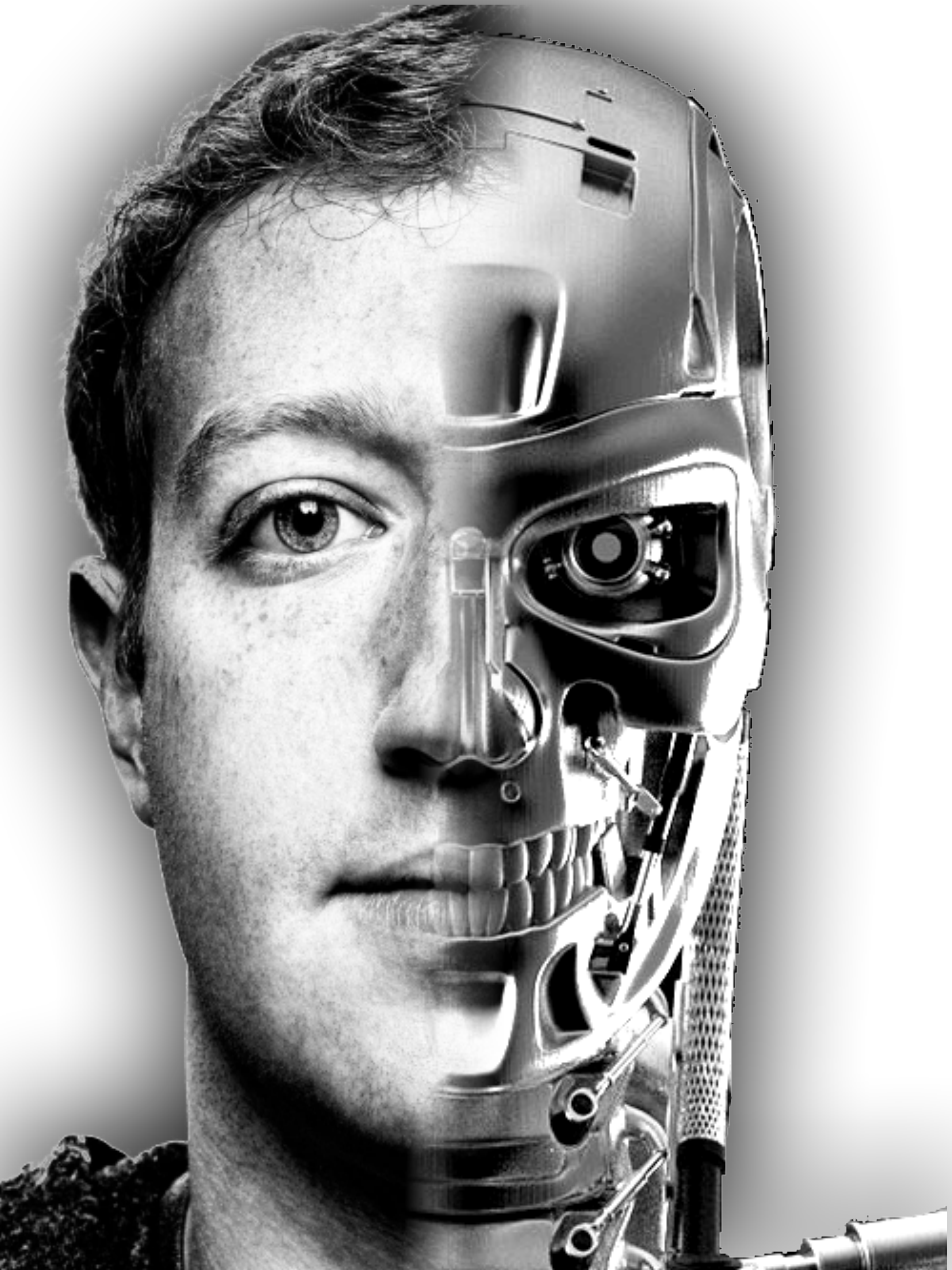


Human Users Detection

stop bots with Nginx + Lua + JavaScript

ROMHACK
CYBERSECURITY CONVENTION
romhack.io

Bloccare i principali tool di scansione ed enumeration

sottotitolo:

Botnet fantastiche e dove trovarle
di J.K. ***Rooting***

# whoami

@Menin_TheMiddle

Andrea Menin a.k.a theMiddle

Application Security Specialist

Security Software Developer

OWASP CRS Contributor

SecJuice Admin (secjuice.com)

Rev3rse Security Co-Founder

rev3rse SECURITY

youtube.com/rev3rsesecurity

Please, Visit / Share / Like / Follow:

coreruleset.org

OWASP ModSecurity Core Rule Set THE 1st LINE OF DEFENSE

secjuice.com

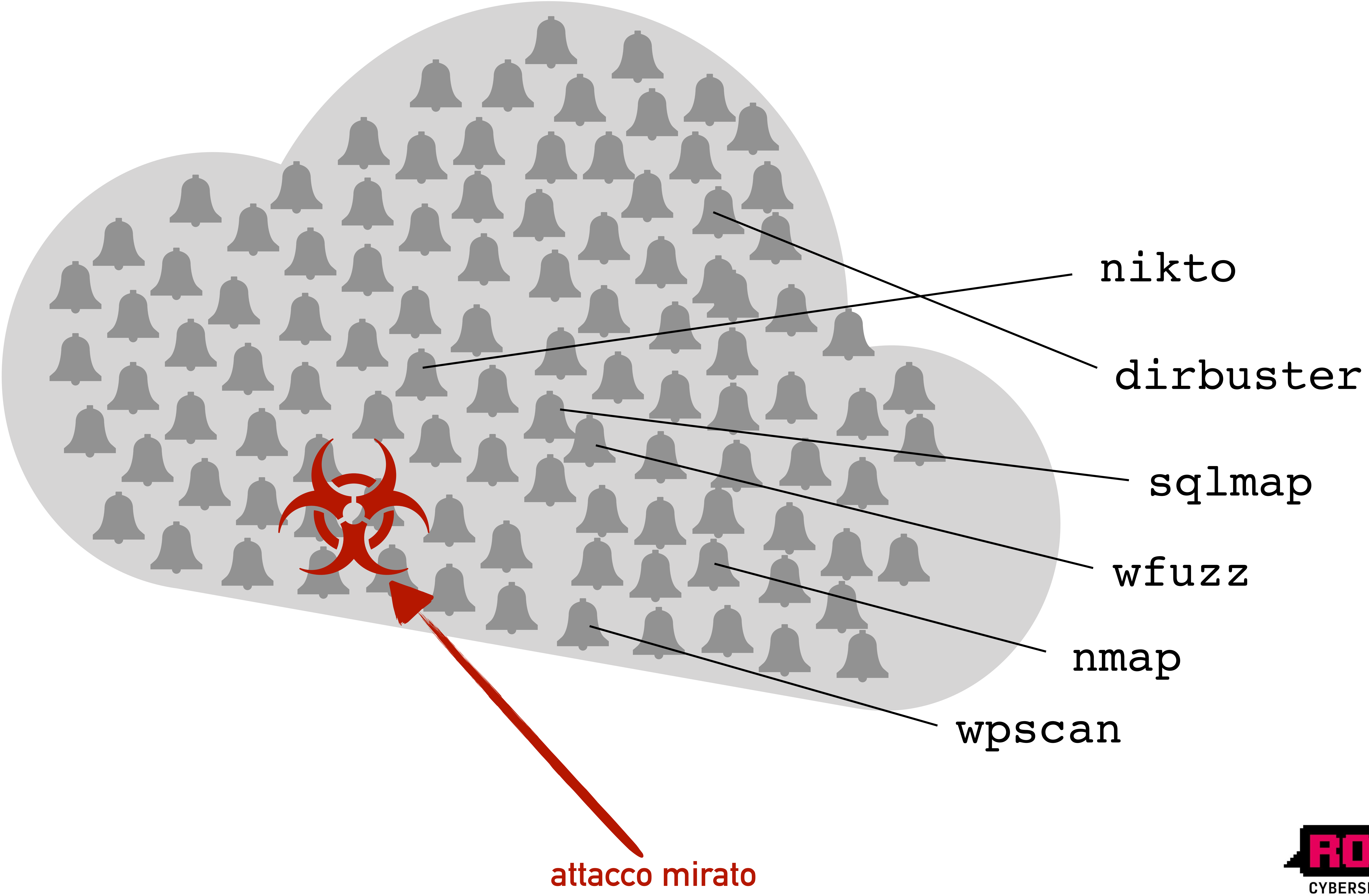
secjuice

Agenda

- Intercettare bot: metodi “standard”
- Challenge JavaScript (overview)
- Come fanno i grandi vendor (CloudFlare)?
- Rendere inefficaci i principali tool di scansione
- Challenge JavaScript (dettaglio tecnico)
- Obfuscation
- Dalla teoria alla pratica
- All you need is Logs!
- Bypass CloudFlare Anti DoS Challenge

In un caos di log / falsi positivi

identificare le vere minacce è complicato…



Metodi “standard”

Filtro su User-Agent:

User-Agent: … Nikto …

User-Agent: ^(?!(Mozilla|Opera))

!User-Agent

Filtro IP

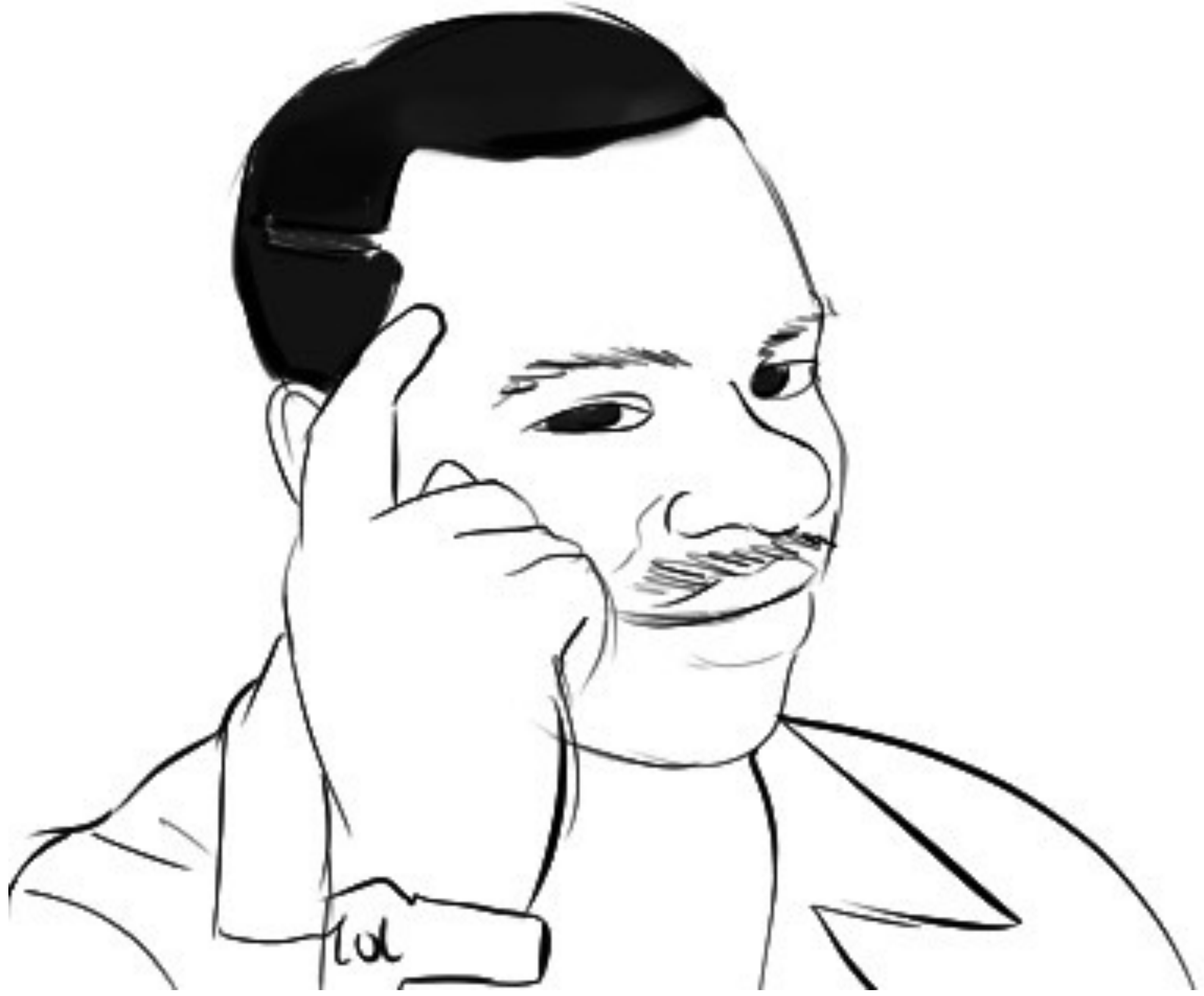
IP filtering / Bad Reputation

Block Geographic Location

Frequenza

Rate limit (request per second)

se blocco le request con user-agent = Nikto non riceverò mai più scansioni!



Metodi “standard”

