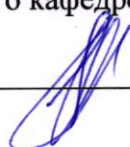


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего
образования
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДЕН
на заседании кафедры
«19» марта 2024 г., протокол № 8
Исполняющий обязанности
заведующего кафедрой



Осипов Г.С.

**ФОНД
ОЦЕНОЧНЫХ СРЕДСТВ
ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

Б1.В.07 Безопасность Web-приложений

Направление подготовки
10.03.01 Информационная безопасность
профиль
Безопасность автоматизированных систем (по отрасли или в сфере профессиональной
деятельности)

**Уровень высшего образования
БАКАЛАВРИАТ**

Южно-Сахалинск,
2024 г.

1. Формируемые компетенции и индикаторы их достижения по дисциплине (модулю)

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
ПКС-3	Способен осуществлять управление средствами защиты информации, в том числе осуществляющими непрерывный мониторинг защищенности автоматизированных систем	ПКС-3.1 - Знает руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; ПКС-3.2 - Умеет определять подлежащие защите информационные ресурсы автоматизированных систем; ПКС-3.3 - Владеет навыками анализа угрозы автоматизированной системе и циркулирующей в ней информации, выбора необходимых средства для обеспечения информационной безопасности.

2. Паспорт фонда оценочных средств по дисциплине (модулю)

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1 семестр			
1.	Тема 1. Архитектура веб-приложений.	ПКС-3	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к зачету
2.	Тема 2. Поиск уязвимостей к атакам CSRF.	ПКС-3	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к зачету
3.	Тема 3. Поиск уязвимостей к атакам XSS.	ПКС-3	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к зачету
4.	Тема 4. Поиск уязвимостей к атакам SQL.	ПКС-3	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к зачету
5.	Тема 5. Отказ в обслуживании (DoS)	ПКС-3	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к зачету
6.	Тема 6. Эксплуатация сторонних зависимостей	ПКС-3	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к зачету
7.	коллоквиумы	ПКС-3	контрольные вопросы, вопросы к коллоквиуму
8.	экзамен	ПКС-3	контрольные вопросы, вопросы к коллоквиуму, вопросы к зачету

Лабораторное занятие №1 (2 ч.)

Тема Архитектура веб-приложений

Вопросы для обсуждения:

1. Обзор современных клиентских (Frontend) и серверные (Backend) фреймворков для создания веб-приложений.
2. Сравнение современных и более ранних версий приложений.
3. Системы аутентификации и авторизации.
4. Веб-серверы.
5. Хранение данных на стороне сервера и на стороне клиента.
6. Обнаружение сторонних зависимостей.
7. Поиск слабых мест в архитектуре приложения.

Лабораторное занятие №2 (4 ч.)

Тема Поиск уязвимостей к атакам CSRF

Вопросы для обсуждения:

1. Понятие CSRF атаки.
2. Влияние уязвимости CSRF на пользователя.
3. Способы защиты от CSRF.
4. Использование csrf-библиотеки.
5. Инициализация CSRF-токена.
6. Валидация CSRF-токена.
7. Реализация CSRF-токена.
8. Недостатки CSRF.
9. Защита от CSRF.
10. Проверка заголовков. CSRF-токен.
11. CSRF-токены без сохранения состояния.
12. Противодействие CRSF на уровне кода.
13. Запросы GET без сохранения состояния.
14. Снижение риска CSRF на уровне приложения.

Лабораторное занятие №3 (6 ч.)

Тема 3. Поиск уязвимостей к атакам XSS.

Вопросы для обсуждения:

1. Обнаружение XSS-уязвимости.
2. Хранимый XSS.
3. Отраженный XSS.
4. XSS-атака на базе DOM.
5. XSS с мутациями.
6. Приемы написания кода для противодействия XSS.
7. Очистка пользовательского ввода.
8. Приемник DOMParser. Приемник SVG. Приемник Blob.
9. Санация гиперссылок. Символьные сущности в HTML

Лабораторное занятие №4 (8 ч.)

Тема Поиск уязвимостей к атакам SQL

Вопросы для обсуждения:

1. Внедрение SQL-кода.
2. Внедрение кода.
3. Внедрение команд.
4. Противодействие внедрению.
5. Противодействие внедрению SQL-кода.
6. Распознавание внедрения SQL-кода.
7. Подготовленные операторы.
8. Более специфические методы защиты.
9. Защита от других видов внедрения.
10. Потенциальные цели внедрения.
11. Принцип минимальных привилегий.
12. Белый список команд.

Лабораторное занятие №5 (8 ч.)

Тема Отказ в обслуживании (DoS)

Вопросы для обсуждения:

1. ReDoS атака.

2. Логические DoS-уязвимости.
3. Распределенная DoS-атака.
4. Противодействие DoS-атакам.
5. Противодействие атакам ReDoS.
6. Защита от логических DoS-атак.
7. Защита от DDoS. Смягчение DDoS-атак.

Лабораторное занятие №6 (8 ч.)

Тема Эксплуатация сторонних зависимостей

Вопросы для обсуждения:

1. Методы интеграции.
2. Ветви и вилки.
3. Приложения с собственным сервером.
4. Интеграция на уровне кода.
5. Диспетчеры пакетов.
6. JavaScript. Java. Другие языки.
7. База данных общеизвестных уязвимостей.
8. Защита сторонних зависимостей.
9. Оценка дерева зависимостей.
10. Моделирование дерева зависимости.
11. Деревья зависимостей на практике.
12. Автоматизированная оценка.
13. Техники безопасной интеграции.
14. Разделение интересов.
15. Безопасное управление пакетами.

Форма контроля	За одну работу		Всего	
	Мин. баллов	Макс. баллов	Мин. баллов	Макс. баллов
Текущий контроль:				
Активная работа на занятии	0,25	0,5	9	18
Выполнение домашнего задания	0,75	0,75	27	27
Выполнение заданий самостоятельной работы	1	3	1	3
коллоквиум	1	3	3	9
Промежуточная аттестация (экзамен)			20	43
Итого за семестр			60	100

Примерные вопросы к зачету

1. Сравнение современных и более ранних версий приложений. Системы аутентификации и авторизации.
2. Веб-серверы. Хранение данных на стороне сервера и на стороне клиента.
3. Обнаружение сторонних зависимостей. Поиск слабых мест в архитектуре приложения.
15. Понятие CSRF атаки. Влияние уязвимости CSRF на пользователя.
16. Способы защиты от CSRF. Использование csrf-библиотеки. Инициализация CSRF-токена.
17. Валидация CSRF-токена. Реализация CSRF-токена.
18. Недостатки CSRF. Защита от CSRF.
19. Проверка заголовков. CSRF-токен. CSRF-токены без сохранения состояния.
20. Противодействие CRSF на уровне кода.
21. Запросы GET без сохранения состояния. Снижение риска CSRF на уровне приложения.
22. Обнаружение XSS-уязвимости. Хранимый XSS. Отраженный XSS.

23. XSS-атака на базе DOM. XSS с мутациями. Приемы написания кода для противодействия XSS.
24. Очистка пользовательского ввода.
25. Приемник DOMParser. Приемник SVG. Приемник Blob. Санация гиперссылок. Символьные сущности в HTML
26. Внедрение SQL-кода. Внедрение кода. Внедрение команд.
27. Противодействие внедрению SQL-кода. Распознавание внедрения SQL-кода.
28. Подготовленные операторы. Более специфические методы защиты. Защита от других видов внедрения.
29. Потенциальные цели внедрения. Принцип минимальных привилегий.
30. ReDoS атака. Логические DoS-уязвимости. Распределенная DoS-атака.
31. Противодействие DoS-атакам. Противодействие атакам ReDoS.
32. Защита от логических DoS-атак. Защита от DDoS. Смягчение DDoS-атак.
33. Методы интеграции. Ветви и вилки. Приложения с собственным сервером.
34. Интеграция на уровне кода. Диспетчеры пакетов.
35. База данных общеизвестных уязвимостей.
36. Защита сторонних зависимостей. Оценка дерева зависимостей.
37. Моделирование дерева зависимости. Деревья зависимостей на практике.
38. Автоматизированная оценка. Техники безопасной интеграции.
39. Разделение интересов. Безопасное управление пакетами.

Критерии оценки:

Оценка «зачтено» выставляется:

- студенту глубоко и прочно усвоившему программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающему, в ответе которого увязывается теория с практикой, он показывает знакомство с литературой, правильно обосновывает и использует рациональные и современные средства решения поставленной проблемы.
- студенту, твердо знающему программный материал, грамотно и по существу, излагающему его, который не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении поставленной задачи.
- студенту, который знает только основной программный материал, но не усвоил особенностей, допускает в ответе неточности, некорректно формулирует основные законы и правила, затрудняется в выполнении практических задач.

Оценка «не зачтено» выставляется студенту, который не знает значительной части программного материала, допускает в ответе существенные ошибки, с затруднениями практические задания.

Составитель _____
(подпись)

Вашакидзе Н.С

«15» марта 2024 г.