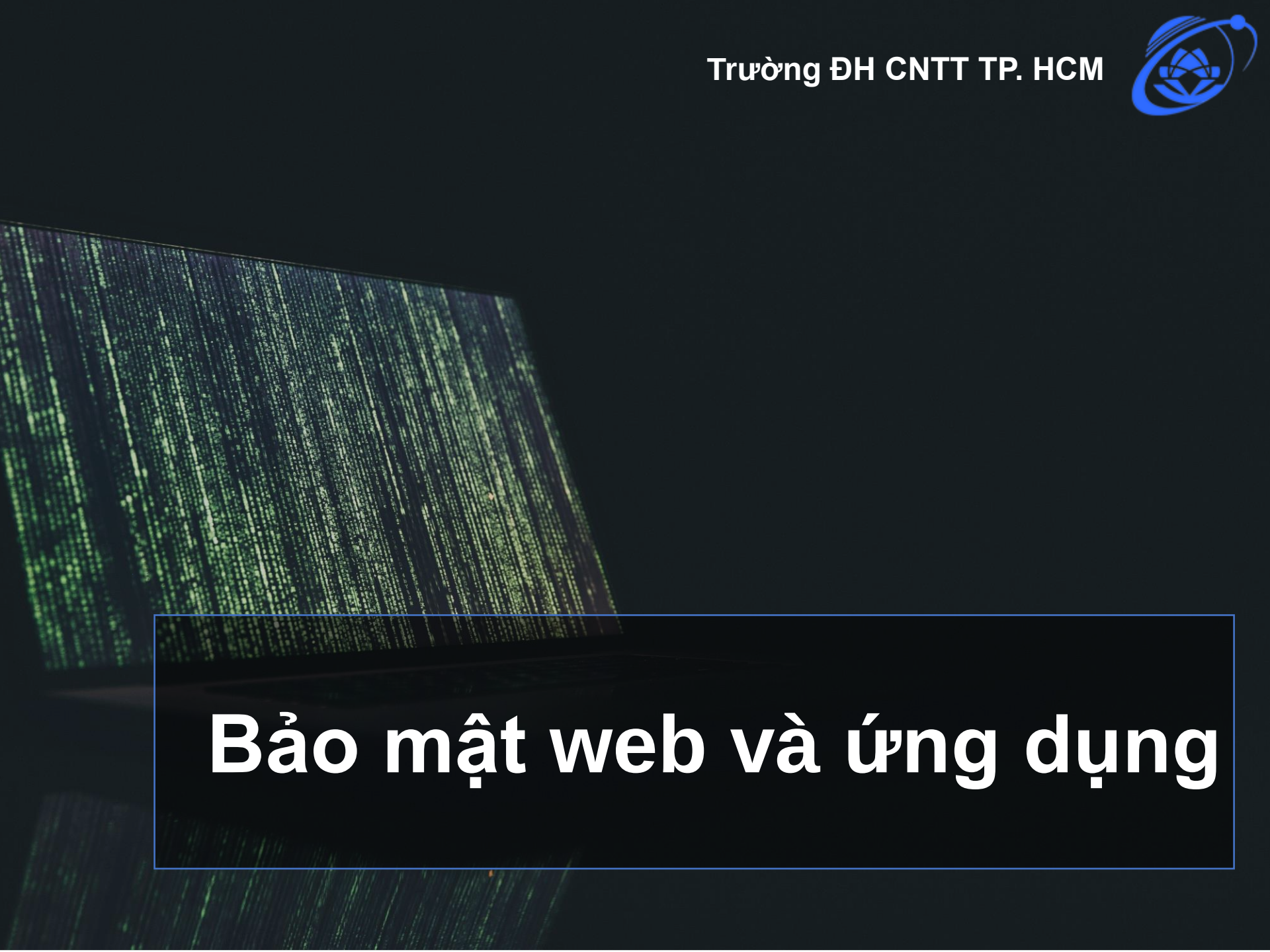
Trường ĐH CNTT TP. HCM



Bảo mật web và ứng dụng

Thông tin môn học

- **Môn học:** Bảo mật web và ứng dụng.
- **30 tiết** lý thuyết (**10** buổi – **3 tiết**/buổi)

