





Beautifier.io

Reverse text

Submit

Burp suite

**Some extensions**

1. Hack bar for chrome
2. Cookie manager
3. Foxy proxy for Firefox

Cross-site scripting: cookies of the victim can be got by giving the payload to the user(victim). Sometime, it might be blocked because of the https.

Cookies: usually stored on client side, live loner, insecure, can be accessed and manipulate

Session: stored on server side, live shorter, more secure, always implement security on servers’ side.

**Directory Brute-Force**

Need: finding login portal for admin using simple user, or checking the bypass ability of authentication.

Tool: Go Buster, Dirbuster,

**Robots.txt**

To disallow files or pages to index on the google.

**Directory Traversal or Path Traversal**

**Bean (challange)**

**Command Injection**

**Wfuzz**

Burp Intruder

Code Injection : using server side language that was used in that system

SQl Injection

To remove end of file error, we put the semicolon where we want.

FLAG{Nginx\_nOt\_aLWays\_sEcUre\_bY\_The\_waY}

${system('ls')}

Web for pentester 1 and 2

DVWA

Abstract.rock