
Presents:

# *Web Application Hacking 101*

## Welcome to EvolveSec Twin Cities.

Grab some food and a beverage and get to know your neighbor.

# Disclaimer

*Do not try to hack into companies, or people's personal accounts.*

***It is illegal.***

*Use your own lab.*

# Following Along

- SSID: Clockwork Guest
- Key:  Welcome1

- Download Burp Suite Free
  - https://portswigger.net/burp/download.html
- Download sqlmap
  - http://sqlmap.org

**Work together with your neighbors and collaborate**

# For The More Advanced Folks

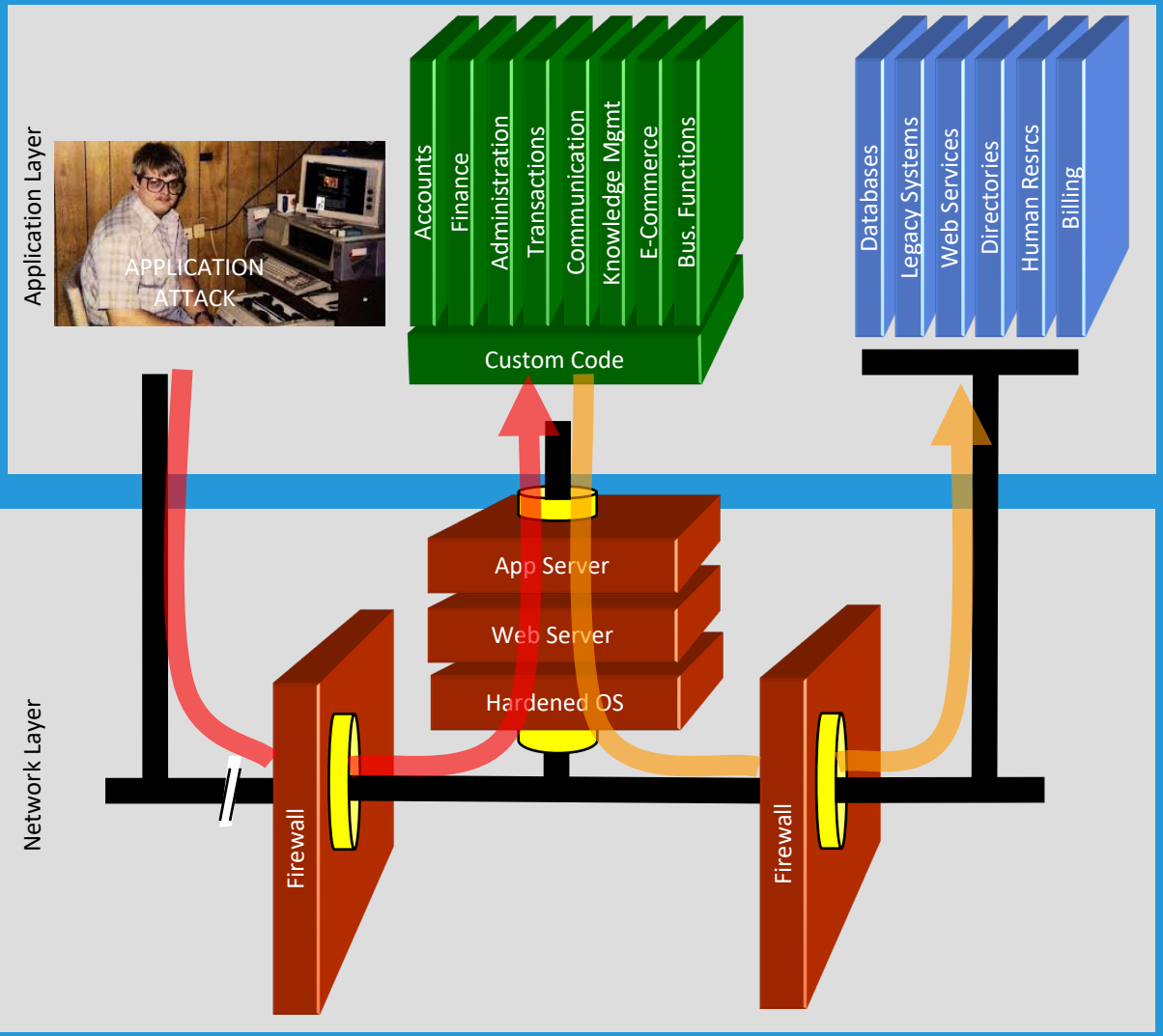
- Extra credit
  - Target: hack.evolvesecurity.io
  - Find as many vulnerabilities as possible
  - Evolve Security socks if you steal data or take control
  - NO DoS please

