МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГЕОДЕЗИИ И КАРТОГРАФИИ
(МИИГАиК)

Факультет геоинформатики и информационной безопасности
Кафедра информационно-измерительных систем

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 5BFEE1D286E9C95A0C0D2C611E434BD5
Владелец: Степанченко Алексей Леонидович
Действителен: с 23.09.2026 по 17.12.2027

«УТВЕРЖДАЮ»
Проректор
А. Л. Степанченко
24 марта 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «Б1.В.ДВ.01.01 РАЗРАБОТКА ПОДСИСТЕМЫ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ»

Уровень высшего образования: магистратура

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль) подготовки: Защита информации в геоинформационных системах и системах сбора пространственных данных

Квалификация (степень) выпускника: магистр

Форма обучения: очная

Год набора (приема на обучение): 2025

Срок получения образования: 2 года

Объем: в зачетных единицах: 4 з.е.
в академических часах: 144 ак.ч.

Москва, 2025

Разработчики:
Преподаватель кафедры Информационно-измерительных систем
Сутягин Д. Д.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки от 26.11.2020 № 1455

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Геоинформатики и информационной безопасности	Председатель ученого совета факультета	Матерухин А. В.	Рассмотрено	14.10.2024, № 10-24

Содержание

1. Цель и задачи освоения дисциплины (модуля)

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

3. Место дисциплины в структуре ОП

4. Объем дисциплины и виды учебной работы

5. Содержание дисциплины
   5.1. Разделы, темы дисциплины и виды занятий
   5.2. Содержание разделов, тем дисциплины и формы текущего контроля

6. Оценочные материалы текущего контроля

7. Оценочные материалы промежуточной аттестации

8. Порядок проведения промежуточной аттестации

9. Материально-техническое и учебно-методическое обеспечение дисциплины
   9.1. Перечень основной и дополнительной учебной литературы
   9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся
   9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине
   9.4. Оборудование и технические средства обучения

10. Методические указания по освоению дисциплины (модуля)

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - сформировать способность проектировать, реализовывать и проверять подсистему защиты веб-приложения: обосновывать режимы данных и требования, защищать ввод, доступ, сеансы и операции с базой, предупреждать XSS и CSRF, безопасно развертывать приложение и документировать его сопровождение.

Задачи изучения дисциплины:

- научиться определять защищаемые сведения, сценарии угроз, границы доверия и проверяемые требования к веб-приложению;
- освоить серверную проверку и нормализацию входов, описание API и анализ результатов фаззинга;
- научиться проектировать аутентификацию, полномочия и жизненный цикл сеансов, корректно применять токены и протоколы доступа;
- освоить выбор и проверку мер против XSS, CSRF и SQL-инъекций на изолированных учебных примерах;
- получить опыт настройки прав базы, сетевых связей, контейнерной среды и WAF в соответствии с назначением приложения;
- научиться оформлять проектную документацию и регламенты выпуска, мониторинга, обновления и восстановления.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ПК-3 Способен разрабатывать проектные решения по защите информации автоматизированных систем (в том числе в геоинформационных системах)

ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности

Знать:

ПК-3.1/Зн1 Нормативно-правовые документы в области защиты информации, определяющие виды тайн и устанавливающие степени конфиденциальности

ПК-3.1/Зн2 Методы безопасности веб-приложения от критических угроз безопасности

ПК-3.1/Зн3 Систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации

Уметь:

ПК-3.1/Ум1 Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности

ПК-3.1/Ум2 Выявлять и устранять потенциальные угрозы безопасности в веб-приложениях

ПК-3.1/Ум3 Обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей

Владеть:

ПК-3.1/Нв1 Методами анализа и оценки информации на предмет ее соответствия критериям отнесения к различным видам тайны и степеням конфиденциальности

ПК-3.1/Нв2 Навыками по применению нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации

ПК-3.2 Определяет типы субъектов доступа и объектов доступа, являющихся объектами защиты

Знать:

ПК-3.2/Зн1 Нормативные и методические документые, регламентирующие классификацию субъектов и объектов доступа