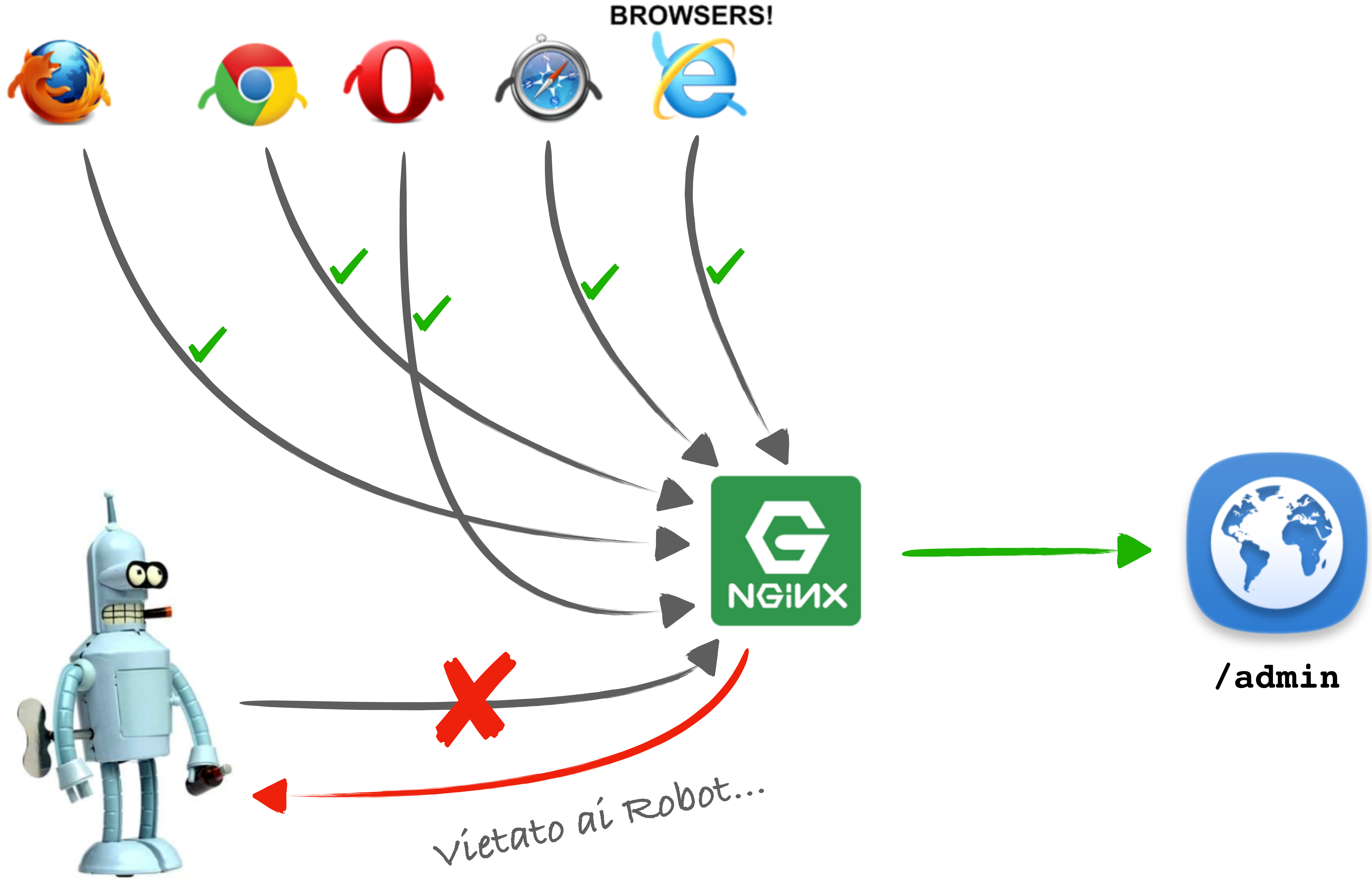
Filtro su User-Agent: **20%**

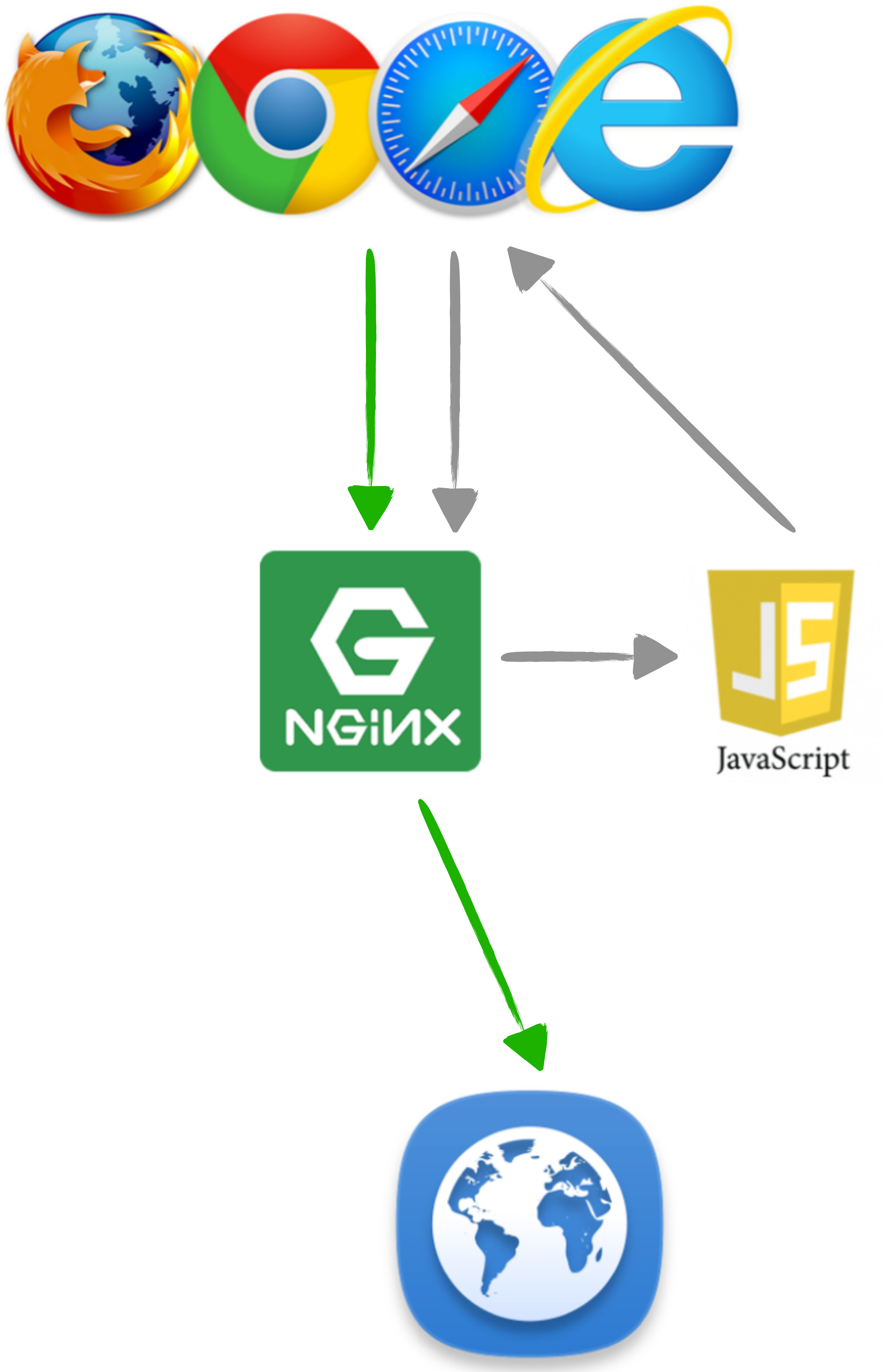
Reputation Database: **15%**

Chrome VS curl

```
console.log(‘Hello World!’);
```

Javascosa?!?


BROWSERS!
NGINX
/admin
Vietato ai Robot...



Il browser invia la richiesta senza token

GET /admin/ HTTP/1.1

Nginx intercetta la richiesta

Genera una pagina HTML + JavaScript + Token

scadenza 20 secondi

Il browser interpreta il JavaScript

Riceve un cookie contenente un Token

scadenza 20 secondi

Il browser viene rediretto su /admin

GET /admin HTTP/1.1

Cookie: token=123abc

Nginx accetta la request

200 OK HTTP/1.1

…body…

~~Nikto2~~

~~Web Scanner~~

~~https://cirt.net/nikto2~~

~~Dirbuster~~ / ~~Dirb~~ / ~~gobuster~~

~~File & Dir Enumeration~~

~~Wfuzz~~

~~Web Application Fuzzing~~

~~Nmap~~

```
nmap --script -http-enum --script-args http-enum.basepath=‘admin/'
```

Request /wp-login.php

Request senza cookie

GET /wp-login.php

Risposta

`<script src="/challenge.js?token=eg76rede7jduekap7…">`

challenge.js non esiste realmente, viene generato da Nginx tramite Lua e contiene la nostra piccola challenge JavaScript.

il token è cifrato e contiene una stringa di testo formattata in questo modo:

`$timestamp $remote_address $user-agent`

Request senza cookie

GET /challenge.js?token=eg76…

accesso solo se token è valido

Risposta

`document.cookie = ([]+!![]+!![]+[+[]])…`

invio cookie al bworser contenente il secondo token (scadenza 20 secondi) offuscato e lo rimando a /wp-login.php