- **Giảng viên lý thuyết:**
  - ThS. **Nguyễn Công Danh**
  - Email: **congdanh.congdanh@gmail.com**

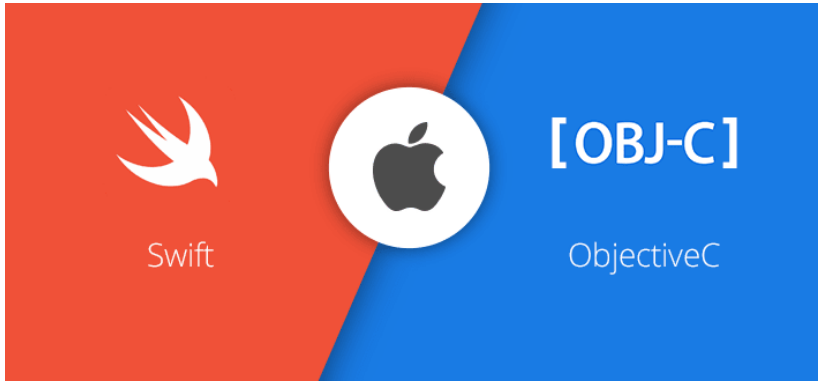
- **Kênh trao đổi thông tin: courses.uit.edu.vn**

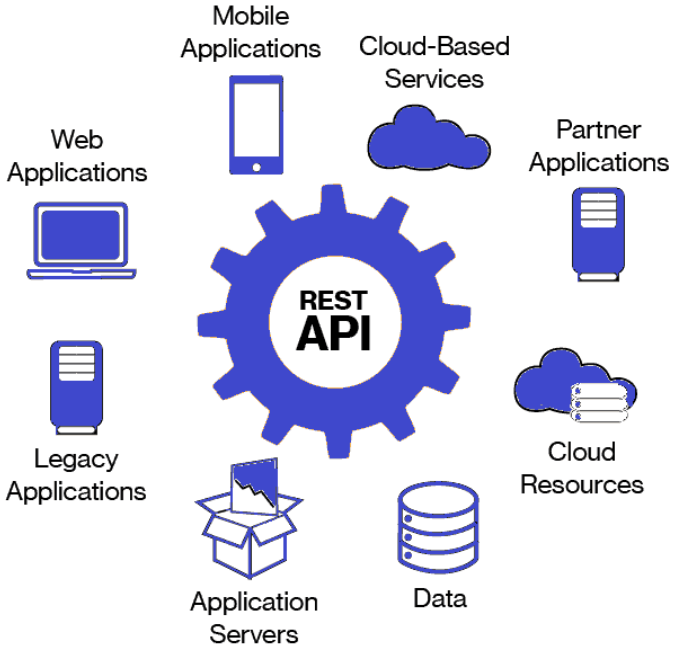
Khảo sát kiến thức

- Ứng dụng web
- Ứng dụng di động (Android/ iOS/…)
- Một số dạng tấn công vào các ứng dụng?
- CTF (Capture the Flag)?

