Перечень теоретических и практических заданий к экзамену по МДК.09.03 Обеспечение безопасности веб-приложений (3 курс, 5 семестр 2025-2026 уч. г.)

Форма контроля: Практическая работа (Информационно-аналитический)
Описательная часть: По выбору выполнить 1 теоретическое задание и 1 практическое задание

Перечень теоретических заданий:

Задание №1

1. Что такое DoS атака?

2. Что такое DDoS атака?

3. Как защитится от DoS и DDoS атак?

Оценка	Показатели оценки
5	Дан ответ на 3 вопроса из 3.
4	Дан ответ на 2 вопроса из 3.
3	Дан ответ на 1 вопрос из 3.

Задание №2

Дать классификацию атак XSS по вектору и способу воздействия. Охарактеризовать основные уязвимости к атакам XSS, связанные с контекстом, в который выводятся данные.

Оценка	Показатели оценки
5	Представлен развернутый ответ на вопрос.
4	Представлен развернутый ответ на вопрос, с незначительными ошибками.
3	Представлен краткий ответ на вопрос.

Задание №3

Дать классификацию атак XSS по вектору и способу воздействия. Охарактеризовать основные уязвимости к атакам XSS, связанные с контекстом, в который выводятся данные.

Оценка	Показатели оценки
5	Представлен развернутый ответ на вопрос.
4	Представлен развернутый ответ на вопрос, с незначительными ошибками.
3	Представлен краткий ответ на вопрос.

Задание №4

Дать классификацию атак XSS по вектору и способу воздействия. Охарактеризовать основные уязвимости к атакам XSS, связанные с контекстом, в который выводятся данные.

Оценка	Показатели оценки
5	Представлен развернутый ответ на вопрос.
4	Представлен развернутый ответ на вопрос, с незначительными ошибками.
3	Представлен краткий ответ на вопрос.

Задание №5

Перечислите основные разновидности атак SQL-injection, опишите механизм действия каждой из них

Оценка	Показатели оценки
5	Приведены не менее 6 разновидностей атак SQL-injection (классическая; «слепая» типа boolean-based; «слепая» типа time-based; error-based; вложенная; фрагментированна), детально разобраны действия каждой из них
4	Приведены не менее 4 разновидностей атак SQL-injection, описаны действия каждой из них, допущены незначительные ошибки
3	Приведено не более 3 разновидностей атак SQL-injection, действия каждой описаны, допущены грубые ошибки

Задание №6

Перечислите основные разновидности атак SQL-injection, опишите механизм действия каждой из них

Оценка	Показатели оценки
5	Приведены не менее 6 разновидностей атак SQL-injection (классическая; «слепая» типа boolean-based; «слепая» типа time-based; error-based; вложенная; фрагментированная), детально разобраны действия каждой из них
4	Приведены не менее 4 разновидностей атак SQL-injection, описаны действия каждой из них, допущены незначительные ошибки
3	Приведено не более 3 разновидностей атак SQL-injection, действия каждой описаны, допущены грубые ошибки

Задание №7

1. Исследовать механизм восстановления паролей выбранного веб-приложения из топ-рейтинга SimilarWeb, дать экспертную оценку с точки зрения безопасности.

2. Исследовать минимально допустимую длину и сложность паролей в произвольных пяти веб-приложениях из топ-рейтинга SimilarWeb, дать экспертную оценку с точки зрения безопасности.

3. Исследовать наличие оракулов в механизмах аутентификации произвольных пяти веб-приложениях из топ-рейтинга SimilarWeb, дать экспертную оценку с точки зрения безопасности.

Оценка	Показатели оценки
5	Выполнены 3 пункта задания.
4	Выполнены 2 пункта задания.
3	Выполнен 1 пункт задания.

Задание №8

Назвать и описать основные типы угроз информационной безопасности веб-приложения.

Оценка	Показатели оценки
5	Представлен развернутый ответ на вопрос.
4	Представлен развернутый ответ на вопрос, с незначительными ошибками.
3	Представлен краткий ответ на вопрос.

Задание №9

Описать самые распространенные виды XSS, причины и механизм их воздействия

Оценка	Показатели оценки
5	Полностью описаны все виды XSS, причины, механизм и результаты их воздействия, даны рекомендации по предотвращению угрозы XSS
4	Описаны все виды XSS и механизм их воздействия, даны рекомендации по предотвращению угрозы XSS
3	Описаны не менее 2 видов XSS и результаты их воздействия

Задание №10

Представить ответы на следующие вопросы:

1. Что такое протокол?

2. Чем отличаются метода GET и POST?

3. Что такое JSON?

Оценка	Показатели оценки

3	Представлены ответы на все вопросы.
4	Представлены ответы на 2 вопроса.
5	Представлен ответ на 1 вопрос.

Задание №11

Назвать и описать основные типы угроз информационной безопасности веб-приложения.

Оценка	Показатели оценки
3	Представлен развернутый ответ на вопрос.
4	Представлен развернутый ответ на вопрос, с незначительными ошибками.
5	Представлен краткий ответ на вопрос.

Задание №12

Назвать меры по предотвращению угроз информационной безопасности веб-приложения.

Оценка	Показатели оценки
3	Представлен развернутый ответ на вопрос.
4	Представлен развернутый ответ на вопрос, с незначительными ошибками.
5	Представлен краткий ответ на вопрос.

Задание №13

1. Описать процедуру проверки веб-приложения на уязвимость к атаке CSRF.

2. Как эксплойт, отправляющий данные типа multipart/form-data.может быть использован при CSRF-атаке, приведите пример.

3. Описать признаки уязвимости веб-приложения к CSRF-атаке

Оценка	Показатели оценки
5	Выполнены 3 пункта задания
4	Выполнены 2 пункта задания
3	Выполнен 1 пункт задания

Задание №14

Произвести тестирование пользовательского интерфейса web приложения:

1. разработать тест-требования и тест-план для проверки пользовательского интерфейса;

2. разработать тест-кейс и тест-сьют для проверки пользовательского интерфейса;

3. произвести выполнение тестовых примеров и сбор информации о выполнении тестов.

Оценка	Показатели оценки
5	Выполнено 3 задания из 3.
4	Выполнено 2 задания из 3.
3	Выполнено 1 задания из 3.

Задание №15

Представить ответы на вопросы:

1. Какие типы тестирования веб-приложения существуют?

2. Какой тип тестирования предпочтителен для анализа веб-приложений?

3. Описать процесс тестирования для одного из типов тестирования.

Оценка	Показатели оценки
5	Представлены 3 пункта задания.
4	Представлены 2 пункта задания.
3	Представлен 1 пункт задания.

Задание №16

Представить ответы на вопросы:

1. Какие типы тестирования веб-приложения существуют?

2. Какой тип тестирования предпочтителен для анализа веб-приложений?

3. Описать процесс тестирования для одного из типов тестирования.

Оценка	Показатели оценки
5	Представлены 3 пункта задания.
4	Представлены 2 пункта задания.
3	Представлен 1 пункт задания.

Задание №17

Провести анализ методов защиты от атак на уровне Backend и обосновать не менее 9 рекомендаций для их предотвращения

Оценка	Показатели оценки
5	Проведен анализ методов защиты от атак на уровне Backend и обоснованы не менее 9 рекомендаций для их предотвращения
4	Сформулированы не менее 9 рекомендаций для предотвращения атак на уровне Backend
3	Сформулированы не менее 5 рекомендаций для предотвращения атак на уровне Backend

Задание №18

Определите не менее 9 базовых принципов разработки безопасных веб-приложений

Оценка	Показатели оценки
5	Проведен анализ потенциальных угроз и обоснованы не менее 9 рекомендаций по разработке безопасных веб-приложений
4	Приведены не менее 9 рекомендаций по разработке безопасных веб-приложений
3	Приведены не менее 7 рекомендаций по разработке безопасных веб-приложений

Задание №19

Какие меры позволяют идентифицировать уязвимости связанные с загрузкой файлов на сервер

Оценка	Показатели оценки
5	Проведен анализ потенциальных уязвимостей и обоснованы не менее 10 рекомендаций, позволяющих идентифицировать уязвимости связанные с загрузкой файлов на сервер
4	Приведены 10 рекомендаций, позволяющих идентифицировать уязвимости связанные с загрузкой файлов на сервер
3	Приведены минимум 7 рекомендаций, позволяющих идентифицировать уязвимости связанные с загрузкой файлов на сервер

Задание №20

Провести анализ методов защиты от атак на уровне Backend и обосновать не менее 9 рекомендаций для их предотвращения

