Web Security and the OWASP Top 10: The Big Picture

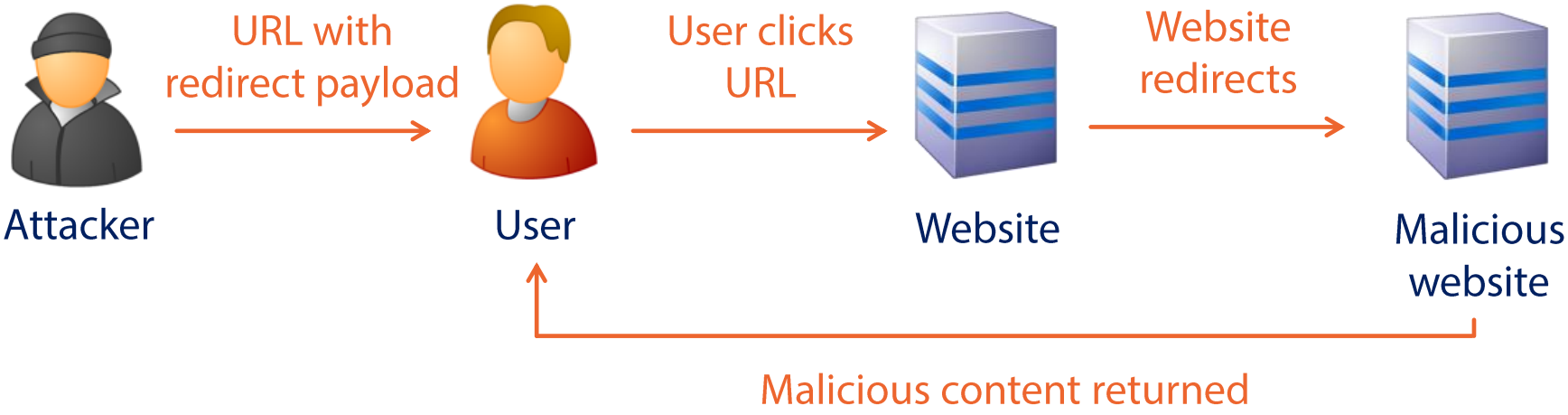
Unvalidated Redirects and Forwards

Troy Hunt
troyhunt.com
@troyhunt

pluralsight
hardcore developer training

Unvalidated Redirects and Forwards Overview

Attack Vectors	Security Weaknesses		Technical Impacts
Exploitability Average	Prevalence Uncommon	Detectability Easy	Impact Moderate



Understanding Unvalidated Redirects and Forwards

"Here's a piece of text on a website with a link to an external website."

/redirect/?url=http://externalwebsite.com

Attacker

http://vulnerablesite.com/redirect/
?url=http://attackersite.com/malware.exe

Common Defences Against Unvalidated Redirects and Forwards

Use a URL whitelist

- What URLs are allowed to be redirect to?
- Abort if the URL is not allowed

Use indirect references

- Pass an ID to the redirect, not a URL
- Resolve the URL from a reference map

Check the referrer

- Did the redirect originate from the site?
- May need to whitelist multiple sites

Unvalidated Redirects and Forwards in the Wild – Government Websites