Web Application Pentesting

Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

CSRF Trigger Tags

CSRF Trigger Tags

-
- <iframe src="XXX" />
- <script src="YYY" />

XMLHttpRequest based Triggering

- Most handy if XSS is found on the Victim website
- Can still work from the Attackers Website with a favorable CORS Policy
  - CORS to be discussed later in great detail

Demo

- OWASP WebGoat

https://github.com/WebGoat/WebGoat/wiki/Installation-(WebGoat-6.0)

Pentester Academy