کاریار ارقام
Carrier Digit
مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی
و برگزارکننده دوره های آموزشی

Web App Penetration Testing and Ethical Hacking

SANS - SEC 542
GWAPT

مدت(ساعت): ۴۰ | **پیش نیاز:** CEH + Kali | **اعتبار دهنده:** SANS

معرفی دوره :

امروزه Web Application ها نقشی بسیار حیاتی برای سازمانها و شرکت های بزرگ و کوچک بازی می کنند. اگر مجموعه شما نتواند به درستی به تست و ایمن سازی Web Application های موجود بپردازد ، نفوذگران با انجام اقدامات بدخواهانه میتوانند به خرابکاریهای متفاوت، سرقت اطلاعات و در نتیجه ضربه زدن به کسب و کار شما اقدام نمایند.گروه امنیت یک مجموعه میبایست در حد امکان به صورت دوره اقدام به تست وضعیت امنیت سرویس ها و نرم افزارهای تحت وب نماید تا نقاط آسیب پذیر در اینگونه برنامه ها تا حد ممکن شناسایی و راه کارهای مناسب برای رفع عیوب آنها نیز توسط تیم امنیت ارائه گردد.

محتوای دوره SEC542 شرکت SANS این کمک را به متخصصان تست نفوذ در زمینه وب مینماید تا با گذراندن این دوره وارد دنیای حرفه ای تست نفوذ پذیری نرم افزارهای تحت وب شوند.

امتیازات دوره :

- اعطای مدرک فارسی و انگلیسی با مجوز رسمی از :
  - مجوز از اداره کل نظام مدیریت امنیت اطلاعات (نما)
  - سازمان مدیریت و برنامه ریزی کشور (معاونت توسعه مدیریت و سرمایه انسانی رئیس جمهوری سابق)
  - شورای عالی انفورماتیک
  - قابلیت ترجمه وتایید قوه قضاییه وامور خارجه
- برگزاری لابراتوارهای دوره مبتنی بر Workshop رسمی دوره
- بهره گیری از اساتید مجرب و تأیید شده با سابقه حضور در پروژه‌های ملی

ویژگی های دوره :

- تدریس مطابق با سرفصل آخرین نسخه منتشر شده توسط اعتبار دهنده SANS
- ارائه ابزار های مورد استفاده در طول دوره
- به اشتراک گذاری تجربیات بومی مدرسان دوره به منظور کاربردی نمودن هرچه بیشتر دوره

اهداف دوره :

- آشنایی با متدولوژی ۴ مرحله ای SANS به منظور انجام WEB Application Penetration Testing
- آشنایی با نحوه آنالیز اولیه ابزارهای Automated WEB Testing
- آشنایی با حملات XSS
- کار با Browser Exploitation Framework

مخاطبان دوره :

- General security practitioners
- Penetration testers
- Ethical hackers
- Web application developers
- Website designers and architects

تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳، ۸ فاکس: ۸۸۰۶۵۲۲۲

Course Outline :	محتوای دوره :
Web Penetration Testing and Ethical Hacking: Introduction and Information Gathering • 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 • Defining a web application test scope and process • Defining types of penetration testing • Heartbleed exploitation • Utilizing the Burp Suite in web app penetration testing **Web Penetration Testing and Ethical Hacking: Configuration, Identity, and Authentication Testing** • Discovering the infrastructure within the application • Identifying the machines and operating systems • Secure Sockets Layer (SSL) configurations and weaknesses • Exploring virtual hosting and its impact on testing • Learning methods to identify load balancers • Software configuration discovery • Exploring external information sources • Learning tools to spider a website • Scripting to automate web requests and spidering • Brute forcing unlinked files and directories • Discovering and exploiting Shellshock **Web Penetration Testing and Ethical Hacking: Injection** • Python for web app penetration testing • Web app vulnerabilities and manual verification techniques • Interception proxies • Zed Attack Proxy (ZAP) • Burp Suite • Information leakage and directory browsing • Username harvesting	• Command Injection • Directory traversal • Local File Inclusion (LFI) • Remote File Inclusion (RFI) • SQL injection • Blind SQL injection • JavaScript for the attacker **Web Penetration Testing and Ethical Hacking: JavaScript and XSS** • Cross-Site Scripting (XSS) • Cross-Site Request Forgery (CSRF) • Session flaws • Session fixation • AJAX • XML and JSON • Logic attacks • Data binding attacks • Automated web application scanners • w3af **Web Penetration Testing and Ethical Hacking: CSRF, Logic Flaws and Advanced Tools** • The sqlmap tool • Metasploit for web penetration testers • Exploring methods to zombify browsers • Browser Exploitation Framework (BeEF) • Leveraging attacks to gain access to the system • How to pivot our attacks through a web application • Understanding methods of interacting with a server through SQL injection • Exploiting applications to steal cookies • Executing commands through web application vulnerabilities • Walking through an entire attack scenario

تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳، ۸ فاکس: ۸۸۰۶۵۲۲۲