ПК-3.2/Зн2 Принципы и методы организационной защиты информации

ПК-3.2/Зн3 Методы атаки и различные методы предотвращения атак

Уметь:

ПК-3.2/Ум1 Определять объекты доступа, которые подлежат защите, на основании их функционального назначения и чувствительности информации

ПК-3.2/Ум2 Выполнять проверку цифровых подписей и других криптографических атрибутов сообщений

ПК-3.2/Ум3 Анализировать результаты верификации и выявлять случаи нарушения целостности или подлинности сообщения

Владеть:

ПК-3.2/Нв1 Навыками работы с системами управления доступом и средствами контроля доступа

ПК-3.2/Нв2 Навыками работы с криптографическими библиотеками и инструментами верификации

ПК-3.2/Нв3 Методиками обеспечения безопасности при обработке и верификации криптографических сообщений

ПК-3.3 Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации

Знать:

ПК-3.3/Зн1 Регламенты работ по обеспечению информационной безопасности автоматизированных систем автоматизированных систем

ПК-3.3/Зн2 Программные, технические и методические средства информационных технологий

Уметь:

ПК-3.3/Ум1 Разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности распределенных информационных систем

ПК-3.3/Ум2 Развертывать веб-приложения в безопасной среде и поддерживать безопасность веб-приложений

ПК-3.3/Ум3 Осуществлять разработку и проектирование информационных систем в соответствии с поставленной задачей

Владеть:

ПК-3.3/Нв1 Навыками разработки проектов нормативных документов, регламентирующих работу по защите информации в организации

ПК-3.3/Нв2 Методами анализа и формализации информационных процессов объекта и связей между ними

ПК-3.4 Понимает принципы построения и функционирования современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем)

Знать:

ПК-3.4/Зн1 Принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем)

ПК-3.4/Зн2 Стек протоколов TCP/IP и модель OSI

ПК-3.4/Зн3 Технологии проектирования и построения защищенных информационных систем

Уметь:

ПК-3.4/Ум1 Анализировать и выбирать оптимальную топологию и архитектуру сети с учетом требований и условий эксплуатации

ПК-3.4/Ум2 Выполнять настройку системного программного обеспечения с учетом требований информационной безопасности

Владеть:

ПК-3.4/Нв1 Навыками проектирования и построения локальных и глобальных компьютерных сетей с использованием современных технологий и оборудования

ПК-3.4/Нв2 Навыками работы с системным программным обеспечением различных платформ в распределённых ИС

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.В.ДВ.01.01 «Разработка подсистемы защиты веб-приложений» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 1.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
1 семестр	144	4	68	40	Экзамен (36)
Всего	144	4	68	40	36

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Практические занятия	Самостоятельная работа	Планируемые результаты обучения, соотнесенные с результатами освоения программы
Раздел 1. Введение в безопасность веб-приложений	**16**	**12**	**4**	ПК-3.1 ПК-3.2

Тема 1.1. Введение в безопасность веб-приложений: настройка среды разработки	16	12	4	ПК-3.3 ПК-3.4
Раздел 2. Проверка ввода и очистка данных	**12**	**8**	**4**	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4
Тема 2.1. Проверка ввода и очистка данных: реализация проверки ввода и очистки в веб-приложении	12	8	4	
Раздел 3. Аутентификация и контроль доступа	**12**	**8**	**4**	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4
Тема 3.1. Аутентификация и контроль доступа: реализация аутентификации и контроля доступа в веб-приложении	12	8	4	
Раздел 4. Управление сеансом	**13**	**8**	**5**	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4
Тема 4.1. Управление сеансом: реализация управления сеансом в веб-приложении	13	8	5	
Раздел 5. Межсайтовый скриптинг (XSS)	**13**	**8**	**5**	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4
Тема 5.1. Межсайтовый скриптинг (XSS): предотвращение и смягчение последствий XSS-атак	13	8	5	
Раздел 6. Межсайтовая подделка запросов (CSRF)	**13**	**8**	**5**	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4
Тема 6.1. Подделка межсайтовых запросов (CSRF): предотвращение и смягчение последствий CSRF-атак	13	8	5	
Раздел 7. SQL Injection	**13**	**8**	**5**	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4
Тема 7.1. Внедрение SQL: предотвращение и смягчение атак путем внедрения SQL	13	8	5	
Раздел 8. Развертывание и обслуживание	**16**	**8**	**8**	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4
Тема 8.1. Развертывание и обслуживание: развертывание безопасного веб-приложения	16	8	8	
Итого	**108**	**68**	**40**	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Введение в безопасность веб-приложений

Тема 1.1. Введение в безопасность веб-приложений: настройка среды разработки

Значение безопасности веб-приложений, распространенные виды атак, OWASP Top 10 и матрица MITRE ATT&CK. Защищаемые сведения, правовые основания режимов данных, цели и ограничения обработки. Оценка рисков: объекты, возможности нарушителя, сценарии и последствия. Архитектура браузер — приложение — СУБД, сетевые связи и границы доверия, соотнесение протоколов с уровнями TCP/IP и OSI. Настройка изолированного учебного стенда; требования защиты и наблюдаемые критерии проверки.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Раздел 2. Проверка ввода и очистка данных

Тема 2.1. Проверка ввода и очистка данных: реализация проверки ввода и очистки в веб-приложении

Проверка ввода, нормализация и очистка данных, их различное назначение. Типы, длины, диапазоны, обязательность и бизнес-ограничения; серверные проверки и недоверенные поля. Фаззинг: входной корпус, изменение входов, воспроизведение и анализ сбоев, пределы проверки. Спецификация OpenAPI: пути, операции, параметры, тело, схемы и ответы; согласование контракта с реализацией.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Раздел 3. Аутентификация и контроль доступа

Тема 3.1. Аутентификация и контроль доступа: реализация аутентификации и контроля доступа в веб-приложении

Аутентификация, авторизация и регистрация событий; субъекты, объекты и операции. RBAC и ABAC, назначение и отзыв прав, проверки полномочий на каждый объект. Политики паролей, хранение хешей, факторы, ограничение попыток и восстановление доступа. JWT: формат, криптографическая защита, издатель, аудитория и время действия. OAuth 2.0 как предоставление ограниченного доступа; OpenID Connect как слой аутентификации. Код авторизации с PKCE, роль Keycloak и подключаемого приложения. Подготовка правил управления доступом.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Раздел 4. Управление сеансом

Тема 4.1. Управление сеансом: реализация управления сеансом в веб-приложении

Жизненный цикл и безопасное управление сеансом, предотвращение захвата и фиксации сеанса. Непредсказуемость идентификаторов, обновление при изменении уровня доверия, завершение на сервере. Cookie: Secure, HttpOnly, SameSite, Domain и Path. Предел бездействия и абсолютный срок, выход пользователя и безопасное журналирование. Библиотеки и инструменты управления сеансами, проверка конфигурации и граничных случаев.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Раздел 5. Межсайтовый скриптинг (XSS)

Тема 5.1. Межсайтовый скриптинг (XSS): предотвращение и смягчение последствий XSS-атак

Межсайтовый скриптинг: отраженный, хранимый и связанный с клиентской обработкой; пересечение классификаций. Учебные инструменты обнаружения и воспроизведения XSS, автоматизированный поиск и анализ результатов. Контекстное экранирование и кодирование, опасные исполняемые контексты. Безопасные способы построения DOM, вывод текста, очистка разрешенного HTML. Политика CSP как дополнительная мера: режим отчетов, применение, nonce и ограничения.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Раздел 6. Межсайтовая подделка запросов (CSRF)

Тема 6.1. Подделка межсайтовых запросов (CSRF): предотвращение и смягчение последствий CSRF-атак

Межсайтовая подделка запросов, условия возникновения при автоматической передаче учетных данных. Шаблон синхронизирующего токена, подписанный double-submit cookie и привязка к сеансу. SameSite и различие site/origin, проверка Origin и Referer, ограничения применимости. Безопасные методы запросов и контроль операций изменения состояния. Фреймворки и библиотеки с CSRF-защитой, проверка корректности интеграции и отказа до изменения данных.

