Zabezpečení webových aplikací v PHP

Kód kurzu: INTPH_SEC

Kurz je vhodný pro vývojáře webových aplikací, kteří chtějí udržet krok s moderními metodami v PHP a dokázat zabezpečit nejen firemní aplikace před nejčastějšími hrozícími útoky a pro kvalitní ochranu citlivých dat v souladu s GDPR.

Co Vás naučíme:

- Na mnoha příkladech budou demonstrovány užitečné novinky v posledních verzích PHP 7+.
- Vývojáři se dále naučí využívat moderní bezpečné kryptografické funkce a algoritmy, dostupné od PHP 7(.2)+ v extenzi cross-platformní knihovny Sodium (pro Java, JavaScript, Python, Perl, ...).
- Na kurzu bude vysvětleno a vyzkoušeno, jak zabezpečit projekt webové aplikace před nejčastějšími způsoby útoků! Jak kódovat webové aplikace v souladu s GDPR compliance.

Požadované vstupní znalosti:

- Znalost PHP přibližně v rozsahu kurzu INTPH1.

Metody výuky:

- Odborný výklad s praktickými ukázkami, cvičení na počítačích.

Studijní materiály:

- Tištěné prezentace probírané látky.

Osnova:

Práce s populárními balíčky PHAR (PHP Archive, obdoba JAR v Javě):

- Vytvoření PHAR archivu z vlastní aplikace,
- Spouštění .phar,
- Použití komprese,
- Zabezpečení proti modifikaci, atd.

Zabezpečení citlivých informací ve webových aplikacích:

- Bezpečné hashovací vs. nedávno prolomené algoritmy,
- Automatické solení od PHP 7+,
- Nový hashovací algoritmus v PHP 7.2+ využívající paměťové náročnosti,
- Způsob lámání hashovaných údajů, atd.

Revoluční cross-platformní knihovna Sodium s moderními kryptografickými funkcemi:

- Využití v základu od PHP 7.2+,
- Instalace z PECL pro PHP 7+.

Symetrické a asymetrické šifrování v PHP:

- S extenzí Sodium (heslo vs. tajný klíč, nonce, veřejný klíč)
- S alternativou OpenSSL, k nově zrušené extenzi mcrypt od PHP 7.2.

Replay attack a ochrana pomocí nonce při šifrování.

Aktuální největší bezpečnostní hrozby webových aplikací a ochrana proti nim v PHP:

- Cross-site Scripting (XSS),
- SQL injektáž a ochrana díky Prepared Statements,
- Web Parameter Tampering,
- Injektáž PHP kódu ve webových aplikacích,
- Local File Inclusion, Remote File Inclusion,
- Path Traversal,
- PHP object injection a ochrana při deserializaci v PHP 7+.

Validace vstupních dat uživatele v PHP 7.

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

Zabezpečení webových aplikací v PHP

Nástroje pro sledování a modifikaci HTTP(S) komunikace, využití sniffovacího nástroje při kontrole zabezpečení webové aplikace.

Tvorba webové aplikace v souladu s GDPR:

- Identifikace citlivých (obecných a zvláštních osobních) údajů,
- Metody jejich ochrany,
- Pseudonimizace a anonymizace citlivých údajů, v PHP tvorba GDPR compliant webových aplikacích.

Citlivé údaje z geolokace a práce s EXIF, ochrana před jejich zneužitím dle GDPR.

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