

Attacks and Defenses Warfare on Web and Mobile Application Systems

H9P48S

HPE course number	H9P48S
Course length	2 days
Delivery mode	ILT
View schedule, local pricing, and register	View now
View related courses	View now

This 2-day course presenting participants with contemporary attacking techniques on web and mobile applications. It targets to help participants understand more about security advance in both attacking and defending sides on the “hacking” battlefield. Participants will have opportunities to try out practical security techniques in this course.

Audience

Web/Mobile Application Developers,
System Architects, Web/Mobile
Application System Administrators,
Information Security Analysts, Penetration
Testers, IT Auditors, and Consultants.

Prerequisites

Participants are expected to have hands-on experience in web and mobile application development, operation and/or review.

Why HPE Education Services?

- IDC MarketScape leader 4 years running for IT education and training*
- Recognized by IDC for leading with global coverage, unmatched technical expertise, and targeted education consulting services*
- Key partnerships with industry leaders OpenStack®, VMware®, Linux®, Microsoft®, ITIL, PMI, CSA, and (ISC)²
- Complete continuum of training delivery options—self-paced eLearning, custom education consulting, traditional classroom, video on-demand instruction, live virtual instructor-led with hands-on lab, dedicated onsite training
- Simplified purchase option with HPE Training Credits

Detailed course outline

Web Protocol and Attack Method	<ul style="list-style-type: none"> · Web Basics & Protocols · Common Web Related Technologies · Security Testing Tools · Hands-on Lab
Web Application Security Risks - Attack & Counter Measures	<ul style="list-style-type: none"> · SQL Injection · Cross-Site Scripting · Cross-Site Request Forgery · Broken Authentication and Session Management · Insecure Direct Object References · Missing Functional Level Access Control · Other Common Web Application Risks · Hands-on Lab
Mobile Application Basics	<ul style="list-style-type: none"> · Basics Concepts & Protocols · Security Testing Tools · Hands-on Lab
Mobile Application Security Risks - Attack & Counter Measures	<ul style="list-style-type: none"> · Common web application security risks in Mobile Apps · Insecure Data Storage · Unintended Data Leakage · Client Side Injection · Lack of Binary Protections · Other Common Mobile Application Risks · Hands-on Lab
Other Aspects in Web/Mobile Application Security	<ul style="list-style-type: none"> · Security in SDLC · Detection of attack · New Challenges and Future Trends

Learn more at
[HPE Education Services for Security](#)

Follow us:



© Copyright 2015–2016 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. The OpenStack Word Mark is either a registered trademark/service mark or trademark/service mark of the OpenStack Foundation, in the United States and other countries and is used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation or the OpenStack community. Pivotal and Cloud Foundry are trademarks and/or registered trademarks of Pivotal Software, Inc. in the United States and/or other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions.

March 2017, c04655154