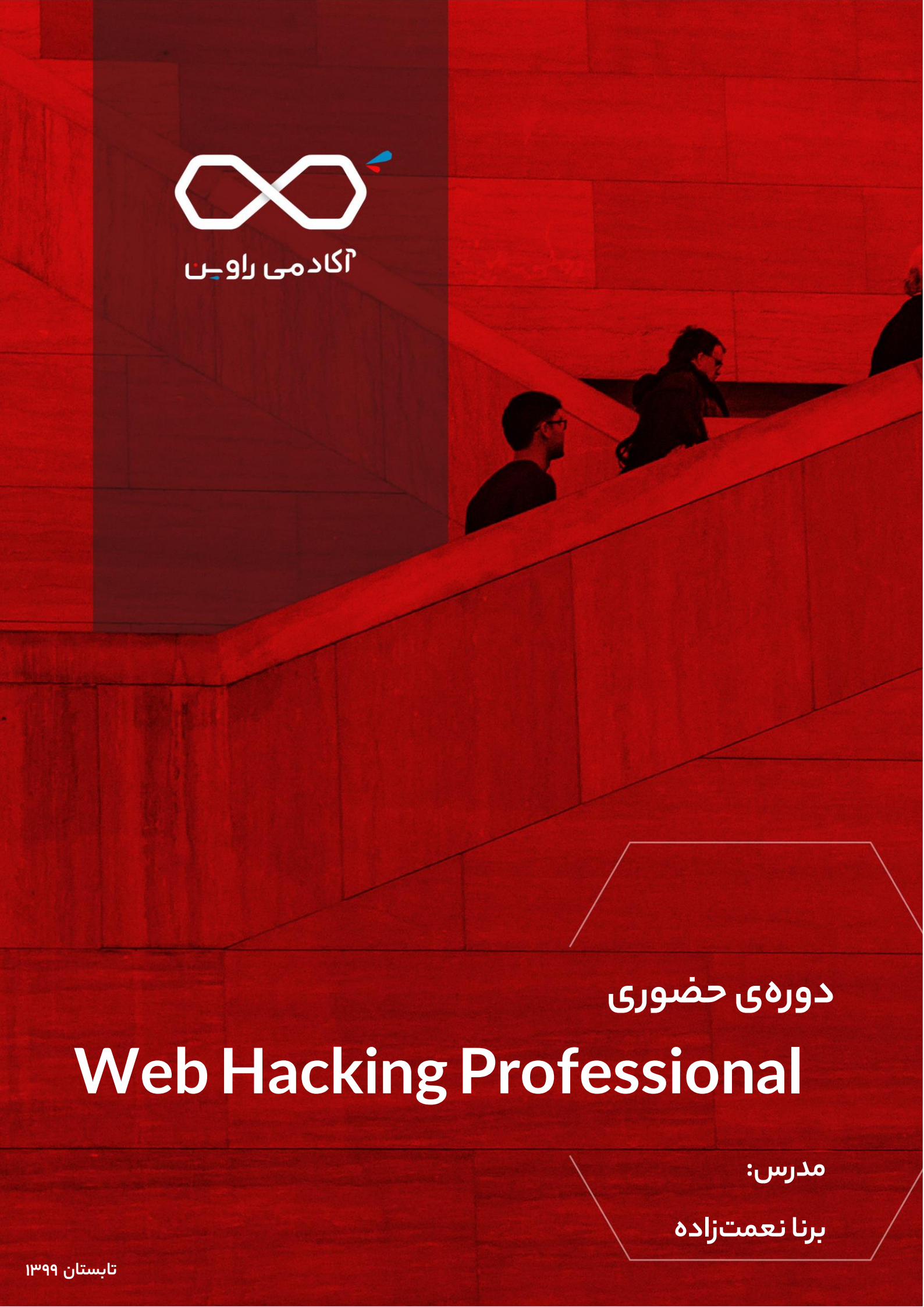

دوره‌ی حضوری

Web Hacking Professional

مدرس:

برنا نعمت‌زاده

تابستان ۱۳۹۹

به‌نام خدا

درباره‌ی این دوره

سال‌هاست که بهره‌برداری از سرویس‌های تحت وب آسیب‌پذیر، یکی از جذاب‌ترین روش‌های موجود بین مهاجمین سایبری برای نفوذ به زیرساخت سازمان‌ها یا ایجاد اختلال در کسب‌وکار آن‌ها است. همین نکته سبب شده است تا ارزیابی امنیت سرویس‌های تحت وب یکی از مهم‌ترین اجزای ارزیابی امنیت و در بسیاری از موارد، پرکاربردترین نوع ارزیابی امنیت باشد که سازمان‌ها به آن اقبال ویژه‌ای داشته و به شکل‌های مختلف مانند پروژه‌های تست نفوذ، باگ‌بانتی، خدمات تیم قرمز و غیره از آن بهره می‌برند. با توجه به اهمیت این موضوع، موسسه‌های آموزشی مختلف در سراسر دنیا با ارایه‌ی دوره‌های آموزشی متنوع، به آموزش متخصصین امنیت وب پرداخته‌اند. آکادمی راوین نیز همگام با آخرین دانش سایبری روز دنیا اقدام به طراحی مسیرهای آموزشی خود در زمینه‌های مختلف امنیت سایبری کرده است. یکی از این مسیرها، مسیر آموزش تخصصی «هک وب و موبایل» می‌باشد که در سه سطح پایه، پیشرفته و خبره طراحی و ارایه شده است.

در این دوره مراحل مختلف تست نفوذ وب بر اساس دانش و تکنیک‌های روز دنیا به صورت نظری و عملی در ۵ بخش زیر آموزش داده خواهد شد:

- **مروری بر مبانی تست نفوذ وب:** در این بخش به معرفی دوره و اهداف آن و همچنین بررسی مبانی تست نفوذ مانند متدلوژی‌ها، خروجی ارزیابی و غیره (به منظور یادآوری) پرداخته می‌شود.
- **مبانی سرویس‌های تحت وب:** این بخش به بررسی کامل پروتکل‌های HTTP و HTTPS، مکانیزم‌های مختلف احراز هویت، کنترل دسترسی و مدیریت Session در وب می‌پردازد. همچنین در این بخش، آماده‌سازی زیرساخت و محیط کاری برای اجرای تست نفوذ را خواهید آموخت.
- **شناسایی:** روش‌های مختلف جمع‌آوری اطلاعات و شناسایی کامل سرویس‌های تحت ارزیابی را به همراه آموزش شیوه‌ی برنامه‌ریزی کردن برای شروع حمله، شامل می‌شود.
- **جستجوی آسیب‌پذیری‌ها و بهره‌برداری از آن‌ها:** در این بخش شیوه‌ی شناسایی انواع آسیب‌پذیری‌های منطقی و فنی بر اساس تکنیک‌های روز دنیا به صورت عملی آموزش داده می‌شود.
- **گزارش‌نویسی:** در پایان، فرآیند ارزیابی را به همراه نتایج به دست آمده در سطوح مدیریتی و فنی مستندسازی خواهیم کرد.

از ویژگی‌های خاص این دوره می‌توان به فرآیند محور بودن (فرآیند ارزیابی را به طور کامل پوشش می‌دهد)، آموزش عملی و بهره‌برداری از دانش روز در زمینه‌ی حملات تحت وب اشاره کرد.

مدت زمان دوره

مدت زمان این دوره ۴۵ ساعت است و به صورت کلاس‌های ۳ ساعته، در طی ۱۵ جلسه به صورت حضوری از ساعت ۱۷ تا ۲۰ روزهای زوج برگزار می‌شود. آغاز جلسات این دوره از روز دوشنبه مورخ ۹۹/۰۵/۲۰ خواهد بود.

