Assignment Week 4:

Practical:

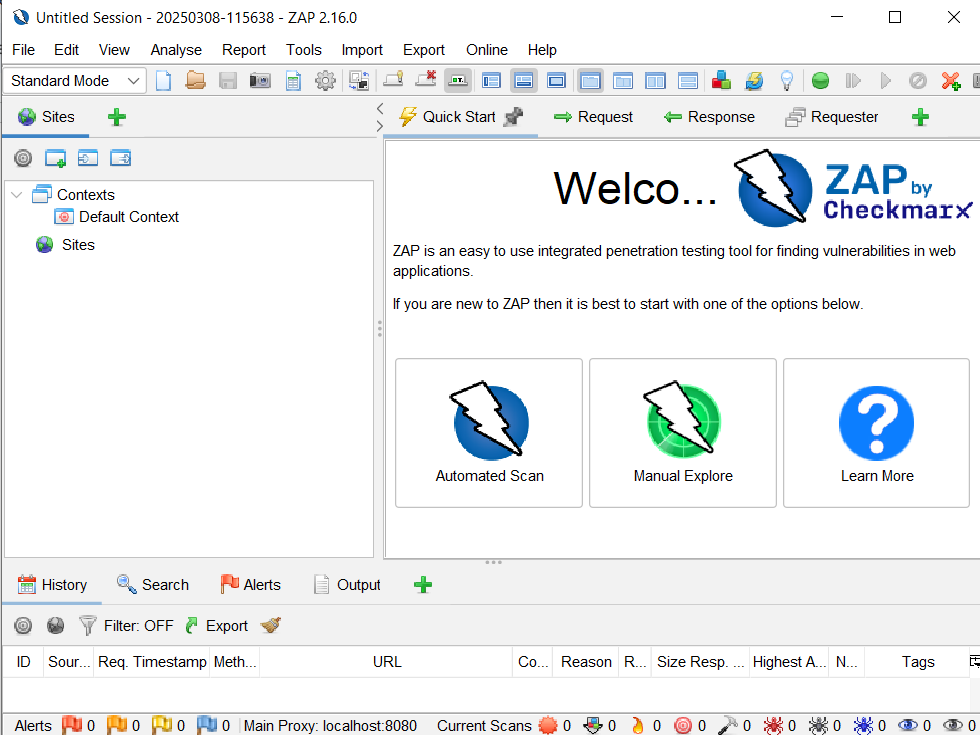
Perform a vulnerability scan on a demo website using online Scanners like OWASP ZAP

Solution

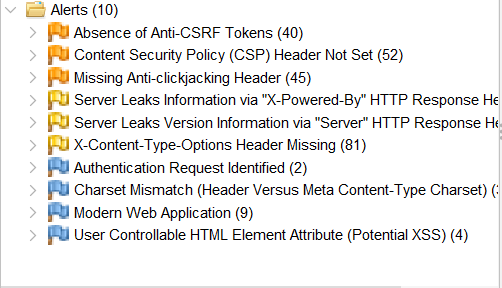
Online Scanner: OWASP ZAP

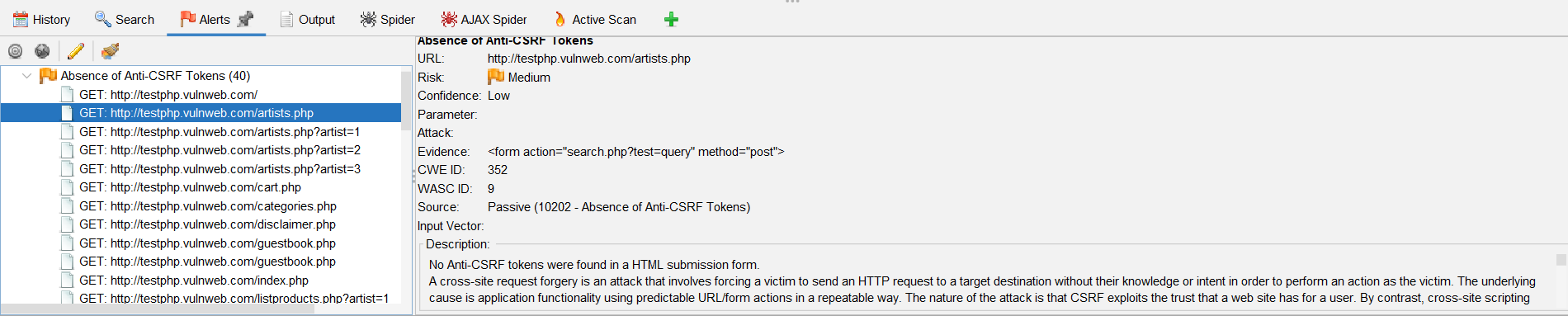
Demo Website:<http://testphp.vulnweb.com/>

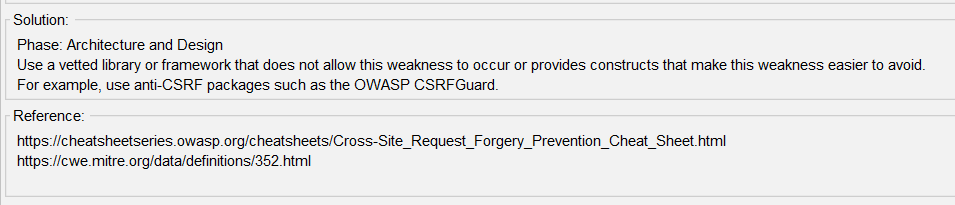
Steps

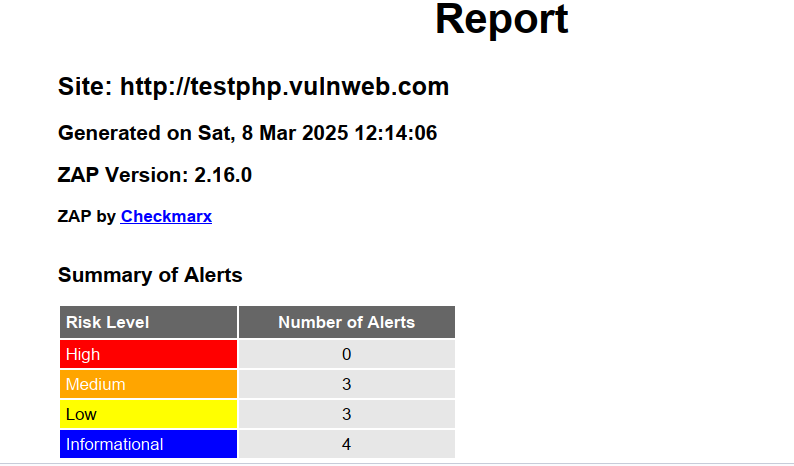


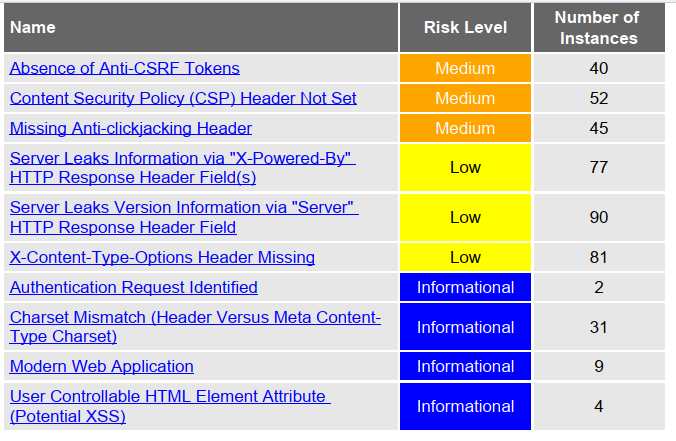












Question 2: Analyse a phishing attack scenerio and identify key indicators of compromise

### **Nigerian-Related Phishing Attack Scenario – NDDC Staff Targeted**

#### **Scenario:**

A staff member of the **Niger Delta Development Commission (NDDC)**, **Mr. Emeka**, receives an email appearing to be from the **Federal Ministry of Niger Delta Affairs (FMNDA)**. The email claims that a **mandatory audit of NDDC staff accounts** is ongoing, requiring immediate verification.

