Web Hacking Black Belt Edition Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Web Hacking Black Belt Edition is an advanced application security course focused on identifying and testing vulnerabilities in modern web applications, APIs, and related endpoints.

The course concentrates on specific areas of application security, advanced vulnerability discovery, and exploitation techniques. Participants will examine security issues that have affected real-world products, appeared in bug bounty programs, and are often missed by modern automated scanners.

The training includes a wide range of current and unconventional web security scenarios. Participants also benefit from access to a state-of-the-art Hacklab throughout the course, allowing the concepts to be reinforced through practical exercises.

Key topics include modern JWT, SAML, and OAuth weaknesses, core business logic issues, cryptographic flaws, RCE scenarios involving serialization and template injection, exploitation over DNS channels, advanced SSRF, HPP, XXE, and SQL Injection topics, serverless security issues, web caching vulnerabilities, and attack chaining based on real-world examples.

Participants are encouraged to become familiar with Burp Suite before attending in order to gain maximum value from the course.

Who Should Attend

This course is designed for:

- Web developers
- Intermediate-level penetration testers
- DevOps engineers
- Network engineers
- Security researchers and analysts
- Security architects
- Security professionals and enthusiasts
- Anyone looking to take their web security skills to a more advanced level

Web Hacking Black Belt Edition Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of the course, participants should be able to:

- Apply security testing techniques to identify and safely validate complex web vulnerabilities that may be missed by scanners and other automated tools.
- Shape testing around real-world attacker behaviour and commonly used tooling so that assessments remain relevant to the threats facing an organisation.
- Adapt offensive security tools to create more tailored testing approaches rather than relying only on standard payloads.
- Recommend controls and corrective actions that reduce the conditions in which vulnerabilities may emerge.
- Understand the potential business impact of web vulnerabilities and communicate that impact to relevant stakeholders.
- Take greater responsibility within security teams and support stronger security awareness across the wider organisation.

Training Outline

Course Structure

The course content is built around carefully selected advanced topics from the current web hacking landscape.

Participants are provided with a customised Kali image containing a range of tools and plugins designed to support the analysis and testing of the vulnerabilities discussed during the course.

The training is delivered by an experienced penetration tester. Real-world stories and case studies help place the technical content into context, while access to a hacking lab, scripts, tools, and student handouts supports the practical learning process.

Detailed answer sheets are also provided at the end of the course, offering step-by-step walkthroughs for the exercises completed during the training.

Lab Setup and Architecture Overview

- Introduction to the lab environment
- Overview of the training architecture

Introduction to Burp Features

- Key Burp Suite capabilities used throughout the course

Attacking Authentication and SSO

- Token hijacking attacks
- Logical bypass and boundary conditions

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Bypassing two-factor authentication
- Authentication bypass through subdomain takeover
- JWT/JWS token attacks
- SAML authorization bypass
- OAuth issues

Password Reset Attacks

- Session poisoning
- Host Header validation bypass
- Case studies involving common password reset failures

Business Logic and Authorization Flaws

- Mass Assignment
- Invite and Promo Code bypass
- Replay Attack
- API Authorization bypass
- HTTP Parameter Pollution (HPP)

XML External Entity (XXE)

- XXE fundamentals
- Advanced XXE exploitation through OOB channels
- XXE through SAML
- XXE in file parsing

Breaking Crypto

- Known Plaintext Attack
- Faulty password reset scenarios
- Padding Oracle Attack
- Hash length extension attacks
- Authentication bypass using .NET Machine Key
- Padding oracle scenarios involving fixed IVs

Remote Code Execution (RCE)

- Java Serialization
- .NET Serialization
- PHP Serialization
- Python Serialization
- Server-Side Template Injection
- Code injection over OOB channels

SQL Injection Masterclass

- Second-order injection
- Out-of-Band exploitation
- SQL Injection through cryptographic workflows
- OS code execution through PowerShell
- Advanced SQL Injection topics
- Advanced SQLMap usage and WAF bypass

BILGINÇ IT Academy

info@bilginc.com

bilginc.com

- Penetration testing GraphQL

Tricky File Upload

- Malicious file extensions
- Circumventing file validation checks
- Testing hardened web servers
- SQL Injection through file metadata

Server-Side Request Forgery (SSRF)

- SSRF against internal network resources
- SSRF involving templates and extensions
- SSRF filter bypass techniques
- Case studies

Attacking the Cloud

- SSRF exploitation
- Serverless exploitation
- Google Dorking in the cloud era
- Cognito misconfiguration and data exfiltration
- Post-exploitation techniques for cloud-hosted applications
- Case studies

Attacking Hardened CMS Platforms

- Identifying and assessing different CMS platforms
- Hardened WordPress, Joomla, and SharePoint environments

Web Caching Attacks

- Security weaknesses associated with web caching

Miscellaneous Vulnerabilities

- Unicode normalization attacks
- Second-order IDOR
- Misconfigured code control systems
- HTTP Desync attacks

Attack Chaining

- Multi-stage vulnerability chaining
- N-tier vulnerability chaining
- Attack sequences that may lead to RCE

Case Studies

- Real-world web security examples
- Unusual XSS and CSRF scenarios

B33r-101

BILGINÇ IT Academy

info@bilginc.com

bilginc.com

- Dedicated course section

Exams and Assessments

This course includes a formal examination as part of the programme.

The exam is provided by NotSoSecure and is included in the course fee. Details such as the assessment format, duration, number of questions, and passing score will be confirmed by the QA account manager or instructor before the exam.