Request con cookie

GET /wp-login.php

Cookie: iamhuman=k8prdus6…

Risposta

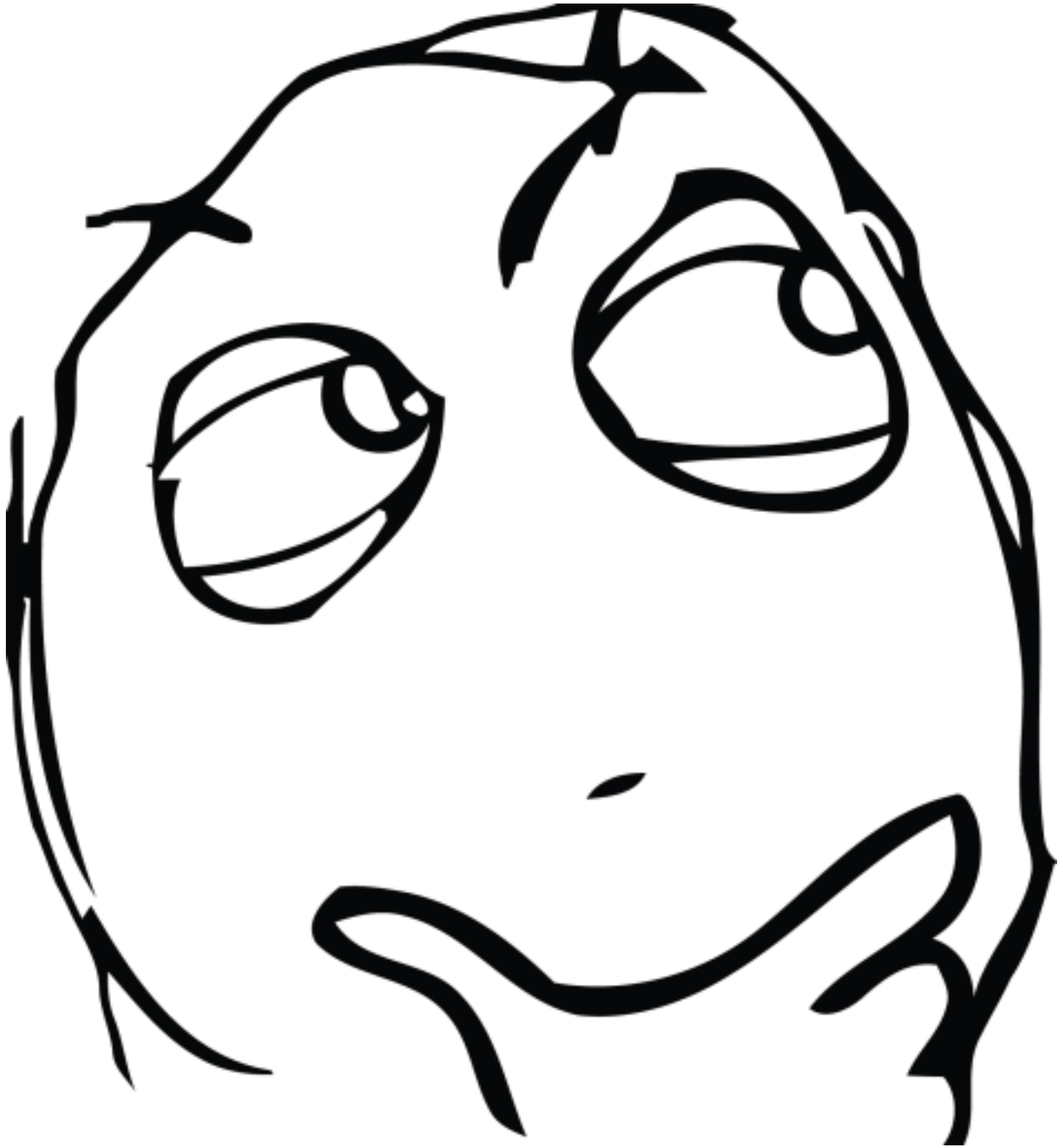
Pagina di autenticazione WordPress

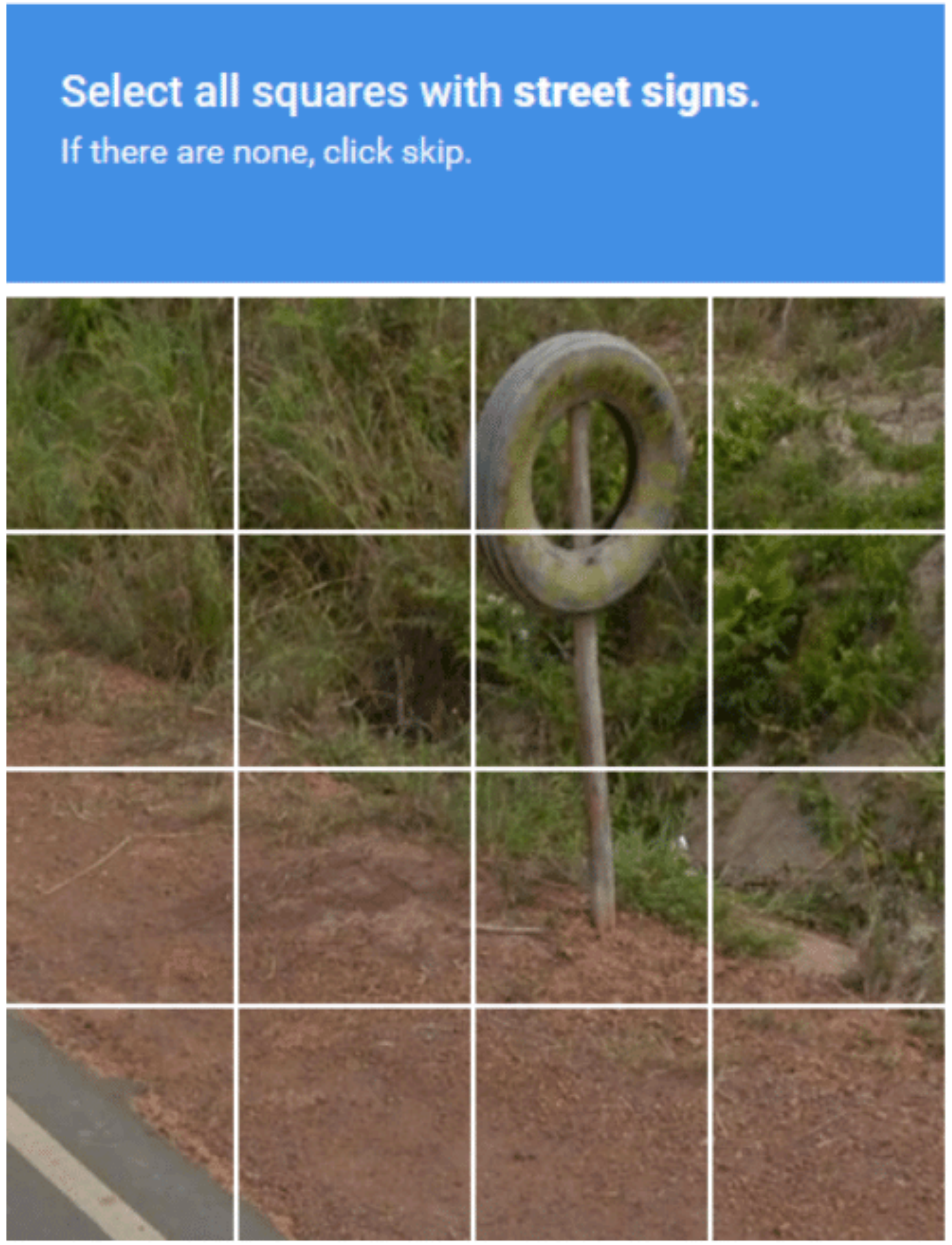
N.B. L'utente avrà a disposizione 20 secondi per poter effettuare l'accesso

Domanda:

Perché non usare un semplice recaptcha?

Google recapthca





Select all squares with street signs.

If there are none, click skip.

Sicuro
https://www.exploit-db.com/search/
EXPLOIT DATABASE
Home
Exploits
Shellcode
Papers
Google
Sì, sono tired!

non sono un robot! sono quello di prima, è la decima ricerca che faccio!

□ Non sono un robot

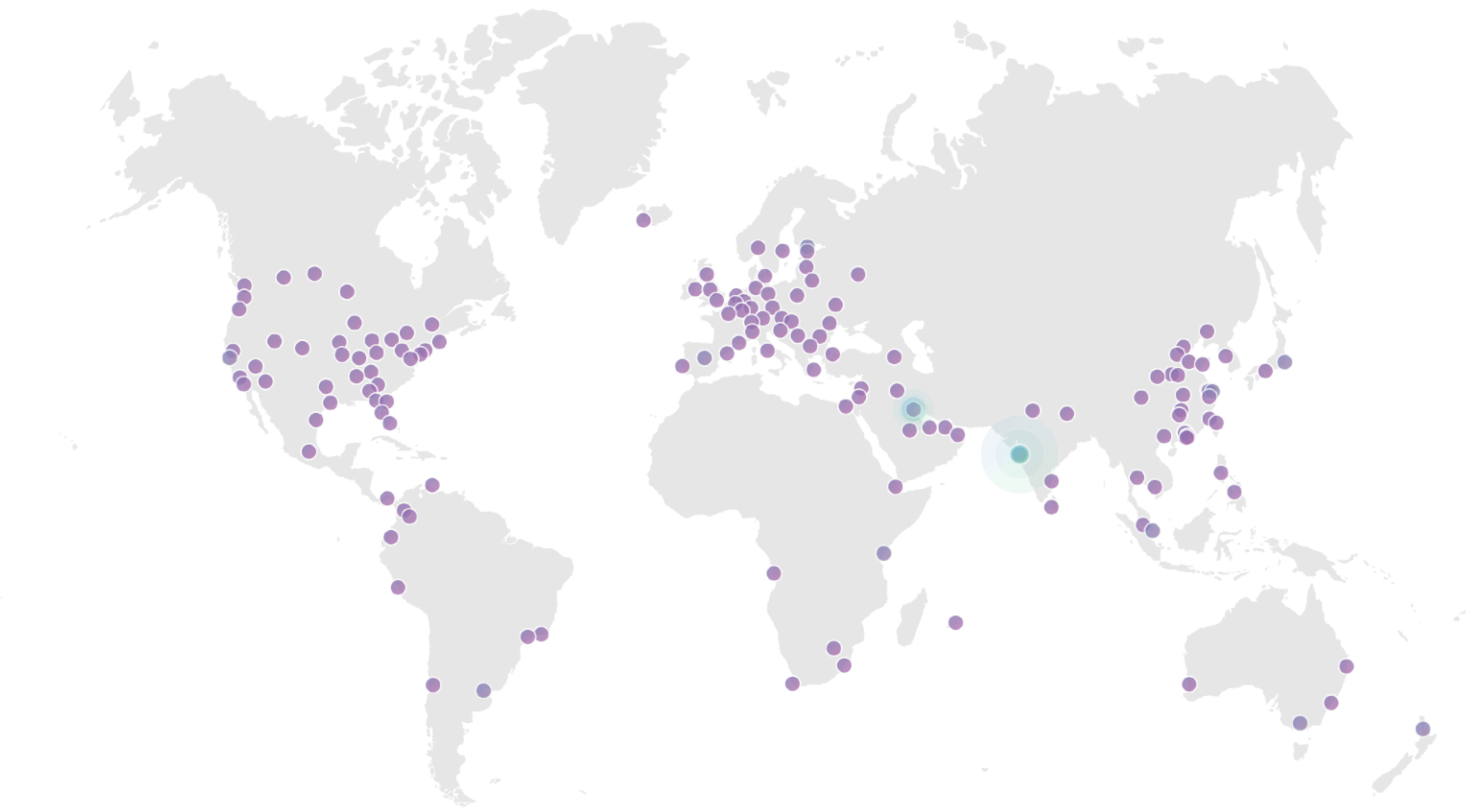
Tired of completing CAPTCHAs?

