**Отчет о проведенном аудите (пентесте) приложения (имя)**

# **Исходные данные**

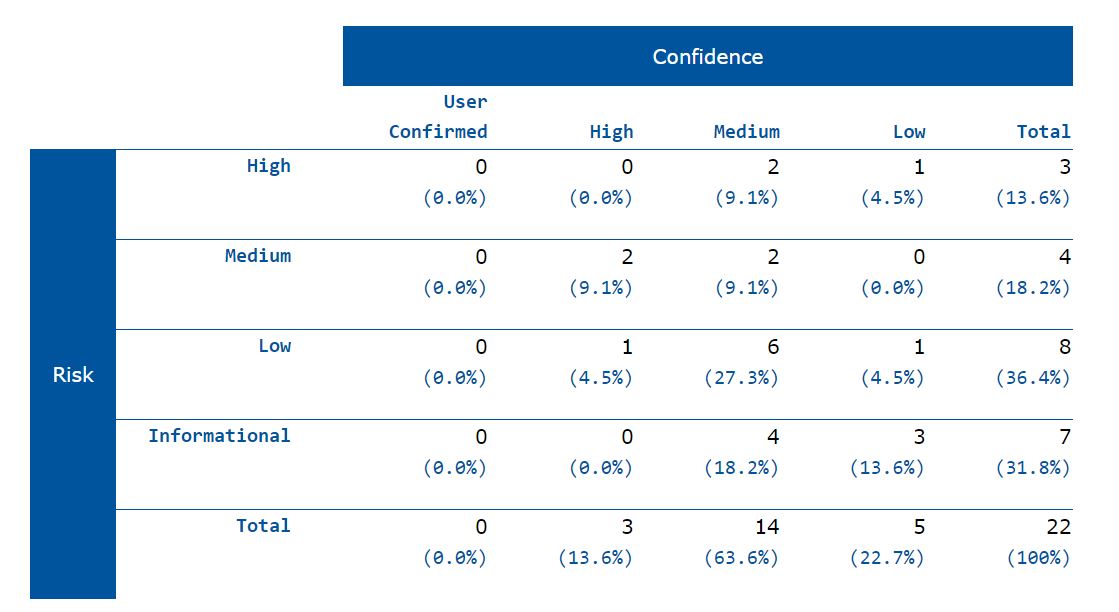
Предоставлен файл docker-compose.yml:

Для проведения пентеста был использован инструмент zap()

# **Отчет по результатам аудита**

На виртуальной машине был поднят docker образ и запущено приложение (имя) на <http://localhost:8080>

Суммарная таблица



Подробное описание четырех найденных уязвимостей

Cloud Metadata Potentially Exposed

CWE 79

Описание:

Cross Site Scripting (Persistent)

CWE 79

Описание:

Cross Site Scripting (Reflected)

CWE 79

Описание:

Content Security Policy (CSP) Header Not Set

CWE 693

Описание:

Missing Anti-clickjacking Header

CWE 1021

Описание:

Sub Resource Integrity Attribute Missing

CWE 345

Описание:

# **Рекомендации по исправлению или нейтрализации перечисленных уязвимостей**

Cloud Metadata Potentially Exposed CWE 79

Исправление:

Cross Site Scripting (Persistent)

CWE 79

Исправление:

Cross Site Scripting (Reflected)

CWE 79

Исправление:

Content Security Policy (CSP) Header Not Set

CWE 693

Исправление:

Missing Anti-clickjacking Header

CWE 1021

Исправление:

Sub Resource Integrity Attribute Missing

CWE 345

Исправление: