

# Zraniteľnosti webových aplikácií - útoky na užívateľa

Kód kurzu: GOC541

Toto školenie vás zasväť do tajov webhackingu a zraniteľností webových aplikácií, ktoré umožňujú útočiť na koncových užívateľov služby. Školenie vám umožní do detailov pochopiť a v praxi si vyskúšať metódy, ktoré bežne používajú útočníci. Zraniteľnosti webových aplikácií umožňujúce útoky na koncových užívateľov 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 zřejmé, môžu mať tieto útoky veľmi vážne dopady vrátane kompletnej prevzatia kontroly nad cieľovým systémom. Zoznámte sa s týmito zraniteľnosťami a otestujte si bezpečnosť svojich webových aplikácií skôr než to za vás urobí nevitáný votrelec. Všetko, čo k tomu budete potrebovať, vás naučíme na tomto praktickom kurze.

## 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.

## 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

#### GOPAS Praha

Kodaňská 1441/46  
101 00 Praha 10  
Tel.: +420 234 064 900-3  
[info@gopas.cz](mailto:info@gopas.cz)

#### GOPAS Brno

Nové sady 996/25  
602 00 Brno  
Tel.: +420 542 422 111  
[info@gopas.cz](mailto:info@gopas.cz)

#### GOPAS Bratislava

Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 248 282 701-2  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2020 GOPAS, a.s.,  
All rights reserved

# Zraniteľnosti webových aplikácií - útoky na užívateľa

- 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
- Vypĺňujeme 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
- Bypass kódu
- Protokoly javascript, vbscript, 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

### GOPAS Praha

Kodaňská 1441/46  
101 00 Praha 10  
Tel.: +420 234 064 900-3  
[info@gopas.cz](mailto:info@gopas.cz)

### GOPAS Brno

Nové sady 996/25  
602 00 Brno  
Tel.: +420 542 422 111  
[info@gopas.cz](mailto:info@gopas.cz)

### GOPAS Bratislava

Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 248 282 701-2  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2020 GOPAS, a.s.,  
All rights reserved

# Zraniteľnosti webových aplikácií - útoky na užívateľa

## 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](mailto:info@gopas.cz)

**GOPAS Brno**  
Nové sady 996/25  
602 00 Brno  
Tel.: +420 542 422 111  
[info@gopas.cz](mailto:info@gopas.cz)

**GOPAS Bratislava**  
Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 248 282 701-2  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2020 GOPAS, a.s.,  
All rights reserved