Khảo sát kiến thức

Khảo sát kiến thức





Khảo sát kiến thức

OWASP

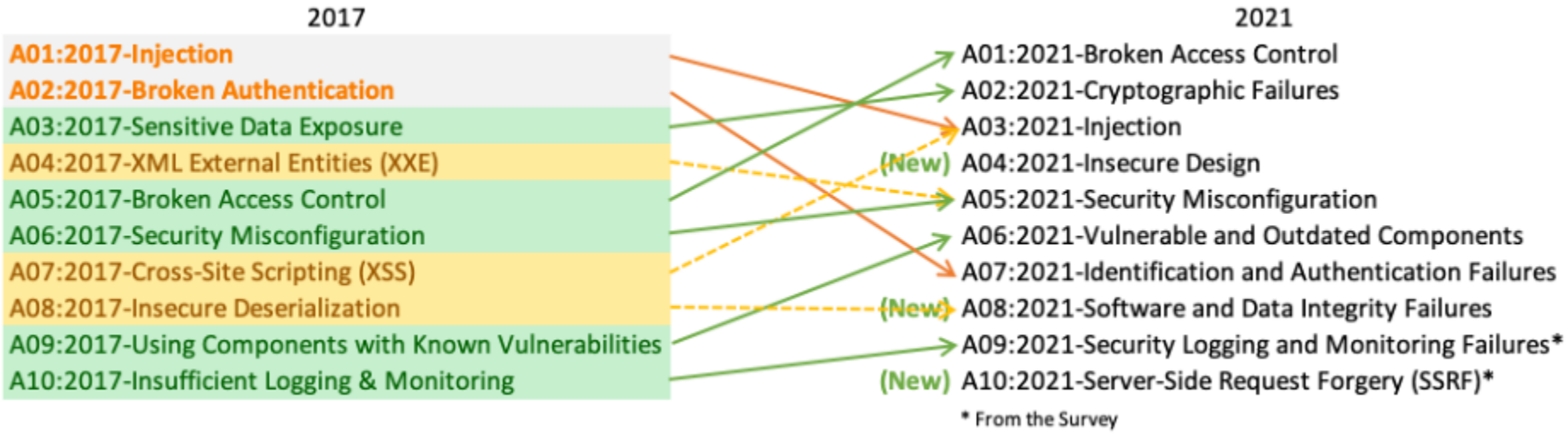
Open Web Application Security Project

OWASP

Mobile Security Project

Khảo sát kiến thức

OWASP
Open Web Application
Security Project



Mục tiêu và Nội dung

- **Mục tiêu:**

  Trang bị những kiến thức cơ bản về bảo mật, bảo vệ dữ liệu và an toàn thông tin.

- **Nội dung:**
  - Công cụ hỗ trợ tìm kiếm lỗ hổng, kiểm thử tự động
  - Đảm bảo an toàn ứng dụng di động (Android/iOS)
  - Kỹ thuật tấn công và thâm nhập ứng dụng web: XSS, CSRF, LFI, SQL Injection,…
  - Một số giải pháp bảo vệ
  - Checklist cho việc kiểm thử
  - Cách viết báo cáo kiểm thử

Yêu cầu

- Lên lớp đúng giờ
- Tìm hiểu trước bài giảng
- Bài tập trên lớp + Đồ án môn học
- Làm nhóm:
  - Không ghi nhóm → sao chép
  - GV kiểm tra bất kỳ thành viên nào trong nhóm
- Sao chép bài → 0 (tất cả các nhóm giống nhau).
- Bất kì thành viên nào trong nhóm không nắm kiến thức của nội dung nhóm thực hiện → trừ điểm cả nhóm

Đánh giá

- **30%** quá trình: đồ án, bài tập, điểm danh
- **30%** thực hành
- **40%** cuối kì

Chuẩn bị

Máy ảo:

- Kali Linux
- OWASP-BWA (OWASP Broken Web Apps)[1]
- Windows 7[2]
- Khác: bWapp Bee-box[3]

[1]: https://sourceforge.net/projects/owaspbwa/files/
[2]: https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/
[3]: https://www.vulnhub.com/entry/bwapp-beebox-v16,53/

OWASP-BWA

OWASP Broken Web Applications Project[1]

- Máy ảo chứa nhiều ứng dụng web có nhiều lỗ hổng: PHP, Java, .Net, CMS (Joomla, Wordpress)
- Dành cho:
  - Học bảo mật ứng dụng web
  - Kiểm tra kỹ thuật đánh giá thủ công
  - Kiểm tra công cụ tự động
  - Kiểm tra công cụ phân tích mã nguồn
  - Quan sát tấn công web
  - Kiểm tra WAF và kỹ thuật tương tự

[1]https://sourceforge.net/projects/owaspbwa/files/

OWASP-BWA

Chia thành **6** nhóm:

- **Training applications**:
  Hướng dẫn, giải thích,…
- **Realistic, intentionally vulnerable applications**:
  Ứng dụng thực tế, lỗ hổng được mô phỏng
- **Old (vulnerable) versions of real application**:
  Wordpress, Joomla

OWASP-BWA

- **Applications for testing tools**:

  Cho việc thử nghiệm các công cụ scan tự động

- **Demonstration pages / small applications**:

  Ứng dụng mẫu, minh họa

- **OWASP demonstration application**:
  - OWASP AppSensor giả lập mạng xã hội và có nhiều lỗ hổng
  - Log bất kỳ tấn công

OWASP-BWA

owaspbwa

OWASP Broken Web Applications Project

Version 1.2

This is the VM for the Open Web Application Security Project (OWASP) Broken Web Applications project. It contains many, very vulnerable web applications, which are listed below. More information about this project can be found in the project User Guide and Home Page.

For details about the known vulnerabilities in these applications, see https://sourceforge.net/p/owaspbwa/tickets/?limit=999&sort=_severity+asc.

!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!

TRAINING APPLICATIONS

OWASP WebGoat	OWASP WebGoat.NET
OWASP ESAPI Java SwingSet Interactive	OWASP Mutillidae II
OWASP RailsGoat	OWASP Bricks
OWASP Security Shepherd	Ghost
Magical Code Injection Rainbow	bWAPP
Damn Vulnerable Web Application	

Web Security Academy

https://portswigger.net/web-security/all-labs

Products | Solutions | Research | Academy | Supp

Dashboard | Learning paths | Latest topics | All content | Hall of Fame | Get started | Get certified

Back to all topics

- SQL injection
- Cross-site scripting
- Cross-site request forgery (CSRF)
- Clickjacking
- DOM-based vulnerabilities
- Cross-origin resource sharing (CORS)
- XML external entity (XXE) injection
- Server-side request forgery (SSRF)
- HTTP request smuggling
- OS command injection
- Server-side template injection
- Path traversal
- Access control vulnerabilities
- Authentication
- WebSockets
- Web cache poisoning

Web Security Academy > All labs

All labs

Mystery lab challenge

Try solving a random lab with the title and description hidden. As you'll have no prior knowledge of the type of vulnerability that you need to find and exploit, this is great for practicing recon and analysis.

Take me to the mystery lab challenge →

SQL injection

LAB APPRENTICE SQL injection vulnerability in WHERE clause allowing retrieval of hidden data →

LAB APPRENTICE SQL injection vulnerability allowing login bypass →

Phần mềm máy ảo

QEMU

Xen Project

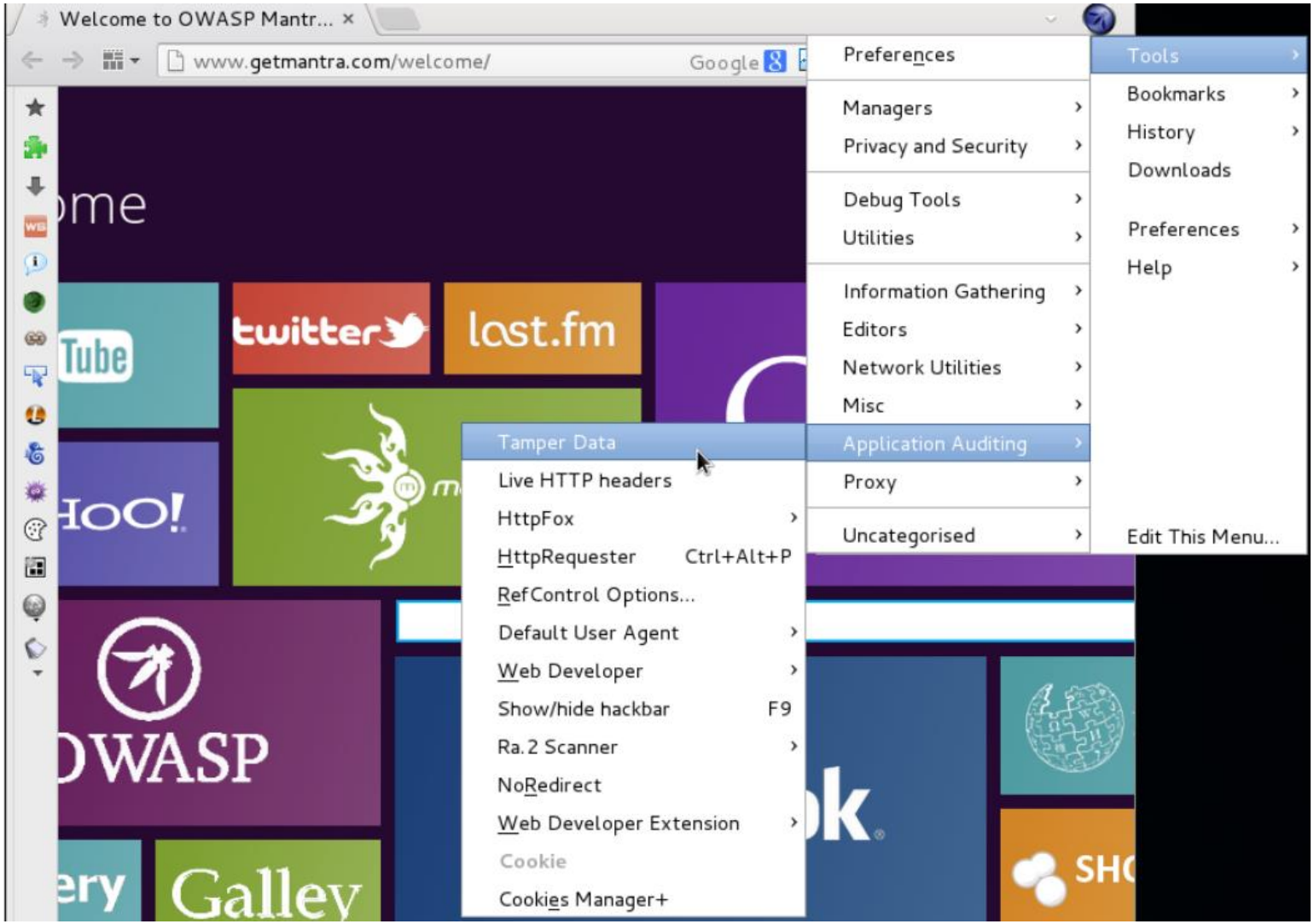
KVM

Trình duyệt

Hỗ trợ trên các trình duyệt

Function	Google Chrome	Mozilla Firefox	Edge/IE	Safari
Switching User Agents	✓	✓	✓	✓
Edit and Replay Requests	✗	✓	✗	✗
Editing Cookies	✓	✓	✓	✗
Editing Local Storage	✓	✓	✓	✗
Disable CSS	✓	✓	✓	✓
Disable Javascript	✓	✓	✗	✓
View Headers	✓	✓	✓	✓
Native screen-shot capture	✓	✓	✓	✗
Offline mode	✓	✓	✗	✗
Encode and Decode	✓	✓	✓	✓

Công cụ trên **OWASP Mantra**



Trình duyệt khác

- **Mantra** on Chromium (MoC): chỉ trên windows
- **Firefox** hoặc **Iceweasel** và add-on:
  - Tamper Data: bắt request, thay đổi data trước khi gửi
  - Cookies Manager+: xem và chỉnh sửa cookie
  - Firebug: in-line debugger
  - Hackbar: thay đổi input không cần thay đổi URL
  - HTTP Requester: thay đổi HTTP Request (GET, POST, PUT) và xem trả lời dạng raw
  - Passive Recon: lấy thông tin public: DNS query, Whois

Add-on hữu ích khác

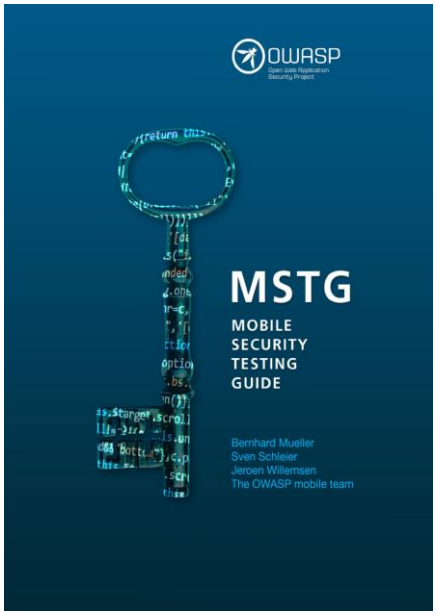
- XSS Me
- SQL Inject Me
- FoxyProxy
- iMacros
- FirePHP
- RESTClient
- Wappalyzer

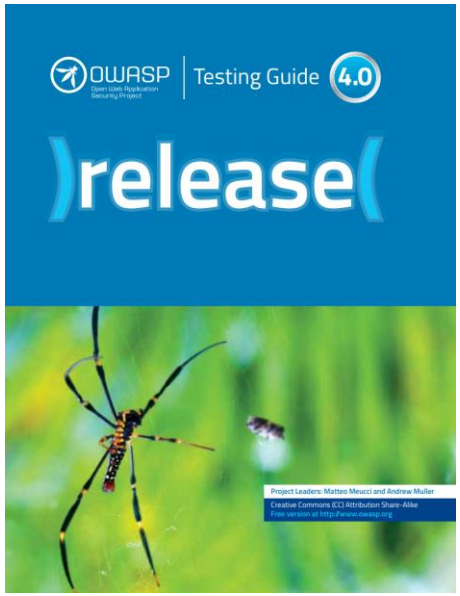
Tài liệu tham khảo

- Gilberto Najera-Gutierrez, **Kali Linux Web Penetration Testing Cookbook-Packt Publishing**, 2016
- Joseph Muniz - Aamir Lakhani, **Web Penetration Testing with Kali Linux**, 2013
- OWASP, **OWASP Web Application Security Quick Reference Guide 0.2**, 2013
- OWASP, **Mobile App Security Checklist 0.9.2**, 2017
- DarkWeb Links: https://darkweblinks.org/

Tài liệu tham khảo

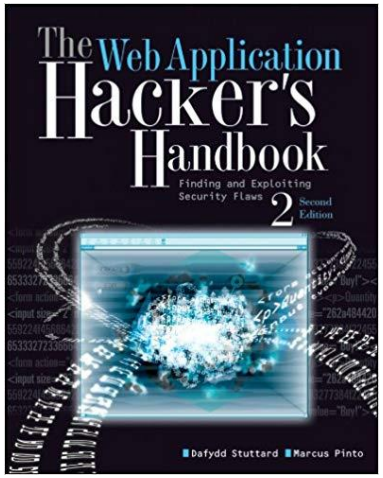
- OWASP, **OWASP Testing Guide** v4.0, 2014.
- OWASP Testing Guide v5 (2019).
  Link: https://github.com/OWASP/OWASP-Testing-Guide-v5
- OWASP Mobile Security Testing Guide - 1.1.3 Release.
  Link: https://github.com/OWASP/owasp-mstg

