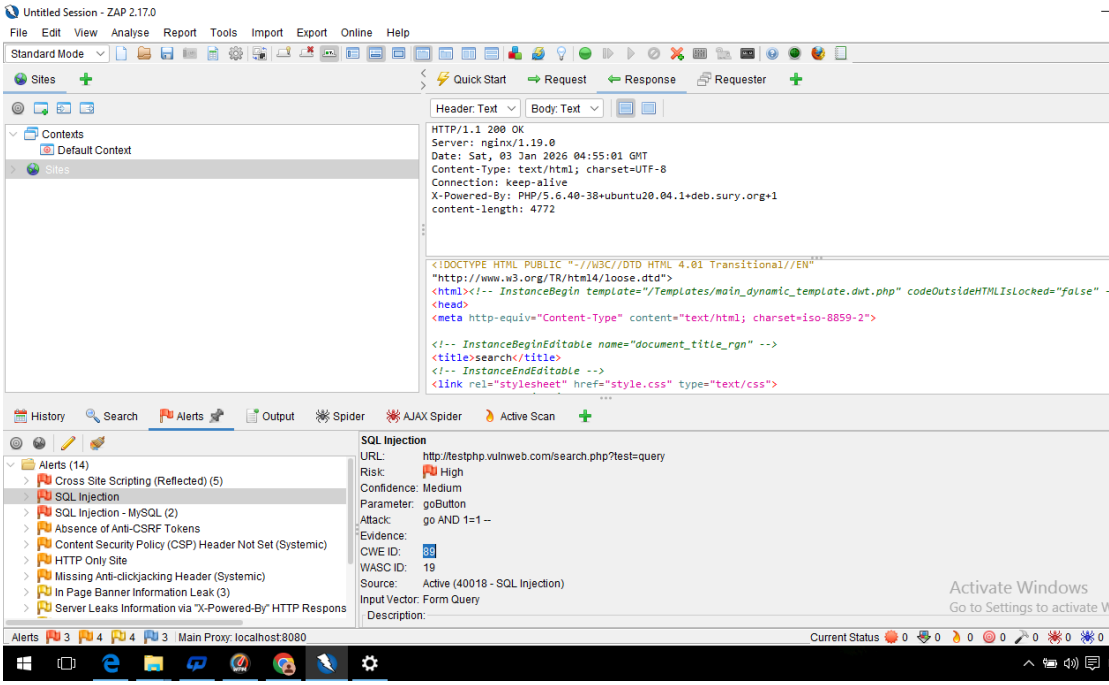
Cyber security internship - task 1

Name:chaudhary ashish haribhai
Tool used:owasp zap
Target website: http://testphp.vulnweb.com

1. **Vulnerability name: sql injection**
   Risk level: high
   Description:
   Sql injection is a security vulnerability that allows an attacker to interfere with the queries that an application makes to its database.
   Impact:
   - **Data leakage**
   - **Unauthorized access**
   - **Database manipulation**

   Solution:
   - **Use prepared statements**
   - **Validate and sanitize user input**
   - **Avoid displaying database error messages**
   - **Screenshot:**



2. **Vulnerability name: cross site scripting (xss - reflected)**
   Risk level: high
   Description:
   Cross site scripting (xss) is a vulnerability that allows attackers to inject malicious javascript code into web pages viewed by users.

Impact:

- **Session hijacking**
- **Cookie theft**
- **User data compromise**

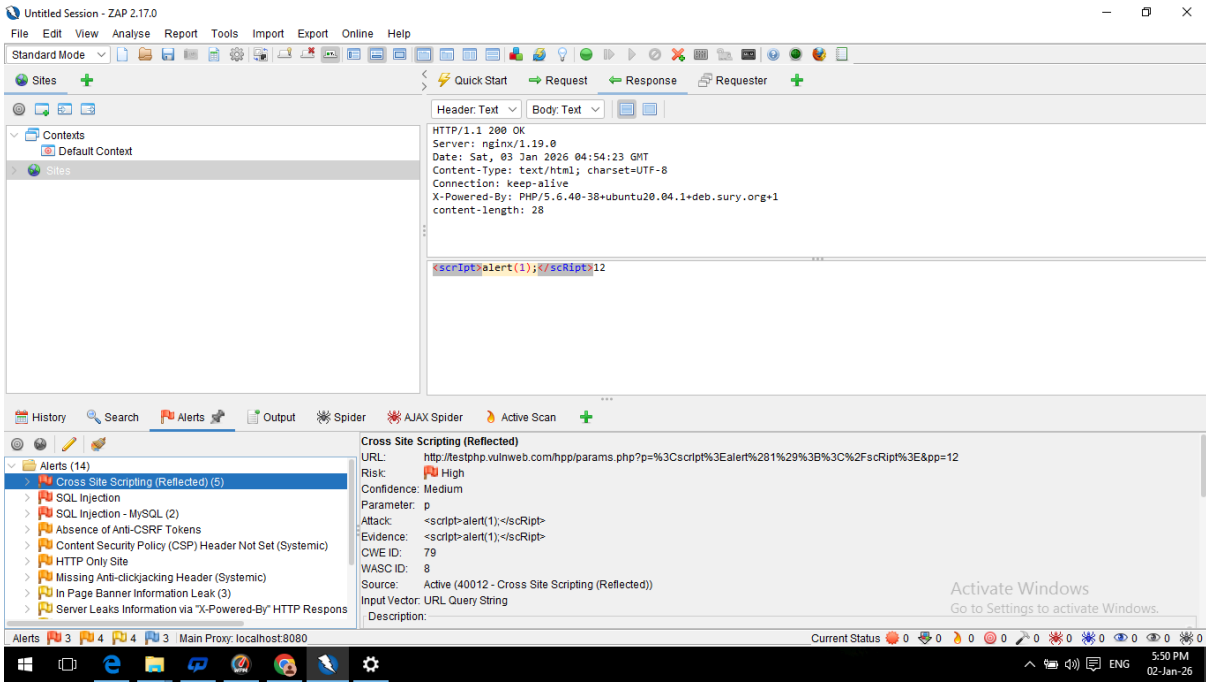
Solution:

-input sanitization

- output encoding

- use content security policy (csp)

Screenshot:



Conclusion:

This security assessment was performed using owasp zap. The scan identified critical vulnerabilities such as sql injection and cross site scripting. These issues should be fixed to improve application security.