مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ - ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

دوره جامع مهندسی امنیت وب | Bug Bounties

شرح مختصر

Bug Bounties

مروری بر دوره

مروری بر دوره

همانطوری که می دانید امروزه اکثر کسب و کارها برروی بستر وب می باشند و وب سایت های زیادی در دنیای امروز وجود دارند که براساس تکنولوژی های وب طراحی می شوند ولی نکته ایی که وجود دارد این است که اکثر این وب سایت فاقد امنیت لازم می باشند از این رو این وب سایت ها مورد توجه هکرها می باشند بنابراین امنیت و تست نفوذ این سایت ها اهمیت زیادی دارند امروزه بسترهایی مانند Bug Bounty در دنیا وجود دارد که در این بستر هکرها می توانند به صورت قانونی باگ وب سایت های شرکت های معروف را پیدا کرده و آنها را به آن شرکت ها گزارش دهند و در قبال آن پاداش دریافت کنند و از آنجایی که این پاداش ها به صورت دلاری می باشد لذا این کسب درآمد در زمینه هک می تواند یک بازار خوب برای متخصصین حوزه امنیت به حساب آید لذا این دوره را به صورتی طراحی کردیم تا شما را برای رسیدن به این تخصص آماده کنیم.

آنچه در این دوره خواهید آموخت

آنچه خواهید آموخت

- آشنایی با مفاهیم اولیه وب
- آشنایی با Information Gathering
- آشنایی با حملات XSS
- آشنایی با حملات SQL Injection
- آشنایی با حملات SSRF
- آشنایی با حملات CSRF

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ - ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- آشنایی با حملات HTML Injection
- آشنایی با حملات Code Injection
- آشنایی با روش های Bypass کردن فیلترینگ های سایت
- ....

سرفصل ها (حضوری)

سرفصل ها

Prerequisites-SQL

Lesson ۱: Introduction to SQL

Lesson ۲: Retrieving Data

Lesson ۳: Updating Data

Lesson ۴: Inserting Data

Lesson ۵: Deleting Data

Lesson ۶: Sorting and Filtering Data

Lesson ۷: Advanced Filtering

Lesson ۸: Summarizing Data

Lesson ۹: Grouping Data

Lesson ۱۰: Using Subqueries

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ - ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Lesson ۱۱: Joining Tables

Lesson ۱۲: Managing Tables

Lesson ۱۳: Using Views

Lesson ۱۴: Stored Procedures

Prerequisites-HTML

Lesson ۱: Introduction to HTML۵ and Web Design

Lesson ۲: How to Create a Simple Web Page

Lesson ۳: How to Format Your Text

Lesson ۴: Adding Web Links and Images

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Lesson ۵: Creating Tables

Lesson ۶: Forms

Lesson ۷: Adding Styles and Classes to Your Web Pages

Lesson ۸: Borders, Backgrounds, and Floating Divs

Lesson ۹: Building Web Page Layouts with CSS

Lesson ۱۰: HTML۵ – What Is It?

Lesson ۱۱: Adding Videos and Graphics with HTML۵

Lesson ۱۲: HTML۵ and CSS۳ – Fonts and Effects

Prerequisites-JavaScript

Variable Naming Rules and JavaScript Data Types

Expressions and Operators

Flow Control

Objects and Arrays

Defining Functions and Methods

Constructors and Inheritance

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ - ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Pattern Matching with Regular Expressions

JavaScript in Browsers

The Document Object Model (DOM)

How to Get Input and Output

Managing Web Page Styles using JavaScript and CSS

Handling Web Page Events

How to Script Tables

How to Script Forms

Introduction to Ajax

SANS SEC۵۴۲

- Overview of the web from a penetration tester's perspective
- Web application assessment methodologies
- The penetration tester's toolkit
- WHOIS and DNS reconnaissance
- Open source intelligence (OSINT)
- The HTTP protocol

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- Secure Sockets Layer (SSL) configurations and weaknesses
- Interception Proxies
- Proxying SSL through BurpSuite Pro and Zed Attack Proxy
- Heartbleed exploitation

- Target profiling
- Collecting server information
- Logging and Monitoring
- Learning tools to spider a website
- Analyzing website contents
- Brute forcing unlinked files and directories
- Fuzzing
- Web authentication mechanisms
- Username harvesting and password guessing
- Burp Intruder

- Session management and attacks
- Authentication and authorization bypass
- Mutillidae
- Command Injection
- Directory traversal
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- Insecure Deserialization

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- SQL injection
- Blind SQL injection
- Error-based SQL injection
- Exploiting SQL injection
- SQL injection tools: sqlmap

- XML External Entity (XXE)
- Cross-Site Scripting (XSS)
- Browser Exploitation Framework (BeEF)
- AJAX
- XML and JSON
- Document Object Model (DOM)
- API attacks
- Data attacks

- Cross-Site Request Forgery (CSRF)
- Python for web app penetration testing
- WPScan
- ExploitDB
- BurpSuite Pro scanner
- Metasploit
- When tools fail

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- Business of Penetration Testing:
    - Preparation
    - Methodology
    - Post Assessment and Reporting

SANS SEC۵۵۲

- Introduction and HTTP basics
    - Managing bug bounty programs
    - Bug hunting tips
    - HTTP review
- Understanding the app
    - Identifying app components
    - Translating business into HTTP requests
    - User profiles and mapping execution path
    - Tracing the data flow
    - Bug bounty case studies
    - Defense perspective
- Hunting for authentication and session flaws
    - Authentication and sessions
    - Parameter identification and session analysis
    - Authentication bypass
        - Parameter manipulation
        - Direct access
        - Bypass multi-factor authentication

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

    - Bug bounty case studies
    - Defense from authentication and session flaws
- Logic attacks and authorization bypass
    - Authorization and business rules
    - Breaking the business logic
    - Attack techniques:
        - Manipulating parameters
        - Reordering requests
    - Bug bounty case studies
    - Defending from logic attacks
- SQL injection
    - SQL attack techniques based on context
    - Boolean-based SQL injection
    - Time-based SQL injection
    - Bug bounty case studies
    - SQL injection defenses

Open redirect

- Open redirect basics
- Open redirect risk
- Bug bounty case studies

Server-side request forgery

- SSRF basics
- Discovering SSRF
- Bug bounty case studies

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- SSRF defenses

Cross-site request forgery

- CSRF basics
- Discovering CSRF
- Bug bounty case studies
- CSRF defenses

Cross-site scripting

- XSS basics: Reflected, stored, and DOM-based XSS
- Discovering XSS flaws
- Tracing the data flow and the context
- Bug bounty case studies: Tricky stored XSS
- Filtering detection and bypass
- Bug bounty case studies: Filter bypass
- XSS defenses: Input validation and output encoding

Client-Side code and APIs

- Client-side code analysis
- Finding the API URIs
- Attacking APIs
- Bug bounty case studies
- API defenses: Input validation and authorization

Combining web attacks

- Successful attack scenarios
- The art of combining web attacks
- Open redirect and SSRF
- Command Injection and CSRF
- Logic and XSS

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- Bug bounty case studies
- Reporting and responsible disclosure
- Evidence and proof-of-concept
- Responsible disclosure
- Future and practice

مخاطبان دوره

مخاطبان دوره

- علاقمندان به حوزه Bug Bounties و تست نفوذ وب و کارشناسان حوزه امنیت

پیش نیاز ها

پیش نیازها

- پیش نیاز های مورد نیاز در دوره تدریس می شود.