

# Certified Ethical Hacker, Part 6 of 8: Web Apps and SQL Injection

page 1

**Meet the expert:** Rafiq Wayani has extensive experience including more than 20 years in IT as Systems Architect, Software Engineer, DBA, and Project Manager. Wayani has instructed in a variety of technical areas, has designed and implemented network and information systems, and is certified across a wide range of platforms and systems including Microsoft Solutions Developer, Systems Engineer, Application Developer, Database Administrator, Trainer; Novell Netware Administrator and Engineer; Master Certified Netware Engineer; and A Certified.

**Prerequisites:** To get the most out of this course, this course assumes that you have a good working knowledge of Linux and Windows based networking environments. It also assumes that you have experience with managing a network, have worked with networking hardware such as switches & routers, are familiar with MS Active Directory (AD) Domain based authentication, know how to work with command-line utilities, and understand the basics of Web Server environments. Many of the demonstrations in this course use the Windows 7 and Kali Linux operating systems which can be downloaded free from the respective sites. All of the demonstrations are created in a virtual environment using Oracle VirtualBox and VMware vSphere 6.

**Runtime:** 01:43:51

**Course description:** In the ongoing war between white hat and black hat hackers, web applications are a longstanding yet continually evolving battleground. Rafiq Wayani examines the new weaponry both sides are bringing to the fight and takes a thorough look at one of the most widely used attack vectors, SQL injection. This course is part of a series covering EC-Council's Certified Ethical Hacker (CEH).

## Course outline:

### Web Application Concepts

- Introduction
- Most Exposed & Least Protected
- Exposure & Protection Cont.
- Summary

### Web Application Threats

- Introduction
- Web Application Threats
- Application Replays Script
- Email Vector
- Decoded Attack Sequence
- Verbose and Blind
- SQL Injection
- Database Driven Page
- Piggybacking with UNION
- Enumerate All Tables
- Subquery Enumerates Columns
- Select Data from the Column
- Summary

### Web App Hacking Methodology

- Introduction
- Web App Hacking Methodology
- Demo: Netsparker
- Web App Hacking Methodology
- Summary

### Web Application Hacking Tools

- Introduction

- Web Application Hacking Tools
- More Hacking Tools
- Summary

### Web App Countermeasures

- Introduction
- Countermeasures
- How to Protect Yourself
- Summary

### Web App Security Tools

- Introduction
- Demo: Kali, Nmap, & Nessus
- Demo: Openwall, pof, & WireShark
- Demo: Netcraft, Yersinia, & PuTTY
- Demo: Cain & Abel and Kismet
- Demo: hping and Secapps
- Summary

### Web Application Pen Testing

- Introduction
- Demo: Veracode
- Demo: Shodan and Arachni
- Demo: Aircrack-ng, AppScan, & Nikto
- Demo: WebScarab, Paterva, & Ironwasp
- Demo: Metasploit & WireShark
- Demo: w3af, Impact Pro, and Kali
- Demo: Netsparker, Nessus & Portswigger
- Demo: Zed Attack & Acunetix
- Demo: BeyondTrust, SQLNinja, & BeEF

- Demo: Dradis & Ettercap
- Summary

### SQL Injection Concepts

- Introduction
- SQL Injection (SQLi)
- How Does SQLi Work?
- Summary

### SQL Injection Types

- Introduction
- Types of SQLi
- How Does SQLi Work?
- Summary

### SQLi Attack Methodology

- Introduction
- Application Security Risks
- OWASP Top 10
- Summary

### SQLi Tools

- Introduction
- SQLi Tools
- Demo: sqlmap
- Demo: SQL Ninja
- Demo: safe3
- Summary

### SQLi Evasion Techniques

- Introduction
- SQLi Evasion Techniques
- SQLi Evasion Techniques Cont.
- Summary

### SQLi Countermeasures

- Introduction

- SQLi Countermeasures
- Demo: Web Application Firewall
- SQLi Countermeasures
- Summary