Pattern Recognition
and Applications Lab

Advanced Web Security

Faculty of Engineering

Ph.D. Program In Electronic and Computer Engineering

Lecturer: Dott. Lorenzo Pisu - lorenzo.pisu[at]unica[dot]it

Language: English

Target students:

Ph.D. Students (DRIEI)

National Ph.D. Students

Master's Degree Students in Computer Engineering, CyberSecurity, and Artificial Intelligence

Master's Degree Students in Internet Engineering

Master's degree Students in Electronic Engineering

The goal of the course.

Web security encompasses a set of practices, technologies, and measures designed to protect websites, web applications, and web users from various online threats. The primary goal of web security is to ensure the confidentiality, integrity, and availability of information exchanged and stored on the internet. This course offers a comprehensive exploration of advanced vulnerabilities impacting web applications, illustrated through practical examples. In the first week, we focus on the main attacks and protections concerning client-side technologies. In the second week, we provide an overview of server-side vulnerabilities along with the many different frameworks, technologies and languages involved.
The course will employ a game-based approach, where students will consolidate the topics through challenges taken from the world of capture-the-flag (CTF) and online training platforms.

Requirements.
None, but the seminar is especially recommended for students who have already completed the course "Web Security and Malware Analysis."

Topics:

- 8 hours – Client-Side Vulnerabilities - Practice Exercises
- 8 hours – Server-Side Vulnerabilities - Practice Exercises

Detailed Table of Contents:

Week 1 - Client-Side Vulnerabilities:

- Cross-Site Scripting (XSS) (Universal, Reflected, Stored, DOM-Based)
- JavaScript Prototype Pollution
- Same-Origin Policy (SOP)
- Cross-Origin Resource Sharing (CORS)
- SameSite
- Content-Security Policy (CSP)
- Iframe Sandbox
- Cross-Site Leaks (XS-Leaks)
- Document Object Model (DOM Clobbering)
- Cross-Site Request Forgery (CSRF)
- Clickjacking
- Cascading Style Sheets (CSS) Injection
- Open Browser Bugs
- Practice excercises

Week 2 - Server-Side Vulnerabilities:

- Server-Side Request Forgery (SSRF)
- XML External Entities (XXE)
- Request Smuggling
- Deserialization Vulnerabilities
- File Upload Vulnerabilities
- Race Conditions
- NoSQL injection (MongoDB, GraphQL)
- Server-Side Template Injection
- Practice exercises

Credits: 2 for Ph.D. Students and 1 for Master's Degree Students. The credits will be given after having passed a final test.

Registrations for the seminar are open, and the course will start on February 19th, 2024. Lectures will be provided in person and online (online participation is reserved ONLY for students unable to attend in person). To register, please fill out this form by February 16th, 2024:

https://forms.office.com/e/BYtF8AnPnn

Important Dates and Seminar Schedule (2024):

The seminar will be held on February 19th, 23rd, 26th and March 1st.

Time: 9:00 to 13:00 (4 hours lecture/day)

Location: Room B0 for all lectures except for the 23rd (LIDIA Software)