

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 / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки/ специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Треньяев

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-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.

ОПК-20 Способен проводить тестирование и использовать средства верификации механизмов защиты информации.

ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.

ПК-3 Способен проектировать программно-аппаратные средств защиты информации компьютерных систем и сетей.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-2.2 Определяет порядок настройки и эксплуатации программных средств системного и прикладного назначений, в том числе отечественного производства, используемых для решения задач профессиональной деятельности

ИОПК-20.1 Понимает принципы организации, состав и алгоритмы работы механизмов защиты информации, стандарты оценивания защищенности компьютерных систем

ИОПК-20.2 Проводит исследование механизмов защиты информации, в том числе с использованием средств верификации, и делает выводы по оценке защищенности и доверия

ИОПК-9.2 Обладает знанием и демонстрирует навыки применения базовых методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных

ИПК-3.3 Проведение аттестации программ и алгоритмов на предмет соответствия требованиям защиты информации

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

- лабораторные работы;
- контрольные задания.

Лабораторные работы (ИОПК-2.2, ИОПК-20.1, ИОПК-20.2, ИОПК-9.2, ИПК-3.3):

1. Поиск уязвимостей к атакам CSRF.
2. Поиск уязвимостей к атакам XSS
3. Поиск уязвимостей к атакам SQL
4. Поиск уязвимостей к атакам IDOR
5. Поиск уязвимостей в механизмах управления сессиями.
6. Методы автоматизации поиска уязвимостей

Примеры заданий и задач (ИОПК-2.2, ИОПК-20.1, ИОПК-20.2, ИОПК-9.2, 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>

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

Обучающийся должен знать ответы на вопросы (ИОПК-9.2, ИОПК-20.1):

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

Оценка «Зачтено» ставится, если студент выполнил лабораторные работы и владеет большей частью теоретического материала. Оценка «Не зачтено» – студент не выполнил лабораторные работы и не освоил большую часть теоретического материала.

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

Теоретические вопросы (ИОПК-9.2, ИОПК-20.1):

1. Протокол HTTP.
2. Политика и механизм Same Origin Policy.
3. Протоколы SSL/TLS.
4. Атаки на протоколы SSL/TLS.
5. Управление доступом в веб-приложениях.
6. Атаки типа «инъекция».
7. Атаки подбора паролей на веб-приложения.
8. Атаки XSS.
9. Атаки CSRF.
10. Атаки SQLI.
11. Атака ClickJacking.
12. Атаки ШОК.
13. Принципы работы сканеров уязвимостей веб-приложений.
14. Основные механизмы защиты веб-приложений.
15. 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, доцент, доцент кафедры компьютерной безопасности.