

[WAPT]

# [Оглавление]

## ✓ Введение в курс

В данном разделе вы узнаете, о чем наш курс, поймете к чему придете по завершению курса.

## ✓ Подготовка рабочего окружения

В разделе будет описана подготовка операционной системы для работы и основные моменты по работе со средой.

## ✓ Общая теория

В этой главе вы узнаете, что такое пентест и аудит информационных систем, рассмотрите основные этапы пентеста по различным методологиям. Вспомните основы механизмов взаимодействия web, основы сетевого взаимодействия. Также будут рассмотрены различные классификаторы уязвимостей, будет проведен экскурс в мир хакинга. Дополнительно будут рассмотрены основы компьютерной вирусологии, типы распространения вирусов, виды нагрузок.

## ✓ Пассивный фаззинг и фингерпринт

Раздел расскажет основные методы пассивного фаззинга, а именно сбора информации с DNS, сбора файлов и директорий, анализа сертификатов, сбора информации о сервере и службах.

## ✓ Активный фаззинг

В данном разделе будут рассмотрены активные методы сбора информации и целевом ресурсе.

## ✓ Уязвимости

В разделе рассмотрены основные типы уязвимостей web приложений, приведены примеры и представлены практические задания.

### ▪ Инъекции

Основной тип уязвимостей на сегодняшний день. Вы узнаете, что такое SQL, SSTI, XXE, CMD, PHP инъекции, научитесь их выявлять и эксплуатировать. Также будут рассмотрены методики обхода web application firewall.

### ▪ Уязвимые компоненты

Раздел расскажет об уязвимостях компонентов web окружения.

### ▪ Обход авторизации

Формы авторизации один из способов проникновения на Web ресурс, в разделе вы узнаете техники обхода авторизации, эксплуатации уязвимостей, основы брутфорса учетных данных.

### ▪ **Мисконфигурейшены**

Неправильная настройка Web приложений может привести к плачевным последствиям. В разделе будут рассмотрены основные векторы атак, приведены примеры их эксплуатации.

### ▪ **Клиентские атаки**

В разделе рассмотрены основные виды клиентских атак, а такие как Clickjacking, XSS, CSRF будут расписаны более подробно, вы научитесь эксплуатации подобных атак, поймете пользу от них.

### ▪ **Системные уязвимости**

Уязвимости серверных операционных систем являются одним из методов проникновения, в данном разделе такие уязвимости будут описаны, приведены примеры их использования.

### ▪ **SSRF**

Server-Side Request Forgery (SSRF) – достаточно обширная уязвимость в плане дальнейших возможностей, в данном разделе этот тип уязвимостей будет разобран, включая различные частные случаи к примеру XSPA.

## ✓ **Пост-эксплуатация**

В разделе будут разобраны методики закрепления в скомпрометированном сервере web приложения, разобраны основные способы повышения привилегий.

## ✓ **Social Engineering**

Социотехническое тестирование является неотъемлемой частью современного пентеста. В разделе будут рассмотрены основные методы такого метода пентеста.

## ✓ **Площадки для практики**

Раздел расскажет о площадках, где можно безнаказанно применить и развить ваши новые навыки, приобретенные в ходе прохождения курса.

## ✓ **Сертификация и литература**

[Служба Поддержки](#)

[8-800-707-5466](#)

с 8:00 до 20:00 по мск

[school@codeby.net](mailto:school@codeby.net)