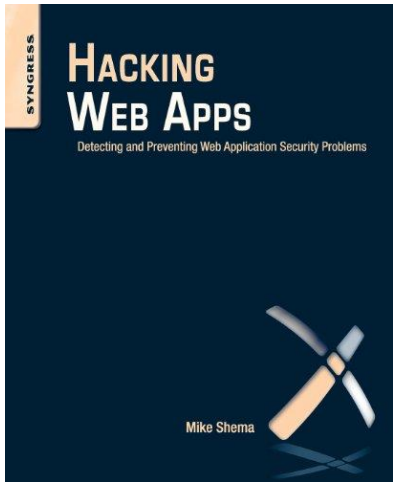




Tài liệu tham khảo

- **The Tangled Web: A Guide to Securing Modern Web Applications**. Michal Zalewski. No Start Press.
- **The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws**. Dafydd Stuttard. 2011.
- **Hacking Web Apps: Detecting and Preventing Web Application Security Problems**. Mike Shema. 2012

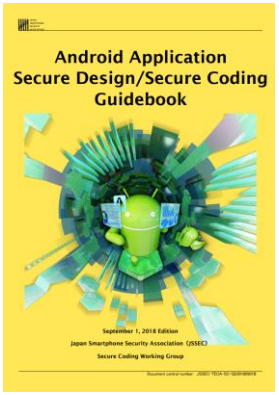


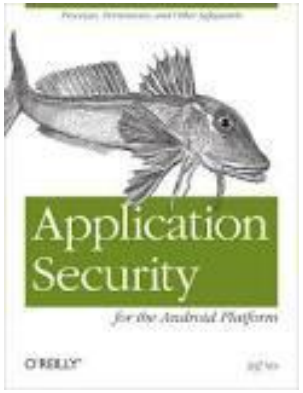


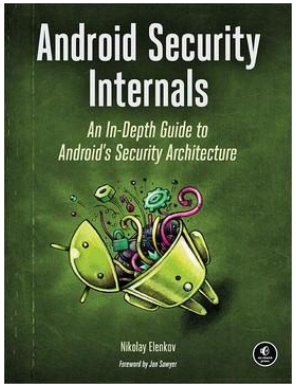
Tài liệu tham khảo

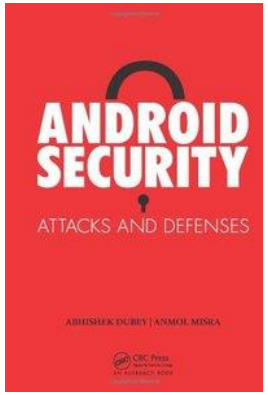
- **Application Security for the Android Platform: Processes, Permissions, and Other**. Jeff Six. 2011
- **ANDROID SECURITY: ATTACKS AND DEFENSES**. Abhishek Dubey, Anmol. 2013.
- **Android Security Internals : An In-Depth Guide to Android's Security Architecture**. Nikolay Elenkov. No Starch Press. 2015.
- **Android Application Secure Design/Secure Coding Guidebook**, 2018. Japan Smartphone Security Association (JSSEC)
- **iOS Application Security: The Definitive Guide for Hackers and Developers** 1st Edition. David Thiel. No Start Press. 2016.
- Mobile Security testing guide:

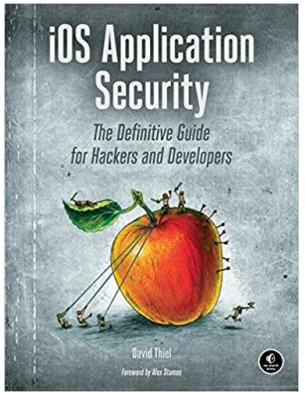
  Link: https://mobile-security.gitbook.io/mobile-security-testing-guide/











Bảo mật web và ứng dụng

Trường ĐH CNTT – ĐHQG
TP. HCM