Текущий контроль

Вид (форма) контроля
Практическая работа

Раздел 7. SQL Injection

Тема 7.1. Внедрение SQL: предотвращение и смягчение атак путем внедрения SQL

SQL-инъекции: вмешательство в структуру команды при небезопасной обработке ввода. Параметризованные запросы, серверные разрешенные варианты имен объектов и сортировки. Фреймворки, ORM и библиотеки, ограничения защиты сырых запросов. Учебные инструменты автоматизированного поиска SQL-инъекций и проверка результатов. Минимальные прямые и наследуемые права учетной записи приложения, обработка ошибок без раскрытия служебных сведений.

Текущий контроль

Вид (форма) контроля
Практическая работа

Раздел 8. Развертывание и обслуживание

Тема 8.1. Развертывание и обслуживание: развертывание безопасного веб-приложения

Развертывание веб-приложения в безопасной среде и сопровождение. Docker: образы, контейнеры, сети, порты, пользователь процесса, постоянные данные и отдельная передача секретов. WAF, анализ срабатываний и ограниченные исключения. CI/CD и DevSecOps: учет версий и зависимостей, согласование конфигурации, проверки перед выпуском. Обновления безопасности, мониторинг, журналирование, проверка восстановления и регламент работы с дефектами.

Текущий контроль

Вид (форма) контроля
Практическая работа

6. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:
- Положением о формах, периодичности, порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.6 «Организация и проведение промежуточной аттестации».
- Положением о порядке осуществления образовательного процесса, проведения текущего контроля успеваемости и промежуточной аттестации обучающихся с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.8 «Проведение промежуточной аттестации с применением ЭО и ДОТ».

Промежуточная аттестация: Экзамен, 1 семестр.

Промежуточная аттестация по дисциплине проводится в форме экзамена. Конкретная форма проведения — компьютерное тестирование по теоретическому материалу или устное собеседование по вопросам билетов — утверждается кафедрой и доводится до сведения обучающихся не позднее чем за месяц до начала промежуточной аттестации. При компьютерном тестировании итоговый результат определяется как отношение количества набранных баллов к максимально возможному количеству баллов. При устном собеседовании билет включает вопросы из перечня вопросов; преподаватель вправе задать дополнительные и уточняющие вопросы.

Критерии оценивания при проведении промежуточной аттестации в форме компьютерного тестирования:

Экзамен оценивается по пятибалльной шкале:
- оценка «отлично» выставляется, если обучающийся набрал 86–100 баллов и продемонстрировал системное и полное освоение содержания дисциплины; ответы правильные, обоснованные и терминологически точные;
- оценка «хорошо» выставляется обучающемуся, набравшему 71–85 баллов, если основное содержание освоено; допущены отдельные неточности, не влияющие на общее понимание материала;
- оценка «удовлетворительно» выставляется обучающемуся, набравшему 56–70 баллов, если освоены базовые понятия и положения, но имеются существенные пробелы и ошибки;
- оценка «неудовлетворительно» выставляется, если обучающийся набрал 0–55 баллов; не освоен необходимый минимум содержания дисциплины; результаты обучения не достигнуты.

Критерии оценивания при проведении промежуточной аттестации в форме устного собеседования по билетам:
Экзамен оценивается по пятибалльной шкале:
- оценка «отлично» выставляется, если даны полные, правильные и логически последовательные ответы; терминология применяется корректно; приведены необходимые обоснования и примеры; дополнительные вопросы раскрыты;
- оценка «хорошо» выставляется обучающемуся, если вопросы раскрыты правильно и достаточно полно; отдельные неточности исправлены после уточняющих вопросов;
- оценка «удовлетворительно» выставляется обучающемуся, если основные положения раскрыты фрагментарно; имеются существенные неточности, однако базовое понимание продемонстрировано;
- оценка «неудовлетворительно» выставляется, если вопросы не раскрыты либо допущены принципиальные ошибки; отсутствует владение базовой терминологией.

7. Оценочные материалы текущего контроля

Раздел 1. Введение в безопасность веб-приложений
Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 1.1. Введение в безопасность веб-приложений: настройка среды разработки

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Классификация данных учебного веб-приложения

Для набора карточек пользователей, открытых публикаций и служебных документов определить защищаемые сведения и обосновать режим доступа по их содержанию и правовым основаниям. Отметить, какие данные можно исключить как ненужные для выбранной функции.

2. Архитектура и границы учебного стенда

Построить схему браузера, сервера приложения и базы данных, указать направления соединений, протоколы и необходимые порты. Обозначить границы доверия, разнести публичный интерфейс и служебный доступ, описать два сценария угроз и соответствующие ограничения соединений.

3. Требования к подсистеме защиты

Подготовить фрагмент технического задания для выбранной функции веб-приложения: данные, роли, угрозы, требования и наблюдаемые условия приемки. Указать применимые нормативные и методические документы без необоснованного объявления полной защищенности.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Упорядочьте подготовку требований к защите нового личного кабинета.

А. Сформулировать требования, направленные на выбранные угрозы

Б. Выяснить назначение и состав обрабатываемых данных
В. Определить существенные угрозы для этих данных

2. Упорядочьте определение режима защиты неизвестного набора документов.

А. Проверить применимые правовые основания и признаки ограничения
Б. Изучить содержание и происхождение набора
В. Зафиксировать обоснованное решение о режиме доступа

3. Упорядочьте подготовку отдельного учебного стенда для проверки веб-приложения.

А. Развернуть компоненты с ограниченными сетевыми связями
Б. Определить границы и необходимые компоненты стенда
В. Проверить доступность нужных функций и изоляцию от посторонних систем

4. Упорядочьте обработку найденного недостатка после его первоначального обнаружения.

А. Подтвердить воспроизводимость и описать условия недостатка
Б. Зафиксировать состояние исправленной версии
В. Подготовить и проверить исправление

Раздел 2. Проверка ввода и очистка данных

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 2.1. Проверка ввода и очистка данных: реализация проверки ввода и очистки в веб-приложении

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Контракт входных данных API

Описать одну операцию приложения в OpenAPI: поля, типы, обязательность, длины и допустимые значения. Сопоставить описание с серверными проверками на корректном, граничном и ошибочном примере.

2. Фаззинг обработчика учебных данных

Проверить изолированный учебный обработчик на небольшом наборе измененных входов. Сохранить вызвавший сбой пример либо обоснованно описать пределы выполненной проверки, не делая вывода об отсутствии всех уязвимостей.

3. Серверная проверка и нормализация

Для формы заказа реализовать или разобрать по коду обработку обязательных полей, форматов и бизнес-ограничений. Проверить прямые обращения в обход формы, эквивалентные представления и лишние поля; объяснить выбранную реакцию сервера.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Упорядочьте разработку проверки параметра по контракту API.

А. Проверить допустимые и недопустимые примеры
Б. Определить тип и ограничения параметра в контракте
В. Реализовать соответствующие проверки на сервере

2. Упорядочьте обработку числа, поступившего строкой, перед выполнением вычисления.

А. Передать допустимое число прикладной функции
Б. Проверить ограничения преобразованного числа
В. Проверить возможность преобразования строки

3. Упорядочьте разбор сбоя, обнаруженного фаззингом.

А. Воспроизвести сбой на сохраненном примере
Б. Подготовить описание подтвержденного дефекта
В. Сохранить вызвавший сбой пример и условия запуска

4. Упорядочьте проверку входа при использовании согласованного канонического представления.

А. Использовать прошедшее проверку значение
Б. Привести вход к выбранному однозначному представлению
В. Проверить его по установленным правилам

Раздел 3. Аутентификация и контроль доступа

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 3.1. Аутентификация и контроль доступа: реализация аутентификации и контроля доступа в веб-приложении

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Роли и права пользователей

Определить субъекты, объекты и операции учебного портала, составить матрицу прав для читателя, редактора и администратора. Проверить разрешенные и запрещенные действия, включая прямое обращение к чужому объекту; описать назначение и отзыв ролей.

2. Проверка токена доступа

На предоставленных учебных токенах проверить различия между чтением полей и принятием токена. Разобрать доверенный алгоритм, подпись, издателя, аудиторию и срок; указать решение для неверного назначения и истекшего срока.

