Бауманский учебный центр «Специалист»

Программа курса Атака и защита веб - сайтов по OWASP Top 10

Код курса: **ОВАСП**

Тема	Ак. часов
Модуль 1. Концепции веб-сайтов • Принципы работы веб-серверов и веб-приложений. Принципы безопасности веб-сайтов и веб-приложений. Что такое OWASP. Обзор классификации OWASP Top 10 2025. Знакомство с инструментами учебной проверки. Использование ИИ-инструментов при анализе веб-приложений (вспомогательно). Настройка лаборатории. • **Практика:** запуск учебного сайта и подготовка окружения, с использованием ИИ-инструментов в процессе анализа учебного приложения. • **Результат:** слушатель ориентируется в классификации 2025 и имеет рабочий учебный стенд.	**1**
Модуль 2. Нарушение контроля доступа • Концепции и принципы нарушений контроля доступа. Административный портал; ограничение доступа к каталогам; обход каталога; небезопасная прямая ссылка на объект (iDOR); подключение файла (LFI/RFI); невалидированный редирект и форвард; подделка запросов на стороне сервера (SSRF). Способы защиты. Использование ИИ для выявления нарушений контроля доступа. • **Практика:** учебные задания по контролю доступа на учебном сайте и формулирование защиты. • **Результат:** слушатель находит типовые нарушения доступа на стенде и называет меры защиты.	**2**
Модуль 3. Небезопасная конфигурация • Принципы атак на конфигурацию. Примеры из программы: robots.txt; раскрытие информации; небезопасное хранение архивов; раскрытие Git; раскрытие Docker API; общие ресурсы в AJAX; CORS; небезопасная конфигурация FTP, WebDAV, SMB, SNMP; «человек посередине» в HTTP. • **Практика:** учебные задания по конфигурации учебного веб-сервера и защита. • **Результат:** слушатель выявляет типовые ошибки конфигурации на стенде.	**2**
Модуль 4. Атака на цепочку поставок • Концепции атак на цепочку поставок. Примеры из программы: CI/CD; переполнение буфера (локальное и удалённое); Log4Shell. Способы защиты. • **Практика:** учебные задания по цепочке поставок на учебном сайте и защита. • **Результат:** слушатель понимает риски поставки компонентов и типовые учебные сценарии этой категории.	**4**
Модуль 5. Криптографические уязвимости • Концепции криптографических дефектов. Примеры из программы: Base64 как «шифрование»; хранение данных в текстовых файлах, HTML5-хранилище и базах; передача учётных данных по HTTP; небезопасное управление ключами. Способы защиты. • **Практика:** учебные задания по криптографии на учебном сайте и защита. • **Результат:** слушатель отличает кодирование от криптозащиты и видит типовые ошибки хранения и передачи секретов.	**1**

Модуль 6. Инъекции • Понятие инъекции. XSS: отражённые и хранимые; XSS в запросах, JSON/AJAX/XML, записях, cookie, User-Agent; защита от XSS. SQL-инъекции: простые (ошибки, объединение), хранимые, слепые (логическая и временная основа); защита. Иные типы из программы: NoSQL, LDAP, XML, манипуляция HTTP-запросом, почтовые заголовки, SSI, PHP-код, команды ОС. Использование ИИ для защиты от инъекций. • **Практика:** учебные задания по инъекциям на учебном сайте и защита. • **Результат:** слушатель выявляет типовые инъекции на стенде и формулирует защиту.	**6**
Модуль 7. Небезопасный дизайн • Концепции небезопасного дизайна. Примеры из программы: валидация только на клиенте; небезопасное восстановление и сброс пароля; ошибки бизнес-логики; CSRF; clickjacking; XXE; небезопасная загрузка файлов. Защитные меры. • **Практика:** учебные задания по дизайну на учебном сайте и защита. • **Результат:** слушатель связывает ошибку проектирования с учебным сценарием и мерой защиты.	**2**
Модуль 8. Сбои аутентификации • Концепции и методы аутентификации. Форма входа; слабые пароли; перебор; универсальный пароль. Управление сеансом: cookie; предсказание идентификатора; фиксация сеанса; выход. Методы защиты. • **Практика:** учебные задания по аутентификации на учебном сайте и защита. • **Результат:** слушатель проверяет учебную аутентификацию и сеанс и называет защиту.	**2**
Модуль 9. Сбои в обеспечении целостности ПО и данных • Концепции целостности. Атаки на целостность портала. Сериализация и принцип атаки на десериализацию. Примеры из программы: обход аутентификации; инъекция бэкдора; атаки на целостность ПО. Способы защиты. • **Практика:** учебные задания по целостности на учебном сайте и защита. • **Результат:** слушатель понимает риск нарушения целостности кода и данных на учебном стенде.	**2**
Модуль 10. Сбои журналирования и оповещений • Концепции журналирования и оповещений. Примеры сбоев. Ограничение доступа устройств и логирование; логирование HTTP-заголовков; десериализация записей журналов. Способы защиты. • **Практика:** учебные примеры сбоев журналирования на стенде и защита. • **Результат:** слушатель видит, чем опасны журналы без оповещения.	**1**
Модуль 11. Некорректная обработка исключительных ситуаций • Концепции. Примеры из программы: заголовок Host; ограничение доступа устройств; подделка HTTP-запросов. Способы защиты. • **Практика:** учебные задания по обработке исключений на учебном сайте и защита. • **Результат:** слушатель связывает некорректную обработку сбоя с учебным сценарием и мерой защиты.	**1**
Аудиторная нагрузка в классе с преподавателем	**24 ак.ч. + 24 ак.ч. самостоятельно**

По окончании обучения на курсе проводится итоговая аттестация. Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе.

Контакты центра

Для частных лиц	Для организаций	E-mail
+7 (495) 232-32-16	**+7 (495) 780-48-44**	**info@specialist.ru**