The Exploit Database has two repositories hosted on **GitHub**. The main exploit database repository is **updated daily and co** sorted by platform, and the exploit database bin-sploits repository holds binary exploits and proofs of concept.

CLOUDFLARE

A Growing Global Network Built for Scale

15 Tbps Capacity and 151 Data Center Global Footprint

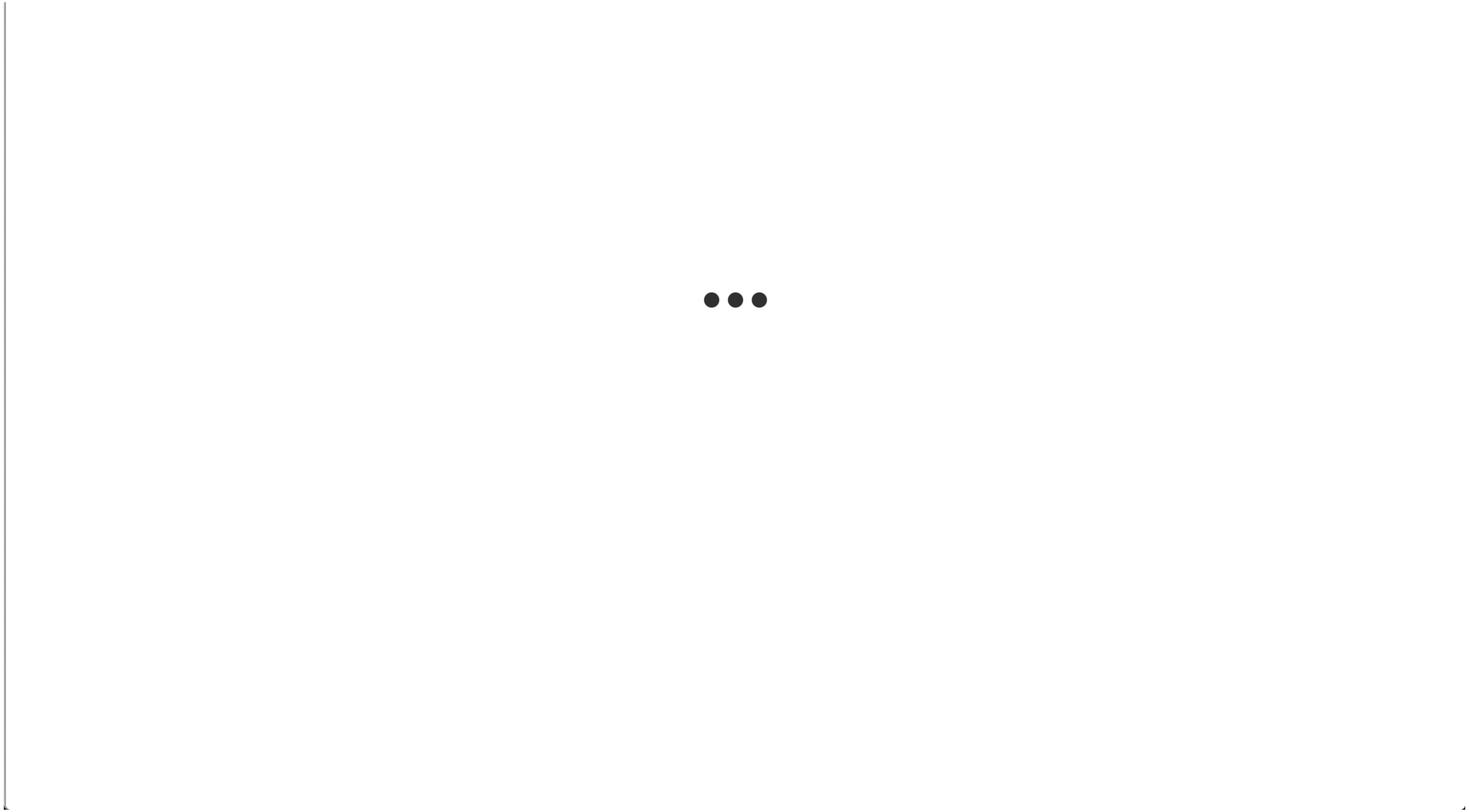


Block Malicious Bot Abuse

Prevent bots from excessive usage and abuse across websites, applications, and API endpoints

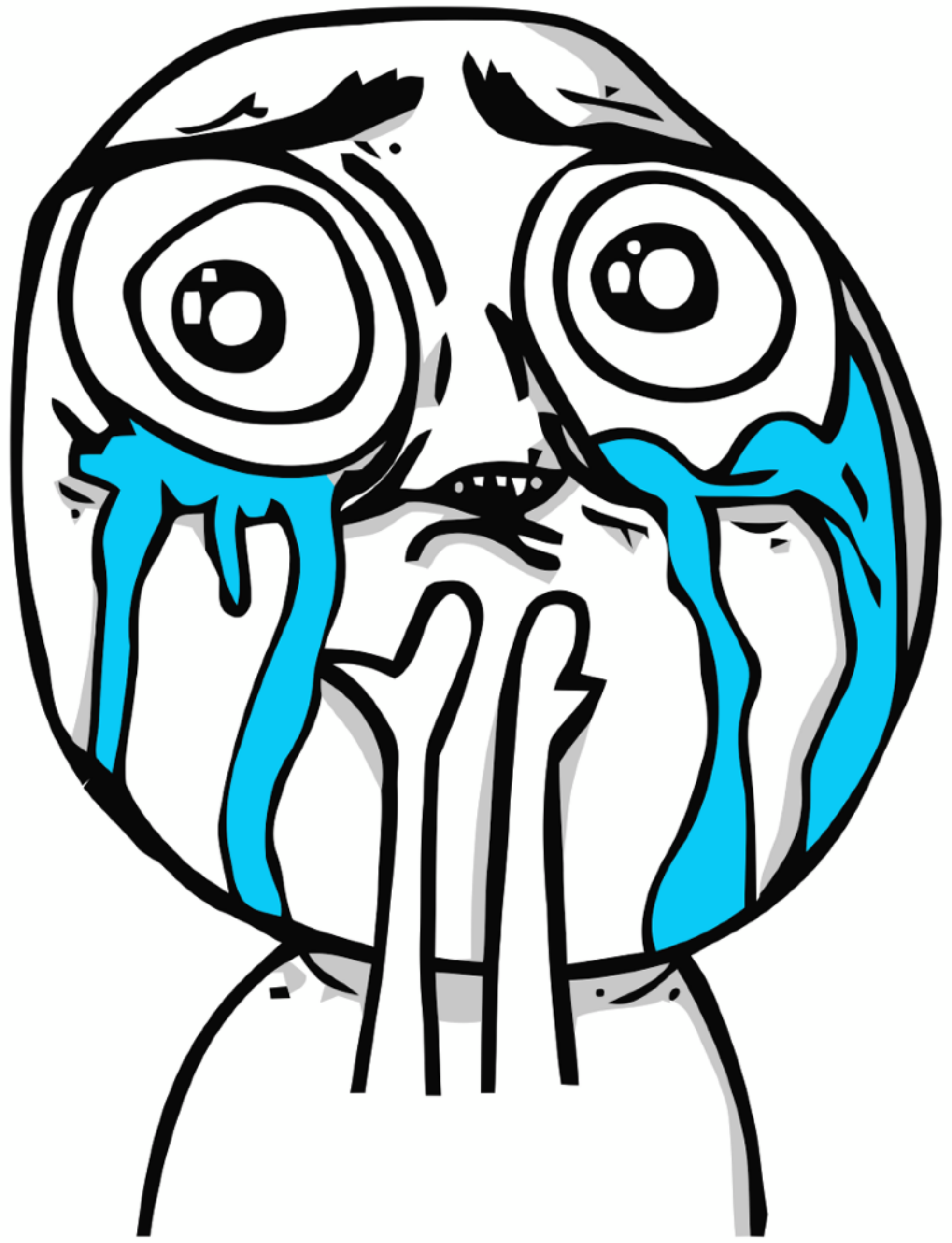
DigitalOcean usa questo sistema sulla pagina di login

tramite il servizio offerto da CloudFlare:



Domanda:

Quindi è possibile bloccare totalmente automatismi come:
web scan, fuzzing o enumeration?

