XSS Attacks

XSS and encoding

ZDResearch
www.zdresearch.com
ZDResearch Advanced Web Hacking

XSS and Encoding

- Encoding techniques are useful in XSS. Research code encoding methods that are usable in XSS evasion
- How can you change XSS payload appearance?

XSS and Encoding - Solution

- We can easily change our payload appearance but the browser must understand it for execution
- We may encode our script in base64 (which bypasses most blacklistings) and place it in a tag (for example META).
- Here is a simple example:
  - <META HTTP-EQUIV="refresh"
  - CONTENT="0;url=data:text/html;base64,PHNjcmlwdD5hbGVydCgndGVzdDMnKTwvc2NyaXB0Pg">
- Also URL schemes can be use to manipulate browser understanding of something. So URL schemes can be dangerous
  - Read more at: https://security.stackexchange.com/questions/148428/which-url-schemes-are-dangerous-xss-exploitable

ZDResearch

XSS and Encoding - Solution - Contd.

- Some useful links about javascript obfuscation (to bypass Blacklists):
  - https://www.danstools.com/javascript-obfuscate/
  - http://www.jsfuck.com/

ZDResearch Advanced Web Hacking

ZDResearch

www.zdresearch.com