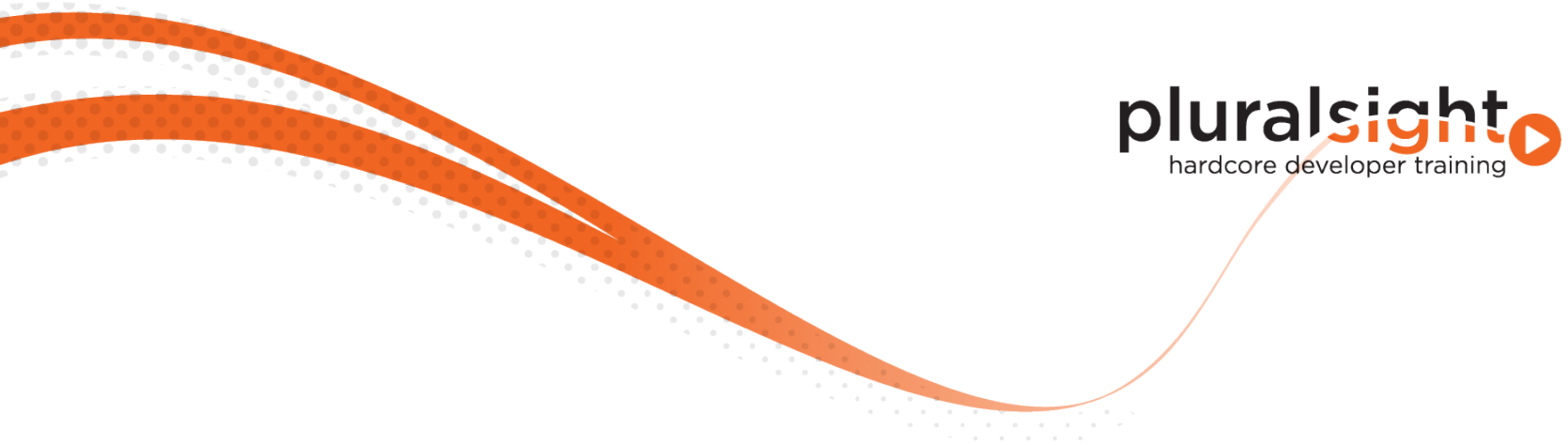
The OWASP Top 10 Web Application Security Risks for ASP.NET

Troy Hunt
troyhunt.com



pluralsight
hardcore developer training

Outline

- Who's getting hacked?
- Who's doing the hacking?
- OWASP and the Top 10
- Applying security in depth

Who's getting hacked?

citibank

LOCKHEED MARTIN

SONY

SEGA®

Linked in

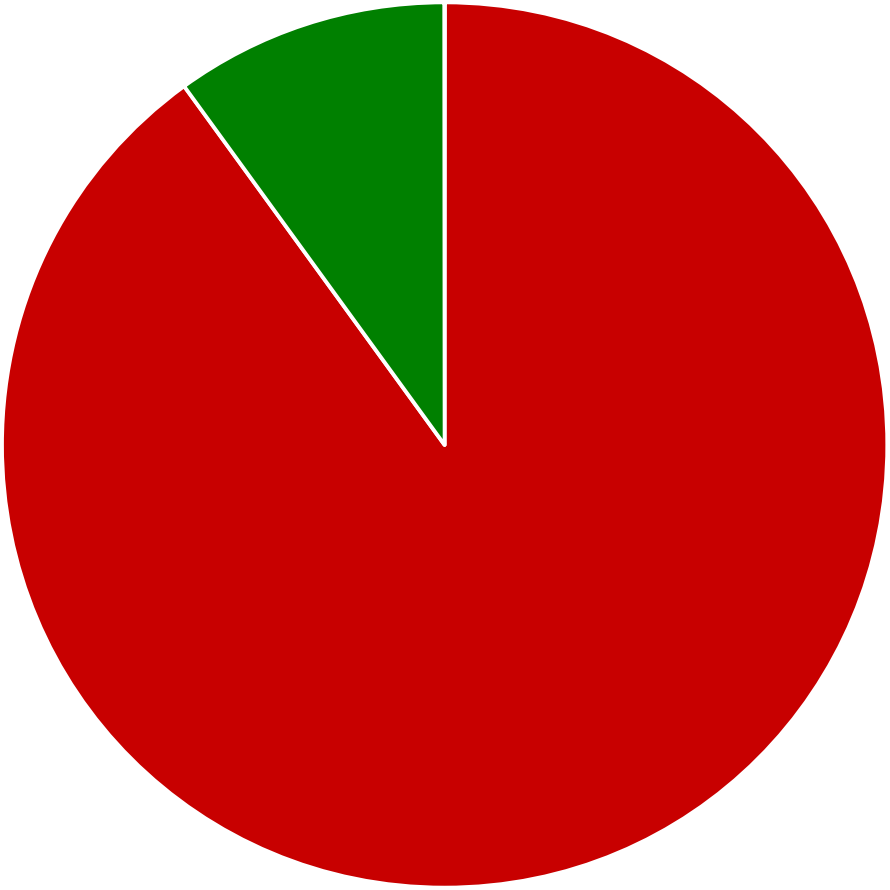
RSA
SECURITY

HBGary
DETECT. DIAGNOSE. RESPOND.

last·fm™
the social music revolution

EVE
ONLINE

90% of websites have serious security flaws



Who's doing the hacking?

