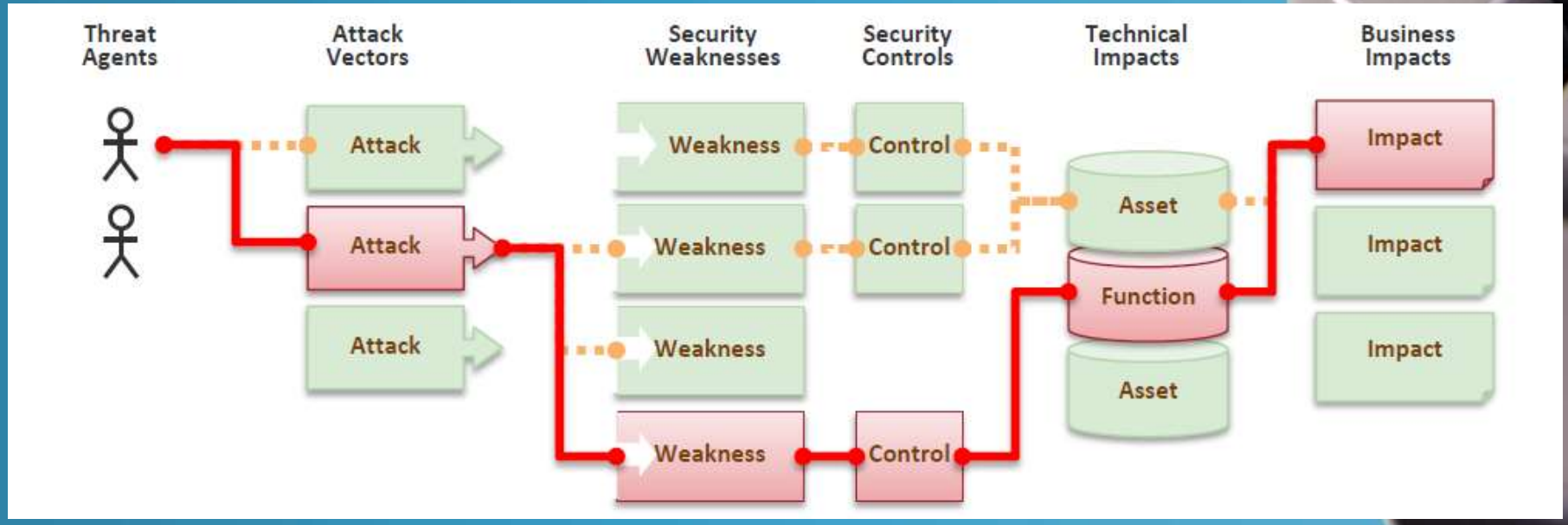
Ethical Hacking

by Douglas Williams

Intro

Attackers can potentially use many different paths through your application to do harm to your business or organization. Each of these paths represents a risk that may, or may not, be serious enough to warrant attention.

Sometimes, these paths are trivial to find and exploit and sometimes they are extremely difficult. Similarly, the harm that is caused may be of no consequence, or it may put you out of business.



What you need

- You don't need to be an expert
- Keep up to date with vulnerabilties
  - OWASP
- Know your tools
  - Manual methods via browser
  - Sqlmap
  - Burp (or any intercept proxy suite)
  - BeEF
- Reminder: It's still *hacking* so make sure you let others know of your actions for CYA purposes

Types of Vulnerabilities

Vulnerability	Description
Injection (SQL, OS, LDAP, & XML)	The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
Broken Authentication	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens.
Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
Cross-Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

Demos

- SQL Injection Demo
  - Manual
  - Using sqlmap
- XSS Demo

Links

- **OWASP Top 10**
  https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013
- **Sqlmap - http://sqlmap.org**
- **BeEF - http://beefproject.com/**