IT Professional Training Center

SEC642: Advanced Web App Penetration Testing, Ethical Techniques Hacking, and Exploitation

(دوره تست نفوذ پیشرفته وب)

خلاصه دوره: آیا وب اپلیکیشن های شما میتوانند در برابر هجوم تکنیک های پیشرفته حمله مقاومت کنند؟

وب اپلیکیشن های مدرن در حالی از تکنولوژی ها و عملیات های جدید پشتیبانی میکنند که هر روز به پیچیدگی آنها افزوده میشود. امروزه وب اپلیکیشن ها با سرعتی بالا در حال پیشرفت هستند. آیا شما برای تست نفوذ وب آماده هستید؟

در این دوره شما مهارت ها و تکنیک های پیشرفته که برای تست نفوذ وب اپلیکیشن های مدرن و تکنولوژی های جدید نیاز است را خواهید آموخت. در اینجا شما با تست ها عملی در دنیای واقعی مهارت خود را افرایش خواهید داد و به یک مختصص تست نفوذ وب تبدیل خواهید شد. در انتهای دوره یک مسابقه CTF (فتح پرچم) برگزار خواهد شد و شما از دانشی که در طول ۵ فصل این دوره یاد گرفتید برای پیروز شدن استفاده خواهید کرد.

این دوره با تکنیک ها و حملات پیشرفته که همه وب اپلیکیشن های پیچیده امروزی ممکن است در برابر آنها آسیب پذیر باشند ، شروع خواهد شد. در ادامه با Framework های جدید وب ، رمزنگاری مرتبط با وب ، Mobile Applications ، HTTP/2 و WebSockets آشنا خواهید شد. و در انتها قبل از CTF ، نحوه بایپس (Bypass) و دور زدن WAF (Web Application Firewall) ، فیلتر های مختلف و سایر تکنیک های دفاعی را خواهید آموخت.

طول دوره:" ۶۰ ساعت

پیشنیاز:

- SANS SEC542: Web App Penetration Testing and Ethical Hacking

"ãl -M"Ú $J $

- چگونه میتوان آسیب پذیری های Backend ، تکنولوژی های جدید و Framework های مدرن را شناسایی و آن ها را اکسپلویت کرد.
- کسب مهارت های تست نفوذ و اکسپلویت تکنولوژی های خاص مانند HTTP/2 ، WebSockets و Node.js
- چگونه میتوان آسیب پذیری های رمزنگاری در اپلیکیشن های مدرن وب را پیدا و ارزیابی کنیم.
- روش هایی برای شناسایی و بایپس مکانیزم های دفاعی مختلف مانند WAF ها

در انتهای دوره مهارت های زیر را یاد خواهید گرفت:

- Perform advanced Local File Include (LFI)/Remote File Include (RFI), Blind SQL injection (SQLi), and Cross-Site Scripting (XSS) combined with Cross-Site Request Forger (XSRF) discovery and exploitation
- Exploit advanced vulnerabilities common to most backend language like Mass Assignments, Type Juggling, and Object Serialization
- Perform JavaScript-based injection against ExpressJS, Node.js, and NoSQL
- Understand the special testing methods for content management systems such as SharePoint and WordPress
- Identify and exploit encryption implementations within web applications and frameworks
- Discover XML Entity and XPath vulnerabilities in SOAP or REST web services and other datastores
- Use tools and techniques to work with and exploit HTTP/2 and Web Sockets

- Identify and bypass Web Application Firewalls and application filtering techniques to exploit the system

مخاطبین دوره:

- متخصصین تست نفوذ وب
- اعضای تیم قرمز (Red Team)
- پرسنل ارزیابی آسیب پذیری
- متخصصین تست نفوذ شبکه
- توسعه دهندگان اپلیکیشن های وب

سرفصل های دوره:

- **SEC642.1: Advanced Attacks**
  Exercises:
  - Getting warmed up with DOM-XSS
  - Exploiting SSRF
  - Exploiting LDAP injection
  - Exploiting NoSQL injection
  - HTTP desynchronization attacks
  - Attacking SAML

  Topics:
  - Review of the testing methodology
  - Using Burp Suite in a web penetration test
  - DOM-XSS to steal and use a CSRF token
  - Discovering and exploiting SSRF
  - Discovering and exploiting LDAP injection
  - Discovering and exploiting NoSQL injection
  - Using HTTP desynchronization attacks
  - Performing privilege escalation in SAML SSO
  - Learning advanced exploitation techniques

- **SEC642.2: Web Cryptography**
  Exercises:
  - Discovering and exploiting hash length extension attacks
  - Exploiting weak keys chosen by the backend system
  - Attacking stream ciphers
  - Discovering and exploiting ECB Shuffling in web applications
  - Discovering and exploiting CBC Bit Flipping in web applications
  - Discovering and exploiting Padding Oracle Attack in web applications

  Topics:
  - Identifying the cryptography used in the web application
  - Identifying and exploiting hash length extension attacks
  - Analyzing and attacking the encryption keys
  - Exploiting stream cipher IV collisions
  - Exploiting Electronic Codebook (ECB) Mode Ciphers with block shuffling
  - Exploiting Cipher Block Chaining (CBC) Mode with bit flipping
  - Vulnerabilities in PKCS#7 padding implementations

- **SEC642.3: Alternative Interfaces and XML**
  Exercises:
  - Playing with WebSockets in SocketToMe
  - Discovering weaknesses in H2O's HTTP/2 implementation
  - Wireshark stream extraction to interact with a mobile server

- Exploiting a REST API
- Exploring and exploiting a GraphQL service
- Exploring and exploiting XML XPath injection
- Exploring and exploiting XXE attacks

Topics:

- Interacting with a mobile application backend
- SOAP and REST web services
- Penetration testing of web services
- GraphQL services
- XML Xpath injection
- XML External Entities (XXE)

- **SEC642.4: Modern Web Frameworks, Part 1**

  Exercises:
  - Mass assignments
  - Template injections
  - Testing for and abusing SSJIs
  - Authentication bypasses with type confusions
  - PHP deserialization lab
  - PHAR deserialization lab

  Topics:
  - Web architectures
  - MVC and its architecture components
  - JavaScript and JavaScript frameworks
  - Server-Side JavaScript
  - Modern PHP
  - PHP deserialization bugs
  - Deserialization through PHA

- **SEC642.5: Modern Web Frameworks, Part II**

  Exercises:
  - Rack Cookie Deserialization lab
  - Elasticsearch and Groovy Sandboxing lab
  - Building Java Payloads
  - Java Deserialization lab
  - Testing and fingerprinting defense based on difficult-to-defend web vulnerabilities
  - Working through XSS defenses compound data URIs
  - Bypassing SQL injection defense with custom tamper scripts in sqlmap
  - RCE Bypass through PHP and its Mail() function

  Topics:
  - Ruby and Rack applications
  - Java, Java Gadgets, and Java Payloads
  - Java Payload Weaponization
  - Java serialization
  - Fingerprinting the defense techniques used
  - Learning how HTML5 injections work
  - Using UNICODE, CTYPEs, and Data URIs to bypass restrictions
  - Bypassing a Web Application Firewall's best-defended vulnerabilities, XSS and SQLi
  - Bypassing application restrictions

- **SEC642.6: Capture-the-Flag Challenge**