# **Тестовое задание на стажировку AppSecCloudCamp**

Мамонтов Алесей

моб.тел: 8034531188

ТГ: @zzollozz

email: dom.zmei@yandex.ru

## **1. Вопросы для разогрева**

1. Расскажите, с какими задачами в направлении безопасной разработки вы сталкивались?
2. Если вам приходилось проводить security code review или моделирование угроз, расскажите, как это было?
3. Если у вас был опыт поиска уязвимостей, расскажите, как это было?
4. Почему вы хотите участвовать в стажировке?

Я так сказать еще студент и реальных задач в направлении безопасности не сталкивался на рабочем месте. За исключением настройки фаервола на рабочей машине

Моделированием угроз тоже сугубо в обучающих целях по методике ФСЕК России и MITRE.

Участие в стажировке даст мне опыт и закрепление полученных ранее знаний и вообще мне интересна эта тема. Ранее закончил курсы по вэб разработке от GB на данном этапе обучаюсь там же на факультете Специалист информационной безопасности

## **2. Security code review**

### **Часть 1. Security code review: GO**

Задание не выполнено не знаком с ЯП GO

### **Часть 2: Security code review: Python**

Требуется определить тип уязвимости в примерах кода на Python и ответить на следующие вопросы:

* Указать строки, в которых присутствуют уязвимости.
* К каким последствиям может привести эксплуатация данных уязвимостей злоумышленником?
* Описать способы исправления уязвимостей.
* Если уязвимость можно исправить несколькими способами, необходимо перечислить их, выбрать лучший по вашему мнению и аргументировать свой выбор.

**Пример №2.1**

from flask import Flask, request

from jinja2 import Template

app = Flask(name)

@app.route("/page")

def page():

name = request.values.get('name')

age = request.values.get('age', 'unknown')

output = Template('Hello ' + name + '! Your age is ' + age + '.').render()

return output

if name == "main":

app.run(debug=True)

**Ответ:**

Уязвимость в строке «*output = Template('Hello ' + name + '! Your age is ' + age + '.').render()*»

Первое надо реализовать валидацию входящих пользовательских данных, (name, age) чтоб избежать ввода не нужного.

Второе в рендере шаблона необходимо заменить конкатинацию строки на ее форматирование типа f’Hello {name}! Your age is {age}.’

**Пример №2.2**

from flask import Flask, request

import subprocess

app = Flask(name)

@app.route("/dns")

def dns\_lookup():

hostname = request.values.get('hostname')

cmd = 'nslookup ' + hostname

output = subprocess.check\_output(cmd, shell=True, text=True)

return output

if name == "main":

app.run(debug=True)

Ответ:

output = subprocess.run(‘nslookup {hostname}’, text=True)

Данный код предоставляет информацию по вводимому пользователем домену.

Модуль subprocess позволяет запускать внешние программы и контролировать их выполнение.

## В последних версиях Python (3.5) и выше была добавлена функция run ее и рекомендуется использовать вместо (call, check\_output и check\_call), также включено значение shell=True что вызывает оболочку для работы промежуточного процесса. При работе с потенциально опасным вводом, который может привести к внедрению вредоносного shell-кода запуск процесса с shell=True не рекомендуется и должен использоваться только в безопасных случаях.

Так же необходимо проверять пользовательские данные и весь блок в функции dns\_lookup обернуть в try except с отслеживанием исключения CalledProcessError, когда код возврата процесса не является 0.

## **3. Моделировани угроз**

Проанализируйте диаграмму потоков данных приложения и ответьте на следующий вопросы:

* Расскажите, какие потенциальные проблемы безопасности существуют для данного сервиса?

*Отказ в обслуживании всех компонентов начиная с самого микрофронта путем направления некорректных запросов - флуда*

* Расскажите, к каким последствиям может привести эксплуатация проблем, найденных вами?

*нарушения целостности нарушения конф. пользователей*

*скомпрометированная база данных*

*Не рабочий сервис полностью или сломаны отдельные сервисы что не даст нормальной работе в целом*

* Расскажите, какие способы исправления уязвимостей и смягчения рисков вы можете предложить по отмеченным вами проблемам безопасности?

*Микрофронт в демилитаризованную зону за фаерфол, так же разграничить права по доступу чтению и записи в работе с базой данных*

* Напишите список уточняющих вопросов, которые вы бы задали разработчикам данного сервиса?

*Где публикуется микрофронт (хост разработчика, сервер компании или в облаке)?*

*На схеме нет нумерации потоков когда проходит аутентификация. По хорошему пока пользователь не аунтифицирован делать он ни чего не может.*

*Где располагаются S3 и БД как подключены?*

*Какое подключение к Slack и Telegram – по API какая там аунтефикация?*

*Как подключены сами разработчики VPN, GRE или ... ?*

*Какие требования к сервису аунтификации?*