XSS Attacks

Prevent XSS

Prevent XSS

- We talked about how xss can be prevented on the server-side. But in the client side, how can we protect the user against XSS attacks?
  - Research about CSP and how CSP can affect XSS
  - Research about X-Content-Type-Options HTTP header

Prevent XSS - Solution

- No-Script and other protection plugins can protect clients against XSS attacks
- CSP stands for Content Security Policy. It Is a W3C specification offering the possibility to instruct the client browser from which location and/or which type of resources are allowed to be loaded. To define a loading behavior, the CSP specification use "directive" where a directive defines a loading behavior for a target resource type.
    - (.. more at https://www.owasp.org/index.php/Content_Security_Policy)
- If we set *X-Content-Type-Options* header to *nosniff*, It prevents the execution of inserted JavaScript into images and other content types

ZDResearch Advanced Web Hacking

ZDResearch

www.zdresearch.com