Программа курса OWASP WSTG

#	Тема	Технологии, понятия	Тип занятия	Часы
1	Введение и цели	- Что такое тестирование на проникновение (пентестинг) - Что такое OWASP - Для чего организациям необходима эта услуга/компетенция - Какие бывают типы веб-сайтов/веб-приложений и чем отличаются - Из каких компонентов состоят веб-сайты/веб-приложения - Что такое уязвимость и угроза - Что такое тест	Лекция	2
2-3	Сбор информации	- Пассивная разведка - Активная развекда - Онлайн сервисы	Лекция	4
4	Тестирование управления конфигурацией и развертывания	- Тестирование конфигурации (сети и веб) - Энумерация - HTTP методы - Права доступа (разрешения) - Облачные хранилища - Полезные инструменты и сервисы	Лекция	2
5	Тестирование управления идентификацией	- Обзор процесса идентификации, аутентификации и авторизации, разбор последовательности - Роли - Процесс регистрации и тестирвания создания учетной записи - Изучение Developer Tools	Лекция	2
6-7	Тестирование аутентификации	- Передача данных - Частые проблемы и ошибки - Обход механизма аутентификации - Парольные политики - Изучение проблем со сменой пароля или сброса пароля - Изучение OWASP ZAP / BurpSuite	Лекция	4
8	Тестирование авторизации	- Обход авторизации - Повышение привилегий - Небезопасное прямое обращение к объектам - Изучение cURL	Лекция	2
9	Тестирование управления сессиями	- Управление сессий - Что такое куки и как с ними работать - Фиксация сессии - Время жизни сессии и перехват сессии	Лекция	2

10-12	Тестирование проверки ввода	- Обзор разных типов иньекций - Атаки на клиента - Атаки на сервер - Типы SQL иньекций - Другие типы иньекций - Работа с головой и телом запроса, исследование доступных параметров - Изучение вспомогательных иснтрументов для автоматизации	Лекция	6
13	Тестирование обработки ошибок	- Какие бывают типы ошибок - Что такое код ошибки - Что такое режим “Debug” и в чем отличие среды разработки от продуктовой	Лекция	1
	Тестирование слабого шифрования	- Протоколы и шифрование - Для чего в протоколах S (HTTPs, FTPs, и т.д.) - Типы атак	Лекция	1
14-15	Тестирование бизнес-логики	- Что такое бизнес логика - Валидация данных/операций - Проверки целостности - Варианты нецелевого использования приложений или функционала - Загрузка файлов	Лекция	4
16-17	Тестирование на стороне клиента	- Атаки с использованием HTML/CSS/JavaScript - Безопасные параметры заголовков - Манипуляция ресурсами пользователя - WebSockets - Хранилище браузера	Лекция	4
18	Изучение стандарта PTES и моделей злоумышленника	- Подход к выполнению процесса тестирования - Документирование - Какие бывают модели злоумышленников и чем отличаются - Требования регуляторов и модели злоумышленников	Лекция	2
19	Баг баунти, фриланс или работа в компании	- Разница подходов - Какие есть площадки и что нужно для регистрации - Что делать, если на чьем-то сайте нашли уязвимость/ошибку - Что нужно для того, чтобы начать зарабатывать - Немного про конкуренцию и рынок - Немного про финансы и налоги	Лекция	2

		- Обзор услуг, которые может оказывать начинающий пентестер		
20	Что такое OWASP TOP10	- Обзор 10 пунктов OWASP для веб приложений - Обзор 10 пунктов OWASP для API	Лекция	2
21-22	OWASP TOP10	- изучение 10 популярных типов угроз веб-приложений - Маппинг уязвимостей по TOP10 - Изучаем процесс репортинга	Лекция	4
23-24	Практические занятия: Лабораторная №1	- Настраиваем окружение (в т.ч. иструменты для работы) - Совместная работа в лаборатории - Обзор реальных кейсов	Практика	4
25-26	Практические занятия: Лабораторная №1	- Обратная связь - Проработка практических навыков и завершение лабораторной (повышение уровня сложности опционально)	Практика	4
27-28	Практическое занятие: Лабораторная №2	- Работа по тестированию - Дополнительно: упражнение по выполнению разведки	Практика	4
29-30	Практическое занятие: Лабораторная №2	- Обратная связь - Выполнение дополнительныъх задач по эксплуатации	Практика	4
31	Контрольное задание	Выполнение контрольного задания	Практика	4
32	Окончание курса	- Подводим итоги - Готовим резюме - Заполняем профиль в LinkedIn		3