

Vulnerability Assessment using OWASP ZAP

1. Introduction

This report documents the process of conducting a vulnerability assessment on a target website using OWASP ZAP. The assessment includes installation of required tools, execution of an active scan, and analysis of the results.

2. Tools Used

- Nessus – Installed for general vulnerability scanning purposes.
- OWASP ZAP (Zed Attack Proxy) – Used to run a security scan on the target web application.

3. Steps Performed

Step 1: Installed Nessus on a Kali Linux system.

Screenshot of installation:

```
(kali@kali)-[~/Downloads]
└─$ sudo apt install ./Nessus-10.8.3-debian10_amd64.deb
[sudo] password for kali:
Note, selecting 'nessus' instead of './Nessus-10.8.3-debian10_amd64.deb'
The following packages were automatically installed and are no longer required:
 fonts-liberation2 libboost-iostreams1.83.0 libgfapi0 libgles1 libhdf5-hl-100t64 libpython3
 ibverbs-providers libboost-thread1.83.0 libgfrpc0 libglusterfs0 libibverbs1 librados2
 libarmadillo12 libcephfs2 libgfxdr0 libglvnd-core-dev liblbfgsb0 librdmacm1
 libbfio1 libegl-dev libgl-mesa-dev libglvnd-dev libnetcdf19t64 libsuperlu
 libblosc2-3 libgdal34t64 libgles-dev libhdf5-103-1t64 libpoppler134 openjdk-23
Use 'sudo apt autoremove' to remove them.

Installing:
 nessus

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 447
Download size: 0 B / 68.8 MB
Space needed: 0 B / 61.2 GB available

Get:1 /home/kali/Downloads/Nessus-10.8.3-debian10_amd64.deb nessus amd64 10.8.3 [68.8 MB]
Selecting previously unselected package nessus.
(Reading database ... 406222 files and directories currently installed.)
Preparing to unpack .../Nessus-10.8.3-debian10_amd64.deb ...
Unpacking nessus (10.8.3) ...
Setting up nessus (10.8.3) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
```

Step 2: Downloaded and installed OWASP ZAP.

Step 3: Performed an active scan on the target: <http://www.itsecgames.com>.

4. ZAP Scan Report Summary

Spider Scan:

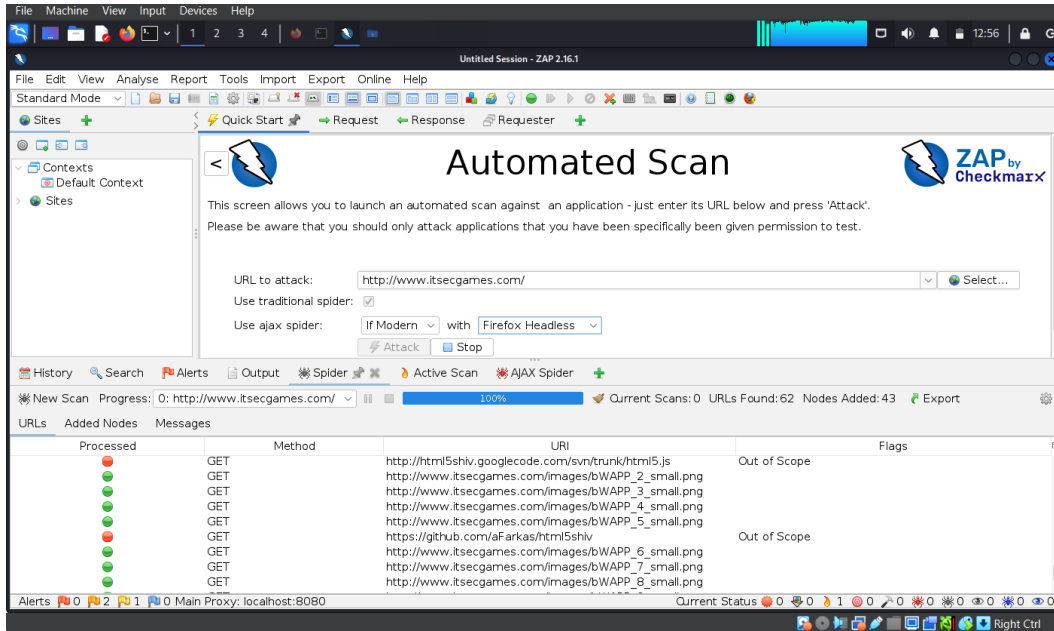
- Total URLs Found: 62
- New Nodes Added: 43

Active Scan:

- Total Requests Sent: 121
- New Alerts Found: 0

Alerts Summary:

- 1 alert (Risk: Medium, Confidence: High)
- 1 alert (Risk: Medium, Confidence: Medium)
- 1 alert (Risk: Low, Confidence: Medium)



5. Observations & Recommendations

- No critical vulnerabilities were found.
- Manual testing is advised to uncover logic flaws and deeper authentication issues.
- Consider enabling authenticated scans for more comprehensive testing.