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

# Zranitelnosti webových aplikací 2 - Útoky proti serverum

| Kód: | DÉLKA: | CENA: |
|---|---|---|
| OTH_GOC542 | 40 Hours (5 DENNÍ) | Kč bez DPH 31,000.00 |

## Description

Toto školení vás zasvětí do tajů webhackingu a zranitelností webových aplikací, které umožňují útočit na aplikační servery a na nich uložená data. Školení Vám umožní do detailu pochopit a v praxi si vyzkoušet metody, které běžně používají útočníci. Zranitelnosti webových aplikací umožňující útoky na server patří mezi nejzávažnější hrozby a důkladně by s nimi měli proto být seznámeni všichni vývojáři a provozovatelé webových aplikací. Vzhledem k tomu, že zneužití tohoto typu zranitelností vede často ke kompletnímu převzetí kontroly nad cílovým systémem, měli byste se s nimi seznámit a otestovat si bezpečnost svých webových aplikací dříve, než to za vás udělá nevítaný vetřelec. Vše, co k tomu budete potřebovat, Vás naučíme na tomto praktickém kurzu.

Toto školení pořádá společnost GOPAS a.s.

## Cíle

Tento jedinečný kurz Webhacking v praxi 2 – útoky proti serverům vám umožní do detailu pochopit a hlavně si na praktických příkladech vyzkoušet metody, kterých běžně využívají útočníci během útoků na webové servery a aplikace. V průběhu kurzu si postupně vysvětlíme vše, co potřebujete znát pro obranu proti těmto útočným technikám.

## Určeno pro

Kurz je urcen vývojárum a provozovatelum webových aplikací, kteří chtejí porozumet postupum útocníku pri napadání webových aplikací. Na mnoha praktických ukázkách si vyzkoušíme postupy útocníku, pri nichž dochází ke kompromitaci serveru a databází. Postupy probírané na tomto kurzu cílí primárne na technologie Apache, PHP a MySQL. Protože se ale dají predstavené principy casto aplikovat i na jiné technologie, doporucujeme návštevu kurzu každému, kdo se chce seznámit s praktikami útocníku a chce získat správné bezpecnostní návyky pri vývoji a provozu webových aplikací a serveru.

## Vstupní znalosti

Kurzu se může zúčastnit každý, kdo má základní znalosti technologií HTTP, HTML a SQL.

## Program

Průzkum prostředí
- Identifikace použitých technologií
- Web Crawling / Spidering
- Hledání neveřejných zdrojů
- Repozitáře
- Open Directory listing
- IIS Tilde File Enumerate
- Apache Multiviews File Enumerate
- HTTP metody

Exploitace použitých technologií
- Guessing
- Hledání exploitů
- Použití exploitů
- Post exploitace
- Shelly

Zranitelnosti a útoky na SSL
- Zranitelnosti jednotlivých šifrovacích algoritmů
- Heartbleed
- Poodle
- BEAST
- CRIME
- BREACH
- a další

Útoky na databázi
- Union-Based SQL injection
- Boolean-Based SQL injection
- Error-Based SQL injection
- Time-Based SQL injection
- Stacked SQL injection
- Stored / Second-order SQL injection
- DNS exfiltration
- Multibyte SQL injection
- SQL injection via binary hash
- Local File Disclosure via SQL injection
- Command execute via SQL injection
- SQL Truncation

Útoky na data
- Chybějící / Nedostatečná autorizace
- Přímý přístup k objektům
- Únik dat při redirektu
- Forced Browsing

Code Execution
- Nezabezpečený upload
- Nezabezpečený download
- Local File Disclosure
- Remote File Inclusion (RFI)
- Local File Inclusion (LFI)
- LFI via file upload
- LFI via session storage
- LFI via environment
- LFI via log
- LFI via phpinfo
- Function Injection
- PHP Object Injection
- Code Execution
- Command Execution
- WebDav a zneužití HTTP metod
- PHP-CGI vulnerability
- SSI Injection

Zranitelnosti XML parserů
- Denial of Services via XML
- Local File Disclosure via XML
- Command Execution via XML
- XML injection
- LDAP injection
- XPATH injection

Crackování hashů
- Hashovací algoritmy
- Solení
- Crackování hashů
- Brute Force / Dictionary attack / Rainbow tables

Podíváme se i na další útoky...
- Zneužití webserveru jako proxy
- HTTP request smuggling
- Privilege escalation / autorization bypass skrz cookie
- HTTP Request hlavičky
- Host Header Injection
- Napadení Session Storage
- Local Session Injection
- Session Puzzling
- ZIP bomby a DoS
- Útoky na sdílených serverech
- Server-Side Request Forgery (SSRF)
- Zranitelnost Shellshock

## Termíny školení

Termíny školení na vyžádání, kontaktujte nás prosím

## Dodatečné informace

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