МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
Факультет «Информационные технологии»

УТВЕРЖДАЮ
Декан факультета
«Информационные технологии»
_____/Д.Г.Демидов/
«16» мая 2022

Рабочая программа дисциплины

«Информационная безопасность»

Направление подготовки/специальность

09.03.03 Прикладная информатика

Профиль/специализация

«Информационные технологии управления бизнесом»

Квалификация

Бакалавр

Формы обучения

Очная

Москва, 2022 г.

Разработчик(и):

ст.преподаватель / М.В.Даньшина /

Согласовано:
Заведующий кафедрой «Инфокогнитивные технологии»,
к.т.н., доцент / Е.А.Пухова /

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Информационная безопасность» относится:

- обучение студентов принципам эффективной организации информационной защиты;
- формирование у них умений восстановления частично потерянной информации.
- закрепление получаемых в семестре знаний и навыков на практике;
- формирование взаимосвязей, получаемых в семестре знаний и навыков с изученными ранее;
- подготовка студентов к деятельности в соответствии с квалификационной характеристикой бакалавра.

К **основным задачам** дисциплины «Информационная безопасность» относятся:

- закрепление основ программирования;
- освоение современных технологий защиты от различных атак в Интернете;
- способность использовать основные принципы информационной безопасности в различных сферах деятельности.

Обучение по дисциплине «Информационная безопасность» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ИОПК-3.1. Знает принципы информационной и библиографической культуры, методы, способы и средства получения, хранения и переработки информации; принципы построения современных информационно-коммуникационных технологий; модели организации данных, сетевые модели, иерархические модели, реляционную модель и объектную модель. ИОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ИОПК-3.3. Владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры, с учетом соблюдения авторского права и требований информационной безопасности.

2 Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» относится к числу учебных дисциплин формируемые участниками образовательных отношений части «ИТ-разработка» основной образовательной программы.

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП:

- «Основы тестирования»,
- «Прикладное проектирование»,
- «Документирование этапов жизненного цикла ИС»,
- «Проектирование баз данных»,
- «Основы разработки КИС»,
- «Мобильная разработка»,
- «Надежность ПО и ИС»,
- «Проектная деятельность».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единицы 108 академических часов).

3.1 Виды учебной работы и трудоемкость (по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			7	
1	**Аудиторные занятия**	**54**	54	
	В том числе:			
1.1	Лекции			
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	54	54	
2	**Самостоятельная работа**	**54**	54	
3	**Промежуточная аттестация**			
	Зачет/диф.зачет/экзамен	**экзамен**	**экзамен**	
	Итого:	**108**	108	

3.2 Тематический план изучения дисциплины (по формам обучения)

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Вводная лекция «Основы информационной безопасности»						
2	Л/р №1 «Защита от XSS INJECTION (постоянной)»	6			3		3
3	Л/р №2 «Защита от XSS INJECTION (отраженной)»	6			3		3
4	Л/р №3 «Защита от FILE INJECTION»	6			3		3
5	Лекция «Уязвимости веб-приложений»						
6	Л/р №4 «Защита от BRUTE FORCE»	6			3		3
7	Л/р №5 «Защита от CLICKJACKING»	6			3		3
8	Л/р №6 «Защита от SQL INJECTION (слепой)»	6			3		3
9	Лекция «Информационная безопасность в Интернет. Тренды»						
10	Л/р №7 «Защита от SQL INJECTION (явной)»	6			3		3
11	Л/р №8 «Защита от загрузки вредоносных файлов»	6			3		3
12	Л/р №9 «Защита от слабого шифрования»	6			3		3
13	Лекция «Защита веб-приложений на PHP»						
14	Л/р №10 «Защита от выполнения команд на сервере»	6			3		3
15	Л/р №11 «Защита от CSRF атаки»	6			3		3
16	Л/р №12 «Защита от раскрытия пути»	6			3		3
17	Лекция «Основные угрозы ИБ»						
18	Л/р №13 «Защита от получения исходного кода приложения (полного)»	6			3		3

19	Л/р №14 «Защита от получения транзакций пользователей»	6			3		3
20	Л/р №15 «Защита от получения данных пользователей»	6			3		3
21	Лекция «Мотивация злоумышленника»						
22	Л/р №16 «Защита от получения полного доступа к серверу»	6			3		3
23	Л/р №17 «Защита от авторизации под произвольным пользователем»	6			3		3
24	Л/р №18 «Защита от перевода средств от лица другого пользователя»	6			3		3
Итого		**108**			**54**		**54**

3.3 Содержание дисциплины

1. Основы информационной безопасности
2. Уязвимости веб-приложений и ИС
3. Информационная безопасность в Интернет. Тренды.
4. Защита веб-приложений на PHP.
5. Основные угрозы ИБ.
6. Мотивация злоумышленника

3.4 Тематика лабораторных занятий

1. ЗАЩИТА ОТ XSS INJECTION (ПОСТОЯННОЙ)

Содержание и порядок выполнения лабораторной работы:

- анализ кода тестового приложения и нахождение указанной уязвимости;
- разработка приложения без указанной уязвимости.

2. ЗАЩИТА ОТ XSS INJECTION (ОТРАЖЁННОЙ)

Содержание и порядок выполнения лабораторной работы:

- анализ кода тестового приложения и нахождение указанной уязвимости;
- разработка приложения без указанной уязвимости.

3. ЗАЩИТА ОТ FILE INJECTION

Содержание и порядок выполнения лабораторной работы:

- анализ кода тестового приложения и нахождение указанной уязвимости;
- разработка приложения без указанной уязвимости.

4. ЗАЩИТА ОТ BRUTE FORCE

Содержание и порядок выполнения лабораторной работы:

- анализ кода тестового приложения и нахождение указанной уязвимости;
- разработка приложения без указанной уязвимости.

5. ЗАЩИТА ОТ CLICKJACKING

Содержание и порядок выполнения лабораторной работы:

- анализ кода тестового приложения и нахождение указанной уязвимости;
- разработка приложения без указанной уязвимости.

6. ЗАЩИТА ОТ SQL INJECTION (СЛЕПОЙ)

Содержание и порядок выполнения лабораторной работы:

- анализ кода тестового приложения и нахождение указанной уязвимости;
- разработка приложения без указанной уязвимости.

7. ЗАЩИТА ОТ SQL INJECTION (ЯВНОЙ)

Содержание и порядок выполнения лабораторной работы:

- анализ кода тестового приложения и нахождение указанной уязвимости;
- разработка приложения без указанной уязвимости.

8. ЗАЩИТА ОТ ЗАГРУЗКИ ВРЕДОНОСНЫХ ФАЙЛОВ

Содержание и порядок выполнения лабораторной работы:

- анализ кода тестового приложения и нахождение указанной уязвимости;
- исправление уязвимости.

9. ЗАЩИТА ОТ СЛАБОГО ШИФРОВАНИЯ

Содержание и порядок выполнения лабораторной работы:

- анализ кода тестового приложения и нахождение указанной уязвимости;
- исправление уязвимости.

10. ЗАЩИТА ОТ ВЫПОЛНЕНИЯ КОМАНД НА СЕРВЕРЕ

Содержание и порядок выполнения лабораторной работы:

- анализ кода тестового приложения и нахождение указанной уязвимости;
- исправление уязвимости.

11. ЗАЩИТА ОТ CSRF АТАКИ

Содержание и порядок выполнения лабораторной работы:

- анализ кода тестового приложения и нахождение указанной уязвимости;
- исправление уязвимости.

12. ЗАЩИТА ОТ РАСКРЫТИЯ ПУТИ

Содержание и порядок выполнения лабораторной работы:

- анализ кода тестового приложения и нахождение указанной уязвимости;
- исправление уязвимости.

13. ЗАЩИТА ОТ ПОЛУЧЕНИЯ ИСХОДНОГО КОДА ПРИЛОЖЕНИЯ (ПОЛНОГО)

Содержание и порядок выполнения лабораторной работы:

- анализ кода тестового приложения и нахождение указанной уязвимости;
- исправление уязвимости.

14. ЗАЩИТА ОТ ПОЛУЧЕНИЯ ТРАНЗАКЦИЙ ПОЛЬЗОВАТЕЛЕЙ

Содержание и порядок выполнения лабораторной работы:

- анализ кода тестового приложения и нахождение указанной уязвимости;
- исправление уязвимости.