این دوره به چه افرادی توصیه می‌شود؟

- کارشناسان ارزیابی امنیت/تست نفوذ/تیم قرمز
- متخصصین فعال در زمینه‌ی Bug Bounty
- مشاورین امنیت سایبری
- کارشناسان خبره‌ی امنیت سایبری در SOC

برای حضور در این دوره چه دانش‌هایی باید داشته باشم؟

از آن‌جایی که این دوره در سطح پیشرفته برگزار می‌شود، مباحث پایه‌ای تست نفوذ وب در آن مطرح نخواهد شد. بنابر این توصیه می‌شود تا شرکت‌کنندگان قبل از حضور در این دوره، حداقل یک دوره‌ی پایه در زمینه‌های مرتبط (مانند دوره‌ی پایه‌ی «هک وب و موبایل» یا دوره‌ی «مبانی هک کلاه‌سفید» در آکادمی راوین) را گذرانده باشند. مهم‌ترین پیش‌نیازهای دانشی و تجربی برای حضور در این دوره به شرح زیر است:

- آشنایی با مفاهیم امنیت وب
- آشنایی ابتدایی با پروتکل‌های مرتبط (مانند HTTP، HTTPS و SSL/TLS)
- آشنایی با انواع حملات سایبری متداول در زمینه‌ی وب
- حداقل یک سال تجربه کاری در زمینه‌ی امنیت سایبری و تست نفوذ

برای ثبت‌نام در این دوره می‌توانید از اینجا اقدام کنید.

آکادمی راوین

سرفصل‌های این دوره

Chapter 1: Introduction to Web Penetration Testing

1.1 Web Penetration Testing Overview

1.1.1 Course Overview

1.1.2 Goals & Scope

1.1.3 Deliverables

1.2 Web Penetration Testing Methodology

1.2.1 OWASP

Chapter 2: Web Application Fundamentals

2.1 Infrastructure of a Web application

2.2 HTTP Request/Response Components

2.3 Core Mechanisms

2.3.1 Authentication

2.3.2 Session Management

2.3.3 Authorization

2.4 Environment Setup for Hacker

Chapter 3: Reconnaissance

3.1 Reconnaissance Goals

3.2 Types of Reconnaissance

3.2.1 External Recon

3.2.1.1 Gathering Initial Information

3.2.1.2 Subdomain Enumeration Techniques

3.2.1.3 Search Engines for Hacker

3.2.1.4 Google Hacking

3.2.1.5 Shodan

4.4 Cross-Site Request Forgery

- 4.4.1 CSRF Overview
- 4.4.2 Identifying Attack Surfaces for CSRF
- 4.4.3 CSRF Exploitation
- 4.4.4 Exploiting CSRF without Anti-CSRF Token
  - 4.4.4.1 Exploiting via Force Browsing
  - 4.4.4.2 Exploiting via Request Methods
  - 4.4.4.3 Exploiting in JSON Contexts
- 4.4.5 Exploiting CSRF with Anti-CSRF Token
  - 4.4.5.1 Weak Randomness
  - 4.4.5.2 Analyzing via Burp Sequencer
  - 4.4.5.3 Identifying Static Parts and Dynamic Parts of Token
  - 4.4.5.4 Exploiting Weak Randomness
  - 4.4.5.5 Bypassing Anti-CSRF Token via XSS
  - 4.4.5.6 Bypassing Anti-CSRF Token via CORS Exploitation

4.5 Server-Side Request Forgery

- 4.5.1 SSRF Overview
- 4.5.2 Identifying Attack Surfaces for SSRF
- 4.5.3 SSRF Types
  - 4.5.3.1 In-Band
  - 4.5.3.2 Out-of-Band

4.6 File & Resource Attacks

- 4.6.1 LFI & RFI Attacks
  - 4.6.1.1 Identifying Attack Surfaces for File Inclusion Attacks
  - 4.6.1.2 LFI and RFI Exploitation
  - 4.6.1.3 LFI to RCE
- 4.6.2 File Upload Attacks
  - 4.6.2.1 File Upload Functionality Overview
  - 4.6.2.2 File Upload Attacks

