

# 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>

# Unvalidated Redirects

# Unvalidated Redirects

- Redirects are necessary
  - Understanding user behavior
    - Exit links and frequency
  - Easy way to route visitors
  - Can be external or internal links
- Unvalidated Redirects
  - Exploit the “trust” of links on a domain
  - Phishing Attack with a trust component

# OWASP Top 10

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability <b>AVERAGE</b>	Prevalence <b>UNCOMMON</b>	Detectability <b>EASY</b>	Impact <b>MODERATE</b>	Application / Business Specific
Consider anyone who can trick your users into submitting a request to your website. Any website or other HTML feed that your users use could do this.	Attacker links to unvalidated redirect and tricks victims into clicking it. Victims are more likely to click on it, since the link is to a valid site. Attacker targets unsafe forward to bypass security checks.	Applications frequently redirect users to other pages, or use internal forwards in a similar manner. Sometimes the target page is specified in an unvalidated parameter, allowing attackers to choose the destination page.  Detecting unchecked redirects is easy. Look for redirects where you can set the full URL. Unchecked forwards are harder, because they target internal pages.		Such redirects may attempt to install malware or trick victims into disclosing passwords or other sensitive information. Unsafe forwards may allow access control bypass.	Consider the business value of retaining your users' trust.  What if they get owned by malware?  What if attackers can access internal only functions

[https://www.owasp.org/index.php/Top\\_10\\_2013-A10-Unvalidated\\_Redirects\\_and\\_Forwards](https://www.owasp.org/index.php/Top_10_2013-A10-Unvalidated_Redirects_and_Forwards)