Оценка	Показатели оценки

5	Проведен анализ методов защиты от атак на уровне Backend и обоснованы не менее 9 рекомендаций (*1. Аутентификация и авторизация, 2. Защита от инъекций, 3. Управление сеансами, 4. Защита от межсайтовой подделки запросов (CSRF), 5. Контроль доступа и авторизация, 6. Мониторинг и аудит безопасности, 7. Обновления и патчи безопасности, 8. Обучение персонала, 9. Тестирование*) для их предотвращения
4	Сформулированы не менее 9 рекомендаций для предотвращения атак на уровне Backend
3	Сформулированы не менее 5 рекомендаций для предотвращения атак на уровне Backend

Задание №21

Какие меры позволяют идентифицировать уязвимости связанные с загрузкой файлов на сервер

Оценка	Показатели оценки
5	Проведен анализ потенциальных уязвимостей и обоснованы не менее 10 рекомендаций (определены: функции загрузки файлов, функциональность загрузки файлов, тестирование типов расширений файлов, проверка типов загружаемых данных (скрипт, шелл-код, вирус), проверка максимального размера файлов, правильности имен файлов (наличие запрещенных символов), аутентификации и контроль доступа при загрузке, наличия уязвимостей при перезаписи файла, отслеживание и регистрация действия во время тестирования, документирование уязвимостей и/или проблем), позволяющих идентифицировать уязвимости связанные с загрузкой файлов на сервер
4	Приведены 10 рекомендаций, позволяющих идентифицировать уязвимости связанные с загрузкой файлов на сервер
3	Приведены минимум 7 рекомендаций, позволяющих идентифицировать уязвимости связанные с загрузкой файлов на сервер

Задание №22

1. Описать процедуру проверки веб-приложения на уязвимость к атаке CSRF.

2. Как эксплойт, отправляющий данные типа multipart/form-data.может быть использован при CSRF-атаке, приведите пример.

3. Описать признаки уязвимости веб-приложения к CSRF-атаке

Оценка	Показатели оценки
5	Выполнены 3 пункта задания
4	Выполнены 2 пункта задания
3	Выполнен 1 пункт задания

Задание №23

1. Описать процедуру проверки веб-приложения на уязвимость к атаке CSRF.

2. Как эксплойт, отправляющий данные типа multipart/form-data может быть использован при CSRF-атаке, приведите пример.

3. Описать признаки уязвимости веб-приложения к CSRF-атаке

Оценка	Показатели оценки
5	Выполнены 3 пункта задания
4	Выполнены 2 пункта задания
3	Выполнен 1 пункт задания

Задание №24

Представить ответы на следующие вопросы:

1. Что такое протокол?

2. Чем отличаются метода GET и POST?

3. Что такое JSON?

Оценка	Показатели оценки
5	Представлены ответы на все вопросы.
4	Представлены ответы на 2 вопроса.
3	Представлен ответ на 1 вопрос.

Задание №25

Определить и описать меры по предотвращению угроз информационной безопасности веб-приложения.

Оценка	Показатели оценки
5	Представлен развернутый ответ на вопрос.
4	Представлен развернутый ответ на вопрос, с незначительными ошибками.
3	Представлен краткий ответ на вопрос.

Задание №26

Представить ответы на вопросы:

1. Какие типы тестирования веб-приложения существуют?

2. Какой тип тестирования предпочтителен для анализа веб-приложений?

3. Описать процесс тестирования для одного из типов тестирования.

Оценка	Показатели оценки
5	Представлены 3 пункта задания.
4	Представлены 2 пункта задания.
3	Представлен 1 пункт задания.

Задание №27

Определите не менее 9 базовых принципов разработки безопасных веб-приложений

Оценка	Показатели оценки
5	Проведен анализ потенциальных угроз и обоснованы не менее 9 рекомендаций по разработке безопасных веб-приложений (Планирование требований безопасности, документированный план безопасности, Практики безопасного кодирования, Минимум зависимости от внешних сущностей, Проверка данных, шифрование и обфускация, Аутентификация и авторизация, Разделение и минимизация привилегий, Изоляция компонентов, Мониторинг и аудит, тестирование на проникновение, Политика безопасности контента, Политика управление сеансами, Защита данных сессии, Обновление компонент))
4	Приведены не менее 9 рекомендаций по разработке безопасных веб-приложений
3	Приведены не менее 7 рекомендаций по разработке безопасных веб-приложений

Задание №28

Назвать два основных способа избежать SQL injection.

