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

Securing Unvalidated / Open Redirects

Securing Redirects

- Avoid use if possible
- Validate them. If redirect URLs are
  - Known
    - Use indirect identifiers e.g. index in an array or an ID column in a database
  - Unknown e.g. Social Media sites
    - Generate URLs with Hashes using long random salts which are rotated
    - Encrypt URLs in links and only redirect if it successfully decrypts
    - Rotate Keys/Salts regularly

Pentester Academy