

Кибербезопасность: веб-пентест

01	Кому подойдёт курс	- Разработчикам - DevOps-специалистам - Сетевым инженерам - Системным администраторам - Тем, у кого небольшой опыт в кибербезопасности Что нужно знать: - Основы сетевых и веб-технологий - Основы программирования - Архитектуру современных веб-приложений - Основы работы с операционными системами Windows, macOS и Linux
02	Чему научитесь на курсе Какие знания и навыки освоите	- Использовать методики безопасной разработки ПО - Использовать методики и инструменты для идентификации уязвимостей - Анализировать уязвимости и тестировать приложения на проникновение - Пользоваться инструментами тестирования: Burp Suite, SQLMap - Пользоваться Docker, Kubernetes, DevSecOps и развёртыванием в облаке - Находить уязвимости OWASP Top 10 и другие - Эффективно управлять секретами для предотвращения утечек - Применять инструменты и методики DevSecOps
03	Как проходит курс	- Теория на платформе Практикума - Практика на индивидуальных стендах, развёрнутых в облаке - Доступ из любой точки мира в удобное время - Воркшопы и вебинары с опытными наставниками - Практические проекты, приближенные к реальности

Что вас ждёт

Документ о полном прохождении курса	Практика, основанная на решении реальных рабочих задач	Программа от экспертов из Яндекса и других крупных компаний
-------------------------------------	--	---

Кибербезопасность: веб-пентест

Сравнение тарифов

	Базовый тариф	Расширенный тариф	Индивидуальный тариф
Длительность	4 месяца	6 месяцев	6 месяцев
Количество проектов	7 проектов без обратной связи	8 проектов с обратной связью	8 проектов с обратной связью
Наставник	✓	✓	✓
Основы безопасной разработки	✗	✓	✓
Контейнеризация и Cloud	✗	✓	✓
DevSecOps	✗	✓	✓
8 личных консультаций по 45 минут	✗	✗	✓
Нагрузка	10–20 часов в неделю	10–20 часов в неделю	10–20 часов в неделю



Кибербезопасность: веб-пентест

4 или 6 месяцев

продолжительность курса

7 или 8 проектов

с обратной связью

Базовый, расширенный и индивидуальный тарифы

3 НЕДЕЛИ 01 Разведка в веб-приложениях	10 НЕДЕЛЬ 02 Анализ защищённости веб-приложений	2 НЕДЕЛИ 03 Правовые аспекты, документирование и отчётность	4 НЕДЕЛИ 04 Итоговый проект: полный аудит безопасности
40 ЧАСОВ ★ Факультативный курс. Инфраструктура и архитектура: основы			

Только расширенный и индивидуальный тарифы

2 НЕДЕЛИ 05 Основы безопасной разработки веб-приложений	4 НЕДЕЛИ 06 Контейнеризация, Cloud и DevSecOps
--	---

3 недели
1 проект

Узнаете, какие виды и методологии тестирования бывают. Настроите тестовую среду — создадите виртуальную машину с Kali Linux. Узнаете, как проводить разведку и какие инструменты использовать на каждом этапе.

Содержание

Темы	Финальный проект 1 спринта
1. Как устроен курс	Освоите ключевые приёмы разведки: фаззинг параметров, брутфорс директорий, анализ хостов и поиск скрытых точек входа. Научитесь собирать данные о системе для подготовки к тестированию безопасности веб-сервисов.
2. Тестирование: виды, этапы и методологии	
3. Инструменты веб-пентеста	
4. Как проводить разведку	

10 недель
4 проекта

Содержание

Темы	Финальный проект 2 спринта
1. Авторизация и аутентификация	Проведёте оценку защищённости веб-приложения и выявите самые популярные уязвимости: XSS, SQL инъекции и уязвимости в механизмах контроля доступа. Научитесь находить подходы к выявлению и эксплуатации ошибок, которые разработчики часто упускают из виду.
2. XSS — Cross-site scripting	
3. CSRF — Cross-site Request Forgery	Финальный проект 3 спринта
4. BAC — Broken Access Control	
5. SQL Injection	Найдёте уязвимости на уровне инфраструктуры: отрабатывайте атаки через XXE, SSRF и LFI. Получите доступ к скрытым данным и исследуйте ошибки в обработке внешних ресурсов.
6. SSRF – Server Sire Request Forgery	
7. XXE – XML External Entity	Финальный проект 4 спринта
8. Уязвимости бизнес-логики	
9. Race Condition	Проанализируете и сломаете механизмы аутентификации: выполните перебор учётных данных, обойдёте многофакторную защиту и изучите векторы атак на JWT токены. Разберётесь в слабостях, которые часто игнорируют разработчики.
10. Небезопасная десериализация	
11. File Upload vulnerabilities	Финальный проект 5 спринта
12. SSTI	
13. Механизмы аутентификации	
14. Механизмы управления доступом	Погрузитесь в тестирование API, найдёте ошибки в авторизации, недостатки проверки уровней доступа и слабости в бизнес-логике. Изучите популярные уязвимости, такие как BOLA, IDOR и другие, в реальной практике.
15. Основные уязвимости API	

Правовые аспекты, документирование и отчётность

03

2 недели
1 проект

Познакомитесь с правовыми нормами в сфере информационной безопасности, что позволит вам правильно ориентироваться в юридических аспектах этой сферы деятельности. Изучите стандарты классификации уязвимостей и научитесь грамотно подготавливать отчёты по обнаруженным уязвимостям.

Содержание

Темы	Финальный проект 6 спринта
1. Основные правовые аспекты специальности	Составите детальный отчёт по итогам пентеста: опишете найденные уязвимости, их влияние на бизнес, используемые методологии и предложите рекомендации. Докажете, что вы не только умеете находить уязвимости, но и готовы работать с реальными проектами и заказчиками.
2. Документирование и отчётность	

Итоговый проект: полный аудит безопасности

04

4 недели
Итоговый проект: полный аудит безопасности

Комплексное упражнение для проверки изученного материала. Вы погрузитесь в полноценное black-box тестирование, самостоятельно выдвинете гипотезы, исследуете систему и найдёте уязвимости, связанные в сложные цепочки.



Факультативный курс. Инфраструктура и архитектура: ОСНОВЫ

40 часов
Доступно для изучения
в любое время

Подготовьтесь к основному курсу: повторите основы сетей и клиент-серверную архитектуру — закрепите принципы работы веб-серверов, браузера, баз данных, API и криптографии, а также протоколы HTTP, HTTPS и SSL/TLS.

Содержание

Темы

- 1. Основы сетей
- 2. Принципы передачи
и защиты данных: HTTP и HTTPS
- 3. Клиент-серверная архитектура



Вебинары и воркшопы

Вебинары и воркшопы проводятся один раз за спринт. Они посвящены нюансам веб-пентеста, ответам на вопросы и разбору наиболее трудных задач. На воркшопах вы сможете отработать полученные знания на практике и углубиться в тестирование веб-приложений.

Далее — модули только расширенного и индивидуального тарифов

Основы безопасной разработки веб-приложений

05

2 недели
1 проект

Содержание

Темы	Финальная практика 7 спринта
1. Принципы безопасной разработки 2. Хранение секретов в базах данных 3. Безопасность и CI/CD	Проанализируете сложные уязвимости: выполните NoSQL-инъекции, поэксплуатируете SSTI для удалённого выполнения команд и исследуете небезопасную десериализацию. Получите практический опыт в атаке сложных цепочек сценариев.

Контейнеризация, Cloud и DevSecOps

06

4 недели
1 проект

Содержание

Темы	Финальный проект 8 спринта
1. Контейнеризация 2. Облачные технологии	Исследуете уязвимости контейнеров и кластеров: найдёте ошибки в их настройке и выполните побег из контейнеров. Разберётесь в защите облачных и контейнерных инфраструктур на практике.

DevSecOps в облачном CI/CD

курс от Яндекс Облака

Темы
1. Введение и подготовка рабочего места 2. Настройка CI/CD-пайплайна и эксплуатация уязвимостей 3. Внедрение DevSecOps-инструментов в CI/CD-пайплайн 4. Визуализация работы DevSecOps-пайплайна, нейтрализация уязвимостей и итоги курса

Индивидуальные онлайн-встречи

Восемь встреч с наставниками, на которых вы сможете обсудить вопросы по курсу, личные проекты и получить ответы на любые интересующие вас темы в сфере автоматизации. Только в индивидуальном тарифе.
