

Специалист по информационной безопасности: веб-пентест

Продолжительность - 6 месяцев

00

Сетевые основы
и клиент-серверные
технологии

40 часов

01

Принципы работы
веб-приложений

1 неделя, (20 часов)

02

Анализ защищенности
веб-приложений

12 недель, (240 часов)

03

Основы безопасной
разработки
веб-приложений

3 недели, (60 часов)

04

Контейнеризация,
Cloud и DevSecOps

2 недели, (40 часов)

05

Правовые аспекты,
документирование
и отчетность

1 недели, (20 часов)

Подарочный
модуль

40 часов

Сетевые основы и клиент-серверные технологии

Подготовьтесь к курсу: Изучите материалы по основам сетей, верстки HTML, CSS, JS, API, криптографии, а также темы “Базы данных” и “Регулярные выражения”.

Спринт 0

Введение. Знакомство

Тема 1. Основы сетей

1. Модель TCP/IP и OSI
2. DNS сервер
3. Прокси сервер

Тема 2. Клиент-серверная архитектура: основные понятия

1. Клиент-серверная архитектура. Введение
2. Веб-сервер: принципы работы
3. Браузер: принципы работы
4. Базы данных: принципы работы
5. Базы данных: основы SQL и NoSQL
6. Работа с основными веб-серверами Nginx, Apache
7. WebSocket: принципы работы
8. API и его роль в современных приложениях
9. Криптография: протоколы шифрования, хэширования и кодирования данных
10. Клиент-серверная архитектура. Заключение

01

1 неделя,
(20 часов)

Принципы работы веб приложений

Познакомьтесь с базовыми принципами работы веб-приложений (протоколами HTTP и заголовками в веб-приложениях). Узнайте какие направления в информационной безопасности существуют и чем занимаются специалисты по тестированию на проникновение.

Спринт 1

2 недели

Принципы работы веб-приложений

Тема 1. Введение в тестирование на проникновение в веб-приложениях

1. Web-penetration testing. Введение
2. Чем занимается специалист в области Web-penetration testing
3. Цели, которые ставит перед собой специалист в области Web-penetration testing
4. Направления в информационной безопасности: AppSec, Redteam, BlueTeam, PurpleTeam, Cyber Intelligence
5. Web-penetration testing. Заключение

Тема 2. Принципы работы протокола HTTP

1. Протокол HTTP. Введение
2. Метод HTTP запросов
3. Request и Response: основные понятия
4. Основные коды ответа от веб-сервера
5. Протоколы HTTP и заголовки в веб-приложениях. Заключение

Тема 3. Подготовка окружающей среды для проведения веб-пентеста

Подготовка среды

Практика

Тест с пометкой зачет/незачет – проверяем, что все знают основные понятия и темы, с которыми столкнутся в программе.

02

12 недель,
(240 часов)

Спринт 2

3 недели

Анализ защищенности веб-приложений

Рассмотрите все этапы проведения веб-пентеста и научитесь искать, эксплуатировать и не допускать уязвимости.

Виды тестирования, классификация уязвимостей и этапы разведки

Тема 1. Тестирование: типы, этапы и методологии

1. Тестирование. Введение
2. Виды тестирования: BlackBox, WhiteBox и GreyBox
3. Основные этапы тестирования на безопасность веб-приложений
4. Методологии и чек-листы тестирования OWASP.
5. Стандарты классификаций уязвимостей: CWE, CVE, CVSS, EPSS
6. Тестирование. Заключение

Тема 2. Безопасность веб-приложений: инструменты тестирования

1. Инструменты тестирования. Введение
2. Автоматизированные инструменты тестирования на безопасность веб-приложений: SonarQube, Nessus, Trivy, MobSF, Dependency check
3. Ручные инструменты тестирования на безопасность веб-приложений: Owasp ZAP, Burp Suite, Metasploit
4. Применение нейросетей для анализа защищенности веб-приложений
5. Инструменты тестирования. Заключение

Тема 3. Reconnaissance and Mapping: инвентаризация внешнего периметра

(Методы проведения активной и пассивной разведки)

1. Этап разведки. Введение
2. Поиск поддоменов
3. Поиск веб-сервисов, баз данных и сторонних компонентов
4. Поиск параметров
5. Поиск скрытых файлов
6. Анализ JavaScript файлов
7. Поиск в GitHub
8. Пассивный сбор данных: Shodan и Censys и др.
9. Этап разведки. Заключение

Спринт 3

3 недели

Основные веб-уязвимости и работа с ними. Часть 1

Тема 1: XSS-уязвимость: Stored, Reflected, DOM

1. XSS-уязвимость. Введение
2. Что такое XSS-уязвимости и как их искать
3. Как эксплуатировать и не допускать XSS-уязвимости
4. XSS-уязвимости. Заключение

Тема 2: Уязвимость Cross Site Request Forgery

1. Уязвимость Cross Site Request Forgery. Введение
2. Что такое уязвимость Cross Site Request Forgery и как их искать
3. Как эксплуатировать и не допускать уязвимость Cross Site Request Forgery
4. Уязвимость Cross Site Request Forgery. Заключение