3. Порядок безопасного входа и восстановления доступа

Подготовить короткий регламент входа, реакции на серию ошибок и восстановления учетной записи учебного портала. Определить ответственных, сообщения пользователю и сведения для журнала; объяснить выбор факторов и ограничений попыток.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Упорядочьте обычный вход по паролю при корректно работающей серверной проверке.

А. Проверить их выбранным серверным механизмом
Б. Создать аутентифицированный сеанс при успешной проверке
В. Получить предъявленные учетные данные

2. Упорядочьте решение о доступе к документу.

А. Проверить разрешение по действующей политике
Б. Определить субъекта, объект и запрошенную операцию
В. Выполнить операцию только при положительном решении

3. Упорядочьте использование токена JWT сервером, который ожидает подписанные токены установленного типа.

А. Использовать подтвержденные сведения для дальнейшего решения
Б. Выполнить предусмотренные проверки криптографии и полей
В. Получить токен как недоверенные данные

4. Упорядочьте укрупненные этапы OAuth с кодом авторизации и PKCE.

А. Получить код авторизации через зарегистрированный адрес возврата
Б. Отправить запрос авторизации с code_challenge
В. Обменять код с соответствующим code_verifier на токен

Раздел 4. Управление сеансом

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 4.1. Управление сеансом: реализация управления сеансом в веб-приложении

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Жизненный цикл сеанса

Реализовать либо проверить по выданной конфигурации создание сеанса, обновление его идентификатора после входа и завершение при выходе. Выбрать атрибуты cookie и проверить, что старый идентификатор не дает прежнего доступа.

2. Пределы срока и наблюдение за сеансами

Для учебного портала определить предел бездействия и общий срок сеанса. Разобрать запросы до и после заданных границ, фоновую активность и безопасную регистрацию событий без публикации действующего идентификатора.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Упорядочьте проверку нового предъявления пароля по ранее сохраненному хешу.

А. Проверить предъявленный пароль штатной функцией проверки хеша
Б. Получить сохраненные параметры и хеш учетной записи
В. Принять решение о результате проверки

2. Упорядочьте обработку выхода из приложения с серверным хранилищем сеансов.

А. Отправить ответ с удалением соответствующей Cookie
Б. Получить запрос выхода для текущего сеанса
В. Прекратить действие его серверной записи

3. Упорядочьте проверку бездействия при поступлении очередного запроса.

А. Сопоставить интервал бездействия с пределом
Б. Отклонить запрос просроченного сеанса либо продолжить допустимый сеанс
В. Получить время последней активности и установленный предел

4. Упорядочьте передачу Cookie от сервера и ее последующее использование браузером.

А. Получить ответ с заголовком Set-Cookie
Б. Добавить Cookie к подходящему следующему запросу
В. Сохранить Cookie с учетом ее атрибутов

Раздел 5. Межсайтовый скриптинг (XSS)

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 5.1. Межсайтовый скриптинг (XSS): предотвращение и смягчение последствий XSS-атак

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Безопасный вывод пользовательского содержимого

В учебной странице проверить вывод обычного комментария и разрешенного форматированного текста. Исправить опасные места в соответствии с контекстом: использовать текстовый вывод либо очистку допустимого HTML, затем сравнить результаты.

2. Проверка политики исполнения сценариев

Для учебной страницы предложить небольшую CSP, проверить разрешенный и запрещенный источник сценария и разобрать различие режима отчетов и применения политики. Если используется nonce, показать правила его обновления для каждого ответа.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Упорядочьте безопасный вывод недоверенной строки в текстовую область HTML-шаблона.

А. Применить соответствующее этому контексту кодирование
Б. Включить результат в вывод шаблона
В. Определить контекст размещения строки

2. Упорядочьте обработку пользовательского форматированного HTML, если часть разметки разрешена.

А. Обработать содержимое подходящим HTML-санитайзером
Б. Вывести проверенное содержимое предусмотренным способом
В. Определить разрешенные элементы и атрибуты

3. Упорядочьте исправление найденного опасного вывода строки через innerHTML, если требуется обычный текст.

А. Заменить интерпретацию HTML безопасным текстовым выводом
Б. Проверить, что контрольная строка отображается текстом
В. Найти путь недоверенных данных к операции вывода

Раздел 6. Межсайтовая подделка запросов (CSRF)

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 6.1. Подделка межсайтовых запросов (CSRF): предотвращение и смягчение последствий CSRF-атак

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Защита операции изменения профиля

Для запроса изменения профиля с cookie-аутентификацией реализовать или проверить схему CSRF-защиты. Рассмотреть корректный токен, отсутствие токена и неверную привязку, убедиться, что отклоненный запрос не изменил данные.

2. Регламент проверки изменяющих запросов

Подготовить краткое правило проектирования и проверки операций, изменяющих данные: методы запросов, CSRF-защита, проверка Origin и условия отказа. Применить правило к двум операциям учебного приложения и оформить найденные исправления.

Раздел 7. SQL Injection

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 7.1. Внедрение SQL: предотвращение и смягчение атак путем внедрения SQL

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Устранение небезопасного построения SQL

Преобразовать учебный запрос с включением клиентской строки в параметризованный. Отдельно разобрать выбор поля сортировки по серверному разрешенному списку; проверить обычные и специально ошибочные значения на учебной базе.

2. Учетная запись приложения в СУБД

Выделить отдельную роль для функции чтения отчетов, определить необходимые объекты и права. Проверить эффективные полномочия с учетом членства в ролях и описать порядок изменения доступа при смене функции.

Раздел 8. Развертывание и обслуживание

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 8.1. Развертывание и обслуживание: развертывание безопасного веб-приложения

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Безопасная схема развертывания

Подготовить конфигурацию либо проект размещения приложения и базы в учебной среде Docker. Указать сети, публикуемые порты, пользователя процесса, постоянные данные и способ передачи секретов; проверить запуск и отсутствие лишних внешних подключений.

2. Настройка WAF перед приложением

На учебных запросах разобрать срабатывание WAF, определить правило и фазу обработки, отличить недопустимый запрос от ложной блокировки. Обосновать точечное изменение и повторить проверку разрешенных и запрещенных действий.

3. Регламент выпуска и сопровождения

Для учебной версии подготовить порядок выпуска: состав зависимостей, проверки, согласование конфигурации, развертывание, наблюдение и восстановление. Описать действия при обнаружении уязвимой зависимости и оформить краткий протокол принятия версии.

8. Оценочные материалы промежуточной аттестации

1 семестр, Экзамен

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Вопросы/Задания:

1. Какие сведения делают сценарий угрозы пригодным для проверки?

2. Чем правовой режим данных отличается от технического ограничения доступа?

3. Для чего подходит OWASP Top 10 и почему его недостаточно для полного заключения о безопасности?

4. Как связаны тактика и техника в MITRE ATT&CK?

5. Как связать требование защиты с приемкой подсистемы?

6. Зачем различать проверку формы значения и его смысла для задачи?

7. Какие элементы API нужно описать, чтобы подготовить проверки запроса и ответа?

8. Какие сведения нужны для воспроизведения сбоя при фаззинге?

9. Почему одной проверки в браузере недостаточно?

10. Чем нормализация отличается от очистки или отказа в обработке?

11. Чем различаются назначение OAuth 2.0 и OpenID Connect?

12. Почему чтение JSON из JWT не равнозначно проверке токена?

13. В чем различие ролевой и атрибутной организации правил доступа?

14. Как ограничение попыток входа связано с удобством и доступностью?

15. Почему для хранения паролей используют специальные функции хеширования?

16. Какие разные задачи решают Secure и HttpOnly?

17. Когда обновление идентификатора сеанса особенно важно?

18. Чем абсолютный предел сеанса отличается от предела бездействия?

19. Почему удаление cookie без прекращения серверного сеанса недостаточно для выхода?

20. Зачем учитывать Domain и Path при создании и удалении cookie?

21. Почему обозначения «хранимый XSS» и «DOM XSS» не всегда взаимоисключающие?

22. Как контекст вывода влияет на выбор защиты от XSS?

23. Когда предпочтительнее textContent, чем innerHTML?