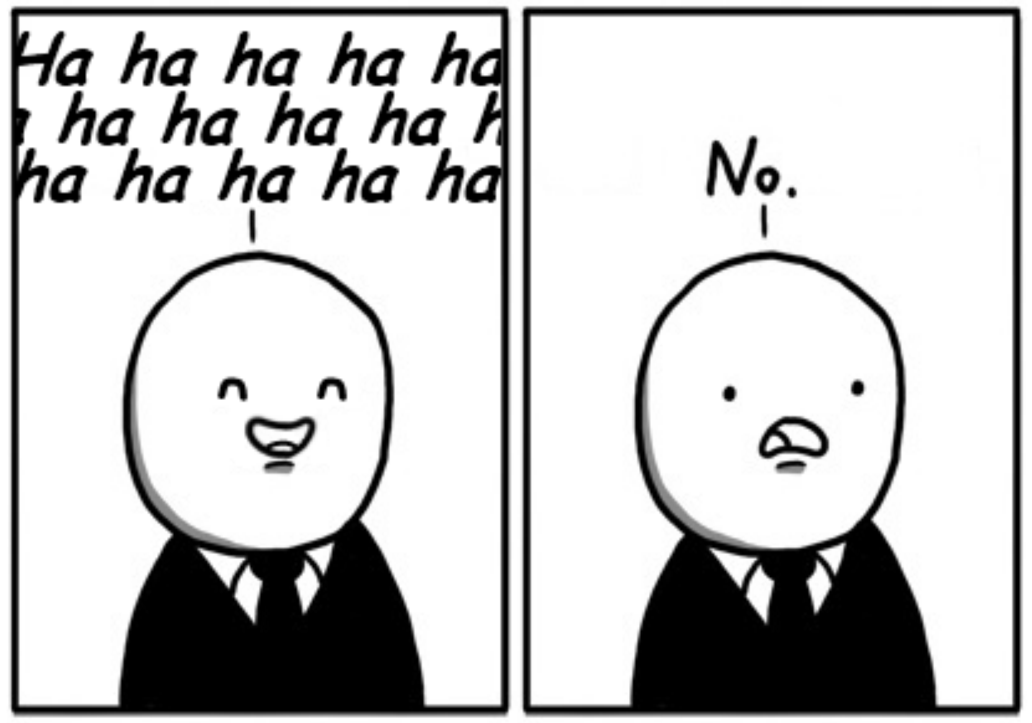


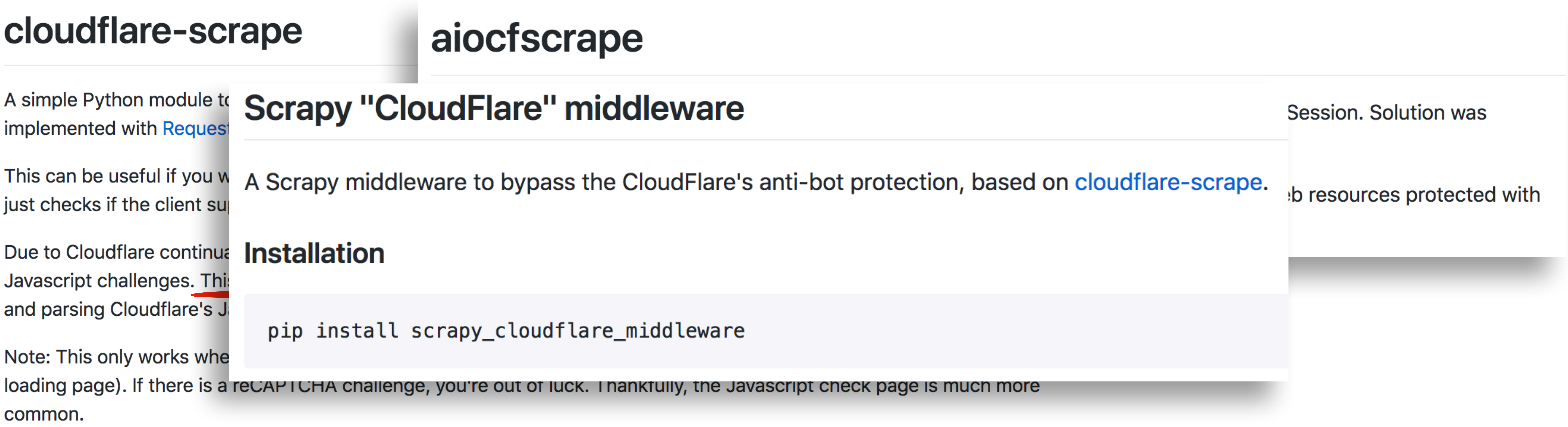
Risposta:

No.

Ma… CloudFlare ci riesce…

se lo vendono vuol dire che è sicuro!





cloudflare-scrape

A simple Python module tc
implemented with Request

This can be useful if you w
just checks if the client su

Due to Cloudflare continu
Javascript challenges. Thi
and parsing Cloudflare's J

Note: This only works whe
loading page). If there is a reCAPTCHA challenge, you're out of luck. Thankfully, the Javascript check page is much more common.

aiocfscrape

Session. Solution was

b resources protected with

Scrapy "CloudFlare" middleware

A Scrapy middleware to bypass the CloudFlare's anti-bot protection, based on cloudflare-scrape.

Installation

```
pip install scrapy_cloudflare_middleware
```

Perché implementarlo se è eludibile?

Vi stupirete di quanto stupidi siano la maggior parte dei tool

nikto, skipfish, dirbuster, wpscan, wfuzz, ecc…
non riescono a risolvere challenge JavaScript

rimuovere il "rumore di fondo" permette di avere meno log da analizzare e di concentrarsi su attacchi mirati

0% di falsi positivi

Come si fa?

Nginx

Possiamo costruire un sistema molto simile a quello usato da CloudFlare usando Nginx

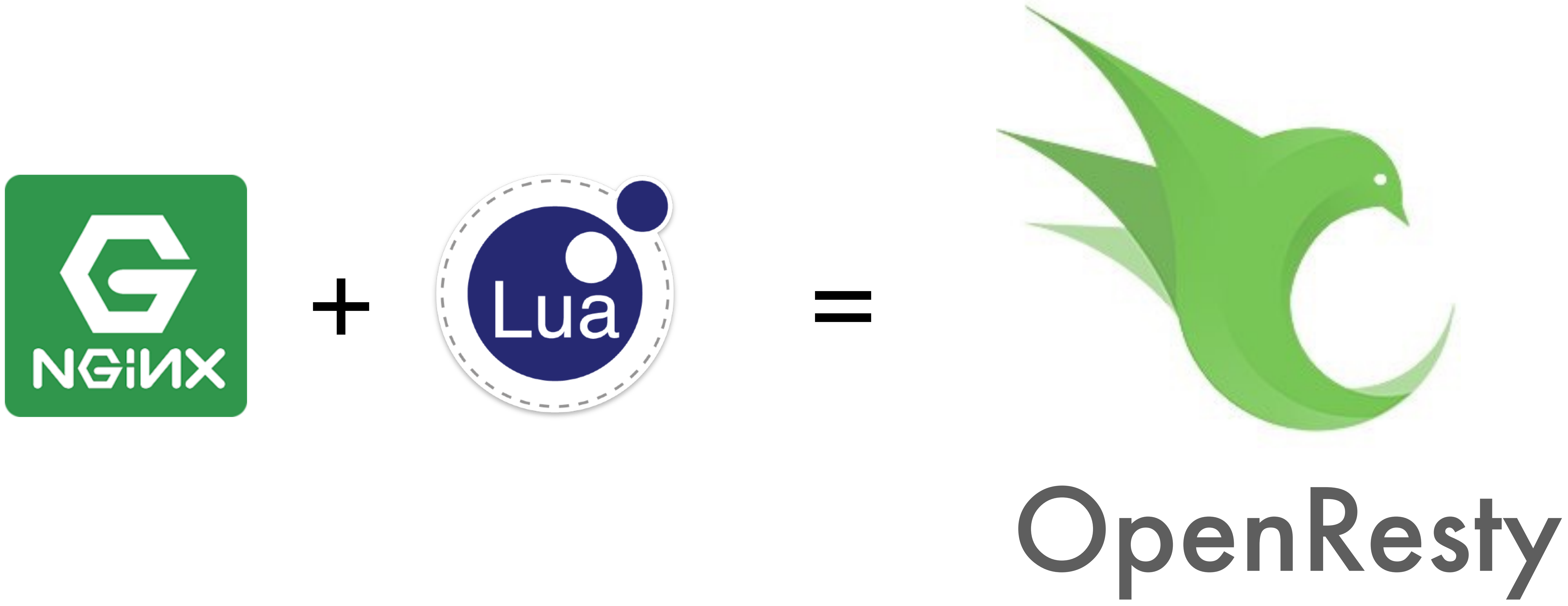
Useremo solo il file di configurazione di Nginx senza aggiungere o modificare codice alla nostra webapp

Generare dinamicamente codice JavaScript modificando semplicemente nginx.conf?

Possiamo fare tutto su nginx.conf

grazie al modulo lua_nginx_module

github.com/openresty/lua-nginx-module



OpenResty è disponibile all'indirizzo

openresty.org

openresty.org/en/download.html
OpenResty®
Scalable Web Platform by Extending NGINX with Lua
Download
Installation
Getting Started
Upgrading
Changes
Events
Components
Community

Download

Yichun Zhang (agentzh) , 14 May 2018 (created 21 Jun 2011)

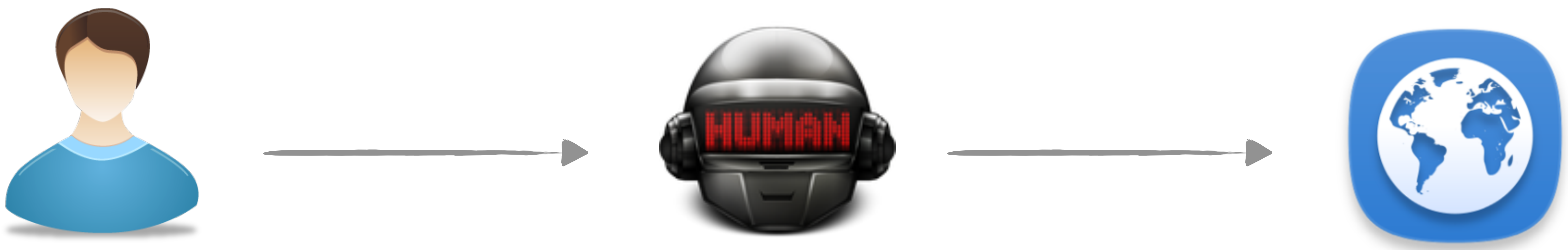
Binary Releases

Linux

OpenResty® provides official pre-built packages for common Linux distributions.

We currently support Ubuntu, Debian, RHEL, CentOS, Fedora, and Amazon Linux.

We also provide official package repositories for our users so that receiving and installing package



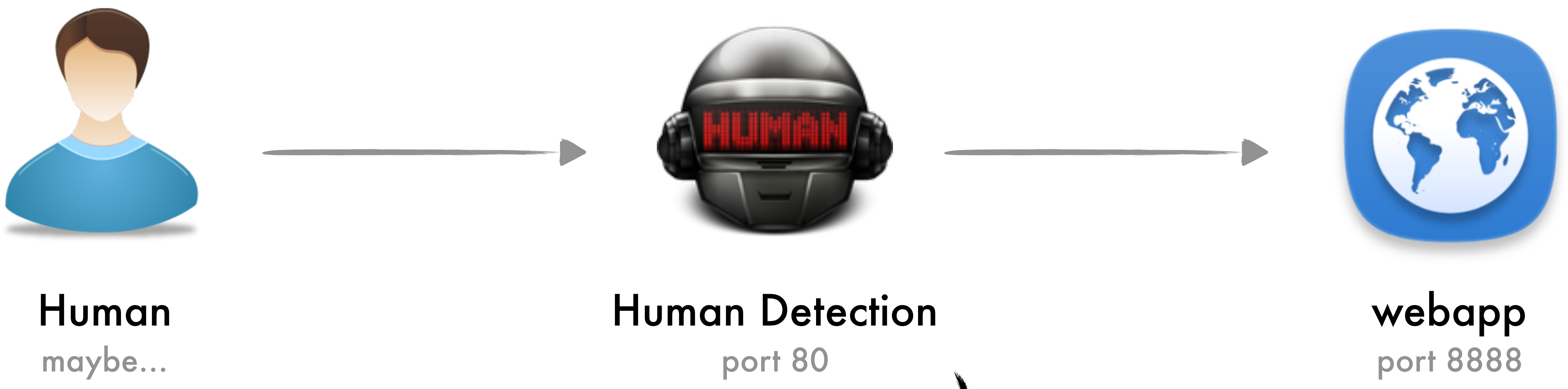
Human
maybe…

Human Detection
port 80

webapp
port 8888

```
server {
   listen 127.0.0.1:8888;
   server_name example.com;

   location / {
      root   html;
      index  index.php;
      …
   }
}
```



```
server {
    listen 80;
    server_name example.com;

    location / {
        proxy_pass http://127.0.0.1:8888;
    }
}
```

encrypted-session-nginx-module

github.com/openresty/encrypted-session-nginx-module

```
encrypted_session_key 'abcdefghijklmnopqrstuvwxyz123456';
encrypted_session_iv '1234567812345678';
encrypted_session_expires 20;

location /admin/ {
    set_encrypt_session $token 'stringa di testo';
    set_encode_base32 $token;
    …
}
```

AES-256 -> base32

```
eg76rede7jduekap71qe7sgrpshpgs68ktb8ocj1arr6u37dcfslc9f
g69tuck8prdus6jh3mc4foh6j7i6lgv798t3hf9n4pohv5pq8c7rvh8
ghkt0pd70jf452i5pck00865og9snqp8ls453ufrubgo======
```

ngx.var.token

encrypted-session-nginx-module

github.com/openresty/encrypted-session-nginx-module

```
ts=2018-09-22T15:30:00.000Z, src=192.168.1.4, ua=Mozilla/5.0 (Macintosh…
```

encrypt AES-256

```
00000000  77 42 32 cb 05 4e 00 5d  27 44 bc ab 90 44 0b b4  |wB2..N.]'D...D..|
00000010  58 44 53 95 29 7f 1a 46  aa 0b 2e 75 b4 9c e4 80  |XDS.)..F...u....|
00000020  05 99 91 44 e7 e2 6d 8c  0e da 2a a9 c9 f4 40 8c  |...D..m...*...@.|
00000030  44 79 17 f4 38 cb 94 fa  f0 54 d2 8a 7c d4 09 79  |Dy..8....T..|..y|
00000040  fe cd ba 25 1c c5 87 e5  00 93 d3 ed c4 ab c3 b9  |...%............|
…
```

encode base32

```
ehtkuchg64w2uc1t5mt34n1h6mx36c1u60r2wc1g61d2r83ke9hkuc9t68q32d
hr5rrjwd1c41up2faddxx6jv3cc4qkabhg40m4urb3d5q78vvkdundefinedk0
```

```
location ~ /wp-login.php {
    set $allowreq 0;

    set_decode_base32 $enciamhuman $cookie_iamhuman;
    set_decrypt_session $plainiamhuman $enciamhuman;

    set_by_lua_block $allowreq {
      … if token ok …
       return 1
      … else …
       return 0
    }

    if ($allowreq = 1) {
       proxy_pass http://127.0.0.1:8888;
    }

    if ($allowreq = 0) {
       content_by_lua_block {
           … challenge javascript …
       }
    }
}
```

decrypt cookie token

se il token è ok,
allora set $allowreq a 1

se $allowreq == 1
forward verso la webapp

se $allowreq == 0
challenge JavaScript

Facciamolo!

descrizione della configurazione e test pratico

Rendiamo difficile recuperare il Token

JavaScript Obfuscation

```
numero “0”: (+[]+[])

numero “1”: (+!![]+[])

numero “2”: (!+[]+!![]+[])

numero “3”: (!+[]+!![]+!![]+[])

numero “4”: (!+[]+!![]+!![]+!![]+[])

numero “5”: (!+[]+!![]+!![]+!![]+!![]+[])

numero “6”: (!+[]+!![]+!![]+!![]+!![]+!![]+[])

numero “7”: (!+[]+!![]+!![]+!![]+!![]+!![]+!![]+[])

numero “8”: (!+[]+!![]+!![]+!![]+!![]+!![]+!![]+!![]+[])

numero “9”: (!+[]+!![]+!![]+!![]+!![]+!![]+!![]+!![]+!![]+[])
```

