



ZDResearch

# ZDResearch

Advanced Web Hacking



Taught by some of the world's most reputable hackers and security experts, active in different criterias; this course brings together up-to-date practical hacking content that can not be learned anywhere else.



Our hands-on labs provide real-life scenarios for students to familiarize themselves with A-Z hacking concepts and practices, and combines incremental levels of content and rigor.

⊕ Course Outline

<https://training.zdresearch.com>



## 1- Web Application Architecture

### 1.1 URL

### 1.2 HTTP

#### 1.2.1 HTTP Syntax

#### 1.2.2 HTTP Requests

#### 1.2.3 HTTP Response

#### 1.2.4 HTTP Status Codes

#### 1.2.5 HTTP and Cookies

#### 1.2.6 HTTP and Authentication

### 1.3 Web Programming

#### 1.3.1 Server Side Programming

#### 1.3.2 Client Side Programming

### 1.4 Server Side Programming

#### 1.4.1 PHP

#### 1.4.2 ASP

#### 1.4.3 .Net

#### 1.4.4 Python

#### 1.4.5 Ruby

#### 1.4.6 Java

### 1.5 Client Side Programming

#### 1.5.1 HTML

#### 1.5.2 XML

#### 1.5.3 CSS

#### 1.5.4 JavaScript





## 1.6 Welcome to Web2

1.6.1 DOM

1.6.2 Ajax

1.6.3 JSON

1.6.4 JSONP

1.6.5 HTML5

1.6.7 REST

## 1.7 Modern Web and policies

1.7.1 SOP

1.7.2 CSP

1.7.3 Browsers

## 2- OWASP TOP TEN 2013

### A1- SQL Injection World

Finding SQL Injection

Authentication Bypass using SQL Injection

Exploiting Error Based SQL Injection

Reading And Writing Files Using SQL Injection

System Take Over Using SQL Injection

Blind SQL Injection

Exploiting Blind SQL Injection

Using Automated Tools

**Hands-On-Lab**



## A2- Session Management

Session Authenticating Flaws

Session Fixation Flaws

Predictable Session Flaws

**Hands-On-Lab**

## A3- Cross Site Scripting

Reflected XSS

Stored (Persistence) XSS

DOM based XSS

XSS Worms

**Hands-On-Lab**

## A4- Insecure Direct Object Reference

Finding and Exploiting Direct Object References

**Hands-On-Lab**

## A5-Security Misconfiguration

Understanding And Abusing Mis-configurations

**Hands-On-Lab**

## A6-Sensitive Data Exposure

Understanding and Abusing Data Leakage

Error Handling Mechanism Bypassing

**Hands-On-Lab**





## A7-Missing Function Level Access Control

Understanding Authorization

ACL Exploitation

RBAC Exploitation

**Hands-On-Lab**

## A8-Cross-Site Request Forgery (CSRF)

What is CSRF

Basic CSRF Exploitation

Advanced CSRF Attacks

CSRF Worms

CSRF Defense Bypass

**Hands-On-Lab**

## A9-Using Components with Known Vulnerabilities

Old Component Attack

**Hands-On-Lab**

## A10-Unvalidated Redirects and Forwards

Abusing Open Redirects

**Hands-On-Lab**



### 3- More Advanced Attacks

#### 3.1 Command Injections

##### 3.1.1 Finding And Exploiting Command Injections

##### 3.1.2 RCE Using Insecure File Extensions

#### 3.2 File Inclusion Attacks

##### 3.2.1 LFI, LFD, RFI

##### 3.2.2 Finding And Exploiting File Inclusions

##### 3.2.3 Converting LFI to RCE

##### 3.2.4 Hands-On-Lab

### 4- Web Services Attacks

#### 4.1.2 Understanding SOAP and Web Services

#### 4.1.3 Attacking Restful APIs

#### 4.1.4 Attacking SOAP Based Applications

#### 4.1.5 Web Service Security Countermeasures

#### 4.1.6 Hands-On-Lab

### 5- Cryptographic Attacks on the Web

#### 5.1.1 Understanding Cryptography

#### 5.1.2 Weak Cipher Attacks

#### 5.1.3 Weak Hashing Attacks

#### 5.1.4 Padding Oracle Attacks

#### 5.1.5 EBC Attacks





5.1.6 MITM Attacks

5.1.7 XOR based Attacks

5.1.8 Signature and MAC Attacks

5.1.9 Randomness Attacks

5.1.10 Hands-On-Lab

## 6- XML based Attacks

6.1.1 XML Injection

6.1.2 XML Entity Injection

6.1.3 Hands-On-Lab

## 7- XPath based Attacks

7.1.1 XPath Injection

7.1.2 Error based Attacks

7.1.3 Blind based attacks

7.1.4 Hands-On-Lab

## 8- Flash Security

8.1.1 Flash Security Configurations

8.1.2 Flash Based XSS

8.1.3 Flash Restriction Bypass

8.1.4 Hands-On-Lab



## 9- HTML5 Security

- 9.1.1 Introduction To HTML5 Security
- 9.1.2 HTML5 Security Headers
- 9.1.3 CORS
- 9.1.4 HTML5 and XSS
- 9.1.5 Local Storage vs. Session Storage
- 9.1.6 WebSockets Security
- 9.1.7 Hands-On-Lab

## 10- More HTTP Attacks

- 10.1.1 HTTP Verp Tampering
- 10.1.2 HTTP Response Splitting
- 10.1.3 Hands-On-Lab

## 11- Web Application Firewalls

- 11.1.1 Introduction To WAFs
- 11.1.2 Practical WAF Attacks
- 11.1.3 Hands-On-Lab

## 12- Source Code Auditing

- 12.1.1 Introduction To Code Auditing
- 12.1.2 Code Audit Methodology
- 12.1.3 Know your target language
- 12.1.4 Tracking Of User Input
- 12.1.5 Finding Exploitable Issues





12.1.6 Auditing OOP Code

12.1.7 Hands-On-Lab

## 13 Capture The Flag

13.1 Real-life lab and final exam

ZDResearch





# ZDResearch

----- Custom Research

----- Penetration Testing

----- Advanced training

----- Binary/Web Analysis (PoC/Exploits)

----- Advanced Web Hacking

<https://training.zdresearch.com>

<https://zdresearch.com>