Enterprise Computing Solutions - Education Services

NABÍDKA ŠKOLENÍ

Prosím kontaktujte nás zde

Arrow ECS, a.s., 28. října 3390/111a, 702 00 Ostrava

Email: training.ecs.cz@arrow.com
Phone: +420 597 488 811

Check Point Advanced Web Hacking (HackingPoint)

Kód:	DÉLKA:	CENA:
CKT_HPAWH	40 Hours (5 DENNÍ)	Kč bez DPH 110,000.00

Description

Školení je vedeno v anglickém jazyce zahraničním lektorem formou virtuální školení.
Cena školení je 5000 USD bez DPH - tato cena bude při fakturaci přepočtena aktuálním kurzem.
This fastpaced class gives attendees an insight into advanced AppSec topics. The class curriculum is split into two: 3 days of Server Side Flaws. 2 days of Client Side Flaws.
We have brought together the most talented experts to challenge our clients. The team has recreated security vulnerabilities based on actual penetration tests and real bug bounties seen in the field. This fastpaced class gives attendees an insight into advanced AppSec topics. The class curriculum is split into two:
• 3 days of Server Side Flaws
• 2 days of Client Side Flaws

Cíle

If you work in the security industry of modern web applications, you will benefit from this class.

Určeno pro

This class is available remotely to all Check Point customers and partners.
Some knowledge of HTML and JavaScript is required, but rookies and experts will be equally satisfied with the class. HTML is a living standard, and so is this class.

Vstupní znalosti

• Basic knowledge of HTML and JavaScript
• Course material will be provided on-site and via access to a private Github repo so all attendees will receive updated material even months after the actual training

This is not a beginner class. To gain the maximum value from the topics being explored, attendees should have a strong understanding of the OWASP top 10 issues.

The class does not cover all AppSec topics and focuses only on advanced identification and exploitation techniques of vulnerabilities.

Program

Server Side Flaws (3 days):
These vulnerabilities affect well-known software/websites and span across multiple technologies, such as .NET framework to Node.js applications. We selected vulnerabilities that typically go undetected by modern scanners, or have less-known exploitation techniques.

• SQL Injection
2nd order injection
NoSQL injection
Out-of-Band exploitation
WAF bypass techniques

• XXE Injection	• Serialization Flaws		• Business Logic Flaws
Blind XXE injection	PHP object injection	• HTTP Parameter Pollution (HPP)	Mass assignment bugs
Case Study of recent XXE bugs	Java serialization flaw	Detecting HPP in application	OS code injection
XXE to Code Execution	Case study of recent serialization flaws	Case study of recent HPP bugs	Crypto attacks

Client Side Flaws (2 days):

These classes focus on offensive attacks and dangerous parts of HTML, JavaScript, and related technologies, the nasty and undocumented stuff. There are dozens of new attack techniques straight from the laboratory of horrors of those maintaining the HTML5 Security Cheat Sheet. We will learn how to attack any Web application— either with unknown legacy features or the half-baked results coming to your browser from the labs of W3C, WHATWG and the ES6 mailing lists.

Whether you want to attack modern web applications or shiny browser extensions and Chrome Packaged Apps, we have that covered.

Some knowledge of HTML and JavaScript is required, but rookies and experts will be equally satisfied with the class. HTML is a living standard, and so is this class.

Course material will be provided on-site and via access to a private Github repo so all attendees will receive updated material even months after the actual training.

• Starts with:	
Client Side flaws (basics)	• Moves on to:
HTTP / Encoding	HTML5 Attacks & Vectors
Character sets	SVG
CSRF and detail	XML
Cross Site-Scripting	Mutation XSS / mXSS
DOM clobbering	Scriptless Attacks
Drag&Drop / Copy&Paste	SOP Bypasses
DOMXSS	Filter Bypasses
Legacy Features	Optimizing your payload

Termíny školení

Termíny školení na vyžádání, kontaktujte nás prosím

Dodatečné informace

Školení je možné zajistit na míru. Kontaktujte nás pro bližší informace.