Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

Безопасность веб-приложений

по направлению подготовки

10.03.01 Информационная безопасность

Направленность (профиль) подготовки:
Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения
Очная

Квалификация
Бакалавр

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями.

ПК-3 Способен проводить анализ уязвимостей внедряемой системы защиты информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-1.4.1 Понимает принципы организации, состав и алгоритмы работы механизмов защиты информации, стандарты оценивания безопасности компьютерных систем и сетей.

ИОПК-1.4.2 Определяет уровень защищенности компьютерных систем и сетей и прогнозирует возможные пути развития действий нарушителя информационной безопасности.

ИОПК-1.4.3 Оценивает соответствие механизмов безопасности требованиям существующих нормативных документов, а также их адекватности существующим рискам.

ИПК-3.1. Проводит анализ уязвимости средств системы защиты информации.

ИПК-3.2. Устраняет выявленные уязвимости системы защиты информации.

ИПК-3.3. Разрабатывает предложения по совершенствованию системы управления защитой информации.

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– лабораторные работы;

– контрольные задания.

Лабораторные работы (ОПК-1.4, ИПК-3.1, ИПК-3.2, ИПК-3.3):

1. Поиск уязвимостей к атакам CSRF (Cross-Site Request Forgery):

Цель: изучить методы и инструменты выявления уязвимостей, связанных с неавторизованными запросами от имени пользователя без его ведома. В рамках данной работы студенты познакомятся с природой CSRF-атак, изучат способы их обнаружения, а также методы защиты веб-приложений от подобных атак.

2. Поиск уязвимостей к атакам XSS (Cross-Site Scripting)

Цель: изучить процессы, связанные с инжекцией вредоносных скриптов и их выполнением в браузере жертвы. Студенты узнают о различных типах XSS-атак (хранимые, отраженные и DOM-базированные), их последствиях и методах предотвращения. Практическая часть предполагает поиск XSS-уязвимостей в тестовом веб-приложении.

3. Поиск уязвимостей к атакам SQL Injection

Цель: ознакомиться с техниками выявления и предотвращения инъекций SQL-кода на серверную сторону приложения. Данная работа включает изучение принципов SQL-инъекций, их потенциальных угроз и способов, которыми злоумышленники могут эксплуатировать данные уязвимости. Студенты проводят поиск SQL-инъекций и разрабатывают стратегии их предотвращения.

4. Поиск уязвимостей к атакам IDOR

Цель: научиться обнаруживать и устранять IDOR-уязвимости, которые позволяют злоумышленникам манипулировать параметрами доступа к объектам. Работа направлена на понимание механики атак, связанных с небезопасными прямыми обращениями к объектам.

5. Поиск уязвимостей в механизмах управления сессиями.

Цель: освоить навыки анализа безопасности механизмов управления сессиями и идентификации уязвимостей. Студенты изучают перехват сессий, угон сессий и недостатки в управлении сессиями, как с точки зрения пользователей, так и администраторов систем.

6. Методы автоматизации поиска уязвимостей

Цель: изучение современных автоматизированных методов и инструментов для поиска уязвимостей в программных системах. Использование различных сканеров безопасности, статического и динамического анализа для повышения эффективности обнаружения уязвимостей.

Критерии оценивания лабораторных работ:

«Зачтено» – студент в целом хорошо разбирается в задаче, знает и использует методы решения практически самостоятельно или при подсказке преподавателя, отвечает на вопросы, возможно с негрубыми ошибками. Представляет работу на защите в целом хорошо, с несущественными замечаниями.

«Не зачтено» – студент слабо разбирается в задаче, не знает или знает плохо методы решения, не отвечает, либо отвечает, но с грубыми ошибками на вопросы преподавателя.

Примеры заданий и задач (ОПК-1.4, ИПК-3.1, ИПК-3.2, ИПК-3.3)

1. В веб-приложении, доступном по адресу https://example.com, выявить уязвимости к атакам Reflected XSS.

2. В веб-приложении, доступном по адресу https://example.com, выявить уязвимости к атакам CSRF.

Примеры задач

1. Сгенерировать цепочку сертификатов (корневой, промежуточный, клиента, сервера и т.д.). Настроить аутентификацию клиента перед веб-сервером по сертификату.

2. На защищаемом сервере установить и настроить систему обнаружения и предотвращения атак Suricata или Snort. Написать следующие правила, реализующие:

обнаружение взаимодействия зараженных браузеров с сервером BeEF обнаружение атаки Heartbleed обнаружение атаки SSRF

3. В тестовом окружении реализовать атаки SSL Strip и HTTP Injection.

4. Имеется веб-приложение, в котором защита от атак CSRF реализована методом Double Submit Cookies. Реализовать атаку, позволяющую обойти механизм защиты от атак CSRF приложения https://example.com если известно, что другие компоненты веб-приложения доступны по адресам:

https://test.example.com
https://aum.example.com
http://blog.example.com

Критерии оценивания решения задачи:

За решение задачи выставляется оценка «зачтено», если верно указан и использован метод решения задачи; корректно реализован алгоритм решения задачи; получен полный и правильный ответ.

За решение задачи выставляется оценка «не зачтено», если ответ отсутствует полностью или допущены ошибки при использовании выбранного метода решения задачи; некорректно реализован алгоритм решения задачи; ответ не получен или получен неверный.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Зачет проводится в письменной/устной форме. Обучающийся должен дать ответы на два вопроса, которые выбираются преподавателем в случайном порядке из списка вопросов (ИОПК-1.4.1, ИОПК-1.4.2, ИОПК-1.4.3, ИПК-3.1):

1. Протокол HTTP.
2. Политика и механизм Same Origin Policy.
3. Механизм сессий.
4. Механизм Cookie.
5. Механизм Content-Security Policy.
6. Протоколы SSL/TLS.
7. Атаки на протоколы SSL/TLS.
8. Тестирование защищенности конфигурации SSL/TLS.
9. Управление доступом в веб-приложениях.
10. Атаки типа «инъекция».
11. Атаки подбора паролей на веб-приложения.
12. Атаки XSS.
13. Атаки CSRF.
14. Атаки SQLI.
15. Атака ClickJacking.
16. Атаки ШОК.
17. Принципы работы сканеров уязвимостей веб-приложений.
18. Автоматизированный поиск уязвимостей.
19. Основные механизмы защиты веб-приложений.
20. Принципы работы межсетевых экранов уровня веб-приложений

А также продемонстрировать навыки выявления уязвимостей в веб-приложениях (в результате сдачи лабораторных работ).

Критерии оценивания:

Оценка «Зачтено» по итогам промежуточной аттестации по дисциплине ставится, если студент выполнил и сдал на оценку «зачтено» лабораторные работы и владеет большей частью теоретического материала.

Оценка «Не зачтено» по итогам промежуточной аттестации по дисциплине – студент не выполнил лабораторные работы (не сдал на оценку «зачтено») и/или не освоил большую часть теоретического материала.

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Для проверки остаточных знаний студенту предлагается ответить на один теоретический вопрос из перечня теоретических вопросов, приведенных в п. 3

Ответ на вопрос предполагает краткое раскрытие основного содержания соответствующего вопроса.

Информация о разработчиках

Останин Сергей Александрович, канд. техн. наук, доцент, доцент кафедры компьютерной безопасности.

Вихорь Наталия Анатольевна, канд. физ.-мат. наук, доцент, доцент кафедры компьютерной безопасности.