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

Рабочая программа дисциплины

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. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Цель и планируемые результаты освоения дисциплины

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-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.

ОПК-20 Способен проводить тестирование и использовать средства верификации механизмов защиты 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. Задачи освоения дисциплины

– изучить основные элементы и механизмы веб-приложений (протокол HTTP, модель DOM, политика SOP, веб-браузеры, веб-серверы, балансировщики нагрузки);

– изучить основные атаки на веб-приложения: XSS, SQL, CSRF, IDOR и др.

– научить обнаруживать и защищаться от атак рассматриваемых классов.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к Блоку 1 «Дисциплины (модули)».

Дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений, предлагается обучающимся на выбор. Дисциплина входит в «Модуль «Специализация».

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Десятый семестр, зачет

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: Компьютерные сети, Основы построения защищённых компьютерных сетей.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:
-лекции: 16 ч.
-лабораторные: 16 ч.
в том числе практическая подготовка: 16 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Архитектура веб-приложений
Основные элементы и механизмы веб-приложений
Тема 2. Поиск уязвимостей к атакам CSRF.
Изучение атаки CSRF на веб-приложение, поиск уязвимостей к атаке
Тема 3. Поиск уязвимостей к атакам XSS
Изучение атаки XSS на веб-приложение, поиск уязвимостей к атаке
Тема 4. Поиск уязвимостей к атакам SQL
Изучение SQL атаки на веб-приложение, поиск уязвимостей к атаке
Тема 5. Поиск уязвимостей к атакам IDOR
Изучение атаки IDOR, поиск уязвимостей к атаке
Тема 6. Поиск уязвимостей в механизмах управления сессиями.
Уязвимые механизмы аутентификации и управления сессией. Тестирование защищенности механизма управления доступом и сессий
Тема 7. Методы автоматизации поиска уязвимостей
Изучение способов автоматизации поиска уязвимостей в программном обеспечении на соответствующих уровнях его разработки.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, контроля выполнения контрольных заданий и лабораторных работ, опросов по лекционному материалу, и фиксируется в форме контрольной точки не менее одного раза в семестр.

Практическая подготовка оценивается по результатам выполненных лабораторных работ.

Оценочные материалы текущего контроля размещены на сайте ТГУ в разделе «Информация об образовательной программе» - https://www.tsu.ru/sveden/education/eduop/.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Зачет в десятом семестре проводится в письменной/устной форме по билетам. Билет состоит из двух теоретических вопросов. Продолжительность зачета 1 час.

Обучающийся должен знать ответы на вопросы, приведенные в оценочных материалах, и продемонстрировать навыки выявления уязвимостей в веб-приложениях. При этом 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.

Оценочные материалы для проведения промежуточной аттестации размещены на сайте ТГУ в разделе «Информация об образовательной программе» - https://www.tsu.ru/sveden/education/eduop/.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в LMS IDO
- https://lms.tsu.ru/course/view.php?id=5918

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

1. Л. Шкляр, Р. Розен. Архитектура веб-приложений. - М.: Эксмо, 2011. - 640 с.
2. OWASP Testing Guide. URL: https://www.owasp.org/index.php/OWASP Testing Guide v4 Table of Contents.

б) дополнительная литература:

1. В. Кочетков. Философия Application Security. URL: https://www.youtube.com/watch?v=mb7tcT-9VXk
2. В. Кочетков. Прикладная теория безопасности приложений. – URL: https://my.webinar.ru/record/622509/?i=574d3d07f32978bOae039c8604b45409

в) ресурсы сети Интернет:

Страница курса на Github.com: https://github.com/tsu-iscd/web-application-security/blob/master/README.md.

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:
– Burp Suite, OWASP ZAP, VirrualBox или VMWare Player, Kali Linux

б) информационные справочные системы:
– Электронный каталог Научной библиотеки ТГУ – http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system
– Электронная библиотека (репозиторий) ТГУ – http://vital.lib.tsu.ru/vital/access/manager/Index
– ЭБС Лань – http://e.lanbook.com/
– ЭБС Консультант студента – http://www.studentlibrary.ru/
– Образовательная платформа Юрайт – https://urait.ru/
– ЭБС ZNANIUM.com – https://znanium.com/
– ЭБС IPRbooks – http://www.iprbookshop.ru/

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения лабораторных занятий, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

15. Информация о разработчиках

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