White Hat Hacking
&
Penetration Testing
of
Web Applications

Tomáš Polešovský
15. 01. 2014
tomas.polesovsky@liferay.com

White Hat Hacking

- White Hat
  - Ethical Hacker
    - Can be certified
  - Name is the trademark … keeps good reputation
  - Follows some unwritten ethical rules
    - Respects privacy
    - Is responsible
    - Has good will to protect all parties
  - Is commonly paid by penetration tests contracts

White Hat Contract

- Ensures both parties are safe from injuries
- Defines time / scope of the penetration test
  - A demo machine with limited access
  - Or public site but no evasive techniques
- Can be paid by:
  - Completeness of testing
  - Time spent
  - Found bugs
- Output is a report containing security issues and severity

Bug Bounties

- Either each company specific Bug Bounty
  - https://bugcrowd.com/list-of-bug-bounty-programs
- Global platforms
  - http://hackerone.com
  - https://bugcrowd.com/
- How it works
  - Company defines scope
    - Sites in scope and out of scope
    - Types of issues interested in (Authenication, Authorization, XSS, ...)
  - Hacker submits a bug
  - Company verifies the reported bug
    - Can mark as invalid or non-relevant
  - If valid, fix and resolve the bug
  - Based on the bug severity assigns the bounty

Training Hacking

- Popular public sites
  - https://hack.me/
  - https://www.hackthissite.org/
- Challenges created by Community
  - Matasano Crypto Challenges (http://cryptopals.com/)
  - XSS Game https://xss-game.appspot.com/
  - XSS challenges https://github.com/cure53/xss-challenge-wiki/wiki/Older-Challenges-and-Write-Ups

Traditional Penetration Testing

- How it works
  - Gathering of all possible information
    - Google, Shodan, Whois, DNS records, IP ranges
  - Scanning attack surface
    - Accessible IP addresses, Open Ports, Running Services, Services impementation, Known bugs
  - Testing
    - Automated / tools - find common vulnerabilities and entry points
    - Manual – find other entry points, vulnerabilities
  - Exploitation
    - Using found vulnerabilities to get further and find other vulnerabilities
  - Report
    - With found vulnerabilities, impact, severity
- Penetration testing is mostly black-box testing
  - If customer provides source codes these can be included in the testing
    - Static code analysis

Pen-testing As a Service

- On-line services
  - Provides HTTP scan of exposed site
- Off-line services
  - Can provide also white-box scan of source codes or binaries
- We have some experience with Veracode
  - We test EE portal
  - Contact person: Sam Kong :)

Basic Pen-testing Tools

- Command-line tools
  - Dig, Whois … DNS, IPs
  - Nmap … port scanning
  - Sqlmap … exploiting SQLi
  - Metasploit … known vulns
- GUI apps
  - Wireshark … sniffing net
  - SOAPUI … SOAP testing
  - OWASP ZAP … web scanner
  - Burp Suite … web scanner
- Browser extensions and add-ons
  - Firebug / Web Developers Tools
  - ModifyHeaders / others
  - HackBar … encoding/decoding
  - RESTConsole / POSTMan - REST
  - WebSecurify … online service behind
- Enterprise scanning apps
  - Acunetix
  - Burp Suite Professional
  - HP Fortify
  - IBM Appscan

Pen-testing Checklists

- To be sure we covered most of we could
- https://www.owasp.org/index.php/Web_Application_Penetration_Testing
  - 4.1 Introduction and Objectives
  - 4.2 Information Gathering
  - 4.3 Configuration and Deployment Management Testing
  - 4.4 Identity Management Testing
  - 4.5 Authentication Testing
  - 4.6 Authorization Testing
  - 4.7 Session Management Testing
  - 4.8 Input Validation Testing
  - 4.9 Error Handling
  - 4.10 Cryptography
  - 4.11 Business Logic Testing
  - 4.12 Client Side Testing

Example Pen-test results

- Penetration testing of Liferay Cloud Services
  - Around 30 vulns found
  - Available administration interface, default passwords, XSS issues, CSRF, SSRF, DoS, Authorization issues, OpenRedirect, Missing authentication for remote API
  - 2nd and 3rd evaluation showed some more issues
    - Remote Code Execution, CSRF, XSS issues, default credentials, authorization issue

DEMO Time

That's all, thank you for listening.

Questions?