COMP2320/COMP6320 Offensive Security

Mehdi Baratipour - mehdi.baratipour@mq.edu.au

https://www.linkedin.com/in/baratipour

Department of Computing

MACQUARIE
University

MACQUARIE
University

COMP2320/COMP6320 Offensive Security

Module 2
Ethical hacking / Penetration testing
Web Applications

MACQUARIE
University

MACQUARIE
University

Table of Contents

1 Introduction

2 Information gathering

3 Find vulnerabilities

4 Tools

MACQUARIE University

Introduction

- Web application architecture
  - Front-end / Client side
    - Programming languages
    - Frameworks
  - Back-end / Server side
    - Programming languages
    - Frameworks
  - Database tier
- Web application security
- Web application ethical hacking
  - Information gathering
  - Find vulnerabilities
  - Exploit vulnerabilities
  - Post exploitation
  - Reporting

Information gathering

- Searching the Internet for any related possible information leakage
- Whois lookup
- Fingerprint web server
- Fingerprint web application
- Test HTTP methods
- Examine web app / server behaviour
- Map application architecture and hierarchy
- Find sensitive directories, files and pages
- Identify Application Entry Points

Find vulnerabilities

- Identity management testing
- Authentication testing
- Authorization testing
- Session management testing
- Input validation testing
- Testing error handling
- Check for weak cryptography
- Business logic testing
- Client-side testing

Find vulnerabilities - Identity Management

- User registration process
- Account provisioning process
- Account enumeration and guessable user account
- Weak or unenforced username policy

Find vulnerabilities - Authentication

- Bypassing authentication
  - Forced browsing
  - Parameter modification
  - Session ID prediction
  - SQL injection
- Credentials transported over an unencrypted channel
- Default credentials
- Weak lock out mechanism
- Weak password policy
- Weak security question answer
- Weak password change or reset functionalities
- Weaker authentication in alternative channel

Find vulnerabilities - Authorization

- Directory traversal
- Privileged escalation
- Insecure direct object reference
- Bypassing authorization

Find vulnerabilities – Session management

- Cookies attributes
- Session fixation
- Exposed session variables
- Cross Site Request Forgery
- Logout functionality
- Session timeout
- Session puzzling

Find vulnerabilities – Session management

- Cookies attributes
- Session fixation
- Exposed session variables
- Cross Site Request Forgery
- Logout functionality
- Session timeout
- Session puzzling

Find vulnerabilities – Input validation

- Reflected Cross Site Scripting
- Stored Cross Site Scripting
- SQL injection
- Command injection
- Buffer overflow

Find vulnerabilities – Error handling

- Error code
  - Web server errors
  - Application server errors
  - Database errors
- Stack traces

Find vulnerabilities – Business logic

- Forge requests
- Lack of proper integrity checks
- Process timing misuse
- Illegal function recalls
- Circumvention of work flows
- Application misuse
- File upload
  - Unexpected file types
  - Malicious files

Find vulnerabilities – Client side

- Cross-Site Scripting
  - DOM-Based
  - Reflected
- Client side URL redirect
- WebSocket
- Web Messaging

Tools

- Burp Suite
- Nikto
- Wfuzz
- DirBuster
- Sqlmap
- Acunetix manual pen testing tools (Free)
- Weevely
- Online services
  - https://w3dt.net
  - https://intodns.com
  - https://sitereport.netcraft.com
  - https://www.ssllabs.com/ssltest/
  - https://builtwith.com
  - https://archive.org
  - https://who.is
  - http://www.domaincrawler.com
  - https://www.shodan.io