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

دوره حرفه ای تست نفوذ وب SANS SEC ۵۴۲

مروری بر دوره

مروری بر دوره

این دوره یکی از از دوره های حرفه ایی تست نفوذ شرکت SANS در زمینه وب می باشد که شما را با آخرین آسیب پذیری های وب آشنا خواهد کرد این دوره بر اساس آخرین سیلابس شرکت SANS می باشد. یکی از مزایای این دوره جزوه و فیلم دوره به صورت فارسی می باشد که در آموزشگاههای دیگر ارائه نمی شود.

آنچه در این دوره خواهید آموخت

آنچه خواهید آموخت

- آشنایی با مفاهیم و پروتکل های وب
- آشنایی با روش های جمع آوری اطلاعات در مورد وب
- آشنایی با روش های بدست آوردن Username و Password یک وب سایت
- آشنایی با انواع روش های Injection مانند SQL Injection و LFI و RFI و ...
- آشنایی با آسیب پذیری های XSS و XXE
- آشنایی با آسیب پذیری CSRF
- آشنایی با نرم افزار های تست نفوذ وب

سرفصل ها (حضوری)

سرفصل ها

SEC۵۴۲.۱: Introduction and Information Gathering

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

- Overview of the web from a penetration tester's perspective
- Exploring the various servers and clients
- Discussion of the various web architectures
- Discovering how session state works
- Discussion of the different types of vulnerabilities
- WHOIS and DNS reconnaissance
- The HTTP protocol
- WebSocket
- Secure Sockets Layer (SSL) configurations and weaknesses
- Heartbleed exploitation
- Utilizing the Burp Suite in web app penetration testing

SEC۵۴۲.۲: Configuration, Identity, and Authentication Testing

- Scanning with Nmap
- Discovering the infrastructure within the application
- Identifying the machines and operating systems
- Exploring virtual hosting and its impact on testing
- Learning methods to identify load balancers
- Software configuration discovery
- Learning tools to spider a website

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

- Brute forcing unlinked files and directories
- Discovering and exploiting Shellshock
- Web authentication
- Username harvesting and password guessing
- Fuzzing
- Burp Intruder

SEC۵۴۲.۳: Injection

- Session tracking
- Authentication bypass flaws
- Mutillidae
- Command Injection
- Directory traversal
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- SQL injection
- Blind SQL injection
- Error-based SQL injection
- Exploiting SQL injection
- SQL injection tools
- sqlmap

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

SEC۵۴۲.۴: XXE and XSS

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

SEC۵۴۲.۵: CSRF, Logic Flaws and Advanced Tools

Cross-Site Request Forgery (CSRF)
Python for web app penetration testing
WPScan
w۳af
Metasploit for web penetration testers
Leveraging attacks to gain access to the system
How to pivot our attacks through a web application
Exploiting applications to steal cookies
Executing commands through web application vulnerabilities
When tools fail

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

مخاطبان دوره

مخاطبان دوره

- کارشناسان امنیت و تست نفوذ و برنامه نویسان صفحات وب

پیش نیاز ها

پیش نیازها

- آشنایی با برنامه نویسی و طراحی صفحات وب