# Перечень теоретических и практических заданий к экзамену по МДК.09.03 Обеспечение безопасности веб-приложений (3 курс, 5 семестр 2023-2024 уч. г.)

**Форма контроля:** Письменный опрос (Опрос)
**Описательная часть:** По выбору выполнить 1 теоретическое задание и 1 практическое задание

**Перечень теоретических заданий:**

**Задание №1**

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

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

**Задание №2**

1. Что такое нежелательный контент ?

2. Что такое Утечки информации ?

3. Что такое Несанкционированный доступ ?

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

**Задание №3**

1. Что подразумевается под мошшеничеством ?

2. Дайте определение Кибертерроризм.

3. Дайте определение Кибервойны.

| Оценка | Показатели оценки |
|---|---|

| | |
|---|---|
| 3 | Дан ответ на 1 вопрос из 3. |
| 4 | Дан ответ на 2 вопрос из 3. |
| 5 | Дан ответ на 3 вопрос из 3. |

**Задание №4**

1. Что нужно сделать для предотвращения сетевых угроз?

2. Как предотвратить утечку данных ?

3. Для каких целей целесообразно использовать прокси сервер??

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

**Задание №5**

1. Нужно ли использовать антивирус если компьютер не подключен к глобальной и локальной сети?

2. Как снизить к минимуму угрозы кибератак у настроенного сервера?

3. Как снизить к минимуму угрозу потери данных?

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

**Задание №6**

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

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

**Задание №7**

1. Что такое code review?

2. Описать принципы безопасных архитектуры и дизайна.

3. Какие бывают виды тестирования приложения?

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

**Задание №8**

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 |
|---|---|
| 3 | Дан ответ на 1 вопрос из 3. |
| 4 | Дан ответ на 2 вопроса из 3. |
| 5 | Дан ответ на все 3 вопроса. |

**Задание №9**

1. Что такое dos атака?

2. Что такое Ddos атака?

3. Как защитится от dos и ddos атак?

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

**Задание №10**

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.

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

**Перечень практических заданий:**

**Задание №1**

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 |
|---|---|
| 3 | Дан ответ на 1 вопрос из 3. |
| 4 | Дан ответ на 2 вопроса из 3. |
| 5 | Дан ответ на все 3 вопроса. |

**Задание №2**

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 | Выполнено 1 задание из 3. |
| 4 | Выполнено 2 задание из 3. |
| 5 | Выполнено 3 задание из 3. |

**Задание №3**

Произвести функциональное тестирование web приложения:

1. Проверка форм.

2. Тестирование базы даннных.

3. Тестирование файлов cookie.

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

**Задание №4**

Произвести тестирование производительности web приложения:

1. Скорость соединения.

2. Нагрузку.

3. Стрессовую нагрузку.

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

**Задание №5**

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 |
|---|---|
| 3 | Выполнено 1 задание из 3. |
| 4 | Выполнено 2 задание из 3. |
| 5 | Выполнено 3 задание из 3. |

**Задание №6**

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 | Выполнено 1 задание из 3. |
| 4 | Выполнено 2 задания из 3. |
| 5 | Выполнены все 3 задания. |

**Задание №7**

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 |
|---|---|
| 3 | Выполнено 1 задание из 3. |
| 4 | Выполнено 2 задание из 3. |
| 5 | Выполнено 3 задание из 3. |

**Задание №8**

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 |
|---|---|
| 3 | Выполнено 1 задание из 3. |
| 4 | Выполнено 2 задания из 3. |
| 5 | Выполнены все 3 задания. |

**Задание №9**

1. Что такое аутентификация?

2. Что такое авторизация?

3 Написать на php пример защищеной авторизации.

| Оценка | Показатели оценки |
|---|---|
| 3 | Выполнено 1 задание из 3 |
| 4 | Выполнено 2 задание из 3 |
| 5 | Выполнено 3 задание из 3 |

**Задание №10**

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 | Выполнено 1 задание из 3. |
| 4 | Выполнено 2 задание из 3. |
| 5 | Выполнено 3 задание из 3. |