

# Zabezpečenie webových aplikácií v PHP

Kód kurzu: INTPH\_SEC

Kurz je vhodný pre vývojárov webových aplikácií, ktorí chcú udržať krok s modernými metódami v PHP a dokázať zabezpečiť nielen firemné aplikácie pred najčastejšími hroziacimi útokmi a ale aj pre kvalitnú ochranu citlivých dát v súlade s GDPR.

## Čo Vás naučíme

- Na mnohých príkladoch budú demonštrované užitočné novinky v posledných verziách PHP 7+.
- Vývojári sa ďalej naučia využívať moderné bezpečné kryptografické funkcie a algoritmy, dostupné od PHP 7 (.2) + v extenzii cross-platformovej knižnice Sodium (pre Java, JavaScript, Python, Perl, ...).
- Na kurze bude vysvetlené a vyskúšané, ako zabezpečiť projekt webovej aplikácie pred najčastejšími spôsobmi útokov!
- Ako kódovať webové aplikácie v súlade s GDPR compliance.

## Požadované vstupné znalosti

Znalosť PHP približne v rozsahu kurzov INTPH1.

## Metódy výučby

Odborný výklad s praktickými ukážkami, cvičeniami na počítačoch.

## Študijné materiály

Tlačené prezentácie preberanej látky.

## Osnova

Práca s populárnymi balíčkami PHAR (PHP Archive, obdobá JAR v Jave):

- Vytvorenie PHAR archívu z vlastnej aplikácie,
- Spúšťanie .phar,
- Použitie kompresie,
- Zabezpečenie proti modifikácii, atď.

Zabezpečenie citlivých informácií vo webových aplikáciách:

- Bezpečné haš vs. nedávno prelomené algoritmy,
- Automatické solenie od PHP 7+,
- Nový hashovací algoritmus v PHP 7.2+ využívajúci pamäťové náročnosti,
- Spôsob lámania hashovaných údajov, atď.

Revolučná cross-platformová knižnica Sodium s modernými kryptografickými funkciami:

- Využitie v základe od PHP 7.2+,
- Inštalácia z PECL pre PHP 7+.

Symetrické a asymetrické šifrovanie v PHP:

- S extenziou Sodium (heslo vs. tajný kľúč, nonce, verejný kľúč)
- S alternatívou OpenSSL, k novo zrušenej extenzii mcrypt od PHP 7.2.

Replay attack a ochrana pomocou nonce pri šifrovaní.

Aktuálne najväčšie bezpečnostné hrozby webových aplikácií a ochrana proti nim v PHP:

- Cross-site Scripting (XSS),
- SQL injektáž a ochrana vďaka Prepared Statements,
- Web Parameter tampering,
- Injektáž PHP kódu vo webových aplikáciách,
- Local File Inclusion, Remote File Inclusion,
- Path Traversal,
- PHP object injection a ochrana pri deserializácii v PHP 7+.

### 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

# Zabezpečenie webových aplikácií v PHP

Validácia vstupných dát užívateľa v PHP 7.

Nástroje na sledovanie a modifikáciu HTTP (S) komunikácie, využitie sniffovacieho nástroja pri kontrole zabezpečenia webovej aplikácie.

Tvorba webovej aplikácie v súlade s GDPR:

- Identifikácia citlivých (všeobecných a zvláštnych osobných) údajov,
- Metódy ich ochrany,
- Pseudonimizácia a anonymizácia citlivých údajov, v PHP tvorba GDPR compliant webových aplikáciách.

Citlivé údaje z geolokácie a práca s EXIF, ochrana pred ich zneužitím podľa GDPR.

**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