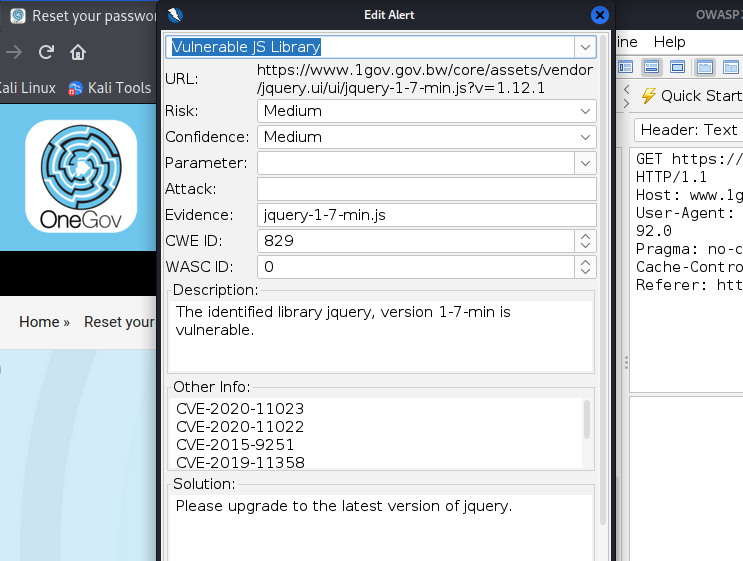
5. In order to gain access to the admin pages’ credentials where needed. Now that we had knowledge of where the admin page was it was easy to navigate to it with the following url

C:\Users\shang\OneDrive\Pictures\finding the admin hidden page.png

The other attempt was to inject the web application database sqlmap and the results proved that the web application has strong security in their databases. The results proved that the database was protected from injection. below is the image showing the result.

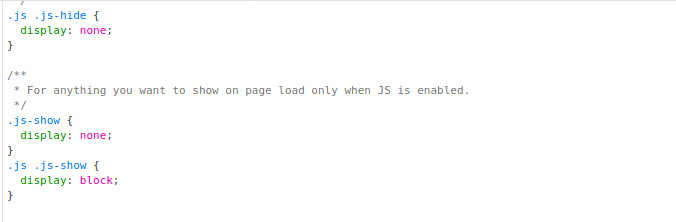


6.OWASP –ZAP was used to spider attack the web app. In order to find some vulnerabilities. This process uses the automated scan. In this exercise we found a major vulnerability which showed that the web app used the outdate JQuery. Below is the image showing the result of the automated scan



Although the threat was medium using the outdate version may pose a major risk in the application security.

Using a different operating system, a code was inspected and the aim was to be able to remove the block feature in JavaScript to none . below is the attempt



This was done after inspecting the web code but it was not successful since the web had the robot.txt file which helps the web to be secure.

**Recommendation**

Upgrade dbms and jQuery

Use web application firewall

SCOPE OF WORK

1. What are the target organization's biggest security concerns: (Examples include disclosure of sensitive information, interruption of production processing, embarrassment due to website defacement, etc.)?

* Using outdate JQuery
* Not using web application firewall
* Available hidden pages
* What specific hosts, network address ranges, or applications should be tested:

1. What specific hosts, network address ranges, or applications should be tested:

* <https://www.1gov.gov.bw/> website is the application being tested

1. The test was performed on a live production environment

Did the penetration test include the following testing techniques:?

Ping sweep of network ranges: \_\_\_\_\_\_\_\_NO\_\_\_\_\_\_\_\_\_\_\_

Port scan of target hosts: \_\_\_\_\_\_\_\_\_\_\_\_YES\_\_\_\_\_\_\_\_\_

Vulnerability scan of targets: \_\_\_\_\_\_\_\_\_YES\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Penetration into targets: \_\_\_\_\_\_\_\_\_\_\_\_\_YES\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Client-side Java/ActiveX reverse engineering: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_YES\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Physical penetration attempts: \_\_\_\_\_\_\_\_\_NO\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Social engineering of people: \_\_\_\_\_NO\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Other: \_\_\_\_\_\_\_\_\_\_SQL injection\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Will penetration test include internal network testing: \_\_\_\_\_\_NO\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ If so, how will access be obtained: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Is social engineering allowed: \_\_\_\_\_\_\_\_\_\_\_NO\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ If so, how may it be used: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Are Denial of Service attacks allowed: \_\_\_\_\_NO(because some people may want to use services\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Are Dangerous checks/exploits allowed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Primary Contact representing Target Organization \_\_\_\_\_\_\_\_S. GWEBU

Date: 03/07/2022

**EXECUTIVE SUMMARY**

In a period of five days shangano Gwebu carried out a penetration test in the 1gov platform website. A few vulnerabilities where found in the web application including, using outdated jQuery and not including web application firewall thus giving attackers more chances of hacking the website. In this exercise few tools where used which include OWASP, ZAP, sqlmap and burp suite. According to shangano Gwebu’s findings 1gov platform has a fair security although it was difficult to conclude because of the time given. Some hidden files where found including admin login page in which a Brute force attack was attempted but it was not successful. Shangano Gwebu recommends updating jQuery and using web application firewall to help make the application more secure than it is.