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 1 - Útoky proti uživatelum

Kód:	DÉLKA:	CENA:
OTH_GOC54	40 Hours (5 dní)	Kč 31,000.00

Description

Toto školení vás zasvětí do tajů webhackingu a zranitelností webových aplikací, které umožňují útočit na koncové uživatele služby. Školení Vám umožní do detailu pochopit a v praxi si vyzkoušet metody, které běžně používají útočníci. Zranitelnosti webových aplikací umožňující útoky na koncové uživatele patří mezi nejčastější typy webových zranitelsností a důkladně by s nimi proto měli být seznámeni všichni vývojáři a provozovatelé webových aplikací. Přestože to nemusí být na první pohled zřejmé, mohou mít tyto útoky velice vážné dopady včetně kompletního převzetí kontroly nad cílovým systémem. Seznamte se s těmito zranitelnostmi a otestujte 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 Zranitelnosti webových aplikací 1 - Útoky proti uživatelům vám umožní do detailu pochopit a hlavně si na praktických příkladech vyzkoušet metody, kterých běžně využívají útočníci. 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, kterí chtejí porozumet postupum útocníku pri napadání webových aplikací. Na mnoha praktických ukázkách si vyzkoušíme postupy útocníku, pri nichž dochází ke krádeži uživatelských úctu, prístupových údaju a relací. Zneužijeme requesty odesílané uživatelem, nebo ukradneme a zneužijeme každé jejich kliknutí.
Kurz mužeme s klidným svedomím doporucit také bežným uživatelum se základní znalostí tvorby webových stránek, kterí by se rádi dozvedeli o možných útocích, jež jim hrozí pri bežném surfování na internetu. Na tomto kurzu se dozvíte mnoho informací jak zlepšit bezpecnostní návyky pri procházení webových stránek, abyste omezili možná rizika.
Postupy probírané na tomto kurzu jsou platforme nezávislé. Získané vedomosti uplatníte v praxi bez ohledu na to, v jakémkoliv programovacím jazyce vyvýjíte své aplikace.

Vstupní znalosti

Kurzu se může zúčastnit každý, kdo má základní znalosti technologií HTML, CSS a Javascript.

Program

Autentizace, Session Management
- Enumerace uživatelů
- Útoky na autentizaci / Guessing
- Captcha – použití 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

Úvod, nástroje
- HTTP protokol
- Použití nástroje Burp Suite
- Web Parameter Tampering / Hidden Fields

Skriptování na straně klienta
- Cross-Site Scripting (XSS)
- Perzistentní XSS
- Reflektovaný XSS
- DOM based XSS
- Blind XSS
- Self XSS
- Bypass kódu
- Protokoly javascript, vbsctipt, data
- XSS a nastavení Content-Type
- Cross-Site Flashing
- Použití nástroje BeEF
- Obrana před XSS
- Too long cookie value
- Příznak 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

Důvěra v uživatele
- Cross-Site Request Forgery (CSRF)
- CSRF a metody GET / POST
- Možnosti obrany před CSRF
- HTTP verb tampering
- Krademe kliknutí pomocí clickjackingu
- Vyplňujeme a odesíláme formuláře pomocí clickjackingu
- Možnosti obrany před clickjackingem

Podíváme se i na další útoky...
- Útoky na local storage
- Útoky na websockety
- Cache Poisoning
- HTTP Parameter Pollution
- Host Header Injection
- Path Relative StyleSheet Import (PRSSI)
- Zneužití uživatele pro napadení intranetu
- Reflected File Download
- CSV injection
- HTTP Response hlavičky pro bezpečný web

Krademe uživatelská data
- Únik dat refererm
- Únik dat při redirektu
- Útoky na CORS
- JavaScript Hijacking
- Problémy callbacků
- WWW-Authenticate attack
- Post & Back Attack
- Cross-site WebSocket hijacking

Termíny školení

Termíny školení na vyžádání, kontaktujte nás prosím

Dodatečné informace

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