Оценка	Показатели оценки
3	Представлен развернутый ответ на вопрос.
4	Представлен развернутый ответ на вопрос, с незначительными ошибками.
5	Представлен краткий ответ на вопрос.

Задание №29

Описать и привести пример защиты веб-приложения от Cross Site Scripting (XSS).

Оценка	Показатели оценки
3	Представлен развернутый ответ на вопрос.

4	Представлен развернутый ответ на вопрос, с незначительными ошибками.
5	Представлен краткий ответ на вопрос.

Перечень практических заданий:

Задание №1

Представить ответы на вопросы:

1. Какие типы тестирования веб-приложения существуют?

2. Какой тип тестирования предпочтителен для анализа веб-приложений?

3. Описать процесс реализации одного из типа тестирования.

Оценка	Показатели оценки
5	Представлены 3 пункта задания.
4	Представлены 2 пункта задания.
3	Представлен 1 пункт задания.

Задание №2

Провести тестирование на устойчивость к атакам отказа в обслуживании.

Оценка	Показатели оценки
5	Задание выполнено в полном объеме.
4	Задание выполнено с незначительными ошибками.
3	Задание выполнено с грубыми ошибками.

Задание №3

Представить алгоритм тестирования защищенности механизма управления доступом и сессиями и реализовать его.

Оценка	Показатели оценки
5	Задание выполнено в полном объеме.
4	Задание выполнено в полном объеме. с несущественными ошибками.
3	Задание выполнено с грубыми ошибками.

Задание №4

1. Произвести тестирование web приложения на XSS.

2. Произвести тестирование web приложения на Cross-Site Scripting.

3. Произвести тестирование web приложения на SQL-инъекция.

Оценка	Показатели оценки
5	Выполнено 3 задания из 3.
4	Выполнено 2 задания из 3.
3	Выполнено 1 задание из 3.

Задание №5

Произвести тестирование производительности web приложения:

1. скорость соединения

2. нагрузку

3. стрессовую нагрузку

Оценка	Показатели оценки
5	Выполнено 3 задания из 3.
4	Выполнено 2 задания из 3.
3	Выполнено 1 задание из 3.

Задание №6

Разработать тест-кейсы и произвести функциональное тестирование web приложения:

1. проверка форм

2. тестирование базы даннных

3. тестирование файлов cookie

Оценка	Показатели оценки
5	Выполнено 3 задания из 3.
4	Выполнено 2 задания из 3.
3	Выполнено 1 задание из 3.

Задание №7

Определить алгоритм поиска уязвимостей к атакам XSS и реализовать его.

Оценка	Показатели оценки
5	Задание выполнено в полном объеме.
4	Задание выполнено с незначительными ошибками.
3	Задание выполнено с грубыми ошибками.

Задание №8

Определить алгоритм поиска уязвимостей к атакам XSS и реализовать его.

Оценка	Показатели оценки
5	Задание выполнено в полном объеме.
4	Задание выполнено с незначительными ошибками.
3	Задание выполнено с грубыми ошибками.

Задание №9

Определить алгоритм поиска уязвимостей к атакам XSS и реализовать его.

Оценка	Показатели оценки
5	Задание выполнено в полном объеме.
4	Задание выполнено с незначительными ошибками.
3	Задание выполнено с грубыми ошибками.

Задание №10

Как автоматически идентифицировать уязвимости, связанные с загрузкой файлов на сервер

Оценка	Показатели оценки
5	Дан полный ответ с описанием инструментария и примерами автоматической идентификации уязвимостей, связанных с загрузкой файлов на сервер
4	Дан ответ с примерами применения средств, позволяющих автоматически идентифицировать уязвимости, связанные с загрузкой файлов на сервер
3	Дан ответ с описанием средств, позволяющих автоматически идентифицировать уязвимости, связанные с загрузкой файлов на сервер

Задание №11

Для чего испрользуются URL следующего типа:

http://www.test.app.com/index?id=1' http://www.test.app.com/index?id=1"
http://www.test.app.com/index?id=1' order by 1000 http://www.test.app.com/index?id=1"--
http://www.test.app.com/index?id=1'/ http://www.test.app.com/index?id=1"#*
http://www.test.app.com/index?id=1 and 1=1— http://www.test.app.com/index?id=1 and 1=2—
http://www.test.app.com/index?id=1' and '1'='1 http://www.test.app.com/index?id=1' and '1'='2

Какую информацию можно получить с их помощью и как ее интерпретировать?

Оценка	Показатели оценки
5	Представлен развернутый ответ.
4	Представлен развернутый ответ с незначительными ошибками.
3	Представлен развернутый ответ с грубыми ошибками.

Задание №12

Как автоматически идентифицировать уязвимости, связанные с загрузкой файлов на сервер

Оценка	Показатели оценки
5	Дан полный ответ с описанием инструментария и примерами автоматической идентификации уязвимостей, связанных с загрузкой файлов на сервер
4	Дан ответ с примерами применения средств, позволяющих автоматически идентифицировать уязвимости, связанные с загрузкой файлов на сервер
3	Дан ответ с описанием средств, позволяющих автоматически идентифицировать уязвимости, связанные с загрузкой файлов на сервер

Задание №13

Для чего используются URL следующего типа:

http://www.test.app.com/index?id=1' http://www.test.app.com/index?id=1"
http://www.test.app.com/index?id=1' order by 1000 http://www.test.app.com/index?id=1"--
http://www.test.app.com/index?id=1'/ http://www.test.app.com/index?id=1"#*
http://www.test.app.com/index?id=1 and 1=1— http://www.test.app.com/index?id=1 and 1=2—
http://www.test.app.com/index?id=1' and '1'='1 http://www.test.app.com/index?id=1' and '1'='2

Какую информацию можно получить с их помощью и как ее интерпретировать?

Оценка	Показатели оценки
5	Представлен развернутый ответ.
4	Представлен развернутый ответ с незначительными ошибками.
3	Представлен развернутый ответ с грубыми ошибками.

Задание №14

Привести алгоритм поиска уязвимостей к атакам XSS и реализовать его

Оценка	Показатели оценки
5	Задание выполнено в полном объеме.
4	Задание выполнено с незначительными ошибками.
3	Задание выполнено с грубыми ошибками.

Задание №15

Привести алгоритм поиска уязвимостей к атакам XSS и реализовать его

Оценка	Показатели оценки
5	Задание выполнено в полном объеме.
4	Задание выполнено с незначительными ошибками.
3	Задание выполнено с грубыми ошибками.

Задание №16

Проанализировать код части бэкенда страницы веб-приложения. Определить наличие уязвимости, причины возникновения, тип, механизм реализации, предложить меры устранения угрозы

```
<?php

if( isset( $_GET[ 'Change' ] ) ) {

  // Получаем вывод

  $pass_new = $_GET[ 'password_new' ];

  $pass_conf = $_GET[ 'password_conf' ];

  // Проверка на совпадение пароля

  if( $pass_new == $pass_conf ) {

  $pass_new = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["___mysqli_ston"], $pass_new ) : ((trigger_error("[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));

  $pass_new = md5( $pass_new );
```

```
  // Обновляем пароли в базе

  $insert = "UPDATE `users` SET password = '$pass_new' WHERE user = '" . dvwaCurrentUser() . "';";

  $result = mysqli_query($GLOBALS["___mysqli_ston"], $insert ) or die( '<pre>' .
((is_object($GLOBALS["___mysqli_ston"])) ? mysqli_error($GLOBALS["___mysqli_ston"]) :
(($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );

  // Сообщение об изменении пароля

  $html .= "<pre>Password Changed.</pre>";

  }

  else {

  // Введенные пароли не совпадают

  $html .= "<pre>Passwords did not match.</pre>";

  }

  ((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___mysqli_res);

}

?>
```

Оценка	Показатели оценки
5	Определено наличие уязвимости веб-приложения, причины ее возникновения, тип угрозы (токены не используются, секретных ключей нет, в форме - уязвимость CSRF), вектор атаки (запуск html-файла пользователем), предложены меры по нейтрализации и устранению угрозы
4	Определено наличие уязвимости веб-приложения, тип угрозы, вектор атаки, с несущественными недочетами предложены меры по нейтрализации угрозы
3	Определено наличие уязвимости веб-приложения, тип угрозы, с ошибками предложены меры по нейтрализации угрозы

Задание №17

1. Описать представленный код.

2. Найти уязвимость в представленном коде.

```php
<?php

public function Auth()
{
    $mysqli = new mysqli('localhost', 'root', 'password', 'database');
    $query = 'SELECT * FROM `users` WHERE `login` = ' . $_GET['login']
        and `password` = ' . $_GET['password'];
    return $mysqli->query($query) or die($mysqli->error);
}
```

3. Исправить уязвимость.

Оценка	Показатели оценки
3	Представлены все пункты задания.
4	Представлены 2 пункта задания.
5	Представлен 1 пункт задания.

Задание №18

Представить ответы на вопросы:

1. Какие типы тестирования веб-приложения существуют?

2. Какой тип тестирования предпочтителен для анализа веб-приложений?

3. Описать процесс тестирования одного из типа тестирования.

Оценка	Показатели оценки
3	Представлены все пункты задания.
4	Представлены 2 пункта задания.
5	Представлен 1 пункт задания.

Задание №19

Провести тестирование защищенности механизма управления доступом и сессиями.

Оценка	Показатели оценки
3	Задание выполнено в полном объеме.
4	Задание выполнено с незначительными ошибками.
5	Задание выполнено с грубыми ошибками.

Задание №20

Провести тестирование на устойчивость к атакам отказа в обслуживании.

Оценка	Показатели оценки
3	Задание выполнено в полном объеме.
4	Задание выполнено с незначительными ошибками.
5	Задание выполнено с грубыми ошибками.

Задание №21

1. Описать представленный код.

2. Найти уязвимость в представленном коде.

```php
<?php

public function Auth()
{
    $mysqli = new mysqli('localhost', 'root', 'password', 'database');
    $query = 'SELECT * FROM `users` WHERE `login` = ' . $_GET['login']
        and `password` = ' . $_GET['password'];
    return $mysqli->query($query) or die($mysqli->error);
}
```

3. Исправить уязвимость.

Оценка	Показатели оценки
5	Выполнены 3 пункта задания.
4	Выполнены 2 пункта задания.
3	Выполнен 1 пункт задания.

Задание №22

Проанализировать механизмы воздействия и меры защиты веб-приложения от Cross Site Scripting (XSS). Привести примеры защиты веб-приложения от Cross Site Scripting (XSS).

Оценка	Показатели оценки
5	Представлен развернутый ответ на вопрос.
4	Представлен развернутый ответ на вопрос, с незначительными ошибками.
3	Представлен краткий ответ на вопрос.

Задание №23

Привести примеры основных способов предотвращения SQL injection.

Оценка	Показатели оценки
5	Представлен развернутый ответ на вопрос.
4	Представлен развернутый ответ на вопрос, с незначительными ошибками.
3	Представлен краткий ответ на вопрос.

Задание №24

1. Описать принципы безопасных архитектуры и дизайна веб-приложения

2. Описать виды и принципы тестирования веб-приложений

3. Составить чек-лист для code review

Оценка	Показатели оценки
5	Выполнено 3 задания из 3.
4	Выполнено 2 задания из 3.
3	Выполнено 1 задание из 3.

Задание №25

Выполнить практические задания:

1. Для бэкапа сервера БД создать задачу Backup db1. Указать клиента (db1-fd) и FileSet (MySQL Database).

2. Для серверов приложений создать задачи Backup app1 и Backup app2. Указать правильное значение в Client (app1-fd и app2-fd) и FileSet (Apache DocumentRoot).

3. Создать задачу Backup lb1 для балансировщика нагрузки, указав соответствующие значения в Client (lb1-fd) и FileSet (SSL Certs and HAProxy Config).

Оценка	Показатели оценки
5	Выполнено 3 пункта задания.
4	Выполнено 2 пункта задания.
3	Выполнен 1 пункт задания.

Задание №26

Определить потенциальную угрозу, которую несет приведенный код. Предложить варианты ее предотвращения

```
<!DOCTYPE html>

<html>

<head>

  <title>Auther</title>

</head>

<body>

  <h1>Добро пожаловать!</h1>

  <p>Введите данные для авторизации:</p>

  <form method="post">

  <input type="text" name="username">

  <input type="password" name="password">

  <input type="submit" value="Отправить">

  </form>

</body>

</html>
```

Оценка	Показатели оценки
5	Верно определена потенциальная угроза (XSS, без экранирования ввода скрипт внедрится в HTML страницы и выполнится в браузере пользователя при просмотре приветствия), предложены варианты ее предотвращения
4	Верно определена потенциальная угроза, предложен вариант ее предотвращения с незначительными ошибками
3	Определены потенциальные угрозы, варианты их предотвращения ошибочны

Задание №27

Выполнить практические задания:

1. Для бэкапа сервера БД создать задачу Backup db1. Указать клиента (db1-fd) и FileSet (MySQL Database).

2. Для серверов приложений создать задачи Backup app1 и Backup app2. Указать правильное

значение в Client (app1-fd и app2-fd) и FileSet (Apache DocumentRoot).

3. Создать задачу Backup lb1 для балансировщика нагрузки, указав соответствующие значения в Client (lb1-fd) и FileSet (SSL Certs and HAProxy Config).

Оценка	Показатели оценки
5	Выполнено 3 пункта задания.
4	Выполнено 2 пункта задания.
3	Выполнен 1 пункт задания.

Задание №28

Выполнить практические задания:

1. Для бэкапа сервера БД создать задачу Backup db1. Указать клиента (db1-fd) и FileSet (MySQL Database).

2. Для серверов приложений создать задачи Backup app1 и Backup app2. Указать правильное значение в Client (app1-fd и app2-fd) и FileSet (Apache DocumentRoot).

3. Создать задачу Backup lb1 для балансировщика нагрузки, указав соответствующие значения в Client (lb1-fd) и FileSet (SSL Certs and HAProxy Config).

Оценка	Показатели оценки
5	Выполнено 3 пункта задания.
4	Выполнено 2 пункта задания.
3	Выполнен 1 пункт задания.

Задание №29

Определить вид потенциальной уязвимости веб-приложения при наличии следующей функции сервиса сохранения паролей пользователей:

```
function savePassword(password) {

  // Создаем хеш-таблицу для хранения паролей

  passwordTable = allocateHashTable(10);

   // Копируем введенный пароль в хеш-таблицу

  copyData(password, passwordTable);

}
```

Каким может быть вектор атаки, ее последствия и как их избежать?

Оценка	Показатели оценки
5	Дан полный развернутый ответ с кодом устранения угрозы
4	Дан полный ответ с кодом устранения угрозы и незначительными ошибками
3	Дан краткий ответ с ошибками, приведенный код не гарантирует полной безопасности

Задание №30

Определить вид потенциальной уязвимости веб-приложения при наличии следующей функции сервиса сохранения паролей пользователей:

```
function savePassword(password) {

  // Создаем хеш-таблицу для хранения паролей

  passwordTable = allocateHashTable(10);

   // Копируем введенный пароль в хеш-таблицу

  copyData(password, passwordTable);

}
```

Каким может быть вектор атаки, ее последствия и как их избежать?

Оценка	Показатели оценки
5	Дан полный развернутый ответ с кодом устранения угрозы переполнения кэша
4	Дан полный ответ с кодом устранения угрозы и незначительными ошибками
3	Дан краткий ответ с ошибками, приведенный код не гарантирует полной безопасности

Задание №31

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.

Оценка	Показатели оценки
3	Задание выполнено в полном объеме.

4	Выполнено 2 пункта задания.
5	Выполнен 1 пункт задания.

Задание №32

1. Для веб-приложения, уязвимого к атаке CSRF, написать эксплоит, 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.

Оценка	Показатели оценки
3	Задание выполнено в полном объеме.
4	Выполнено 2 пункта задания.
5	Выполнен 1 пункт задания.

Задание №33

Выполнить практические задания:

1. Для бэкапа сервера БД создайте задачу Backup db1. Укажите клиента (db1-fd) и FileSet (MySQL Database).

2. Для серверов приложений нужно создать задачи Backup app1 и Backup app2. Укажите правильное значение в Client (app1-fd и app2-fd) и FileSet (Apache DocumentRoot).

3. Создайте задачу Backup lb1 для балансировщика нагрузки, указав соответствующие значения в Client (lb1-fd) и FileSet (SSL Certs and HAProxy Config).

Оценка	Показатели оценки
3	Задание выполнено в полном объеме.
4	Выполнено 2 пункта задания.
5	Выполнен 1 пункт задания.

Задание №34

Осуществить поиск уязвимостей к атакам XSS.

Оценка	Показатели оценки
3	Задание выполнено в полном объеме.

4	Задание выполнено с незначительными ошибками.
5	Задание выполнено с грубыми ошибками.