securitum

Language course: Polish

Websecurity **Master**

The most practical and comprehensive application security course on the market!

12 four-hour training sessions in an accessible form

MODULE I

Basics of Web Application Security

1750 PLN NET

MODULE II

Advanced Security of Web Applications

1750 PLN NET

BUNDLE AND SAVE

BASIC AND ADVANCED MODULE

~~3500~~ PLN NET ▸▸▸ 2950 PLN NET

WHY IS THIS COURSE SO GOOD?

- Over 50 hours of hands-on training from experienced trainers-practitioners
- Optimal format: online, live four-hour sessions once a week, course duration: 12 weeks
- Flexible participation options: join one or both modules
- Access to a dedicated training LAB for self-paced exercises
- Six months of access to live session recordings
- Access to a knowledge-sharing platform (Discord), consultations with trainers and participants
- Certificate of participation in the training (available in both Polish and English)

Free!

E-book

of the best-selling book *Web Application Security*

WHAT A COURSE PARTICIPANT GAINS

- Ability to identify potential attacks on web applications
- Knowledge to apply protective methods against attacks
- Skills to independently conduct penetration tests
- Information about key tools and documentation
- Unique expertise from practitioners, helpful in career development

WHAT A COMPANY GAINS

- Increasing the organization's resilience to cyberattacks
- Improving the quality of application code
- Accelerating the application deployment and acceptance process
- Valuable expert knowledge for the organization
- Outstanding support for employees

COURSE START: OCTOBER 8, 2024

https://websec.sekurak.pl/

FOR WHOM?

THE COURSE IS DIVIDED into two modules to meet the needs of beginners and advanced participants

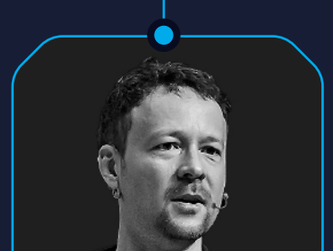
- Testers
- Programmers
- DevOps
- Pentesters
- System administrators

TRAINERS

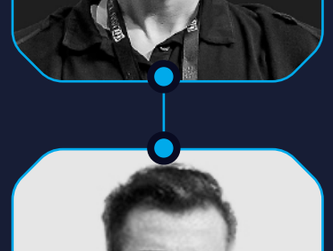
Marek Rzepecki. A professional, ethical hacker from the Securitum team and a passionate enthusiast of offensive cybersecurity. He has conducted hundreds of independent security audits of web and mobile applications, network infrastructures, and DDoS resilience tests for major companies both in Poland and abroad. A trainer who has trained thousands of individuals in Poland and internationally on application and IT infrastructure security. A speaker at industry conferences and author of educational materials.

Kamil Jarosiński. IT security consultant at Securitum. On a daily basis, he tests the security of web applications, APIs, cloud environments, and hardware in the largest banks, mobile operators, and e-commerce industry. Active trainer, and speaker at industry conferences. In his free time, he participates in *bug bounty* programs with reported vulnerabilities at Sony, HCL Software and Telekom Deutschland.

Mateusz Lewczak. An experienced programmer, interested in low-level aspects of Security, who uses his creativity in his free time to develop hacking tools. He has been awarded many times for outstanding academic achievements (including the Prime Minister's Scholarship). He is an IT security consultant at Securitum and a member of the international IEEE Institute, which brings together ambitious IT professionals.



Michał Sajdak. Founder of Securitum and sekurak.pl. Co-author and editor of the best-selling books: *Web Application Security and Introduction to IT Security*. Originator of the Sekurak.Academy and MEGA Sekurak Hacking Party projects. Certified Ethical Hacker with over fifteen years of experience in the field of technical IT security.



Robert Kruczek. Pentester, a social engineer, and ethical hacker from the Securitum team, is also a programmer and gamer in his spare time. Participant in *bug bounty* programs – with a place in the OLX Hall of Fame. He has reported security vulnerabilities for, among others, BlaBlaCar, OVH, ERCOM and more. An experienced pentester of desktop and web applications. A person who effectively breaks physical security (and not only that), verifying the organization's security during social engineering tests. Speaker at industry conferences, author of texts on sekurak.pl.

