Основные уязвимости в безопасности WEB приложений

Код: SECR-010

Длительность: 24 ч.

Описание:

Основу курса составляют детальное описание и практические задания по наиболее популярными современными уязвимостями OWASP Top-10 2017. Участники курса изучат способы их идентификации статически (включая SAST) и динамически (включая DAST), а также надежными методами устранения уязвимостей.

Слушателям будут представлены примеры кода, содержащего уязвимости, на нескольких языках программирования (Java, PHP, .NET, Python, JS). Также будут предложены «живые» приложения, которые позволят понять принципы работы уязвимостей и научиться самостоятельно их находить.

Курс разработан и проводится специалистами-практиками с опытом работы в Application Security более 8 лет. Знания, передаваемые участникам курса многократно проверены на «боевых» проектах и являются основой безопасной разработки приложений.

Цели:

После обучения участник сможет избегать уязвимости OWASP Top-10 при разработке веб-приложений и находить их статическими и динамическими методами в уже написанном коде/конфигурации.

Разбираемые темы:

- Что такое Application Security, зачем и как это делать (0,5 ч теория).
- Обзор OWASP TOP 10 (0,5 ч теория).
- A1:2017-Injection (1 ч теория + 2 ч практика).
- A2:2017-Broken Authentication (1 ч теория + 1 ч практика).
- A3:2017-Sensitive Data Exposure (1 ч теория + 1 ч практика).
- A4:2017-XML External Entities (XXE) (1 ч теория + 1 ч практика).
- A5:2017-Broken Access Control (1 ч теория + 1 ч практика).
- A6:2017-Security Misconfiguration (0,5 ч теория + 1 ч практика).
- A7:2017-Cross-Site Scripting (XSS) (2 ч теория + 2 ч практика).
- A8:2017-Insecure Deserialization (1 ч теория + 1 ч практика).
- A9:2017-Using Components with Known Vulnerabilities (0,5 ч теория + 0,5 ч практика).

- A10:2017-Insufficient Logging&Monitoring (0,5 ч теория + 0,5 ч практика).
- A8:2013-Cross-Site Request Forgery (CSRF) (0,5 ч теория + 1 ч практика).
- Выходное тестирование (1 ч.).

Целевая аудитория:

- Разработчики, Старшие разработчики;
- Специалисты по тестированию;
- Специалисты по безопасности;
- Архитекторы веб-приложений.

Предварительная подготовка – общее:

Участники курса должны уметь работать с веб-браузером, читать и писать код современных веб-приложений и понимать их основные принципы работы: HTTP, Cookies, Proxies.