Zranitelnosti webových aplikací 2 - Útoky proti serverům

Kód kurzu: GOC542

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.

Pro koho je kurz určen

Kurz je určen vývojářům a provozovatelům webových aplikací, kteří chtějí porozumět postupům útočníků při napadání webových aplikací. Na mnoha praktických ukázkách si vyzkoušíme postupy útočníků, při nichž dochází ke kompromitaci serveru a databází.
Postupy probírané na tomto kurzu cílí primárně na technologie Apache, PHP a MySQL. Protože se ale dají představené principy často aplikovat i na jiné technologie, doporučujeme návštěvu kurzu každému, kdo se chce seznámit s praktikami útočníků a chce získat správné bezpečnostní návyky při vývoji a provozu webových aplikací a serverů.

Co vás naučíme

Náš 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.

Požadované vstupní znalosti

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

Osnova kurzu

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

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved

- Heartbleed
- Poodle
- BEAST
- CRIME
- BREACH
- a další

Útoky na data

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

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

Crackování hashů

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

Zranitelnosti XML parserů

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

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved

Zranitelnosti webových aplikací 2 - Útoky proti serverům

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

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

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved