Report

1).Findings:

The site of acunetix acuform url: <http://testasp.vulnweb.com/> is a vulnerable site which consists of multiple types of vulnerabilities some of the common type are SQL injection and XSS.

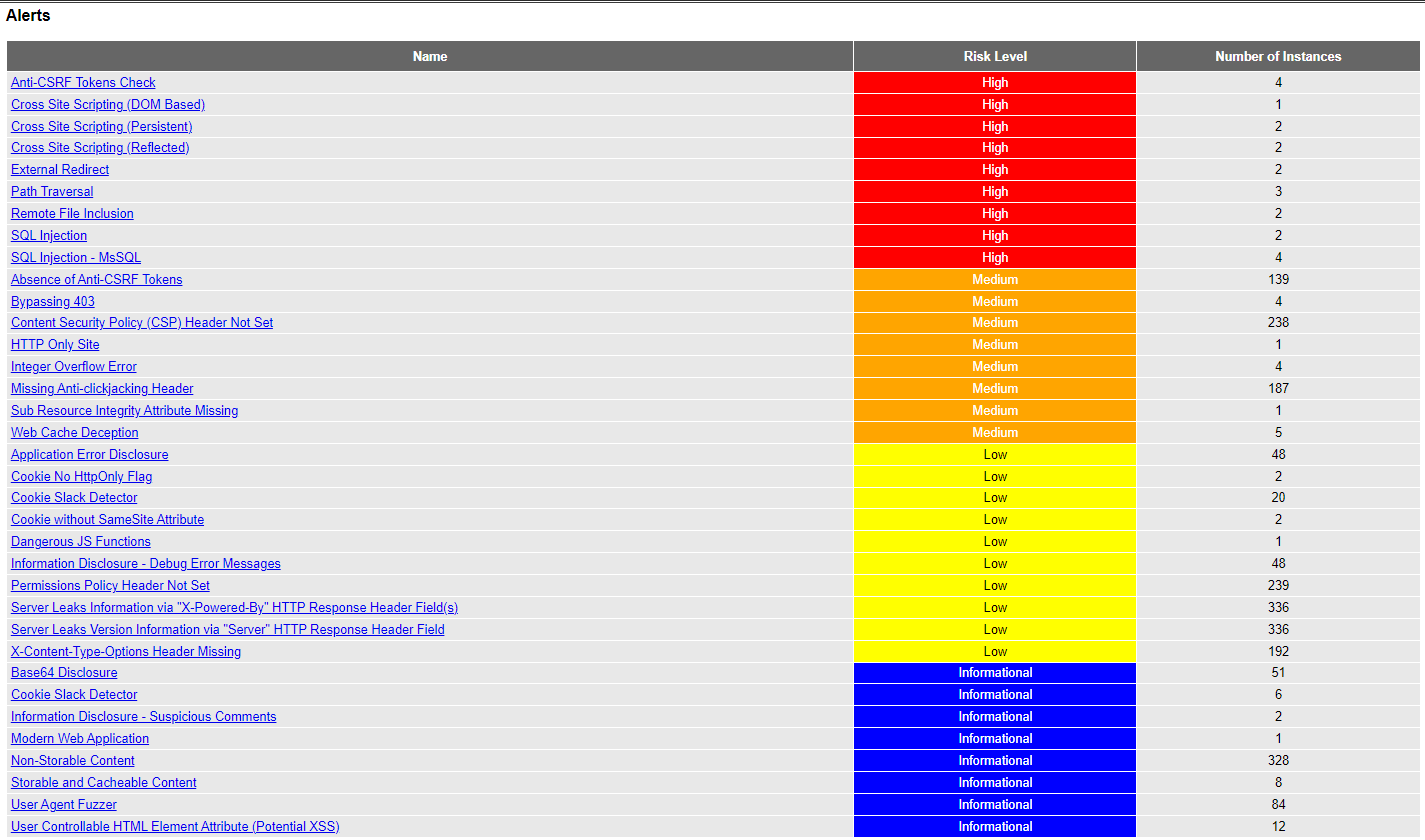
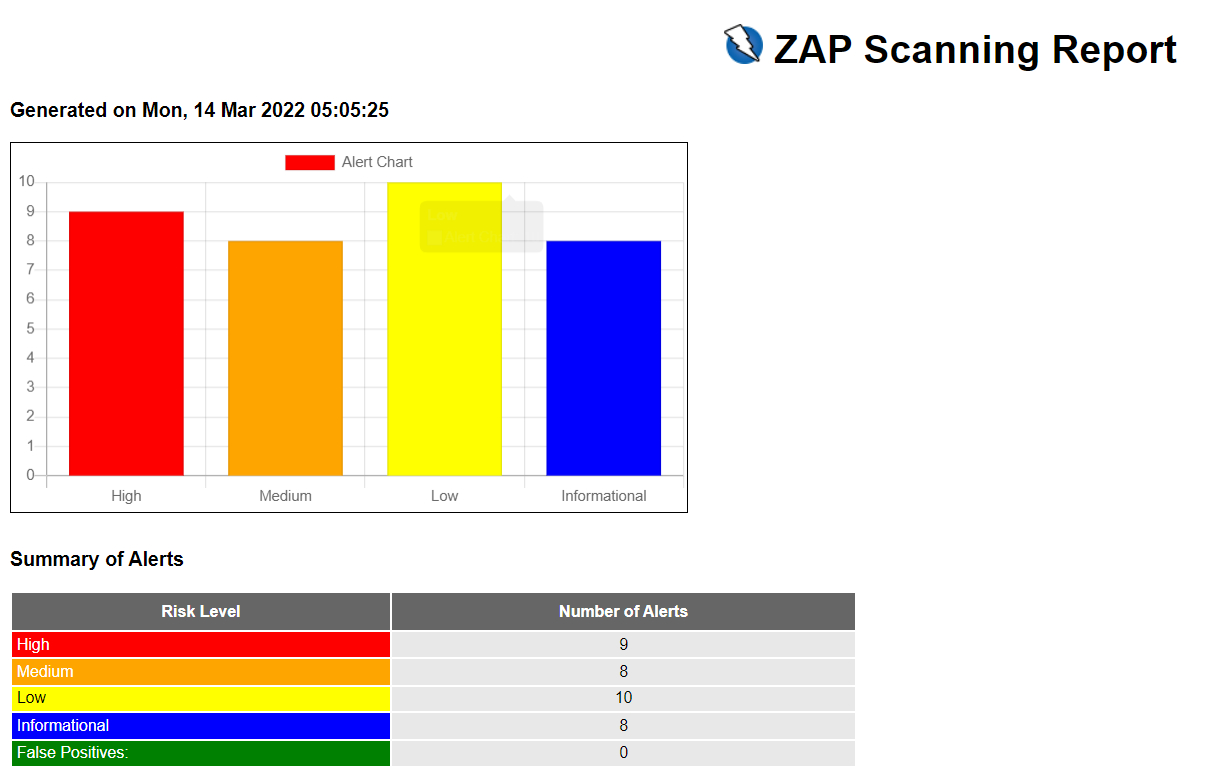
2).Risk Assessment:

High: 9

Medium: 8

Low: 10

Informational: 8



3).High Severity Vulnerability:

Name : SQL Injection

Impact:

A SQL Injection attack consist or insertion or injecting of a SQL query through input field from the client to the application. A successful SQL injection attack can give the attacker an opportunity to execute, read, modify and update the database.

4).Instances:

There has been 6 instances where the high severity vulnerability have been detected in the site of acunetix acuform. SQL Injection and MsSQL vulnerabilities are the High severity vulnerabities that has been exploited.

SQL Injection:

1.) URL: <http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F>

Method: POST

Parameter: tfUName

Attack: ZAP' AND '1'='1' –

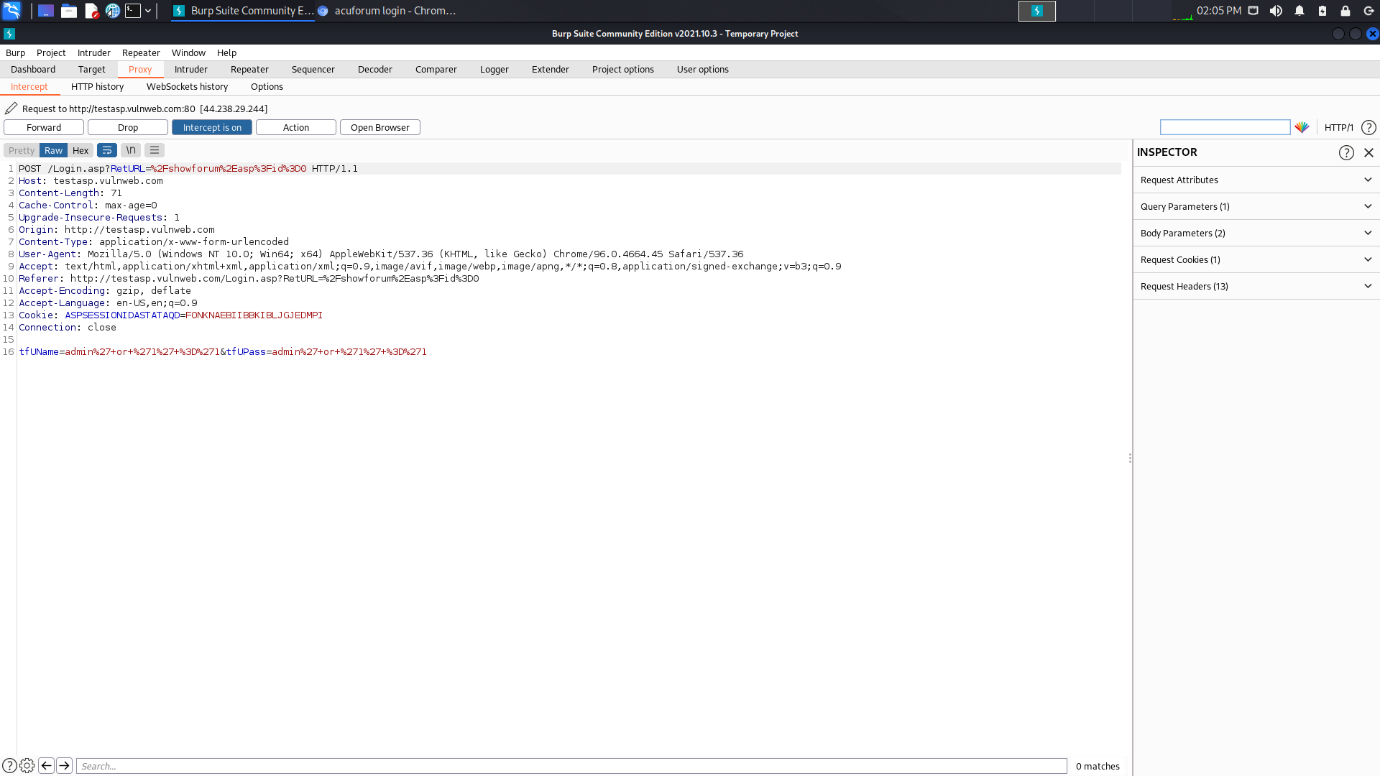
2.) URL: <http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F>

Method: POST

Parameter: tfUPass

Attack: ZAP' AND '1'='1' –

Screenshot:



Tags: [OWASP\_2021\_A03](https://owasp.org/Top10/A03_2021-Injection/), [WSTG-v42-INPV-05](https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05-Testing_for_SQL_Injection), [OWASP\_2017\_A01](https://owasp.org/www-project-top-ten/2017/A1_2017-Injection.html)

CWE Id: [89](https://cwe.mitre.org/data/definitions/89.html)

SQL Injection – Ms SQL:

3.) URL: <http://testasp.vulnweb.com/Search.asp?tfSearch=ZAP>

Method: GET

Parameter: tfSearch

Attack: ZAP) WAITFOR DELAY '0:0:15' –

4.) URL: <http://testasp.vulnweb.com/showforum.asp?id=2>

Method: GET

Parameter: id

Attack: 2" WAITFOR DELAY '0:0:15' –

5.) URL: <http://testasp.vulnweb.com/showthread.asp?id=40>

Method: GET

Parameter: id

Attack: 40 WAITFOR DELAY '0:0:15' –

6.) URL: <http://testasp.vulnweb.com/showthread.asp?id=40>

Method: POST

Parameter: id

Attack: 40 WAITFOR DELAY '0:0:15' –

Tags: [OWASP\_2021\_A03](https://owasp.org/Top10/A03_2021-Injection/), [WSTG-v42-INPV-05](https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05-Testing_for_SQL_Injection), [OWASP\_2017\_A01](https://owasp.org/www-project-top-ten/2017/A1_2017-Injection.html)

CWE Id: [89](https://cwe.mitre.org/data/definitions/89.html)

5).Solution:

Phase: Architecture and Design

When the set of acceptable objects is being used such as filenames or URLs, is limited or known, create a mapping from a set of fixed values to the actual filenames or URLs.

eg: ID 1 could map to "inbox.txt" and ID 2 could map to "profile.txt". Features such as the ESAPI AccessReferenceMap provide this capability.

Phase: Architecture and Design; Operation

Run the code in sandbox environment that would enforce strict boundaries between the process and the operating system.

Do \*not\* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality.