Перечень теоретических и практических заданий к экзамену по МДК.09.03 Обеспечение безопасности веб-приложений (3 курс, 5 семестр 2024-2025 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

Представить ответы на следующие вопросы:

1. назвать принципы создания и функционирования распределенных баз данных;
2. объяснить технологии объектного связывания данных и реплицирования данных;
3. охарактеризовать существующие технологии и модели «Клиент-сервер».

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

Задание №2

Представить ответы на следующие вопросы:

1. Что такое нежелательный контент?

2. Что такое Утечки информации?

3. Что такое Несанкционированный доступ?

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

Задание №3

Представить ответы на следующие вопросы:

1. Что такое веб-аналитика?

2. Назвать основные методы веб-аналитики.

3. Описать процесс настройки системы аналитики.

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

Задание №4

Опишите части резервного копирования:

- Периодический запуск копирования.
- Запуск восстановления по требованию.
- Тестирование процесса копирования.

Оценка	Показатели оценки
5	Представлено полное описание.
4	Представлено описание 2 частей резервного копирования.
3	Представлено описание 1 части резервного копирования.

Задание №5

Представить ответы на следующие вопросы:

1. Что нужно сделать для предотвращения сетевых угроз?

2. Как предотвратить утечку данных?

3. Для каких целей целесообразно использовать прокси сервер?

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

Задание №6

Представьте описание следующих процессов:

1. Развертывание приложений веб-служб.

2. Отмена развертывания приложений веб-служб.

3. Повторное развертывание приложений веб-служб

Оценка	Показатели оценки
5	Представлено описание всех процессов.
4	Представлено описание 2 процессов.
3	Представлено описание 1 процесса.

Задание №7

Представить ответы на следующие вопросы:

1. Как оценить работу саппорта?

2. Разница поддержки в зависимости от канала?

3. Что такое каналы взаимодействия?

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

Задание №8

Представить ответы на следующие вопросы:

1. Назвать принципы резервного копирования.

2. Назвать задачи резервного копирования.

3. Назвать задачи регламента резервного копирования.

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

Задание №9

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 №10

Представить ответы на следующие вопросы:

1. Для чего проводится тестирование ПО?

2. Назвать принципы тестирования.

3. Назвать этапы тестирования.

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

Задание №11

Представьте ответы на следующие вопросы:

1. Назвать основные критерии в организации процесса тестирования.

2. Назвать цели и область тестирования.

3. Назвать основные документы, которые составляются в процессе тестирования.

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

Задание №12

Представить ответы на следующие вопросы:

1. Принцип работы системы контроля версий.
2. Задачи для системы контроля версий.
3. Типы систем контроля версий.

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

Задание №13

Представить ответы на следующие вопросы:

1. Что такое система контроля версий?

2. Какие задачи решает система контроля версий?

3. Популярные ошибки при работе с Git.

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

Задание №14

Назвать характеристики, типы и виды хостингов.

Оценка	Показатели оценки
5	Задание выполнено в полном объеме.
4	Представлены характеристики и виды хостингов.
3	Представлены только виды хостингов.

Задание №15

Представить ответы на следующие вопросы:

1. Дайте характеристику 10 видам уязвимостей веб сайтов.
2. Назовите виды сетевых атак.
3. Что является наиболее эффективным средством для защиты от сетевых атак?

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

Задание №16

Представить ответы на следующие вопросы:

1. Что такое выделенный сервер?

2. Может ли сайт обойтись без хостинга?

3. Чем отличается виртуальный хостинг от VPS?

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

Задание №17

Представить ответы на следующие вопросы:

- Что понимается под несанкционированным воздействием на защищаемую информацию?
- Дайте понятие конфиденциальности, целостности и доступности информации.
- Дайте определение информационной безопасности.

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

Задание №18

Представить ответы на следующие вопросы:

1. Что такое SQL инъекции?
2. На какие два вида делятся HTML инъекции?
3. Перечислите 22 вида уязвимостей веб сайтов.

Оценка	Показатели оценки

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

Задание №19

Представить ответы на вопросы:

1. Что такое система управления сайтам?

2. Какие бывают платформы администрирования и управления содержимым сайта?

3. Как узнать, на какой платформе построен сайт?

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

Задание №20

Представить ответы на следующие вопросы:

1. Назвать инструменты сбора и анализа поисковых запросов.

2. Для чего они нужны?

3. Представить краткую характеристику 2 инструментов.

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

Перечень практических заданий:
Задание №1

1. Что такое аутентификация?

2. Что такое авторизация?

3 Написать на php пример защищеной авторизации и регистрацией.

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

Задание №2

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	Задание выполнено в полном объеме.
4	Выполнено 2 пункта задания.
3	Выполнен 1 пункт задания.

Задание №3

Написать следующие команды:

1. Изменение размера шрифта конкретной страницы.

2. Вывод потомков узла head.

3. Получить первый дочерний заголовок узла head и вывести его первого соседа.

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

Задание №4

Провести следующие виды мониторинга:

1. Мониторинг виртуальных машин.

2. Мониторинг контейнеров.

3. Мониторинг веб-серверов.

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

Задание №5

Провести мониторинг Supervisor’а и кастомных сервисов, а также мониторинг доступности URL’ов, доменов и SSL-сертификатов.

Оценка	Показатели оценки
5	Задание выполнено в полном объеме.
4	Задание выполнено с небольшими нарушениями.
3	Задание выполнено с грубыми нарушениями.

Задание №6

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
5	Задание выполнено в полном объеме.
4	Выполнено 2 пункта задания.
3	Выполнен один пункт задания.

Задание №7

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.

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

Задание №8

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
5	Задание выполнено в полном объеме.
4	Выполнено 2 пункта задания.
3	Выполнен один пункт задания.

Задание №9

Выполнить практическое задание:

1. Разработать план резервного копирования (ИС).
2. Составить отчет Word о выполненной работе.

Оценка	Показатели оценки
5	Задание выполнено в полном объеме.
4	Задание содержит незначительные ошибки.
3	Задание содержит грубые ошибки.

Задание №10

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

Задание №11

Произвести функциональное тестирование web приложения:

1. Проверка форм.

2. Тестирование базы данных.

3. Тестирование файлов cookie.

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

Задание №12

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 №13

Произвести тестирование пользовательского интерфейса web приложения:

1. разработать тест-требований и тест-планов для проверки пользовательского интерфейса;

2. разработать тест-требований и тест-планов 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 задание из 3.

Задание №14

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 №15

Выполнить практические задания:

1. Создать локальный репозиторий или копировать репозиторий существующего проекта.

2. Фиксировать изменения локально.

3. Отправлять изменения на GitHub.

4. Зарегистрировать аккаунты разработчиков вашего проекта.

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

Задание №16

Выполнить проверку индивидуального веб-приложения (курсового проекта) по техническому заданию.

Оценка	Показатели оценки
5	Задание выполнено в полном объеме.
4	Задание содержит незначительные ошибки.
3	Задание содержит грубые ошибки.

Задание №17

Провести сравнительный анализ хостингов. Представить сравнительную таблицу и вывод.

Оценка	Показатели оценки
5	Задание выполнено в полном объеме.
4	Задание выполнено с незначительными ошибками.
3	Задание содержит грубые ошибки.

Задание №18

Составить отчет по основным показателям использования Веб-приложения интернет-почта "Gmail" (рейтинг, источники и поведение пользователей, конверсия и другие).

Оценка	Показатели оценки
5	Задание выполнено в полном объеме.
4	Задание содержит незначительные ошибки.
3	Задание содержит грубые ошибки.

Задание №19

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

2. 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.

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

Оценка	Показатели оценки

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

Задание №20

Осуществить редактирование HTML-кода с использованием систем администрирования.

Оценка	Показатели оценки
5	Задание выполнено в полном объеме.
4	Задание выполнено с незначительными ошибками.
3	Задание содержит грубые ошибки.

Задание №21

Используя сторонние инструменты провести валидацию кода:

1. Валидация HTML.

2. Валидация CSS.

3. Валидация адаптивности.

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