Тема 3: Уязвимость Broken Access Control

1. Уязвимость Broken Access Control. Введение
2. Что такое уязвимость Broken Access Control и как их искать
3. Как эксплуатировать и не допускать уязвимость Broken Access Control
4. Уязвимость Broken Access Control. Заключение

Тема 4: Уязвимость File upload vulnerabilities

1. Уязвимость File upload vulnerabilities. Введение
2. Что такое уязвимости типа File upload vulnerabilities и как их искать
3. Как эксплуатировать и не допускать уязвимости типа File upload vulnerabilities
4. Уязвимости типа File upload vulnerabilities. Заключение

Тема 5: SQL-инъекции

1. Уязвимость типа SQL-инъекция. Введение
2. Что такое уязвимости типа SQL-инъекция и как их искать
3. Как эксплуатировать и не допускать уязвимости типа SQL-инъекция
4. Уязвимости типа SQL-инъекция. Заключение

Практика

Проект-стенд с несколькими уязвимостями, где участникам курса нужно их найти и эксплуатировать.

Спринт 4

2 недели

Основные веб-уязвимости и работа с ними. Часть 2

Тема 1. Уязвимость ХХЕ

Урок 1. ХХЕ-уязвимость. Введение

Урок 2. Что такое ХХЕ-уязвимости и как их искать

Урок 3. Как эксплуатировать и не допускать ХХЕ-уязвимости

Урок 4. ХХЕ-уязвимости. Заключение

Тема 2. Небезопасная десериализация

1. Небезопасная десериализация. Введение

2. Что такое небезопасная десериализация и как ее искать

3. Как эксплуатировать и не допускать Небезопасную десериализацию

4. Небезопасная десериализация. Заключение

Тема 3. Уязвимость Server Sire Request Forgery

1. Уязвимость Server Sire Request Forgery. Введение

2. Что такое уязвимость Server Sire Request Forgery и как их искать

3. Как эксплуатировать и не допускать уязвимость Server Sire Request Forgery

4. Уязвимость Server Sire Request Forgery. Заключение

Тема 4. Уязвимость Race Condition

1. Уязвимость Race Condition. Введение

2. Что такое уязвимость Race Condition и как их искать

3. Как эксплуатировать и не допускать уязвимость Race Condition

4. Уязвимость Race Condition. Заключение

Тема 5. Уязвимости бизнес логики

1. Уязвимость бизнес логики. Введение

2. Что такое уязвимости бизнес логики и как их искать

3. Как эксплуатировать и не допускать уязвимости бизнес логики

4. Уязвимости бизнес логики. Заключение

Практика

Проект-стенд с несколькими уязвимостями, где участникам курса нужно их найти и эксплуатировать, а после передать флаги (ответы) нам.

Спринт 5

2 недели

Ошибки авторизации и аутентификации

**Тема 1: Авторизация и аутентификация:
что это и как работает**

1. Авторизация и аутентификация. Введение
2. Основные способы использования авторизаций и аутентификаций в веб-приложениях
3. Основные правила работы сеансов в веб-приложениях
4. Авторизация и аутентификация. Заключение

Тема 2: Основные уязвимости авторизации и аутентификации

1. Основные уязвимости авторизации и аутентификации. Введение
2. Basic Auth: принципы работы и связанные с ней уязвимости
3. OAuth: принципы работы и связанные с ней уязвимости
4. JWT: принципы работы и связанные с ней уязвимости
5. Мультифакторная аутентификация (2fa): принципы работы и связанные с ней уязвимости
6. SSO: принципы работы и связанные с ней уязвимости
7. Основные уязвимости авторизации и аутентификации. Заключение

Практика

Участникам курса даны несколько разных форм авторизации, на которых развернуты уязвимости. Им нужно найти и проэксплуатировать эти уязвимости, а также передать найденные флаги и подготовить отчет о проделанной работе.

Спринт 6

2 недели

Основные уязвимости API

Тема 1: Уязвимости API. Часть 1

1. Уязвимости API. Часть 1. Введение
2. Broken object level authorization: что это такое и как с этим работать
3. Broken authentication: что это такое и как с этим работать
4. Broken object property level authorization: что это такое и как с этим работать
5. Unrestricted resource consumption: что это такое и как с этим работать
6. Broken function level authorization: что это такое и как с этим работать
7. Уязвимости API. Часть 1. Заключение

Тема 2: Уязвимости API. Часть 2

1. Уязвимости API. Часть 2. Введение
2. Unrestricted Access to Sensitive Business Flows: что это такое и как с этим работать
3. Server side request forgery: что это такое и как с этим работать
4. Improper inventory management: что это такое и как с этим работать
5. Unsafe consumption of API: что это такое и как с этим работать
6. Уязвимости API. Часть 2. Заключение

Практика

Участникам курса даны несколько разных API, на которых развернуты уязвимости. Им нужно найти и проэксплуатировать эти уязвимости, а также передать нам флаги и подготовить отчет о проделанной работе.

