# Введение

## **Описание вида тестирования**

Pentest/RedTeam/AppSec

## **Описание объекта тестирования**

Например, для AppSec объект – это определенное приложение или сайт

## **Краткие сведения о количестве найденных уязвимостей и их ранжирование по уровню критичности**

Мы нашли 5 критичных, 4 средней критичности и 2 низкой критичности уязвимостей

## **Выводы о защищенности объекта тестирования**

Здесь опишите своими словами, что хотите обратить внимание в первую очередь.

## **Выходные данные**

Даты проведения тестирований

Количество затраченного времени (в часах)  
  
Специалисты, проводившие тестирование

# Описание проведенных работ

1. Анализ механизма хранения данных  
2. Анализ документации, архитектуры, используемых технологий и функций мобильного приложения.

3. и так далее

# Описание результатов тестирования

|  | Название параметра | Содержание |
| --- | --- | --- |
| 1. | Название уязвимости | * риск, * тип уязвимости, * уязвимое место |
|  | Оценка уязвимости | * уровень риска, * оценка по десятибалльной шкале CVSS [сайт](https://www.first.org/cvss/calculator/3.0) |
|  | Описание уязвимости | подробный рассказ об расположении уязвимости, потенциальном способе эксплуатации уязвимости, возможном импакте |
|  | Затронутые хосты | хосты, которые потенциально могут содержать эту уязвимость |
|  | Рекомендации по устранению | Ваши персональные рекомендации, как именно можно исправить каждую уязвимость. |

# Дополнительная информация

Словарь основных терминов (оформляется в виде таблицы)

| термин/аббревиатура | определение/расшифровка |
| --- | --- |
|  |  |

# Заключение

своими словами о возможных сценариях компрометации определенных частей инфраструктуры на основе найденных уязвимостей во время тестирования

CVSS (посмотреть параметры оценки на [сайте](https://www.first.org/cvss/calculator/3.0))