Яндекс Практикум

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 обучению: Пройдите уроки по основам сетей, вертки HTML, CSS, JS, API, криптографии, а также изучите темы “Базы данных” и “Регулярные выражения”.

Спринт 0

Введение. Знакомств

Тема 1. Основы сетей

Урок 1. Модель TCP\IP и OSI.

Урок 2. DNS сервер.

Урок 3. Прокси сервер.

Тема 2. Клиент-серверная архитектура: основные понятия.

Урок 1. Клиент-серверная архитектура. Введение.

Урок 2. Веб-сервер: принципы работы.

Урок 3. Браузер: принципы работы.

Урок 4. Базы данных: принципы работы.

Урок 5. Базы данных: основы SQL и NoSQL

Урок 6. Работа с основными веб-серверами Nginx, Apache.

Урок 7. Websocket: принципы работы.

Урок 8. API и его роль в современных приложениях

Урок 9. Криптография: протоколы шифрования, хэширования и кодирования данных.

Урок 10. Клиент-серверная архитектура.

Заключение.

01

1 неделя,
(20 часов)

Принципы работы веб приложений

Познакомитесь 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.

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

Тема 2. Принципы работы протокола HTTP

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

Тема 3. Подготовка окружающей среды для проведения веб-пентеста

Урок. Подготовка среды

Практика

Задание тест с пометкой зачет/не зачет – проверяем, что все знают основные понятия и темы, с которыми столкнутся в программе.

02

12 недель,
(240 часов)

Анализ защищенности веб-приложений

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

Спринт 2

3 недели

Виды тестирования, классификация уязвимостей и этапы разведки

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

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

Тема 3. Reconnaissance and Mapping: инвентаризация внешнего периметра
(Методы проведения активной и пассивной разведки)
Урок 1. Этап разведки. Введение.
Урок 2. Поиск поддоменов.
Урок 3. Поиск веб-сервисов, баз данных и сторонних компонентов .
Урок 4. Поиск параметров.
Урок 5. Поиск скрытых файлов
Урок 6. Анализ JavaScript файлов.
Урок 7. Поиск в GitHub.
Урок 8. Пассивный сбор данных: Shodan и Censys и др.
Урок 9. Этап разведки.
Заключение.

Спринт 3

3 недели

Основные веб-уязвимости и работа с ними. Часть 1

Тема 1: XSS-уязвимость: Stored, Reflected, DOM
Урок 1. XSS-уязвимость. Введение
Урок 2. Что такое XSS-уязвимости и как их искать
Урок 3. Как эксплуатировать и не допускать XSS-уязвимости
Урок 4. XSS-уязвимости.
Заключение.

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

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

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

Тема 5: SQL-инъекции
Урок 1. Уязвимость типа SQL-инъекция. Введение
Урок 2. Что такое уязвимости типа SQL-инъекция
и как их искать
Урок 3. Как эксплуатировать и не допускать уязвимости типа
SQL-инъекция
Урок 4. Уязвимости типа SQL-инъекция.
Заключение

Практика

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

Спринт 4

2 недели

Основные веб-уязвимости и работа с ними. Часть 2

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

Тема 2. Небезопасная десериализация
Урок 1. Небезопасная десериализация. Введение
Урок 2. Что такое небезопасная десериализация
и как ее искать
Урок 3. Как эксплуатировать и не допускать Небезопасную
десериализацию
Урок 4. Небезопасная десериализация.
Заключение

Тема 3. Уязвимость Server Sire Request Forgery
Урок 1. Уязвимость Server Sire Request Forgery. Введение
Урок 2. Что такое уязвимость Server Sire Request Forgery
и как их искать
Урок 3. Как эксплуатировать и не допускать уязвимость Server
Sire Request Forgery
Урок 4. Уязвимость Server Sire Request Forgery.
Заключение.

Тема 4. Уязвимость Race Condition
Урок 1. Уязвимость Race Condition. Введение
Урок 2. Что такое уязвимостб Race Condition и как их искать
Урок 3. Как эксплуатировать и не допускать уязвимость
Race Condition
Урок 4. Уязвимость Race Condition.
Заключение.

Тема 5. Уязвимости бизнес логики
Урок 1. Уязвимость бизнес логики. Введение
Урок 2. Что такое уязвимости бизнес логики и как их искать
Урок 3. Как эксплуатировать и не допускать уязвимости
бизнес логики
Урок 4. Уязвимости бизнес логики.
Заключение

Практика

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

Неделя доработок

Спринт 5

2 недели

Ошибки авторизации и аутентификации

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

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

Тема 2: Основные уязвимости авторизации и аутентификации

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

Практика

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

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

Практика

Студентам 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.

Неделя доработок

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

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

Проект

Учебный проект по теме спринта.

04

3 недели,
(60 часов)

Контейнеризация, Cloud и DevSecOps

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

Спринт 8

3 недели

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

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

Тема 3. DevSecOps: основные понятия, принципы и инструменты.

Урок 1. DevSecOps. Введение

Урок 2. Основные принципы DevSecOps и их роль в безопасной разработке веб-приложений.

Урок 3. Инструменты и практики DevSecOps в облачных средах: политика доступа, логирование и отслеживание угроз

Урок 4. Интеграция безопасности при контейнеризации и развертывании в облаке

Урок 5. Автоматизация проверок безопасности контейнеров и веб-приложений: использование CI/CD пайплайнов.

Урок 6. DevSecOps. Заключение

Проект

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

05

3 недели,
(60 часов)

Правовые аспекты, документирование и отчетность

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

Спринт 9

3 недели

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

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

Проект

Финальная практика

Итоговый проект

3 недели

50 часов

Диплом: 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.

Яндекс Практикум

Вебинары

Вебинары проводятся регулярно, их количество зависит от модуля. Они посвящены нюансам работы, инструментам веб-пентестера, ответам на возникающие входе обучения вопросы. Часть воркшопов будут практическими в формате CTF, где студенты 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 обучения. 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.