

Аннотация рабочей программы дисциплины (модуля) Б1.В.07 Безопасность Web-приложений

Цели дисциплины

Целями освоения дисциплины Безопасность Web-приложений является формирование профессиональных компетенций будущих специалистов в области информационной безопасности, формирование у студентов системного и аналитического мышления, формирование у студентов знаний об основных типах атак на веб-приложения и методах их предотвращения.

Задачи дисциплины

Основными задачами изучения дисциплины являются:

- изучение основных элементов и механизмов веб-приложений (протокол HTTP, модель DOM, политика SOP, веб-браузеры, веб-серверы, балансировщики нагрузки);
- – изучение основных видов атак на веб-приложения: XSS, SQL, CSRF, IDOR и др.
- – приобретение навыков обнаружения и защиты от атак рассматриваемых классов.

Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
ПКС-3	Способен осуществлять управление средствами защиты информации, в том числе осуществляющими непрерывный мониторинг защищенности автоматизированных систем	ПКС-3.1 - Знает руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; ПКС-3.2 - Умеет определять подлежащие защите информационные ресурсы автоматизированных систем; ПКС-3.3 - Владеет навыками анализа угрозы автоматизированной системе и циркулирующей в ней информации, выбора необходимых средства для обеспечения информационной безопасности.

Содержание разделов дисциплины

Тема 1. Архитектура веб-приложений

Обзор современных клиентских (Frontend) и серверные (Backend) фреймворков для создания веб-приложений. Сравнение современных и более ранних версий приложений. Системы аутентификации и авторизации. Веб-серверы. Хранение данных на стороне сервера и на стороне клиента. Обнаружение сторонних зависимостей. Поиск слабых мест в архитектуре приложения.

Тема 2. Поиск уязвимостей к атакам CSRF

Понятие CSRF атаки. Влияние уязвимости CSRF на пользователя. Способы защиты от CSRF. Использование csurf-библиотеки. Инициализация CSRF-токена. Валидация CSRF-токена. Реализация CSRF-токена. Недостатки CSRF. Защита от CSRF. Проверка заголовков. CSRF-токен. CSRF-токены без сохранения состояния. Противодействие CSRF на уровне кода. Запросы GET без сохранения состояния. Снижение риска CSRF на уровне приложения.

Тема 3. Поиск уязвимостей к атакам XSS.

Обнаружение XSS-уязвимости. Хранимый XSS. Отраженный XSS. XSS-атака на базе DOM. XSS с мутациями. Приемы написания кода для противодействия XSS. Очистка пользовательского ввода. Приемник DOMParser. Приемник SVG. Приемник Blob. Санация гиперссылок. Символьные сущности в HTML

Тема 4. Поиск уязвимостей к атакам SQL

Внедрение SQL-кода. Внедрение кода. Внедрение команд. Противодействие внедрению.²⁹⁷

Противодействие внедрению SQL-кода. Распознавание внедрения SQL-кода. Подготовленные операторы. Более специфические методы защиты. Защита от других видов внедрения. Потенциальные цели внедрения. Принцип минимальных привилегий. Белый список команд.

Тема 5. Отказ в обслуживании (DoS)

ReDoS атака. Логические DoS-уязвимости. Распределенная DoS-атака. Противодействие DoS-атакам. Противодействие атакам ReDoS. Защита от логических DoS-атак. Защита от DDoS. Смягчение DDoS-атак.

Тема 6. Эксплуатация сторонних зависимостей

Методы интеграции. Ветви и вилки. Приложения с собственным сервером. Интеграция на уровне кода. Диспетчеры пакетов. JavaScript. Java. Другие языки. База данных общеизвестных уязвимостей. Защита сторонних зависимостей. Оценка дерева зависимостей. Моделирование дерева зависимости. Деревья зависимостей на практике. Автоматизированная оценка. Техники безопасной интеграции. Разделение интересов. Безопасное управление пакетами.