ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Безопасность веб-приложений

Код модуля
1156863(1)

Модуль
Информационные технологии

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Бородин Андрей Михайлович	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр "Информационная безопасность"
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр "Информационная безопасность"
3	Поршнев Сергей Владимирович	д.т.н., профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ

Согласовано:

Управление образовательных программ Т.Г. Комарова

Авторы:

- **Бородин Андрей Михайлович, Доцент,**
- **Пономарева Ольга Алексеевна, Доцент,**
- **Поршнев Сергей Владимирович, директор Учебно-научного центра "Информационная безопасность", УНЦ ИБ**

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Безопасность веб-приложений

1.	**Объем дисциплины в зачетных единицах**	5	
2.	**Виды аудиторных занятий**	Лекции Лабораторные занятия	
3.	**Промежуточная аттестация**	Экзамен	
4.	**Текущая аттестация**	Отчет по лабораторным работам	1

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Безопасность веб-приложений

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины, указанного в табл. 1.3 РПМ-РПД.

Таблица 1

Код и наименование компетенции	**Планируемые результаты обучения (индикаторы)**	**Контрольно-оценочные средства для оценивания достижения результата обучения по дисциплине**
1	**2**	**3**
ОПК-10 -Способен использовать методы и средства криптографической защиты информации при решении задач профессиональной деятельности	З-1 - Различать основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в телекоммуникационных системах З-2 - Объяснять особенности применения криптографических методов и средств защиты информации для защиты систем электронного документооборота П-1 - Иметь опыт использования и исследования криптографических средств защиты информации, разрабатываемых различными фирмами-производителями, при	Лабораторные занятия Лекции Отчет по лабораторным работам Экзамен

	решении профессиональных задач У-1 - Анализировать программные модели средств криптографической защиты информации	
ОПК-7 -Способен создавать программы на языках высокого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования	З-1 - Различать алгоритмические основы программирования на языках общего назначения З-2 - Различать языки программирования общего назначения П-1 - Иметь опыт разработки алгоритмов для последующего создания программ на языках общего назначения П-2 - Иметь опыт использования типовых инструментальных средств программирования для решения профессиональных задач У-1 - Формулировать способы организации программ и инструментария программирования при решении профессиональных задач	Лабораторные занятия Лекции Отчет по лабораторным работам Экзамен

3. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ МОДУЛЯ В БАЛЬНО-РЕЙТИНГОВОЙ СИСТЕМЕ (ТЕХНОЛОГИЧЕСКАЯ КАРТА БРС)

3.1. Процедуры текущей и промежуточной аттестации по дисциплине

1. Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0.5		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
активность студента на занятии	*7,17*	*100*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.5		
Промежуточная аттестация по лекциям – экзамен **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.5**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – не предусмотрено		

Текущая аттестация на практических/семинарских занятиях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– не предусмотрено		
Промежуточная аттестация по практическим/семинарским занятиям–нет **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– не предусмотрено**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0.5		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Отчет по лабораторным работам	7,15	100
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -1		
Промежуточная аттестация по лабораторным занятиям –нет **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям – не предусмотрено**		
4. Онлайн-занятия: коэффициент значимости совокупных результатов онлайн-занятий –не предусмотрено		
Текущая аттестация на онлайн-занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по онлайн-занятиям -не предусмотрено		
Промежуточная аттестация по онлайн-занятиям –нет **Весовой коэффициент значимости результатов промежуточной аттестации по онлайн-занятиям – не предусмотрено**		

3.2. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Текущая аттестация выполнения курсовой работы/проекта	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
Весовой коэффициент текущей аттестации выполнения курсовой работы/проекта– не предусмотрено		
Весовой коэффициент промежуточной аттестации выполнения курсовой работы/проекта– защиты – не предусмотрено		

4. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

4.1. В рамках БРС применяются утвержденные на кафедре/институте критерии (признаки) оценивания достижений студентов по дисциплине модуля (табл. 4) в рамках контрольно-оценочных мероприятий на соответствие указанным в табл.1 результатам обучения (индикаторам).

Таблица 4

Критерии оценивания учебных достижений обучающихся

Результаты обучения	**Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам**
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Другие результаты	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения. Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

4.2 Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5

Шкала оценивания достижения результатов обучения (индикаторов) по уровням

Характеристика уровней достижения результатов обучения (индикаторов)				
№ п/п	**Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)**	**Шкала оценивания**		
		Традиционная характеристика уровня		**Качественная характеристика уровня**
1.	Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)
2.	Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам,	Неудовлетворительно	Не зачтено	Недостаточный (Н)

	имеются существенные ошибки и замечания, требуется доработка	(менее 40 баллов)		
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

5. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПО ДИСЦИПЛИНЕ МОДУЛЯ

5.1. Описание аудиторных контрольно-оценочных мероприятий по дисциплине модуля

5.1.1. Лекции

Самостоятельное изучение теоретического материала по темам/разделам лекций в соответствии с содержанием дисциплины (п. 1.2. РПД)

5.1.2. Лабораторные занятия

Примерный перечень тем

1. Основы PHP.Формы. Работа с файловой системой
2. Основы работы с базами данных
3. Размещение Web-сайта на сервере
4. Внутренняя поисковая оптимизация (SEO)
5. Внешняя поисковая оптимизация (SEO)
6. Методы шифрования. SQL-инекция. XSS-инъекции

LMS-платформа − не предусмотрена

5.2. Описание внеаудиторных контрольно-оценочных мероприятий и средств текущего контроля по дисциплине модуля

Разноуровневое (дифференцированное) обучение.

Базовый

5.2.1. Отчет по лабораторным работам

Примерный перечень тем

1. Сбор информации о веб-приложении.
2. Тестирование защищенности транспортного уровня
3. Тестирование защищенности механизма управления доступом.
4. Тестирование защищенности механизма управления сессиями
5. Поиск уязвимостей к атакам CSRF
6. Поиск уязвимостей к атакам XSS.
7. Сканирование уязвимостей веб-приложений.

Примерные задания

Цель работы

Целью лабораторной работы является обучение методам и средствам сбора информации об анализируемом веб-приложении.

Краткие теоретические сведения

Одним из первых этапов анализа защищенности любой компьютерной системы является сбор информации. В зависимости от

используемой методологии анализа защищенности вебприложения могут применяться различные методы и средства сбора информации. Стоит отметить, что сбор информации, как правило, не характерен для методологии инструментального анализа

защищенности (сканирования), а характерен для методологии тестирования на возможность проникновения.

Постановка задачи

Выполнить сбор информации об анализируемом вебприложении www.test.app.com

Цель работы

Целью лабораторной работы является обучение методам и средствам тестирования защищенности служб SSL/TLS.

Краткие теоретические сведения

Защита транспортного уровня веб-приложения основана на использовании протоколов семейства SSL/TLS, имеющих значительное количество механизмов, функций и параметров защиты, реализация и конфигурация которых определяет в конечном итоге уровень защищенности веб-приложения. Несмотря на то, что в настоящее время известно много автоматизированных средств тестирования защищенности SSL/TLS (например, сервис www.ssllabs.com, программы SSLscan и SSLyze), детали их реализации, как правило, неизвестны или требуют дополнительного исследования, что иногда не позволяет полностью доверять результатам их работы. Одним из низкоуровневых и надежных средств тестирования защищенности служб SSL/TLS является клиент OpenSSL.

Постановка задачи

Выполнить тестирование защищенности служб SSL/TLS вебсервера www.test.app.com

Цель работы

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

Краткие теоретические сведения

Одним из основных механизмов защиты современных вебприложений является механизм управления доступом. Обычно выделяют следующие этапы управления доступом [8]: − идентификация – установление идентификационных данных;

− аутентификация – подтвержденное установление идентификационных данных;

− авторизация – назначение прав идентификационным данным. При входе в веб-приложение (sign in, log in) пользователь идентифицируется (сообщает свой идентификатор) и аутентифицируется (доказывает, что он именно тот пользователь, чей идентификатор был сообщен).

Постановка задачи

Выполнить тестирование защищенности механизма управления доступом исследуемого веб-приложения.

Цель работы

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

Краткие теоретические сведения

Сессия веб-приложения – это последовательность HTTPзапросов и соответствующих им HTTP-ответов, ассоциированных с конкретным пользователем. Протокол HTTP не имеет встроенных механизмов управления сессиями (stateless protocol) и поэтому механизм управления сессиями реализуется логикой вебприложения. Как минимум, сессия создается при успешной аутентификации пользователя в веб-приложении. При этом генерируется уникальный идентификатор (токен) сессии, ассоциированный с этим пользователем. Данный идентификатор передается в каждом HTTP-запросе и является аналогом пароля пользователя, так как любой HTTP-запрос, содержащий такой идентификатор, будет воспринят веб-приложением как запрос от легитимного пользователя.

Постановка задачи

Выполнить тестирование защищенности механизма управления сессиями исследуемого веб-приложения.

Цель работы

Целью лабораторной работы является обучение методам и средствам идентификации и эксплуатации уязвимостей вебприложений к атакам CSRF.

Краткие теоретические сведения

Атака Cross-Site Request Forgery (CSRF или XSRF) переводится как «Межсайтовая подделка запросов» [14, 15]. Данная атака заключается в том, что злоумышленник вынуждает браузер пользователя отправить без ведома последнего произвольный HTTP-запрос.

Уязвимость к атаке CSRF обусловлена недостатками отсутствия или некорректности проверки веб-приложением источника (origin) HTTP-запросов.

Постановка задачи

Выполнить

Цель работы

Целью лабораторной работы является обучение методам и средствам идентификации и эксплуатации уязвимостей вебприложений к атакам XSS.

Краткие теоретические сведения

Атака Cross-Site Scripting (XSS) – это атака на веб-приложение, использующая недостатки неправильной обработки данных и позволяющая выполнить произвольный сценарий (JavaScript, VBScript) в контексте источника (origin) уязвимого вебприложения.

Атаки XSS классифицируются по вектору и способу воздействия. По вектору воздействия атаки XSS бывают отраженными (reflected), устойчивыми (persistent) и основанными на объектной модели документа (DOM-based). По вектору атаки XSS делятся на активные и пассивные.

Постановка задачи

Выполнить идентификацию и эксплуатацию уязвимостей к атакам XSS.

Цель работы

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

Краткие теоретические сведения

В настоящее время не существует технического решения, позволяющего полностью автоматизировать процесс анализа защищённости веб-приложений [19, 20]. Как показывает практика, средства анализа защищённости должны использоваться только на первом этапе тестирования таких приложений для предварительного поиска потенциальных уязвимостей. В целом сканеры безопасности могут помочь идентифицировать хорошо известные проблемы с безопасностью веб-приложений или, по крайней мере, облегчить работу по их поиску.

Постановка задачи

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

LMS-платформа − не предусмотрена

5.3. Описание контрольно-оценочных мероприятий промежуточного контроля по дисциплине модуля

5.3.1. Экзамен

Список примерных вопросов

1. Основы PHP.Формы. Работа с файловой системой
2. Сессии. HTTP-заголовки ответа сервера.
3. Основы работы с базами данных
4. Сокеты и сетевые функции
5. Размещение Web-сайта на сервере
6. Продвижение сайтов.
7. Внутренняя поисковая оптимизация (SEO)
8. Индексация сайта
9. Источники угроз информационной безопасности и меры по их предотвращению
10. Регламенты и методы разработки безопасных веб-приложений
11. Безопасная аутентификация и авторизация
12. Повышение привилегий и общая отказоустойчивость системы
13. Проверка корректроности данных, вводимых пользователем
14. Публикация изображений и файлов
15. Методы шифрования. SQL-инекция. XSS-инъекции
16. Планирование, организация и проектирование web-сайта
17. Основы web-технологий
18. Web-дизайн

LMS-платформа − не предусмотрена

5.4 Содержание контрольно-оценочных мероприятий по направлениям воспитательной деятельности

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения	**Контрольно-оценочные мероприятия**
Формирование информационной культуры в	целенаправленная работа с информацией	Технология самостоятельной работы	ОПК-7	З-2	Лабораторные занятия Отчет по

сети интернет	для использования в практических целях				лабораторным работам Экзамен