The email contains a **"Verify Your Account"** link, leading to a **fake NDDC portal**. Mr. Emeka enters his **username and password**, unknowingly handing them over to the attacker.

A few hours later:

* **His email starts sending phishing messages** to other NDDC employees.
* **Unauthorized financial transactions** occur in the NDDC procurement system.
* **Sensitive internal documents** are downloaded by an unknown IP address.

## **Draft Phishing Email Example**

### **📌 Subject: Urgent: NDDC Staff Account Audit – Action Required**

**From:** it-support@fmn-delta-gov.ng *(Fake address, real one should be fmn.gov.ng)* **To:** Mr. Emeka  
 **Date:** March 8, 2025

**Dear Mr. Emeka,**

In compliance with the Federal Government's **Anti-Corruption and Transparency Initiative**, all **Niger Delta Development Commission (NDDC) staff accounts** are undergoing a **mandatory audit**.

As part of this process, you are required to verify your staff credentials to **avoid suspension of your official email and payroll access**.

✅ **Click below to verify your account now:** 👉 [Verify Now](http://nddc-staffportal-gov.ng) *(Fake link! Looks official but is malicious.)*

This verification is compulsory and must be completed before **March 10, 2025** to ensure compliance with the **Presidential Monitoring Task Force**.

If you have any questions, contact **NDDC IT Support** at it-support@fmn-delta-gov.ng.

Thank you,  
 **IT Support Team** **Niger Delta Development Commission (NDDC)** **Official Website:** [www.nddc.gov.ng](http://www.nddc.gov.ng) *(Real link included to add legitimacy.)*

## **Key Indicators of Compromise (IoCs) in the Email**

### **1. Fake Sender Address**

* **Fake Email:** it-support@fmn-delta-gov.ng *(Extra "delta" to mimic FMNDA domain.)*
* **Real Email Should Be:** it-support@nddc.gov.ng.

### **2. Urgent Language and Threats**

* "Failure to verify your staff credentials will result in **account suspension**."
* "Must be completed before **March 10, 2025**."

### **3. Suspicious Link**

* **Malicious:** http://nddc-staffportal-gov.ng *(Fake domain, pretending to be official.)*
* **Real NDDC Portal:** https://staff.nddc.gov.ng.

### **4. Social Engineering Tricks**

* References **"Presidential Monitoring Task Force"**, which may sound authoritative.
* Uses a **real government logo** and fake **FMNDA references** to appear legitimate.

## **How This Phishing Attack Could Harm NDDC**

🚨 **Email Takeover:** The attacker can use Mr. Emeka’s email to phish more staff.  
 🚨 **Financial Fraud:** Procurement and fund disbursement systems can be accessed.  
 🚨 **Leak of Sensitive Documents:** Memos, project contracts, and budget plans can be stolen.

## 

## **How to Mitigate and Respond**

### **1. Immediate Actions**

✅ **Reset Mr. Emeka’s Password** and enforce **Multi-Factor Authentication (MFA).** ✅ **Block the malicious domain** (nddc-staffportal-gov.ng).  
 ✅ **Check NDDC's email logs** for suspicious login attempts.

### **2. Long-Term Prevention Strategies**

🚀 **Train NDDC staff on phishing awareness.** 🚀 **Enable email filtering tools (SPF, DKIM, DMARC) to block fake emails.** 🚀 **Regularly audit login logs and network activity.** 🚀 **Restrict financial transactions to authorized devices.**