АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
«Технологии защиты веб-ресурсов»

по основной профессиональной образовательной программе по направлению подготовки 10.03.01 «Информационная безопасность» (уровень бакалавриата)

Направленность (профиль): Организация и технологии защиты информации (в сфере техники и технологий, связанных с обеспечением защищенности объектов информатизации)
Общий объем дисциплины – 4 з.е. (144 часов)
Форма промежуточной аттестации – Зачет.
В результате освоения дисциплины у обучающихся должны быть сформированы компетенции с соответствующими индикаторами их достижения:
- ПК-3.2: Способен организовывать защиту данных в информационных системах;

Содержание дисциплины:
Дисциплина «Технологии защиты веб-ресурсов» включает в себя следующие разделы:
Форма обучения очная. Семестр 7.
1. Общее представление об организации защиты данных в веб-ресурсах. Технологии получения и безопасной передачи информации в сети Интернет. Основные принципы организации защиты данных в веб-ресурсах. Принципы безопасного использования веб-ресурсов. Понятие безопасности приложений и классификация опасностей. Источники угроз информационной безопасности и меры по их предотвращению. Регламенты и методы разработки безопасных веб-приложений.
2. Современные угрозы безопасности веб-ресурсов. Классификация современных угроз безопасности веб-ресурсов OWASP Top 10. Уязвимости, связанные с внедрением команд и кода: SQL, NoSQL, OS, LDAP. Недостатки механизмов аутентификации. Уязвимости, ведущие к разглашению конфиденциальной информации. Внедрение внешних XML-сущностей. Недостатки контроля доступа. Некорректная настройка параметров безопасности. Межсайтовое выполнение сценариев. Небезопасная десериализация. Использование компонентов с известными уязвимостями. Недостатки журналирования и мониторинга.
3. Аудит безопасности и организация защиты данных в веб-ресурсах. Роль аудита безопасности веб-ресурсов при организации защиты данных в информационных системах. Тестирование на проникновение как важный элемент аудита безопасности веб-ресурса. Методы "черного", "серого" и "белого" ящика при тестировании на проникновение. Этапы проведения тестирования на проникновение. DNS-разведка. Сбор информации из открытых источников (OSINT). Сбор информации о сервере. Сканирование контента. Фаззинг входных параметров. Поиск утечек данных. Тестирование аутентификации. Отслеживание и перехват сессий. Атака с внедрением команд ОС. Включение файлов и обход каталогов. SQL-инъекции. XXE. Межсайтовое выполнение сценариев. Межсайтовая подделка запроса. Атаки на логические уязвимости веб-ресурсов. Методы и средства организации защиты данных в веб-ресурсах..
4. Методы и средства безопасной разработки веб-ресурсов. Обзор рекомендаций OWASP по безопасной разработке веб-ресурсов. Безопасное взаимодействие и работа с данными из БД. Использование безопасных сторонних библиотек и фреймворков. Использование безопасных алгоритмов аутентификации. Организация защиты от DDoS-атак. Шифрование веб-трафика с использованием SSL. Проверка корректности пользовательских данных на клиенте и сервере. Безопасная конфигурация инфраструктуры веб-ресурса..

Разработал:
старший преподаватель
кафедры ИВТиИБ П.А. Теплюк

Проверил:
Декан ФИТ А.С. Авдеев