- We need to acknowledge that there are different actors playing different roles
- Their motivations, experience and resources have an important impact on the security design of websites
- Security is very frequently about degrees – it's about determining to what extent investment must be made
- Consider that question in light of the following three categories of attacker:

1. Hacktivists

- They often claim to be motivated by a higher cause…
- …yet it's frequently not much more than opportunistic snatching and grabbing
- They're regularly young, inexperienced and not conscious of the social consequences of their actions
- They're very poorly funded but quite vocal after a successful attack
- We know them by collective names such as Anonymous and LulzSec

2. Online criminals

- **This group's motivation is cash**
- **They're looking for assets of value which may include:**
  - Financial data which can be directly exploited or on-sold
  - Personal data that can be used for identity theft
  - Means of distributing malware and creating botnets
- **They have a degree of funding and may operate in a very well organised fashion**

3. Nation states

- This is the group whose activities are increasingly being referred to by the term “cyber warfare”
- Their targets include those of national security or political interest both internationally and domestically
- They are *extremely* well funded – no target is too big or beyond their reach with enough time and money
- One or more nation states were allegedly behind Stuxnet, Duqu and Flame

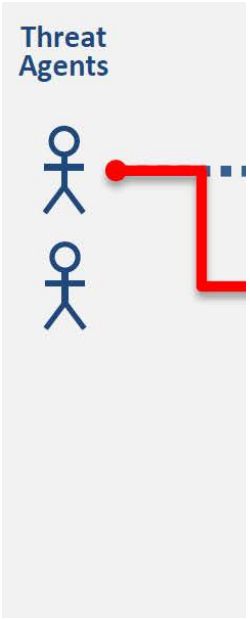
OWASP and the Top 10

- OWASP is the Open Web Application Security Project
- They're a not-for-profit worldwide charitable organisation focussed on improving the security of software on the web
- They produce a document called The Top Ten Most Critical Web Application Security Risks
- The "Top 10" is a technology agnostic guide for managing common website security risks
- It is frequently a reference point for security specialists and developers alike

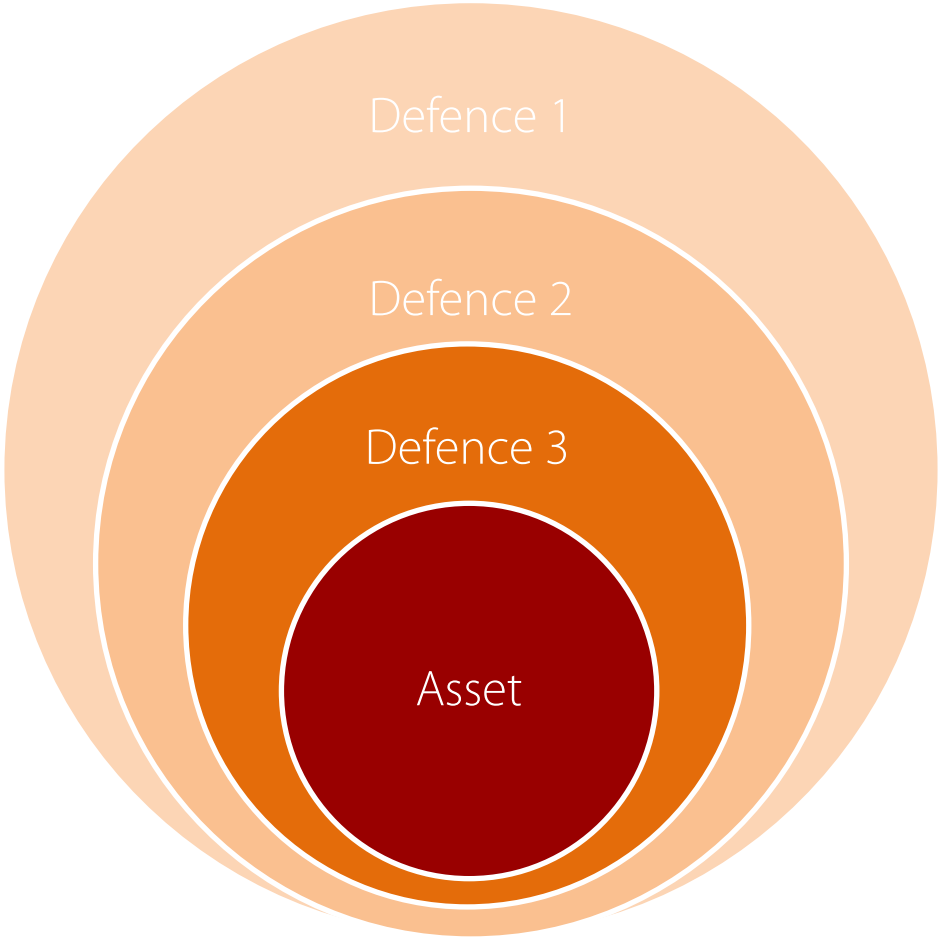
The Top 10

1. Injection
2. Cross-Site Scripting (XSS)
3. Broken Authentication and Session Management
4. Insecure Direct Object References
5. Cross-Site Request Forgery (CSRF)
6. Security Misconfiguration
7. Insecure Cryptographic Storage
8. Failure to Restrict URL Access
9. Insufficient Transport Layer Protection
10. Unvalidated Redirects and Forwards

Understanding application security risks



We'll be looking at security in depth



Security doesn't end with the Top 10

- **We're going to look at the Top 10 risks in great detail**
  - The definitions of the risks
  - How they're exploited
  - Multiple ways of mitigating them
- **Security goes well beyond just technology implementation though**
  - Business processes may pose risks
  - Social engineering may still exploit people risks
  - Other technology risks remain outside the scope of this course
- **This is a rapidly evolving landscape**
  - Attackers are in an arms race to outsmart builders
  - New risks and attack vectors are constantly emerging
  - Stay vigilant!