# Why Target Web Applications?

1. Available 24x7
2. Accessible from anywhere in the world
3. Attached to juicy databases

# Application Types

- Web
  - Uses web browser as client
- Thick
  - Client installed locally on operating system
  - Desktop (Mac / Windows / Linux)
  - Mobile (Android / iOS)
- Application program interface (API)
  - Server to server




Source: OWASP

EVOLVESECURITY

# Application Vulnerabilities

**OWASP Top 10 2013**

- A1 Injection
- A2 Broken Authentication and Session Management
- A3 Cross Site Scripting (XSS)
- A4 Insecure Direct Object References
- A5 Security Misconfiguration
- A6 Sensitive Data Exposure
- A7 Missing Function Level Access Control
- A8 Cross Site Request Forgery (CSRF)
- A9 Using Components with Known Vulnerabilities
- A10 Unvalidated Redirects and Forwards

# The Common Tools

- Kali Linux - Penetration Testing Linux Distro
- Nmap – Port Scanner
- Netcat – TCP/IP “Swiss Army Knife”
- Nessus – Vulnerability Scanner
- Nikto – Web Sever / Application Vulnerability Scanner
- SQL Map – Automated SQL Injection Tool
- Burp Suite Pro – Web Proxy / Testing Tool

# Manual Testing vs. Tools

**Tools can’t replace manual testing**

Real hackers (and penetration testers) don’t rely on automated tools.

# Lab (Vulnerable Application)

- Vulnerable OS and Web Application
  - Originally created by Fred Donovan and Michael Born
  - Updated and deployed by Jim Holcomb
  - Mal-Practice Hospital
    - hack.evolvesecurity.io

# OK Let's Play

- Download Burp Suite Free
  - https://portswigger.net/burp/download.html
- Download sqlmap
  - http://sqlmap.org

# Burp Suite Tutorial

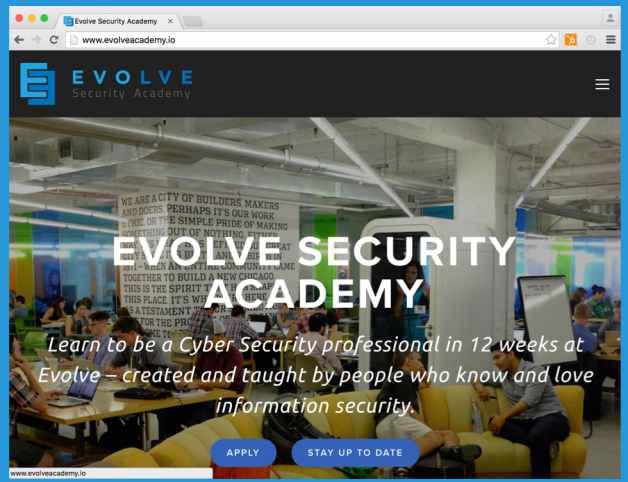
- Web proxy
- Lots of tools that make testing easy
- Best suite of web testing tools available

# Burp Suite Tutorial

1. Setup proxy
2. Clear browser cookies and web cache (history)
3. Turn on Intercept Server Responses

# Web Proxy

## Web Browser




HTTP Request

8080/TCP

HTTP Response

Random Ephemeral TCP

## Web Proxy


HTTP Request

80/TCP

HTTP Response

80TCP

## Web Server

EVOLVESECURITY

# Understand the Authentication

- Web communication is typically *stateless*
- Web applications commonly use cookies for authentication
  - Token(s) instead of passwords
  - Safer than passing username and password with each request
  - Cookie hijacking is possible

# Authenticated Testing

- Authenticate to application
  - username: ecoles
  - password: (tinks)
- Explore with Burp
  - Manually crawl the site
  - Manually check with Repeater
  - Use Intruder w/ SQLi list

# SQL Injection

- The ability to talk directly to the database via a vulnerable application parameter.
  - E.g. /blog/?**cat=**2
- Normal SQLi
  - The application returns a database error
- Blind SQLi
  - No database error is returned
  - We have to rely on time based checks to verify

# SQL Injection Test

- Choose a parameter to test
  - E.g. /blog/?**cat=**2

# SQLMap

- Automated SQL injection tool
- Check banner
  - `# sqlmap -r vulnerable_request.txt --banner`
- Dump entire database
  - `# sqlmap -r vulnerable_request.txt --dump`

# Thank you.

# Q&A

# Contact


- Paul Petefish
  - Paul@EvolveSecurity.io
- Bobby Custer
  - BCuster@EvolveSecurity.io


**www.EvolveSecurity.io**