15. ЗАЩИТА ОТ ПОЛУЧЕНИЯ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ

Содержание и порядок выполнения лабораторной работы:

- анализ кода тестового приложения и нахождение указанной уязвимости;
- исправление уязвимости.

16. ЗАЩИТА ОТ ПОЛУЧЕНИЯ ПОЛНОГО ДОСТУПА К СЕРВЕРУ

Содержание и порядок выполнения лабораторной работы:

- анализ кода тестового приложения и нахождение указанной уязвимости;
- исправление уязвимости.

17. ЗАЩИТА ОТ АВТОРИЗАЦИИ ПОД ПРОИЗВОЛЬНЫМ ПОЛЬЗОВАТЕЛЕМ

Содержание и порядок выполнения лабораторной работы:

- анализ кода тестового приложения и нахождение указанной уязвимости;
- исправление уязвимости.

18. ЗАЩИТА ОТ ПЕРЕВОДА СРЕДСТВ ОТ ЛИЦА ДРУГОГО ПОЛЬЗОВАТЕЛЯ

Содержание и порядок выполнения лабораторной работы:

- анализ кода тестового приложения и нахождение указанной уязвимости;
- исправление уязвимости.

4 Учебно-методическое и информационное обеспечение

4.1 Основная литература

1. Краковский, Ю. М. Защита информации : учебное пособие / Ю. М. Краковский. — Ростов-на-Дону : Феникс, 2016. — 347 с. — ISBN 978-5-222-26911-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/102279 (дата обращения: 28.09.2023). — Режим доступа: для авториз. пользователей.

4.2 Дополнительная литература

1. Леонтьев, А. С. Защита информации : учебное пособие / А. С. Леонтьев. — Москва : РТУ МИРЭА, 2021. — 79 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182491 (дата обращения: 28.09.2023). — Режим доступа: для авториз. Пользователей.

4.3 Электронные образовательные ресурсы

Защита информации https://online.mospolytech.ru/course/view.php?id=10487

4.4 Лицензионное и свободно распространяемое программное обеспечение

1. Visual Studio Code
2. Браузеры Chrome, Edge, Firefox

3. OpenVPN с правами для запуска у студентов
4. FileZilla
5. PuTTy
6. Git
7. Node.js 18
8. Python 3.10
9. Wireshark

4.5 Современные профессиональные базы данных и информационные справочные системы

1. https://owasp.org/

5 Материально-техническое обеспечение

Для проведения лабораторных работ и самостоятельной работы студентов подходят аудитории, оснащенные компьютерами с программным обеспечением в соответствии со списком в пункте 4.5 и подключенные к интернету.

Число рабочих мест в аудитории должно быть достаточным для обеспечения индивидуальной работы студентов.

Рабочее место преподавателя должно быть оснащено компьютером с подключенным к нему проектором или иным аналогичным по функциональному назначению оборудованием.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

Методика преподавания дисциплины «Информационная безопасность» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков у обучающихся:

- выполнение лабораторных работ в лабораториях вуза; посещение лекций;
- индивидуальные и групповые консультации студентов преподавателем;
- посещение профильных конференций и работа на мастер-классах экспертов и специалистов в веб-технологиях, веб-разработке, Интернет-маркетинге и других профессиональных областях.

Самостоятельная внеаудиторная работа студентов состоит из подготовки к выполнению и защите лабораторных работ, изучению теоретического материала, а также подготовки к промежуточной аттестации во время экзаменационной сессии.

Рекомендуется:

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются *аудиторные занятия, лекции, лабораторные работы.*

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты и записи, готовятся к проведению и обрабатывают результаты лабораторных работ, готовятся к промежуточной аттестации, а также самостоятельно изучают отдельные темы учебной программы.

На занятиях студентов, в том числе предполагающих практическую деятельность, осуществляется закрепление полученных, в том числе и в процессе самостоятельной работы, знаний. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста в области Веб-технологий.

Самостоятельная работа осуществляется индивидуально. Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на аудиторных занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- выполнение лабораторных работ, зачет.

