Zraniteľnosti webových aplikácií - útoky na užívateľa

Kód kurzu: GOC541

Toto školenie vás zasvätí do tajov webhackingu a zraniteľností webových aplikácií, ktoré umožňujú útočiť na koncových uživateľov služby. Školenie vám umožní do detailov pochopiť a v praxi si vyskúšať metódy, ktoré bežne používajú útočníci. Zraniteľnosti webových aplikácií umožňujúce útoky na koncových uživateľov patria medzi najčastejšie typy webových zraniteľností a dôkladne by s nimi preto mali byť zoznámení všetci vývojári a prevádzkovatelia webových aplikácií. Aj keď to nemusí byť na prvý pohľad zrejmé, môžu mať tieto útoky veľmi vážne dopady vrátane kompletného prevzatia kontroly nad cieľovým systémom. Zoznámte sa s týmito zraniteľnosťami a otestujte si bezpečnosť svojich webových aplikácií skôr než to za vás urobí nevítaný votrelec. Všetko, čo k tomu budete potrebovať, vás naučíme na tomto praktickom kurze.

Pobočka	Dní	Katalógová cena	ITB
Praha	5	31 000 Kč	75
Brno	5	31 000 Kč	75
Bratislava	5	1 350 €	75

Všetky ceny sú uvedené bez DPH.

Termíny kurzu

	Dátum	Dní	Cena kurzu	Typ výučby	Jazyk výučby	Lokalita
G	12.05.2025	5	31 000 Kč	Prezenčný	CZ/SK	Gopas Praha Prezenční
	19.05.2025	5	1 350 €	Online	CZ/SK	Gopas Bratislava Online
	19.05.2025	5	31 000 Kč	Online	CZ/SK	Gopas Praha Online
	07.07.2025	5	31 000 Kč	Prezenčný	CZ/SK	Gopas Brno Prezenční
	28.07.2025	5	31 000 Kč	Prezenčný	CZ/SK	Gopas Praha Prezenční
	13.10.2025	5	31 000 Kč	Prezenčný	CZ/SK	Gopas Brno Prezenční
	03.11.2025	5	31 000 Kč	Prezenčný	CZ/SK	Gopas Praha Prezenční

Všetky ceny sú uvedené bez DPH.

Pre koho je kurz určený

Kurz je určený vývojárom a prevádzkovateľom webových aplikácií, ktorí chcú porozumieť postupom útočníkov pri napádaní webových aplikácií. Na mnohých praktických ukážkach si vyskúšame postupy útočníkov, pri ktorých dochádza ku krádeži užívateľských účtov, prístupových údajov a relácií. Zneužijeme requesty odosielané užívateľom alebo ukradneme a zneužijeme každé ich kliknutie.
Kurz môžeme s kľudným svedomím doporučiť tiež bežným užívateľom so základnou znalosťou tvorby webových stránok, ktorí by sa radi dozvedeli o možných útokoch, ktoré im hrozia pri bežnom surfovaní na internete. Na tomto kurze sa dozviete veľa informácií ako zlepšiť bezpečnostné návyky pri prechádzaní webových stránok, aby ste obmedzili možné riziká.
Postupy preberané na tomto kurze sú platforme nezávislé. Získané vedomosti uplatníte v praxi bez ohľadu na to, v akom programovacom jazyku vyvíjate svoje aplikácie.

Čo vás naučíme

Náš jedinečný kurz Zraniteľnosti webových aplikácií 1 - Útoky proti užívateľom vám umožní do detailu pochopiť a hlavne si na praktických príkladoch vyskúšať metódy, ktoré bežne využívajú útočníci. V priebehu kurzu si postupne vysvetlíme všetko, čo potrebujete poznať pre obranu proti týmto útočným technikám.

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

Zraniteľnosti webových aplikácií - útoky na užívateľa

Požadované vstupné znalosti

Kurzu sa môže zúčastniť každý, kto má základné znalosti technológií HTML, CSS a Javascript.

Osnova kurzu

Úvod, nástroje

- HTTP protokol
- Použitie nástroja Burp Suite
- Web Parameter Tampering / Hidden Fields

Autentizácia, Session Management

- Enumerácia užívateľov
- Útoky na autentizáciu/Guessing
- Captcha – použitie a chyby
- Citlivé údaje v URL
- Session Stealing
- Session Prediction
- Session Fixation
- Session Donation
- Cross-Site Cooking
- Cross-Subdomain Cooking
- Session Puzzling
- Insufficient Session Expiration
- Insufficient logout
- Logout action availability

Dôvera v užívateľa

- Cross-Site Request Forgery (CSRF)
- CSRF a metódy GET/POST
- Možnosti obrany pred CSRF
- HTTP verb tampering
- Kradneme kliknutím pomocou clickjackingu
- Vyplňujeme a odosielame formuláre pomocou clickjackingu
- Možnosti obrany pred clickjackingom

Skriptovanie na strane klienta

- Cross-Site Scripting (XSS)
- Perzistentný XSS
- Reflektovaný XSS
- DOM based XSS
- Blind XSS
- Self XSS

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

- Bypass kódu
- Protokoly javascript, vbsctipt, data
- XSS a nastavenie Content-Type
- Cross-Site Flashing
- Použitie nástroja BeEF
- Obrana pred XSS
- Too long cookie value
- Príznak HttpOnly
- Cross-Site Tracing
- Reflected HTTP Request Header
- Open Redirect
- HTTP Response Splitting (CRLF injection)
- HTTPResponse Smuggling
- File Download via Open redirect
- Content Spoofing
- Cross-Site Messaging

Kradneme užívateľské dáta

- Únik dát refererom
- Únik dát pri redirekte
- Útoky na CORS
- JavaScript Hijacking
- Problémy callbackov
- WWW-Authenticate attack
- Post &Back Attack
- Cross-site WebSocket hijacking

Pozrieme sa aj na ďalšie útoky...

- Útoky na local storage
- Útoky na websockety
- Cache Poisoning
- HTTP Parameter Pollution
- Host Header Injection
- Path Relative StyleSheet Import (PRSSI)
- Zneužitie užívateľa pre napadnutie intranetu
- Reflected File Download
- CSV injection
- HTTP Response hlavičky pre bezpečný web

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk