ЦЕНТРАЛЬНЫЙ УНИВЕРСИТЕТ

УТВЕРЖДЕНА

Решением Ученого совета
АНО ВО «Центральный университет»
«07» марта 2024 г.
Протокол №1

Рабочая программа дисциплины (модуля)
«Безопасность Web-приложений»

Направление подготовки: *02.03.01 Математика и компьютерные науки*

Направленность (профиль) подготовки: *Программа двух дипломов НИУ ВШЭ и ЦУ «Прикладная математика и информатика»*

Квалификация (степень) выпускника: *бакалавр*

Форма обучения: *очная*

Срок освоения программы: *4 года*

Год набора: *2024*

Москва
2024

Электронный документ

Содержание

1. **Краткая характеристика дисциплины (модуля)** 3
2. **Перечень планируемых результатов обучения** 4
3. **Тематический план** 4
4. **Содержание дисциплины (модуля)** 6
5. **Учебно-методическое обеспечение** 7
6. **Материально-техническое обеспечение** 7
7. **Методические и оценочные материалы** 9

1. Краткая характеристика дисциплины (модуля)

Рабочая программа дисциплины (модуля) «Безопасность Web-приложений» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по специальности 02.03.01 Математика и компьютерные науки, профиль «Программа двух дипломов НИУ ВШЭ и ЦУ «Прикладная математика и информатика», утвержденный приказом Министерства науки и высшего образования Российской Федерации № 807 от 23.08.2017 года.

Изучение дисциплины (модуля) «Безопасность Web-приложений» важно для защиты данных пользователей и предотвращения кибератак, которые могут привести к финансовым потерям и утрате доверия. Это позволяет разработчикам создавать надежные и устойчивые к угрозам приложения, обеспечивая безопасность и стабильность работы в интернете.

Место дисциплины (модуля) в структуре образовательной программы

Настоящая дисциплина (модуль) включена в учебные планы по программам подготовки бакалавриата по направлению 02.03.01 Математика и компьютерные науки, профиль «Программа двух дипломов НИУ ВШЭ и ЦУ «Прикладная математика и информатика» и входит в вариативную часть Блока 1, формируемую участниками образовательных отношений.

Дисциплина (модуль) является выборной и доступна для изучения на 2, 3 или 4 курсе в 4, 5, 6, 7 или 8 семестрах на выбор.

Цель изучения дисциплины (модуля): освоение методов и практик защиты веб-приложений от различных угроз и уязвимостей для обеспечения их надежной и безопасной работы.

Задачи изучения дисциплины (модуля) направлены на формирование у студентов следующий знаний, умений и навыков:

- знание типовых проблем безопасности приложений;
- знание способов предотвращения проблем с безопасностью;
- умение использовать инструменты, применяемые для эксплуатации уязвимостей;
- умение анализировать причины возникновения уязвимостей;
- навык проведения тестирования защищенности Web-приложений;
- навык проведения аудита кода Web-приложений на предмет безопасности.

2. Перечень планируемых результатов обучения

Компетенции, формируемые в результате освоения дисциплины (модуля) при проведении учебных занятий в форме контактной работы обучающихся с педагогическими работниками Университета и в форме самостоятельной работы обучающихся:

Компетенция	Содержание компетенции	Индикатор компетенции	Перечень планируемых результатов обучения по дисциплине (модулю)
УК-1.	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1.	Знает методы поиска и анализа информации в области искусственного интеллекта, основные принципы критической оценки источников информации и их релевантности
		УК-1.2.	Умеет критически оценивать источники информации и синтезировать данные из различных источников для решения задач, применять системный подход к анализу и решению комплексных проблем
		УК-1.3.	Имеет практический опыт работы с современными инструментами и технологиями для обработки информации, формулировании и структурировании задач на основе полученной информации
ОПК-1.	Способен консультировать и использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики в профессиональной деятельности	ОПК-1.1.	Знает основные концепции и теории в области математического анализа и смежных дисциплин; методы и подходы, используемые в различных областях математики
		ОПК-1.2.	Умеет применять математические методы для решения профессиональных задач
		ОПК-1.3.	Имеет практический опыт разработки и реализация математических моделей в профессиональной деятельности
ОПК-6	Способен разрабатывать алгоритмы и компьютерные программы, пригодные	ОПК-6.1.	Знает алгоритмы разработки, компьютерные программы, а также алгоритмы вычислительной математики в области

	для практического применения		искусственного интеллекта
		ОПК-6.2.	Умеет разрабатывать математические программные продукты и комплексы с использованием современных технологий программирования в области искусственного интеллекта
		ОПК-6.3.	Имеет практический опыт разработки интеллектуальных информационных систем для визуализации результатов исследований в области искусственного интеллекта
ПК-1.	Способен формулировать задачи с математической точностью, обосновывать утверждения строго и анализировать полученные результаты в области математики и компьютерных наук	ПК-1.1.	Знает методы и подходы к формулированию задач, а также основные принципы математического доказательства и анализа результатов
		ПК-1.2.	Умеет корректно ставить и формулировать математические задачи, применять строгие методы доказательства и анализировать полученные результаты
		ПК-1.3.	Имеет опыт работы с задачами в области математики и компьютерных наук, включая применение математических методов для решения практических задач

3. Тематический план

№п/п	Наименование раздела дисциплины (модуля)	Трудоемкость, академические часы				ТКУ (текущий контроль успеваемости)
		Очная форма				
		Контактная работа		Контроль	Самостоятельная работа	
		Лекции	Семинары (практические занятия)			
1	Криптография и защита данных	6	4	2	26	Кейс Коллоквиум
2	Безопасность Linux	6	4	2	26	Кейс Коллоквиум
3	Безопасность веб-приложений	6	4	2	26	Кейс Коллоквиум
4	Управление идентификацией и доступом (IAM)	6	4	2	26	Кейс Коллоквиум
5	Управление секретами и контейнерная безопасность	6	4		26	Коллоквиум Проект
	Зачет с оценкой			2		
	Итого:	***30***	***20***	***10***	***130***	
Объем дисциплины (модуля) (в ак. ч.)		***190***				
Объем дисциплины (модуля) (в зач. ед.)		***5***				

4. Содержание дисциплины (модуля)

№п/п	Наименование раздела дисциплины (модуля)	Содержание дисциплины (модуля) по темам
1	Криптография и защита данных	Основы криптографии. Генератор псевдослучайных чисел. Метод оценки эффективности ГПСЧ. Сеть Фейстеля. Хэши. Коллизии хэшей и радужные таблицы. Блочные шифры. AES как пример блочного шифра. Ассиметричное шифрование и цифровая подпись. Алгоритм RSA, Diffie-Helman. Шифрование на эллиптических кривых.
2	Безопасность Linux	Управление доступом в Linux. Пользователи и их права. DAC модель, ACL. PAM как средство авторизации в систему. Механизм TOTP. Настройка аудита. Изоляция в Linux. CGroups, Namespaces, Capabilities. Бинарные уязвимости и эксплуатация libc. Безопасность сетевого стека Linux. Интерфейсы, туннели, firewall, теория PKI и работы сертификатов
3	Безопасность веб-приложений	Теория и практика Web уязвимостей. SQL injection, CSRF, path traversial, XSS. Теория и практика Web уязвимостей. RCE, LFI, SSTI, IDOR, SSRF, DoS и Race Conditions. Сканеры безопасности;
4	Управление идентификацией и доступом (IAM)	Протокол авторизации и аутентификации. Рассматриваем варианты на основе LDAP и KeyCloak. OIDC и OpenID. Spring Security
5	Управление секретами и контейнерная безопасность	Инфраструктура хранения секретов. Vault. Основы контейнерной безопасности. Container Escapes

5. Учебно-методическое обеспечение

Университет располагает полным набором лицензионного и свободно распространяемого программного обеспечения, включая продукты отечественного производства.

Каждый студент в течение всего периода обучения получает индивидуальный неограниченный доступ к электронно-библиотечной системе и электронной информационно-образовательной среде университета. Эти системы предоставляют возможность доступа к ресурсам из любой точки, где есть подключение к сети Интернет, как на территории университета, так и за его пределами.

Студентам обеспечен удаленный доступ к современным профессиональным базам данных и информационным справочным системам.

Основная литература:

1. Безопасность веб-приложений. Разведка, защита, нападение - СПб:Питер, 2022: ISBN. - Текст : электронный. - URL: https://znanium.com/catalog/product/2125433.

2. Яворски, П. Ловушка для багов. Полевое руководство по веб-хакингу : практическое руководство / П. Яворски. - Санкт-Петербург : Питер, 2020. - 272 с. - (Серия «Библиотека программиста»). - ISBN 978-5-4461-1708-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1733750.

3. Райс, Л. Безопасность контейнеров. Фундаментальный подход к защите контейнеризированных приложений / Л. Райс. - Санкт-Петербург : Питер, 2021. - 224 с. - ISBN 978-5-4461-1850-2. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2140361.

4. Треволт, Д. Защита и укрепление Linux : практическое руководство по защите системы Linux от кибератак / Д. Треволт ; пер. с англ. А. А. Слинкина. – Москва : ДМК Пресс, 2023. - 620 с. – ISBN 978-5-93700-220-4. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2204246.

5. Полуэктова Н. Р. Разработка веб-приложений : учебник для вузов / Н. Р. Полуэктова. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 204 с. — (Высшее образование). — ISBN 978-5-534-18645-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567610.

6. Тузовский А. Ф. Проектирование и разработка web-приложений : учебник для вузов / А. Ф. Тузовский. — Москва : Издательство Юрайт, 2025. — 219 с. — (Высшее образование). — ISBN 978-5-534-16300-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561176.

Дополнительная литература:

1. Сысолетин Е. Г. Разработка интернет-приложений : учебник для вузов / Е. Г. Сысолетин, С. Д. Ростунцев ; под научной редакцией Л. Г. Доросинского. — Москва : Издательство Юрайт, 2025. — 80 с. — (Высшее образование). — ISBN 978-5-534-17124-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/562916.

2. Web-разработки в asp. Net web forms : учебник для вузов / С. Т. Гуляева, В. В. Миронов, Н. О. Котелина, И. И. Лавреш. — Москва : Издательство Юрайт, 2025. — 134 с. — (Высшее образование). — ISBN 978-5-534-19885-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/569218.

6. Материально-техническое обеспечение

Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех

видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

Помещения, которые представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Изучение дисциплины (модуля) обеспечивается в учебных аудиториях, оснащенных:

— столами и стульями;
— компьютерной техникой;
— механическими калькуляторами;
— специализированным оборудованием, включая демонстрационное оборудование.

Помещения для самостоятельной работы обучающихся, в том числе приспособленные для использования инвалидами и лицами с ограниченными возможностями здоровья, оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.

Обучающимся предоставляется доступ (в том числе удаленный) к ресурсам информационно-телекоммуникационной сети «Интернет», электронным ресурсам (в том числе электронным библиотечным системам, современным профессиональным базам данных и информационным справочным системам):

№	Наименование портала (издания, курса, документа)	Ссылка
1.	Научная электронная библиотека elibrary.ru библиотека	https://elibrary.ru/defaultx.asp
2.	База данных для IT-специалистов	https://habr.com
3.	База данных ScienceDirect	https://www.sciencedirect.com
4.	Официальный сайт Министерства науки и высшего образования Российской Федерации	https://minobrnauki.gov.ru/
5.	Федеральный портал «Российское образование"	https://www.edu.ru/
6.	Информационная система "Единое окно доступа к образовательным ресурсам"	http://window.edu.ru/
7.	Единая коллекция цифровых образовательных ресурсов	http://school-collection.edu.ru/
8.	Федеральный центр информационно - образовательных ресурсов	http://fcior.edu.ru/

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), в том числе комплект лицензионного программного обеспечения, современные профессиональные базы данных и информационные справочные системы:

Наименование ПО	Производство	Лицензионное / свободно распространяемое
Операционные системы:		
Microsoft Imagine (Windows Client, Server)	зарубежное	лицензионное
Браузеры:		
Яндекс.Браузер	отечественное	свободно распространяемое
Google Chrome	зарубежное	свободно распространяемое
Офисные приложения:		

Microsoft Imagine (Visio, OneNote)	зарубежное	лицензионное
TeXstudio	зарубежное	свободно распространяемое
Adobe Acrobat Reader	зарубежное	свободно распространяемое
Программное обеспечение для планирования и учета времени:		
Toggle app	зарубежное	свободно распространяемое
Системы управления проектами:		
Microsoft Imagine (Project)	зарубежное	лицензионное
Системы управления базами данных:		
Microsoft Imagine (SQL Server)	зарубежное	лицензионное
Системы резервного копирования (backup):		
Acronis Backup Advanced for HyperV	зарубежное	лицензионное
Справочно-правовые системы:		
КонсультантПлюс: справочно-правовая система	отечественное	лицензионное
Средства антивирусной защиты:		
Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition	отечественное	лицензионное
Среды разработки:		
Visual Studio Code	зарубежное	свободно распространяемое
Bash (Unix shell)	зарубежное	свободно распространяемое
Anaconda	зарубежное	свободно распространяемое
Robotic Operating System	зарубежное	свободно распространяемое
CopelliaSim	зарубежное	свободно распространяемое
Google Colaboratory	зарубежное	свободно распространяемое
Пакеты программных средств и библиотек:		
AutoPsy	зарубежное	свободно распространяемое
Interactive Disassembler (IDA)	зарубежное	свободно распространяемое
Системы управления библиографической информацией:		
Zotero	зарубежное	свободно распространяемое
Сервисы и службы:		
Bind	зарубежное	свободно распространяемое
Docker	зарубежное	свободно распространяемое

7. Методические и оценочные материалы

Методические указания для обучающихся по освоению дисциплины (модуля)

В процессе изучения дисциплины (модуля) «Безопасность Web-приложений» в рамках текущего контроля успеваемости используются такие виды учебной работы, как лекции, семинары, коллоквиумы, кейсы, проект, а также различные виды самостоятельной работы обучающихся по заданию преподавателя, направленные на развитие навыков профессиональной лексики, закрепление практических профессиональных компетенций, поощрение инициатив.

Лекция – систематическое, последовательное, монологическое изложение преподавателем учебного материала, как правило, теоретического характера.

В процессе лекций рекомендуется вести конспект лекций: кратко и схематично фиксировать основные идеи, выводы и обобщения лекции; выделять важные мысли, ключевые слова и термины. Необходимо отметить вопросы или материалы, которые вызывают затруднения, и попытаться найти ответы в рекомендованной литературе. Если разобраться в материале не удается, следует сформулировать вопрос и задать его преподавателю на консультации или во время семинарского (практического) занятия.

Семинар — это форма учебной деятельности, проводимая в учебном заведении под

руководством преподавателя, где студенты активно участвуют в обсуждениях, практических заданиях и других формах взаимодействия.

Для успешной подготовки к семинару рекомендуется заранее ознакомиться с темой занятия и основными материалами, чтобы иметь возможность активно участвовать в обсуждении. Также полезно подготовить вопросы и идеи для обсуждения, что поможет глубже понять материал и продемонстрировать заинтересованность.

Кейс – практическая работа студентов над реальными или смоделированными задачами, что позволяет студенту применять теоретические знания на практике.

Студент самостоятельно разрабатывает стратегию решения поставленной задачи, что способствует развитию навыков критического мышления и самостоятельного принятия решений. Такой подход помогает подготовить будущих специалистов к реальным вызовам в их профессиональной деятельности.

Коллоквиум – устные ответы на вопросы, список которых известен студенту заранее.

В процессе подготовки к коллоквиуму необходимо проанализировать учебные материалы, ознакомившись с лекциями, учебниками и дополнительными источниками, акцентируя внимание на ключевых темах. Рекомендуется создать структурированные конспекты, выделяя основные идеи, термины и формулы.

Проект – исследовательская работа по курсу и презентация результатов.

Для успешной подготовки к проекту: четко определите цели и задачи проекта, распределите роли и обязанности между участниками, а также установите сроки выполнения каждой части работы. Регулярно проводите встречи для обсуждения прогресса и решения возникающих вопросов.

Самостоятельная работа – работа студентов, направленная на углубленное изучение отдельных тем и вопросов учебной дисциплины (модуля).

В процессе самостоятельной работы студенты взаимодействуют с рекомендованными материалами при минимальном участии преподавателя. Задачи студента включают работу с конспектами лекций (обработка текста), повторное изучение учебных материалов, планов и тезисов ответов, изучение дополнительных тем, выполнение учебно-исследовательских заданий и другое.

Система оценивания результатов обучения по дисциплине (модулю)

Критерии получения уровня и оценивания сформированности компетенций по дисциплине (модулю) «Безопасность Web-приложений»

Оценивание уровня учебных достижений, обучающихся по дисциплине (модулю), осуществляется в виде текущего контроля успеваемости и промежуточной аттестации.

Промежуточная аттестация по дисциплине (модулю) осуществляется в форме ***зачета с оценкой***, при этом проводится оценка компетенций, сформированных по дисциплине.

Для оценивания текущего контроля успеваемости и промежуточной аттестации используется десятибалльная шкала оценивания, которая соотносится с традиционной пятибалльной шкалой следующим образом:

Десятибалльная оценка	Пятибалльная оценка	Оценка за зачет	Общая характеристика результата обучения по дисциплине (модулю)
10	Отлично	Зачтено	Студент полностью владеет знаниями, изложенными в рабочей программе, и
9	Отлично	Зачтено	

Десятибалльная оценка	Пятибалльная оценка	Оценка за зачет	Общая характеристика результата обучения по дисциплине (модулю)
8	Отлично	Зачтено	глубоко осмысляет дисциплину. Он самостоятельно и логически последовательно отвечает на все вопросы, акцентируя внимание на наиболее важном. Умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя ключевые моменты и устанавливая причинно-следственные связи. Четко формулирует ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты дисциплины (модуля) с практическими задачами.
7	Хорошо	Зачтено	Студент обладает знаниями предмета почти в полном объеме рабочей программы и самостоятельно, логически последовательно и всесторонне отвечает на все вопросы, акцентируя внимание на наиболее значимых моментах. Он умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя его ключевые аспекты и устанавливая причинно-следственные связи. Формулирует свои ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные ситуационные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты предмета с практическими задачами.
6	Хорошо	Зачтено	
5	Удовлетворительно	Зачтено	Студент обладает базовыми знаниями по дисциплине (модулю), но испытывает трудности при самостоятельных ответах и использует неточные формулировки. В ходе ответов он допускает ошибки, касающиеся сути вопросов. Студент способен решать только самые простые
4	Удовлетворительно	Зачтено	

Десятибалльная оценка	Пятибалльная оценка	Оценка за зачет	Общая характеристика результата обучения по дисциплине (модулю)
			задачи и владеет лишь минимальным набором методов исследования.
3	Не сдан	Не зачтено	Студент не овладел обязательным минимумом знаний по предмету и не может ответить на вопросы, даже если преподаватель задает дополнительные наводящие вопросы.
2	Не сдан	Не зачтено	
1	Не сдан	Не зачтено	

Дисциплина (модуль) «Безопасность Web-приложений» оценивается следующим образом:

Активность	Вес	Описание
Кейс	40%	Практическая работа студентов над реальными или смоделированными задачами, что позволяет студенту применять теоретические знания на практике
Коллоквиумы	30%	Устные ответы на вопросы, список которых известен студенту заранее
Проект	30%	Защита итогового проекта

Формула расчёта итоговой оценки по дисциплине (модулю) «Безопасность Web-приложений»: «0,4 × среднее за кейсы + 0,3 × среднее за коллоквиумы + 0,3 × проект».

Текущий контроль успеваемости обучающихся по дисциплине (модулю)

Примерные задания для кейсов

Кейс 1: Криптография и защита данных

Задание 1: Реализуйте простой генератор псевдослучайных чисел (ГПСЧ) на основе алгоритма Linear Congruential Generator (LCG) в Python. Оцените его эффективность методом оценки энтропии (например, с использованием теста NIST или Diehard) и сравните с cryptographically secure ГПСЧ (например, os.urandom). Напишите отчет о результатах и рекомендациях по использованию в веб-приложениях.

Задание 2: Изучите сеть Фейстеля и реализуйте упрощенную версию блочного шифра (например, DES-подобный) на Python. Зашифруйте и расшифруйте текстовое сообщение, объяснив, как предотвращать коллизии в хэш-функциях (например, SHA-256). Продемонстрируйте атаку с использованием радужных таблиц на слабый хэш и предложите меры защиты.

Задание 3: Реализуйте ассиметричное шифрование с использованием RSA и цифровую подпись в Python (библиотека cryptography). Сгенерируйте ключи, зашифруйте данные, подпишите их и проверьте подпись. Сравните с Diffie-Hellman для обмена ключами и эллиптическими кривыми (ECC). Напишите скрипт для симуляции защищенного обмена сообщениями между двумя сторонами.

Кейс 2: Безопасность Linux

Задание 1: Настройте управление доступом в Linux: создайте пользователей и группы, примените DAC (Discretionary Access Control) и ACL (Access Control Lists) для

файлов. Используйте PAM (Pluggable Authentication Modules) для настройки TOTP (Time-based One-Time Password) аутентификации. Проверьте доступ и настройте аудит с помощью auditd, проанализировав логи на предмет несанкционированного доступа.

Задание 2: Изучите механизмы изоляции в Linux: настройте CGroups, Namespaces и Capabilities для контейнера (например, с Docker). Эксплуатируйте бинарную уязвимость в libc (например, через buffer overflow) и продемонстрируйте, как изоляция предотвращает эскалацию привилегий. Напишите отчет о рисках и мерах защиты.

Задание 3: Настройте безопасность сетевого стека Linux: создайте туннель (например, SSH или WireGuard), настройте firewall с iptables/ufw и теорию PKI (Public Key Infrastructure). Сгенерируйте самоподписанный сертификат и настройте HTTPS-сервер (nginx). Проведите сканирование на уязвимости с nmap и предложите улучшения для защиты интерфейсов.

Кейс 3: Безопасность веб-приложений

Задание 1: Создайте простое веб-приложение (например, на Flask или Django) и внедрите уязвимости: SQL injection, CSRF и XSS. Затем исправьте их, используя подготовленные запросы, токены CSRF и sanitization. Протестируйте с помощью сканера (например, OWASP ZAP) и напишите отчет о найденных уязвимостях и мерах защиты.

Задание 2: Реализуйте уязвимости RCE (Remote Code Execution), LFI (Local File Inclusion), SSTI (Server-Side Template Injection), IDOR (Insecure Direct Object References), SSRF (Server-Side Request Forgery), DoS и Race Conditions в тестовом приложении. Эксплуатируйте их и разработайте патчи, включая rate limiting для DoS и валидацию для SSRF.

Задание 3: Используйте сканеры безопасности (например, Burp Suite, Nikto) для аудита реального или тестового веб-сайта. Выявите уязвимости из OWASP Top 10, проведите пентест и предложите рекомендации по защите (например, Content Security Policy для XSS). Напишите детальный отчет с примерами эксплойтов и мерами mitigation.

Кейс 4: Управление идентификацией и доступом (IAM)

Задание 1: Настройте систему аутентификации и авторизации на основе LDAP: установите OpenLDAP, создайте пользователей и группы, интегрируйте с веб-приложением (например, через PHP). Реализуйте OIDC (OpenID Connect) с KeyCloak для SSO (Single Sign-On). Протестируйте аутентификацию и напишите отчет о преимуществах.

Задание 2: Интегрируйте Spring Security в Java-приложение для управления доступом: настройте роли, аутентификацию и авторизацию. Реализуйте OpenID для внешней аутентификации (например, через Google). Проведите тестирование на уязвимости (например, privilege escalation) и предложите улучшения.

Задание 3: Создайте политику IAM: определите роли, разрешения и жизненный цикл учетных записей. Используйте KeyCloak для управления пользователями в мульти-тенантном приложении. Симулируйте сценарий компрометации и восстановления доступа, написав план реагирования на инциденты.

Кейс 5: Управление секретами и контейнерная безопасность

Задание 1: Настройте инфраструктуру хранения секретов с HashiCorp Vault: установите Vault, создайте секреты (пароли, ключи), интегрируйте с приложением (например, через API). Реализуйте ротацию секретов и аудит доступа. Напишите скрипт для автоматической загрузки секретов в контейнер.

Задание 2: Изучите основы контейнерной безопасности: настройте Docker-контейнер с минимальными привилегиями, используйте non-root пользователя и read-only filesystem. Проведите анализ на уязвимости (с помощью Trivy или Clair) и предложите hardening (например, seccomp profiles).

Задание 3: Демонстрируйте и предотвратите Container Escapes: создайте уязвимый контейнер (например, с привилегированным режимом), эксплуатируйте escape (например, через mount namespace) и примените меры защиты (например, AppArmor или SELinux). Напишите отчет о рисках и лучших практиках для Kubernetes-подобных сред.

Примерные описания и критерии оценивания к коллоквиумам

Коллоквиум по теме «Уязвимости в механизмах аутентификации»

Описание коллоквиума:

Студенты должны продемонстрировать понимание основных уязвимостей, связанных с аутентификацией пользователей. В частности, необходимо уметь объяснять причины слабых паролей, преимущества многофакторной аутентификации, типичные уязвимости сессий, способы перехвата учетных данных, а также методы атак перебором (brute force) и способы их предотвращения.

Примерные вопросы:

— Почему слабые пароли представляют угрозу безопасности?
— Какие преимущества даёт многофакторная аутентификация?
— Какие уязвимости могут возникнуть при управлении сессиями?
— Какие методы используются для перехвата учетных данных?
— Как работает атака перебором (brute force) и как её можно предотвратить?
— Какие существуют рекомендации по созданию надёжных паролей?
— Что такое сессионный hijacking и как от него защититься?

Критерии оценивания (10 баллов):

— **10–9 баллов:** Полное и точное объяснение всех перечисленных уязвимостей; грамотное описание механизмов атаки и методов защиты; приведены примеры и рекомендации.
— **8–7 баллов:** Хорошее понимание основных уязвимостей, но с незначительными упущениями или неточностями; примеры приведены частично.
— **6–5 баллов:** Частичное понимание темы, описаны только некоторые уязвимости; отсутствуют детали по методам защиты.
— **4–3 балла:** Поверхностные знания, ответы фрагментарны и не структурированы.
— **2–0 баллов:** Ответы не соответствуют теме, отсутствует понимание ключевых понятий.

Коллоквиум по теме «SQL-инъекции и их эксплуатация»

Описание коллоквиума:

Студенты должны уметь объяснять природу SQL-инъекций, механизмы внедрения вредоносного SQL-кода, способы обхода аутентификации, методы извлечения и модификации данных. Также требуется знание способов защиты, включая использование подготовленных выражений (prepared statements).

Примерные вопросы:

— Что такое SQL-инъекция и как она возникает?
— Каким образом SQL-инъекция может использоваться для обхода аутентификации?
— Какие данные можно извлечь с помощью SQL-инъекции?
— Как можно изменить данные в базе с помощью SQL-инъекции?
— Что такое подготовленные выражения и как они защищают от SQL-инъекций?
— Какие существуют методы обнаружения и предотвращения SQL-инъекций?
— Чем опасны ошибки валидации входных данных?

Критерии оценивания (10 баллов):

— **10–9 баллов:** Чёткое и полное объяснение всех аспектов SQL-инъекций; приведены примеры атак и эффективных методов защиты; продемонстрировано понимание технических деталей.
— **8–7 баллов:** Хорошее понимание темы с небольшими пропусками; описаны основные техники атак и защиты.
— **6–5 баллов:** Частичное понимание, описаны только базовые понятия; отсутствуют детали или примеры.
— **4–3 балла:** Поверхностное знание, ответы неполные и неструктурированные.
— **2–0 баллов:** Отсутствие понимания темы, неадекватные ответы.

Коллоквиум по теме «Атаки на браузер и механизмы защиты»

Описание коллоквиума:

Студенты должны продемонстрировать знание основных видов атак на браузер (XSS, CSRF), уметь объяснять механизм их действия и последствия. Требуется понимание механизмов защиты, таких как Content Security Policy (CSP), защита cookie (HttpOnly, Secure), а также важность своевременного обновления и патчей браузера.

Примерные вопросы:

— Что такое Cross-Site Scripting (XSS) и как она работает?
— Какие типы XSS существуют?
— Что такое Cross-Site Request Forgery (CSRF) и как с ней бороться?
— Как работает Content Security Policy (CSP) и какую роль она играет в защите?
— Какие атрибуты cookie помогают повысить безопасность (HttpOnly, Secure)?
— Почему важно регулярно обновлять браузер?
— Какие ещё механизмы защиты браузера вы знаете?

Критерии оценивания (10 баллов):

— **10–9 баллов:** Детальное и точное объяснение атак и методов защиты; приведены примеры и рекомендации по безопасности.
— **8–7 баллов:** Хорошее понимание основных понятий, но с некоторыми пропусками; описаны ключевые методы защиты.
— **6–5 баллов:** Частичное понимание темы; описаны только отдельные атаки или методы защиты.
— **4–3 балла:** Поверхностные знания, ответы фрагментарны.
— **2–0 баллов:** Отсутствие понимания темы, ответы не по существу.

Примерное описание и критерии оценивания к проекту

Описание проекта:

Студентам предлагается разработать комплексное исследование и практическую демонстрацию уязвимостей и методов защиты, изученных в ходе курса. Проект должен включать анализ выбранного Web-приложения или создание прототипа с намеренно встроенными уязвимостями по темам аутентификации, shell-инъекций, SQL-инъекций, XXE-атак и атак на браузер. Студентам необходимо продемонстрировать умение выявлять и эксплуатировать эти уязвимости, а также реализовать и обосновать меры защиты, обеспечивающие безопасность приложения. Итоговый продукт должен содержать

теоретическую часть с описанием уязвимостей и их последствий, практическую часть с примерами атак и защитных механизмов, а также рекомендации по повышению безопасности.

Критерии оценивания:

— **Полнота охвата тем:** Проект должен затрагивать все ключевые темы курса — уязвимости аутентификации, shell-инъекции, SQL-инъекции, XXE-атаки, а также атаки на браузер и соответствующие методы защиты.

— **Глубина анализа уязвимостей:** Оценка способности студента выявлять и подробно описывать механизмы работы уязвимостей, их последствия и пути эксплуатации.

— **Практическая демонстрация:** Наличие и качество практических примеров эксплуатации уязвимостей и реализации механизмов защиты, подтверждающих теоретические выводы.

— **Обоснованность и эффективность защитных мер:** Корректность выбора и реализация методов защиты, их адекватность по отношению к выявленным уязвимостям, а также объяснение принципов работы этих мер.

— **Структура и качество оформления:** Логичность изложения, ясность и полнота описания, грамотность оформления документации и кода.

— **Инновационность и самостоятельность:** Проявление творческого подхода в выборе объекта исследования, методов анализа и защиты, а также самостоятельность выполнения работы.

— **Соответствие требованиям безопасности:** Проект должен демонстрировать понимание современных стандартов и практик обеспечения безопасности Web-приложений.

— **Обоснование выводов и рекомендаций:** Наличие чётких, аргументированных рекомендаций по улучшению безопасности рассматриваемого приложения или прототипа.

Задания для промежуточной аттестации по дисциплине (модулю)

№ п/п	Задание	Ответ	Компетенция
1.	Какой из перечисленных методов наиболее эффективно защищает от атак перебором паролей? а) Использование длинных и сложных паролей б) Применение однофакторной аутентификации в) Отключение сессий г) Игнорирование логов аутентификации	а	УК-1
2.	Что из перечисленного является основной причиной уязвимостей в механизмах сессий? а) Использование HTTPS б) Отсутствие защиты от перехвата cookie в) Применение многофакторной аутентификации г) Регулярное обновление паролей	б	УК-1
3.	Какой подход наиболее соответствует правовым нормам и ресурсным ограничениям для защиты от SQL-инъекций? а) Игнорирование пользовательского ввода б) Отключение базы данных в) Хранение паролей в открытом виде г) Использование подготовленных выражений (prepared statements)	г	УК-1
4.	При эксплуатации shell-инъекции злоумышленник может: а) Выполнить произвольный код на сервере б) Только просмотреть содержимое веб-страницы	а	ОПК-6

	в) Удалить только cookie браузера г) Изменить только настройки браузера		
5.	Какой из методов наиболее эффективен для предотвращения XSS-атак? а) Игнорирование обновлений браузера б) Использование слабых паролей в) Внедрение Content Security Policy (CSP) г) Отключение cookie с флагом HttpOnly	в	ПК-1
6.	Какой механизм защиты cookie предотвращает доступ к ним со стороны JavaScript? а) Secure б) HttpOnly в) SameSite г) CSP	б	ОПК-1
7.	Что из перечисленного является эффективным способом защиты от CSRF-атак? а) Отключение сессий б) Использование только GET-запросов для критичных операций в) Игнорирование обновлений браузера г) Использование токенов в формах	г	ОПК-6
8.	Какой принцип информационной безопасности означает, что данные не должны быть изменены или уничтожены несанкционированно? а) Доступность б) Конфиденциальность в) Целостность г) Аутентификация	в	ОПК-1
9.	Назовите тип атаки, при которой злоумышленник пытается подобрать пароль перебором.	Brute force (перебор)	УК-1
10.	Как называется механизм, предотвращающий выполнение внешних XML-сущностей?	Отключение обработки внешних сущностей (XXE protection)	УК-1
11.	Какой заголовок HTTP используется для реализации политики Content Security Policy?	Content-Security-Policy	ПК-1
12.	Как называется флаг cookie, который обеспечивает передачу cookie только по защищённому соединению?	Secure	ПК-1