REGISTRATION AND DETAILS

https://websec.sekurak.pl/

Additional questions: Aneta Jandziś
aneta.jandzis@securitum.pl
Phone +48 (12) 352 33 82
+48 516 824 029

AGENDA

MODULE 1

Basics of Web Application Security

Session #1: Practical Introduction to Web Application Security:

- Review of real, current vulnerabilities in web applications (from the last year). Live shows.
- Basics of web application reconnaissance.
- Basics of using Burp Suite and HTTP protocol basics.
- Demonstration of a multi-stage attack on a web application.
- Introduction to web application security testing:
  1. How to plan application security tests;
  2. Automatic tests vs manual tests;
  3. Reporting.

Session #2: A Condensed Introduction to OWASP Top Ten:

- Overview of all 10 vulnerability classes.
- Overview of general strategies for defending applications against attacks.
- Live shows.
- LAB for participants to complete.

Session #3: Vulnerabilities/Problems in Authentication/Authorization Mechanisms:

- Secure storage of passwords in applications
- How can hackers bypass two-factor authentication and how to prevent this?
- Issues with password reset mechanisms.
- IDOR class vulnerabilities.
- JWT security.
- Review of unusual vulnerabilities that enable bypassing authentication/authorization.
- LAB for participants to complete.

Session #4: Overview of Common Vulnerabilities in Web Applications (part I):

- RCE/*Command Injection* class vulnerabilities:
  1. Upload mechanisms;
  2. *Command Injection* vulnerability review;
  3. Problems in libraries;
  4. Other vulnerabilities leading to code execution in the operating system (review).
- LAB for participants to complete.

Session #5: Overview of Common Vulnerabilities in Web Applications (part II):

- An overview of common vulnerabilities occurring in web applications:
  1. *SQL Injection*;
  2. *NoSQL Injection*,
  3. Manipulation of XML files leading to unauthorized access to data on the server (XXE);
  4. SSRF vulnerability;
  5. *Path Traversal* vulnerability.
- LAB for participants to complete.

Session #6: Multi-stage Exercise Summarizing the Basic Training Module:

- Reconnaissance.
- Exploitation of several vulnerabilities.
- Privilege escalation in the attacked system.

MODULE 2

Advanced Security of Web Applications

Session #1: Advanced Web Application Security (vulnerability review, part I):

- Deserialization vulnerabilities.
- SSTI vulnerability.
- *Mass Assignment* vulnerability.
- How can enabled debugging mechanisms lead to the compromise of a web application?
- LAB for participants to complete.

Session #2: Advanced Web Application Security (vulnerability review, part II):

- What is WAF?
- WAF bypass techniques.
- *HTTP request smuggling*.
- Selected security problems of cache mechanisms in web applications.
- Browser mechanisms for securing web applications and their users.
- LAB for participants to complete.

Session #3: REST API Security:

- Bypassing access restrictions to HTTP methods.
- *Server-Side Request Forgery* (SSRF) and XXE vulnerabilities in the context of REST APIs.
- API key leaks.
- OAuth2 security.
- Selected classic web vulnerabilities in the context of REST APIs.
- LAB for participants to complete.

Session #4: Basics of Frontend Security of Web Applications (part I – XSS vulnerability):

- *Cross-Site Scripting* – the most important vulnerability in the client-side world.
- *Same Origin Policy* overview and training on the practical effects of XSS.
- XSS types.
- Discussion of XSS entry points (GET/POST parameters, Flash files, SVG files, file upload).
- Characteristics of XSS exit points (dangerous JS functions, HTML contexts).
- Discussion of methods of protection against XSS, techniques of bypassing XSS filters.
- XSS and allowing HTML code fragments.
- LAB for participants to complete.

Session #5: Basics of Frontend Security of Web Applications (part II – Other frontend vulnerabilities):

- JS libraries (jQuery, Angular, React, Knockout).
- Selected issues related to the security of HTML5 API elements.
- *JSON Hijacking* vulnerability.
- CSRF vulnerability.
- LAB for participants to complete.

Session #6: Multi-stage Exercise Summarizing the Advanced Module of the Course:

- Exploitation of several vulnerabilities.
- Bypassing filters/WAF.
- Exploiting security issues in classic applications and REST APIs.