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

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Информационная безопасность

Форма обучения
Очная

Квалификация
Магистр

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
А.Ю. Матросова

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-4 Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.

ПК-2 Способен оценить уровень безопасности компьютерных систем и разработать программно-аппаратные средства защиты информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-4.3 Использует современные информационно-коммуникационные технологии для решения задач в области прикладной математики и информатики с учетом требований информационной безопасности.

ИПК-2.1 Осуществляет проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации, разработку требований к программно-аппаратным средствам защиты информации компьютерных систем.

ИПК-2.2 Осуществляет разработку требований по защите, формирование политик безопасности компьютерных систем и сетей, проектирование программно-аппаратных средств защиты информации компьютерных систем.

ИПК-2.3 Осуществляет проведение анализа безопасности компьютерных систем, проведение сертификации программно-аппаратных средств защиты информации и анализ результатов, разработку и тестирование средств защиты информации компьютерных систем.

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:
– опросы по материалам лекций;
– лабораторная работа.

Вопросы текущего контроля (ИОПК-4.3)

- Как работает http протокол?
- Что такое Same Origin Policy?
- Что такое Content Security Policy&
- Для чего нужны протоколы SSL/TLS?
- Как осуществляется управление доступом в веб-приложениях?
- Что такое атаки типа «инъекция»?
- Атаки подбора паролей на веб-приложения.
- Что такое атаки XSS, CSRF, SQLI, ClickJacking, ШОК?
- Как работают сканеры уязвимостей веб-приложений?
- Как осуществить поиск уязвимостей?
- Основные механизмы защиты веб-приложений.
- Что такое межсетевой экран?
- Назовите принципы работы межсетевых экранов уровня веб-приложений.

Примеры лабораторных работ (ИОПК-4.3, ИПК-2.1, ИПК-2.2, ИПК-2.3):

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.

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

4. 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

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

6. 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 лабораторной работы: оценка «зачтено» выставляется, если студент правильно выполнил задание (выявил уязвимости, реализовал атаку, или настроил систему обнаружения и предотвращения атак и пр.), и может объяснить алгоритм, реализуемый в лабораторной работе. Оценка «не зачтено» выставляется, если студент слабо разбирается в задаче, не знает или знает плохо методы решения, не отвечает, либо отвечает, но с грубыми ошибками на вопросы преподавателя.

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

Зачет по дисциплине проводится в письменной или устной форме. Обучающийся должен дать ответы на два вопроса, которые выбираются преподавателем в случайном порядке из списка вопросов.

Теоретические вопросы к экзамену (ИОПК-4.3, ИПК-2.2, ИПК-2.3)

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.

Оценка «Зачтено» ставится, если студент выполнил лабораторные работы и владеет большей частью теоретического материала (ответ изложен систематизировано и последовательно, раскрыто содержание материала вопроса). Оценка «Не зачтено» – студент

не выполнил лабораторные работы и не освоил большую часть теоретического материала (полностью отсутствует ответ; не раскрыто основное содержание вопроса; обнаружено незнание или непонимание большей, или наиболее важной части вопроса).

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

Для проверки остаточных знаний студенту предлагается ответить на один теоретический вопрос из перечня теоретических вопросов (ИОПК-4.3, ИПК-2.3):

1. Какие виды уязвимостей веб-приложений вы знаете?
2. Как выявить уязвимости к атакам Reflected XSS?
3. Как выявить уязвимости к атакам CSRF?
4. Как тестируется защищенность конфигурации SSL/TLS?
5. Для чего используются TLS сертификаты?
6. Как осуществляется управление доступом в веб-приложениях?
7. Назовите принципы работы сканеров уязвимостей веб-приложений.
8. Какие основные механизмы защиты веб-приложений?
9. Назовите принципы работы межсетевых экранов уровня веб-приложений.

Теоретические вопросы для проверки остаточных знаний предполагают краткое раскрытие основного содержания соответствующего вопроса.

Информация о разработчиках

Останин Сергей Александрович, канд. техн. наук, заведующий кафедрой компьютерной безопасности