bWAPP html injection

owaspbricks file upload

detection of open ports and versioning

https://www.youtube.com/watch?v=0yyi8RVfJ-w&list=PLWPirh4EWFpESKWJmrgQwmsnTrL\_K93Wi&index=21(cross site scripting, js)

spa"/><script>alert("test popup");</script>(Reflected XSS)

(Stored XSS)

<p>test&lt;/p&gt;&lt;script&gt;alert(\"test popup\");&lt;/script&gt;<\/p>

remove token

change token

change name for ex in jwt and generate new token

**CSV injection:**

This occur in file with export functionality

=cmd|'/C notepad'!'A1'

=cmd|' /C calc'!A0

**Sensitive information in session storage**

Inspect under session storage info should not display

**Unrestricted File Upload**

Compromise the web server by uploading and executing a web-shell which can run commands, browse system files, browse local resources, attack other servers, and exploit the local vulnerabilities, and so forth.

preventions

Uploaded directory should not have any "execute" permission.

Limit the file size to a maximum value in order to prevent denial of service attacks. {Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.[1]

In a distributed denial-of-service attack. (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source}.

<https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload>

TYPES OF UNRESTRICTED FILE UPLOAD:

1. Simple file upload: we can upload any file.
2. Content type verification: intercept a request and change the content-Type.

**CORS header manipulation**

Access-Control-Allow-\*(domain name should be there instead of \*)

**The OWASP Top 10 list consists of the 10 most seen application vulnerabilities in 2020:**

1. Injection

2. Broken Authentication

3. Sensitive Data Exposure

4. XML External Entities (XXE)

5. Broken Access Control

take over one or more accounts giving the attacker the same privileges as the attacked user. ... Due to poor design and implementation of identity and access **controls**

6. Security Misconfigurations

7. Cross-Site Scripting (XSS)

8. Insecure Deserialization

9. Using Components with known vulnerabilities

10. Insufficient logging and monitoring

**Disclosure of technical information in error messages:**

Hit any URL and observe weather it shows sensitive info or not.