Security in PHP Web applications

Course code: INTPH_SEC

The course is suited for web application developers who want to keep up with modern PHP methods and can not only secure corporate applications against the most common threats and for quality protection of sensitive data in line with GDPR.

What we teach you:

- In many instances, useful updates will be demonstrated in the latest versions of PHP 7+.
- Developers will learn to use advanced secure cryptographic features and algorithms available from PHP 7 (.2) + in the extension of the Sodium cross-platform library (for Java, JavaScript, Python, Perl ...).
- The course will be explained and tested how to secure the web application project against the most common ways of attack! How to encode web applications in accordance with GDPR compliance.

Required skills:

- Knowledge of PHP approximately in the INTPH1 course.

Teaching methods:

- Professional explanation with practical samples and examples.

Teaching materials:

- Powerpoint handouts and module printouts.

Course syllabus:

Working with popular PHAR packages (PHP Archive, JAR similar to Java):

- Creating a PHAR archive from your own application,
- Starting .phar,
- Using compression,
- Security against modification, etc.

Secure sensitive information in web applications:

- Safe hash vs. recently broken algorithms,
- Automatic salting from PHP 7+,
- New hash algorithm in PHP 7.2+ using memory requirements,
- How to break data, etc.

Revolutionary cross-platform library Sodium with modern cryptographic features:

- Base usage from PHP 7.2+,
- Installation from PECL for PHP 7+.

Symmetric and asymmetric encryption in PHP:

- With Sodium extension (password vs. secret key, nonce, public key)
- With an OpenSSL alternative, to the newly removed extensions mcrypt from PHP 7.2.

Replay attack and nonce protection when encrypted.

The most current security threats to web applications and their protection in PHP:

- Cross-site Scripting (XSS),
- SQL injection and protection through Prepared Statements,
- Web Parameter Tampering,
- Injection of PHP code in web applications,
- Local File Inclusion, Remote File Inclusion,
- Path Traversal,
- PHP object injection and deserialization protection in PHP 7+.

Validation of user input in 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

Security in PHP Web applications

Tools for tracking and modifying HTTP (S) communications, using sniffing tools to control web application security.
Creating a web application in accordance with GDPR:

- Identification of sensitive (general and special personal) data,
- Methods of their protection,
- Pseudonimization and anonymization of sensitive data, PHP creation of GDPR compliant web applications.

Sensitive data from geolocation and work with EXIF, protection against abuse according to 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