آکادمی راوین

4.7 Core Mechanisms Attacks

4.7.1 Authentication Attacks

4.7.1.1 Authentication Components overview

4.7.1.2 Attacking Authentication Components

4.7.1.3 Attacking 2FA

4.7.1.4 Attacking Multi–Factor Authentications

4.7.2 Session Management Attacks

4.7.2.1 Session Hijacking

4.7.2.2 Session Hijacking via XSS

4.7.2.3 Session Hijacking via Packet Sniffing

4.7.2.4 Session Fixation

4.7.2.5 Session Overloading

4.8 CMS–Based Attacks

4.8.1 WordPress

4.8.2 Joomla

Chapter 5: Finding Logical Vulnerabilities

5.1 Introduction to Logical Vulnerabilities

5.2 Attacking Access Control Mechanism

5.2.1 Vertical Access Control Issues

5.2.2 Horizontal Access Control Issues

5.2.3 Insecure Direct Object Reference

5.2.4 Attacking Multi–Step Functionalities

5.3 Attacking Application's Flow

5.4 Race Condition

Chapter 6: Reporting

آکادمی راوین

درباره‌ی آکادمی راوین

شاید اغراق نباشد اگر بگوییم این روزها بزرگ‌ترین چالش پیش روی سازمان‌ها، شرکت‌ها و استارتاپ‌های فعال در صنعت فناوری اطلاعات، کمبود نیروی انسانی متخصص در کشور است. در حالی‌که تعداد افراد جویای کار هر روز بیشتر می‌شود، کماکان اغلب شرکت‌ها در تامین نیروی متخصص مورد نیاز خود با مشکلات جدی مواجه هستند.

با توجه به چالش‌های موجود در کشور، تصمیم گرفتیم تا با تاسیس «آکادمی راوین» قدمی در راستای هرچه کوچک‌تر کردن شکاف تخصصی موجود بین افراد جویای کار و نیاز شرکت‌های فعال در صنعت فناوری اطلاعات کشور برداریم. بر همین اساس، تمام دوره‌های آموزشی این موسسه مبتنی بر مسیرهای شغلی (Career Path) و به صورت تخصصی در زمینه‌ی امنیت سایبری طراحی و تدوین شده است. همچنین «آکادمی راوین» دو مسیر اصلی را برای تمام دوره‌های خود در نظر گرفته، به‌گونه‌ای که هر دوره‌ی آموزشی در یکی از این دو مسیر قرار می‌گیرد:

۱. مسیر «امنیت دفاعی» که با رنگ آبی مشخص شده است. دوره‌های آموزشی این مسیر، با هدف امن‌سازی زیرساخت‌ها و نرم‌افزارهای سازمان‌ها به منظور پیش‌گیری از نفوذ یا شناسایی و ردیابی نفوذگران طراحی شده است. همچنین این دوره‌ها شامل تحلیل روش‌ها و بدافزارهای مورد استفاده مهاجمین نیز می‌شود.
۲. مسیر «امنیت تهاجمی» که با رنگ قرمز مشخص شده است. هدف از این دوره‌های آموزشی، ارزیابی امنیتی زیرساخت‌های شبکه، نرم‌افزارهای وب، موبایل و غیره می‌باشد. به عبارت دیگر متخصصان این حوزه با شبیه‌سازی رفتار نفوذگران، نقاط ضعف و آسیب‌پذیری‌های امنیتی موجود را قبل از آن‌ها شناسایی می‌کنند.

تمام دوره‌های این موسسه در هر دو مسیر «آبی» و «قرمز»، بر اساس آخرین دانش روز دنیا و هم سطح دوره‌های ارایه شده در موسسات بزرگ بین‌المللی طراحی شده است و توسط به‌نام‌ترین مدرسین ایرانی و غیر ایرانی تدریس می‌شود. آخرین دوره‌های ارایه شده در آکادمی راوین را می‌توانید در صفحه‌ی دوره‌های آموزشی در وب‌سایت این موسسه دنبال کنید.

سهروردی شمالی، بین هویزه و خرمشهر، کوچه‌ی نقدی، پلاک ۳۶، واحد سوم
info@ravinacademy.com

با ما در ارتباط باشید

https://twitter.com/ravinacademy

https://linkedin.com/company/ravin-academy/about

https://t.me/ravinacademy

info@ravinacademy.com

سهروردی شمالی، بین هویزه و خرمشهر، کوچه‌ی نقدی، پلاک ۳۶، واحد سوم

۰۲۱-۸۸۵۰۲۴۴۲