7.2 Шкала и критерии оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**

ОПК-2				
	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины.	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины. Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины. Свободно оперирует приобретенными знаниями.

7.3 Оценочные средства

7.3.1 Текущий контроль

В результате освоения дисциплины формируются следующие компетенции: ОПК-2

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплины в соответствии с учебным планом и календарным графиком учебного процесса.

7.3.2 Промежуточная аттестация

Шкалы оценивания результатов промежуточной аттестации и их описание:

ФОРМА ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ: ЭКЗАМЕН.

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по

дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

К промежуточной аттестации допускаются только студенты, выполнившие все виды учебной работы, предусмотренные рабочей программой по дисциплине «Информационная безопасность» – выполнение и защита Лабораторных работ согласно полученному заданию с достижением порогового значения оценки.

Шкала оценивания	**Описание**
Отлично	Среднее значение для всех формируемых на момент проведения аттестации уровней компетенций – 5. Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Среднее значение для всех формируемых на момент проведения аттестации уровней компетенций – 4. Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Среднее значение для всех формируемых на момент проведения аттестации уровней компетенций – 3. Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не достигнуто пороговое значение хотя бы для одного уровня формируемых на момент проведения аттестации компетенций. Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.4 Перечень оценочных средств

№ ОС	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Устный опрос / собеседование, (УО)	Средство контроля, организованное как презентация обучающимся результатов выполнения Курсового проекта с демонстрацией наглядных материалов и ответов на вопросы педагогических работников (работника) на тему доклада, теме, проблеме и т.п.	Контрольные вопросы
2	Проект (П)	Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированности аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся.	Типовая программа экзамена

7.5 Описание оценочных средств

1. Прогресс информационных технологий и необходимость обеспечения информационной безопасности.
2. Основные понятия информационной безопасности.
3. Структура понятия информационная безопасность.
4. Система защиты информации и ее структура.
5. Экономическая информация как товар и объект безопасности.
6. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
7. Персональные данные и их защита.
8. Информационные угрозы, их виды и причины возникновения.
9. Информационные угрозы для государства.
10. Информационные угрозы для компании.
11. Информационные угрозы для личности (физического лица).
12. Действия и события, нарушающие информационную безопасность.
13. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
14. Способы воздействия информационных угроз на объекты.
15. Внешние и внутренние субъекты информационных угроз.
16. Компьютерные преступления и их классификация.

17. Исторические аспекты компьютерных преступлений и современность.
18. Субъекты и причины совершения компьютерных преступлений.
19. Вредоносные программы, их виды.
20. История компьютерных вирусов и современность.
21. Государственное регулирование информационной безопасности.
22. Деятельность международных организаций в сфере информационной безопасности.
23. Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации.
24. Доктрина информационной безопасности России.
25. Уголовно-правовой контроль над компьютерной преступностью в России.
26. Федеральные законы по ИБ в РФ.
27. Политика безопасности и ее принципы.
28. Фрагментарный и системный подход к защите информации.
29. Методы и средства защиты информации.
30. Организационное обеспечение ИБ.
31. Организация конфиденциального делопроизводства.
32. Комплекс организационно-технических мероприятий по обеспечению защиты информации.
33. Инженерно-техническое обеспечение компьютерной безопасности.
34. Организационно-правовой статус службы безопасности.
35. Защита информации в Интернете.
36. Электронная почта и ее защита.
37. Защита от компьютерных вирусов.
38. «Больные» мобильники и их «лечение».
39. Популярные антивирусные программы и их классификация.
40. Организация системы защиты информации экономических объектов.
41. Криптографические методы защиты информации.
42. Этапы построения системы защиты информации.
43. Оценка эффективности инвестиций в информационную безопасность.
44. План обеспечения непрерывной работы и восстановления функционирования автоматизированной информационной системы.
45. Управление информационной безопасности на государственном уровне.
46. Аудит ИБ автоматизированных банковских систем.
47. Электронная коммерция и ее защита.
48. Менеджмент и аудит информационной безопасности на уровне предприятия.
49. Информационная безопасность предпринимательской деятельности.
50. Обеспечение информационной безопасности должностных лиц и представителей деловых кругов.