24. В каком случае требуется очистка разрешенного HTML?

25. Какую роль CSP выполняет вместе с защитой вывода?

26. Как автоматическая передача cookie связана с CSRF?

27. Почему проверять нужно не только наличие, но и корректность CSRF-токена?

28. Чем same-site отличается от same-origin в контексте браузерной защиты?

29. Почему нельзя сравнивать Origin только по началу строки?

30. Почему меры против XSS важны даже при наличии CSRF-защиты?

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Мызникова Т. А. Основы информационной безопасности: учебное пособие / Т. А. Мызникова. - Омск: ОмГУПС, 2017. - 82 с. - 978-5-949-41160-5. - Текст: электронный // Издательство Лань: [сайт]. - URL: https://e.lanbook.com/book/129192 - Режим доступа: по подписке

2. Галатенко В. А. Основы информационной безопасности: учебное пособие / В. А. Галатенко. - Основы информационной безопасности - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. - 266 с. - 978-5-4497-3316-0. - Текст: электронный // IPR SMART: [сайт]. - URL: https://www.iprbookshop.ru/142285.html - Режим доступа: по подписке

3. Лапонина О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: учебное пособие / О. Р. Лапонина; под редакцией В. А. Сухомлина. - Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. - 605 с. - 978-5-4497-3470-9. - Текст: электронный // IPR SMART: [сайт]. - URL: https://www.iprbookshop.ru/142292.html - Режим доступа: по подписке

Дополнительная литература

1. Нестеров С. А. Основы информационной безопасности / С. А. Нестеров. - 2-е изд., стер. - Санкт-Петербург: Лань, 2022. - 324 с. - 978-5-8114-9489-7. - Текст: электронный // Издательство Лань: [сайт]. - URL: https://e.lanbook.com/book/195510 - Режим доступа: по подписке

2. Овчинникова Е. А. Организационно-правовые основы информационной безопасности. Ч.1: учебное пособие / Е. А. Овчинникова, Г. В. Попков; под редакцией С. Н. Новикова. - Организационно-правовые основы информационной безопасности. Ч.1 - Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2022. - 193 с. - 2227-8397. - Текст: электронный // IPR SMART: [сайт]. - URL: https://www.iprbookshop.ru/138773.html - Режим доступа: по подписке

9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

Не используются.

Ресурсы «Интернет»

1. https://scholar.google.ru/ - Гугл Академия
2. https://www.elibrary.ru/ - НЭБ eLIBRARY
3. https://intuit.ru/ - Электронная образовательная среда "ИНТУИТ"
4. https://e.lanbook.com/ - Электронная библиотечная система "Лань"
5. https://rusneb.ru/ - Национальная электронная библиотека (НЭБ)
6. https://owasp.org/www-project-web-security-testing-guide/ - OWASP Web Security Testing Guide
7. https://owasp.org/www-community/Threat_Modeling_Process - OWASP: базовый процесс моделирования угроз

9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)

1. Sublime Text 3;
2. 7Zip;
3. Microsoft Office;
4. Notepad++;
5. Microsoft Visual Studio;

Перечень информационно-справочных систем
(обновление выполняется еженедельно)

Не используется.

9.4. Оборудование и технические средства обучения

Компьютерный класс

Автоматизированное рабочее место (АРМ) - 15 шт.
Доска настенная одноэлементная - 2 шт.
Проектор - 1 шт.

Учебная аудитория

Автоматизированное рабочее место (АРМ) - 1 шт.

Проектор - 2 шт.
Доска настенная одноэлементная - 1 шт.

Смешанный тип
Автоматизированное рабочее место (АРМ) - 1 шт.
Доска настенная одноэлементная - 2 шт.
Интерактивная панель - 1 шт.
Проектор - 1 шт.

10. Методические указания по освоению дисциплины (модуля)

С целью успешного освоения данного предмета студенту необходимо выполнять домашние работы по указанным преподавателям темам и представленным на занятиях материалам. Для более успешного выполнения работы студенту предлагается использование учебно-методических материалов, соответствующих указанной теме.

Самостоятельная работа студентов описывается и регулируется методическими рекомендациями по дисциплине.

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.