

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

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. Матророва

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Цель и планируемые результаты освоения дисциплины

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. 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. Дисциплина входит в модуль «Специализация».

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

Третий семестр, зачет

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются компетенции, сформированные в ходе освоения образовательных программ предшествующего уровня образования.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:

-лекции: 18 ч.

-лабораторные: 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 лабораторных работ, опросов по лекционному материалу, и фиксируется в форме контрольной точки не менее одного раза в семестр.

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 третьем семестре проводится в письменной/устной форме. Обучающийся должен дать ответы на два вопроса, которые выбираются преподавателем в случайном порядке из списка вопросов, приведенных в оценочных материалах и продемонстрировать навыки выявления уязвимостей в веб-приложениях (в результате сдачи лабораторных работ). Продолжительность зачета 1 час.

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.

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://moodle.tsu.ru/course/view.php?id=5918>

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

в) Методические указания по организации самостоятельной работы студентов.

Самостоятельная работа организуется в следующих формах: работа с материалами лекций; изучение вопросов, выносимых за рамки лекционных занятий; подготовка к лабораторным занятиям; подготовка к рубежному контролю по теме/разделу (аттестации).

Следует целенаправленно, систематически и планомерно работать с конспектами лекций; изучать рекомендуемую литературу, добывая новые/обобщая полученные знания; тратить не менее часа в день на самостоятельную работу; консультироваться с преподавателем при возникновении вопросов; активно использовать учебно-методический комплекс на базе LMS IDO ТГУ; работать с тематическими форумами в сети Интернет.

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](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=574d3d07f32978b0ae039c8604b45409>

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, VirtualBox 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, заведующий кафедрой компьютерной безопасности.