7.6 Типовая программа экзамена

ВРЕМЯ ВЫПОЛНЕНИЯ ЗАДАНИЯ

4 астрономических часа. Перерывы во время выполнения задания не предполагаются.

ЗАДАНИЕ ЭКЗАМЕНА

Руководства банка весьма довольно вашими успехами в мобильной разработке и резким увеличением числа клиентов. Победа в конкурсе "Лучшее банковское мобильное приложение" открыло перед вами горизонт новых задач, одна из которых лежит в области информационной безопасности.

Многочисленные жалобы клиентов выявили существенную проблему в используемом программном обеспечении – наличие уязвимостей веб-приложений и сервисов, с которыми Вы работали. Как специалисту наиболее хорошо знакомым с их *API* (к сожалению разработчик собственно ПО исчез из поля зрения банка, по слухам последний раз его видели на Канарских островах… но служба безопасности активно его ищет) Вам поручено провести аудит сервисов и обнаружить все уязвимости.

Руководство банка после прискорбного исчезновения разработчика не вполне доверяет вам, поэтому тестирование будет производиться по методу “чёрного ящика”, то есть изначально у вас не будет доступа к исходному коду приложения (хотя впоследствии, при успешном взломе, Вы сможете посмотреть данный код). В первую очередь аудиту должно подвергнуться хорошо известное стандартное банковское приложение, имеющее знакомый интерфейс и возможности – авторизация, получение списка друзей, проведение транзакции и получение списка транзакций. Именно оно, благодаря успеху мобильного приложения, наиболее часто используется клиентами.

Срочность и важность задачи вынудило руководство банка объявить существенную награду за успешное выполнение задания, даже если оно выполнено лишь частично. Премия зависит как от сложности, критичности и количества обнаруженных уязвимостей, приводящих к утечке персональных данных материальным и репутационным потерям, так и от полноты их описания и рекомендаций по устранению. Но помните – ваша дальнейшая судьба как сотрудника банка зависит от полноты решенной задачи, старайтесь найти как можно больше уязвимостей иначе будете уволены.

ВХОДНЫЕ ДАННЫЕ

Для того, чтобы тесты не повредили рабочее ПО, администраторы банка создали две виртуальные машины в формате *Virtualbox*, полностью копирующие системы действующих серверов, которые Вы можете использовать для работы.

1. Виртуальная машина с действующим веб-приложением для тестирования. После запуска образа веб- приложение доступно по локальному адресу виртуальной машины (http://192.168.56.12). Использованием данной виртуальной машины как-либо кроме протокола *HTTP*, либо тестирование уязвимости других протоколов не подразумевается. Исходя из этого на ней отсутствует графическая оболочка, и машина защищена паролем.
2. Виртуальная машина Kali Linux 2016.2 со специальным дистрибутивом Linux с графической оболочкой и предустановленной возможностью ввода текста на русском языке для проведения тестирования. Данная виртуальная машина находится в той же виртуальной подсети, что и машина с веб-приложением – таким образом, имеется возможность использовать инструменты, входящие в состав Kali Linux, напрямую на тестируемом приложении.

ВЫХОДНЫЕ ДАННЫЕ

В результате работы в папке "*Рабочий стол/ФИО - Номер группы/WEBSECURE*" должен быть предоставлен файл *report.docx,* содержащий следующую информацию.

Вашу ФИО.

Номер группы.

Таблицу с отчетом по найденным уязвимостям, содержащую следующую информацию:

№ по порядку:

- вид уязвимости;
- место расположение в веб-сервисе;
- используемый способ обнаружения уязвимости;
- описание уязвимости;
- потенциальные угрозы для рассматриваемого веб-приложения;
- методы устранения уязвимостей данного типа;
- причины возникновения уязвимости в данном веб-приложении;
- рекомендации по устранению уязвимости;
- скриншоты экранов, показывающие процесс обнаружения и результат использования уязвимости злоумышленником.

УСЛОВИЯ ВЫПОЛНЕНИЯ РАБОТЫ

Для выполнения задания допускается использование только установленных средств и ПО локального компьютера и указанных виртуальных машин. Не допускается использование интернет в любом виде, *flash*-накопителей, телефонов, ноутбуков, материалов на серверах.

КРИТЕРИИ ОЦЕНКИ ЗАДАНИЯ

№	Найденная уязвимость или возможность совершить действие	Награда, $
XSS INJECTION (ПОСТОЯННАЯ)		**2000**
1	Нахождение	200
2	Полное описание	800
3	Рекомендации по исправлению	1000
XSS INJECTION (ОТРАЖЁННАЯ)		**1000**
4	Нахождение	100
5	Полное описание	400
6	Рекомендации по исправлению	500
FILE INJECTION		**2000**
7	Нахождение	200
8	Полное описание	800
9	Рекомендации по исправлению	1000
BRUTE FORCE		**3000**
10	Нахождение	300
11	Полное описание	1200
12	Рекомендации по исправлению	1500
CLICKJACKING		**1000**
13	Нахождение	100
14	Полное описание	400
15	Рекомендации по исправлению	500
SQL INJECTION (СЛЕПАЯ)		**3000**
16	Нахождение	300
17	Полное описание	1200
18	Рекомендации по исправлению	1500
SQL INJECTION (ЯВНАЯ)		**2000**

19	Нахождение	200
20	Полное описание	800
21	Рекомендации по исправлению	1000
ЗАГРУЗКА ВРЕДОНОСНЫХ ФАЙЛОВ		**2000**
22	Нахождение	200
23	Полное описание	800
24	Рекомендации по исправлению	1000
СЛАБОЕ ШИФРОВАНИЕ		**2000**
25	Нахождение	200
26	Полное описание	800
27	Рекомендации по исправлению	1000
ВЫПОЛНЕНИЕ КОМАНД НА СЕРВЕРЕ		**4000**
28	Нахождение	400
29	Полное описание	1600
30	Рекомендации по исправлению	2000
CSRF АТАКА		**1000**
31	Нахождение	100
32	Полное описание	400
33	Рекомендации по исправлению	500
РАСКРЫТИЕ ПУТИ		**1000**
34	Нахождение	100
35	Полное описание	400
36	Рекомендации по исправлению	500
ПОЛУЧЕНИЕ ИСХОДНОГО КОДА ПРИЛОЖЕНИЯ (ПОЛНОГО)		**6000**
37	Нахождение	600
38	Полное описание	2400
39	Рекомендации по исправлению	3000
ПОЛУЧЕНИЕ ТРАНЗАКЦИЙ ПОЛЬЗОВАТЕЛЕЙ		**1000**
40	Нахождение	100
41	Полное описание	400
42	Рекомендации по исправлению	500
ПОЛУЧЕНИЕ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ		**1000**
43	Нахождение	100
44	Полное описание	400
45	Рекомендации по исправлению	500
ПОЛУЧЕНИЕ ПОЛНОГО ДОСТУПА К СЕРВЕРУ		**10 000**
46	Нахождение	1000
47	Полное описание	4000
48	Рекомендации по исправлению	5000
АВТОРИЗАЦИЯ ПОД ПРОИЗВОЛЬНЫМ ПОЛЬЗОВАТЕЛЕМ		**1000**
49	Нахождение	100
50	Полное описание	400
51	Рекомендации по исправлению	500
ПЕРЕВОД СРЕДСТВ ОТ ЛИЦА ДРУГОГО ПОЛЬЗОВАТЕЛЯ		**1000**
52	Нахождение	100
53	Полное описание	400
54	Рекомендации по исправлению	500

СООТВЕТСТВИЕ НАБРАННЫХ БАЛЛОВ ОЦЕНКЕ ЭКЗАМЕНА

Результат работы оценивается согласно приведенным выше критериям, выполнение каждого из которых увеличивает результирующее вознаграждение на указанное значение. Максимальное виртуальное вознаграждение, получаемое студентом за успешное выполнение задания с учетом всех критериев – 44 000$. Итоговое вознаграждение преобразуется в оценку согласно следующей таблиц**е.**

Диапазон баллов	Оценка
0 … 11 999	Неудовлетворительно
12 000 … 15 999	Удовлетворительно
16 000 … 21 999	Хорошо
22 000 … 44 000	Отлично

Набранные баллы и соответствующая им оценка имеет рекомендательный характер – экзаменатор имеет право скорректировать оценку в ту или иную сторону.