Web Security and the OWASP Top 10: The Big Picture

Using Components with Known Vulnerabilities

Troy Hunt
troyhunt.com
@troyhunt

pluralsight
hardcore developer training

Using Components with Known Vulnerabilities Overview

Attack Vectors	Security Weaknesses		Technical Impacts
Exploitability Average	Prevalence Widespread	Detectability Difficult	Impact Moderate

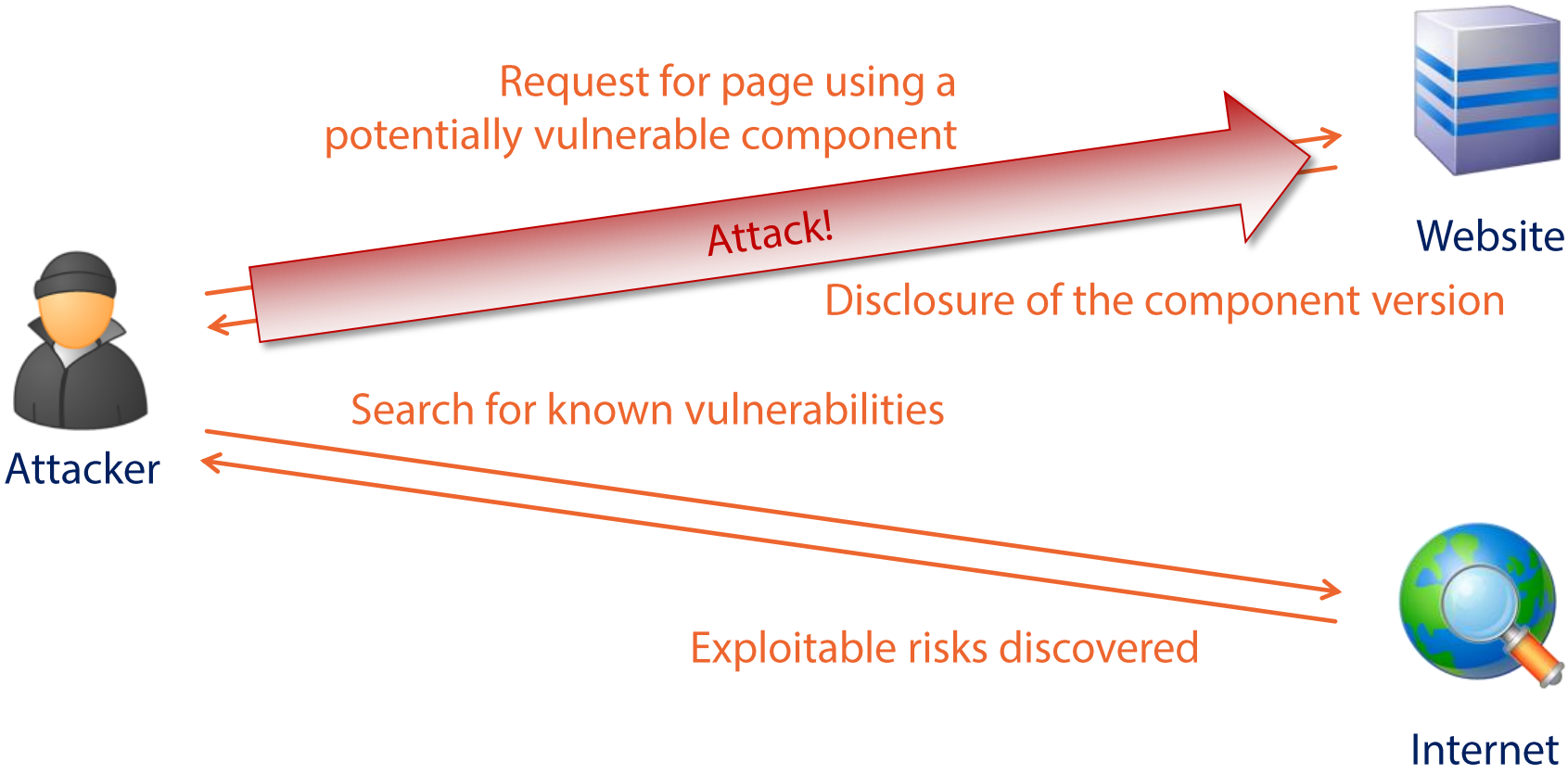
Attacker

Exploitation of vulnerable component

- Circumvent access controls
- Local file inclusion
- SQL injection, XSS or CSRF
- Vulnerable to brute force login

Website

Understanding Components with Known Vulnerabilities



Common Defences Against Components with Known Vulnerabilities

Identify components and versions

- Components are often used haphazardly
- Keep track of components and versions

Components should be monitored

- Keep abreast of project updates
- Monitor CVEs impacting the components

Keep components updated

- Use the framework's package management
- Regularly monitor new releases

Using Components with Known Vulnerabilities in the Wild – WordPress Brute Force

Massive WordPress Attack Targets Weak Admin Passwords

By Scott Gilbertson

If you're using the popular open source blogging tool WordPress to power your website, you may be vulnerable to a new web-based attack.

If your WordPress admin pages suddenly become sluggish, unreachable or you're unable to log in there's a good chance your site is being attacked.

According to CloudFlare CEO Matthew Prince, the attack is using brute force against WordPress' admin pages using the old default username "admin" and then trying thousands of passwords. There's nothing new about that approach, but what makes this attack different, and particularly potent, is that the attackers have some 90,000 unique IP addresses at their disposal.