03

3 недели,
(60 часов)

Основы безопасной разработки веб-приложений

Данный модуль познакомит и научит вас принципам безопасной разработки и безопасного хранения данных.

Спринт 7

3 недели

Тема 1: Принципы дизайна безопасной разработки и требования для разработки веб-приложений

1. Принципы дизайна безопасной разработки. Введение
2. Концепция разработки Security by Design
3. Методология минимальных привилегий: основные понятия
4. Обработка пользовательского ввода
5. Управление пользовательской сессией
6. Управление зависимостями
7. Тестирование безопасности кода (CI/CD)
8. Принципы дизайна безопасной разработки. Заключение

Тема 2. Принципы хранения секретов в базах данных

1. Принципы хранения секретов в базах данных. Введение
2. Основные правила для работы с базами данных
3. Основные способы хранения конфиденциальных данных в базах данных
4. Лучшие практики работы с секретами
5. Принципы хранения секретов в базах данных. Заключение

Проект

Проект в портфолио по теме спринта.

04

3 недели,
(60 часов)

Спринт 8

3 недели

Контейнеризация, Cloud и DevSecOps

Узнаете, как правильно хранить данные в контейнерах и в облаках.

Тема 1: Контейнеризация: развертывание веб-приложений в контейнерах

1. Контейнеризация. Введение
2. Контейнеризации: определение и ее роль в разработке веб-приложений
3. Инструменты контейнеризации: Docker, Kubernetes
4. Контейнеризация: преимущества и недостатки
5. Создание контейнеров для веб-приложений с использованием Docker
6. Развертывание контейнеризованных веб-приложений в облачных платформах на примере Яндекс облака
7. Обеспечение безопасности контейнеризованных веб-приложений: контроль доступа, управление конфигурацией и мониторинг
8. Контейнеризация. Заключение

Тема 2: Облачные технологии в веб-приложениях и их безопасность.

1. Облачные технологии. Введение
2. Основы облачных технологий и их роль в веб-разработке
3. Архитектура облачных сред и принципы их безопасности
4. Уязвимости облачной инфраструктуры: анализ
5. Подходы к оценке и обеспечению безопасности серверов и хранилищ данных в облаке
6. Тестирование безопасности в облачных средах: методы и инструменты
7. Разработка безопасной архитектуры и настройка облачных ресурсов
8. Облачные технологии. Заключение

Тема 3. DevSecOps: основные понятия, принципы и инструменты

1. DevSecOps. Введение
2. Основные принципы DevSecOps и их роль в безопасной разработке веб-приложений
3. Инструменты и практики DevSecOps в облачных средах: политика доступа, логирование и отслеживание угроз
4. Интеграция безопасности при контейнеризации и развертывании в облаке
5. Автоматизация проверок безопасности контейнеров и веб-приложений: использование CI/CD пайплайнов
6. DevSecOps. Заключение

Проект

Участникам курса дана облачная инфраструктура, где развернуто несколько уязвимостей. Им нужно найти и проэксплуатировать эти уязвимости, а также передать флаги и подготовить отчет о проделанной работе.

05

3 недели,
(60 часов)

Спринт 9

3 недели

Правовые аспекты, документирование и отчетность

Познакомьтесь с правовыми аспектами и законами по использованию и хранению данных, а также научитесь составлять отчеты и документировать свою деятельность.

Тема 1. Пентест: основные правовые аспекты профессии

1. Основные правовые аспекты профессии. Введение
2. Что нужно знать пентестеру: правовые нормы РФ в сфере информационной безопасности
3. Что нужно знать: основные законы в пентесте
4. GDPR: основные правовые нормы
5. Основные правовые аспекты профессии. Заключение

Тема 2. Пентест: документирование и отчетность

1. Документирование и отчетность. Введение
2. Подготовка отчета по найденным уязвимостям: подходы и принципы
3. Формирование тикетов для разработчиков
4. Как контролировать устранение уязвимости
5. Заключение

Проект

Финальная практика

Итоговый проект

3 недели

50 часов

Итоговый проект: полный аудит безопасности

Проведение полного аудита безопасности: выявление уязвимостей и выдача рекомендаций по их устранению/эксплуатации.

Вам дана сеть и с двумя хостами. Нужно провести полный аудит этих хостов, а именно:

- провести разведку с использованием изученных инструментов;
- найти и проэксплуатировать уязвимость, найти флаги;
- подготовить отчет о проведенном тестировании;
- подготовить рекомендации по доработке.

Вебинары

Вебинары проводятся регулярно, их количество зависит от модуля. Они посвящены нюансам работы, инструментам веб-пентестера, ответам на возникающие вопросы. Часть воркшопов будут практическими в формате CTF, где участники курса делятся на команды и в реальном времени пытаются взломать веб-приложения и получить флаги, чтобы заработать рейтинговые очки.

Программа трудоустройства

Программа становится доступна в конце курса. В ней расскажем о том, как правильно составить резюме, создать портфолио и сделать свой отклик заметнее с помощью сопроводительного письма.

Также обсудим процесс подготовки к собеседованию: на какие софт-скиллы и хард-скиллы сделать фокус.