TRAINING

Binary House provides security training tailored to developers, IT engineers, and employees with access to sensitive information.

These trainings help attendees understand not only various security principles, but also vulnerabilities, their detection, and subsequent prevention.

Trainings can take place in your company or at our premises. During the initial discussion, we will ascertain your needs and prepare a non-binding offer along with the training content.

A brief overview of covered topics:

- Testing tools
- Insecure user access points
- Bad authentication and authorization implementation (SAML, JWT, Oauth)
- Component configuration problems
- Session management
- Cryptography
- Etc.

Course duration: 1 to 2 days

WEB APPLICATION SECURITY

This intensive technical course is designed for web application developers and testers. The provided study materials are based on the experience of the instructors and are compatible with the OWASP Top 10 security project. During the course, we analyse the general vulnerabilities found among various programming languages. Course participants learn about the most common vulnerabilities in web applications through hands-on laband practical exercises on virtual computers. The exercises and presentations are stored on a USB key that participants receive during the initial training phase.

Course objective

The main objective is to help developers clarify secure programming techniques in practice. After completing the course, participants can develop applications more securely, and retrospectively identify and eliminate covered problems.

MOBILE APPLICATION SECURITY

This intensive technical course is designed for mobile app developers and testers. The provided study materials are based on the experience of the instructors and are compatible with the OWASP Top 10 Mobile Risks security project. Course participants learn about the most common vulnerabilities in mobile applications. During the training, we use practical exercises with vulnerable applications. These exercises and presentations are stored on a USB key that participants receive during the initial training phase.

Course objective

The main objective is to help developers clarify secure programming techniques in practice. After completing the course, participants can develop applications more securely, and retrospectively identify and eliminate covered problems.

A brief overview of covered topics:

- Modeling threats on mobile devices
- iOS and Android platform particularities
- API interface vulnerabilities
- Method of data storage
- Bad implementation of authentication and authorization
- Cryptography and secure communication
- Etc.

Course duration: 2 to 3 days

CUSTOM TRAINING

Our employees have several years of experience in many IT security areas. The areas below are not a comprehensive listing. If you are interested in other IT security topics, please contact us.

Possible areas of training:

- Penetration testing
- Security awareness for employees
- Cryptography

Course duration: by agreement