CloudFlare usa la stessa tecnica

JavaScript Obfuscation

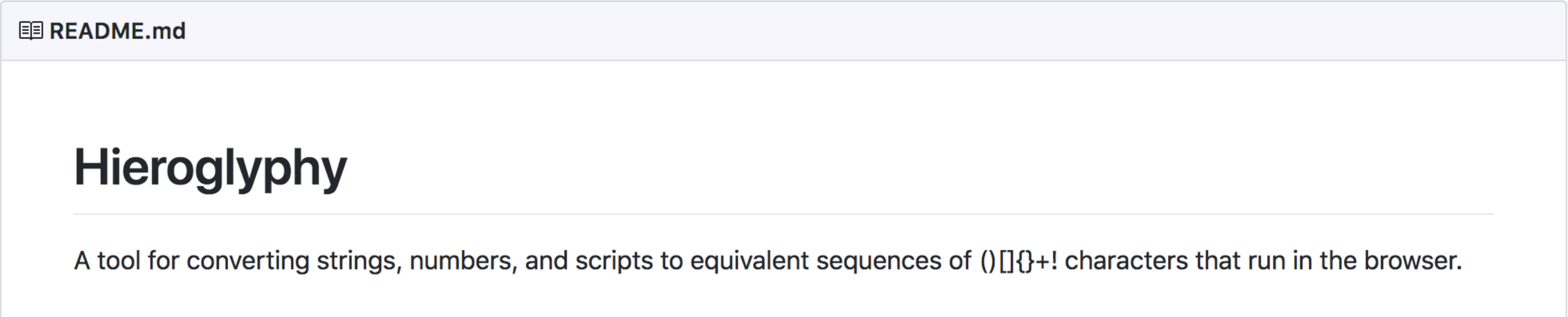
```
bash-3.2$ curl 'https://cloud.digitalocean.com/login'
<!DOCTYPE HTML>
<html lang="en-US">
<head>
  <meta charset="UTF-8" />
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />
```

...

```
    <script type="text/javascript">
  //<![CDATA[
  (function(){
    var a = function() {try{return !!window.addEventListener} catch(e) {return !1} },
    b = function(b, c) {a() ? document.addEventListener("DOMContentLoaded", b, c) : document.attachEvent("onreadystatechange", b)};
    b(function(){
      var a = document.getElementById('cf-content');a.style.display = 'block';
      setTimeout(function(){
        var s,t,o,p,b,r,e,a,k,i,n,g,f, TpdNpSi={"GVGoBj":+((!+[]+!![]+!![]+!![]+!![]+!![]+!![]+!![]+[])+(+!![])+(!+[]+!![]+!![]+!![]+!![]+!![]+!![
])+(!+[]+!![]+!![]+!![]+!![])+(+[])+(!+[]+!![]+!![]+!![])+(!+[]+!![])+(!+[]+!![]+!![]+!![])+(!+[]+!![]+!![]))/+((!+[]+!![]+!![]+!![]+!![]+!![]+!![]+!![
]+!![]+!![]+[])+(!+[]+!![]+!![]+!![])+(!+[]+!![]+!![]+!![]+!![]+!![]+!![]+!![]+!![])+(!+[]+!![]+!![]+!![]+!![]+!![]+!![]+!![]+!![])+(!+[]+!![]+!![
]+!![]+!![]+!![])+(!+[]+!![]+!![]+!![]+!![])+(+!![])+(!+[]+!![])+(!+[]+!![]+!![]+!![]+!![]+!![]))};
        t = document.createElement('div');
        t.innerHTML="<a href='/'>x</a>";
        t = t.firstChild.href;r = t.match(/https?:\/\//)[0];
        t = t.substr(r.length); t = t.substr(0,t.length-1);
        a = document.getElementById('jschl-answer');
        f = document.getElementById('challenge-form');
        ;TpdNpSi.GVGoBj*=+((!+[]+!![]+!![]+!![]+!![]+!![]+!![]+!![]+!![]+[])+(!+[]+!![])+(+[])+(!+[]+!![]+!![]+!![])+(+!![])+(!+[]+!![]+!![]+!![]+
!![]+!![]+!![]+!![]+!![])+(!+[]+!![]+!![]+!![]+!![]+!![]+!![]+!![])+(!+[]+!![])+(!+[]+!![]+!![]))/+((!+[]+!![]+!![]+!![]+!![]+!![]+!![]+!![]+[])+(
!+[]+!![]+!![]+!![]+!![]+!![])+(+[])+(!+[]+!![]+!![]+!![]+!![]+!![])+(+[])+(!+[]+!![]+!![])+(!+[]+!![])+(!+[]+!![]+!![]+!![]+!![]+!![]+!![])+(!+[]
+!![]));TpdNpSi.GVGoBj*=+((!+[]+!![]+!![]+!![]+!![]+!![]+!![]+!![]+[])+(!+[]+!![]+!![]+!![]+!![])+(!+[]+!![]+!![]+!![]+!![]+!![]+!![]+!![])+(!+[]+
!![]+!![]+!![]+!![])+(!+[]+!![]+!![]+!![]+!![]+!![]+!![]+!![]+!![])+(!+[]+!![]+!![]+!![]+!![]+!![]+!![]+!![]+!![])+(!+[]+!![]+!![]+!![]+!![])+(+[]
)+(!+[]+!![]+!![]))/+((!+[]+!![]+!![]+[])+(!+[]+!![])+(!+[]+!![])+(!+[]+!![]+!![]+!![]+!![]+!![]+!![]+!![]+!![])+(!+[]+!![]+!![]+!![]+!![]+!![]+!!
[]+!![]+!![])+(!+[]+!![])+(!+[]+!![])+(!+[]+!![]+!![])+(!+[]+!![]+!![]+!![]+!![]));a.value = +TpdNpSi.GVGoBj.toFixed(10) + t.length; '; 121'
        f.action += location.hash;
```

hieroglyphy.py

github.com/mattaereal/hieroglyphy-py



README.md

Hieroglyphy

A tool for converting strings, numbers, and scripts to equivalent sequences of ()[]{}+! characters that run in the browser.

```
[andreamenin@theMiddlePro ~/g/hieroglyphy-py>
[andreamenin@theMiddlePro ~/g/hieroglyphy-py> ./hieroglyphy.py
# Copyright (c) <2012> <Matías Ariel Ré Medina>
# Hieroglyphy, port from JavasCript version by <Patricio Palladino>
[!] Usage: ./hieroglyphy.py script <File>|number <Number>|string <String>
[!] Examples:
        ./hieroglyphy.py script file.js
        ./hieroglyphy.py string "alert('xss')"
        ./hieroglyphy.py number 1337
[andreamenin@theMiddlePro ~/g/hieroglyphy-py>
[andreamenin@theMiddlePro ~/g/hieroglyphy-py>
[andreamenin@theMiddlePro ~/g/hieroglyphy-py> ./hieroglyphy.py string "hello"
# Copyright (c) <2012> <Matías Ariel Ré Medina>
# Hieroglyphy, port from JavasCript version by <Patricio Palladino>
[*] Encoded string below: hello
([]+[][(![]+[])[!+[]+!![]+!![]]+({}+[])[+!![]]+(!![]+[])[+!![]]+(!![]+[])[+[]]][({}+[])[!+[]+!![]+!![]+!![]+!![]]+({}+[])[+!![]]+([][+[]]+[])[+!![]]+(![]+[])[
!+[]+!![]+!![]]+(!![]+[])[+[]]+(!![]+[])[+!![]]+([][+[]]+[])[+[]]+({}+[])[!+[]+!![]+!![]+!![]+!![]]+(!![]+[])[+[]]+({}+[])[+!![]]+(!![]+[])[+!![]]]((!![]+[])[
+!![]]+([][+[]]+[])[!+[]+!![]+!![]]+(!![]+[])[+[]]+([][+[]]+[])[+[]]+(!![]+[])[+!![]]+([][+[]]+[])[+!![]]+({}+[])[!+[]+!![]+!![]+!![]+!![]+!![]+!![]]+(![]+[])
[!+[]+!![]]+({}+[])[+!![]]+({}+[])[!+[]+!![]+!![]+!![]+!![]]+(+{}+[])[+!![]]+(!![]+[])[+[]]+([][+[]]+[])[!+[]+!![]+!![]+!![]+!![]]+({}+[])[+!![]]+([][+[]]+[])
[+!![]])())[+[]]+([][+[]]+[])[!+[]+!![]+!![]]+(![]+[])[!+[]+!![]]+(![]+[])[!+[]+!![]]+({}+[])[+!![]]
andreamenin@theMiddlePro ~/g/hieroglyphy-py>
```

Facciamolo!

descrizione della configurazione e test pratico

All you need is Logs!

ModSecurity -> Logstash -> Elasticsearch <- Kibana

WAF Matched Rules Messages

Rule Message to Site

Rule matching counter

11,231

Requests matching rules

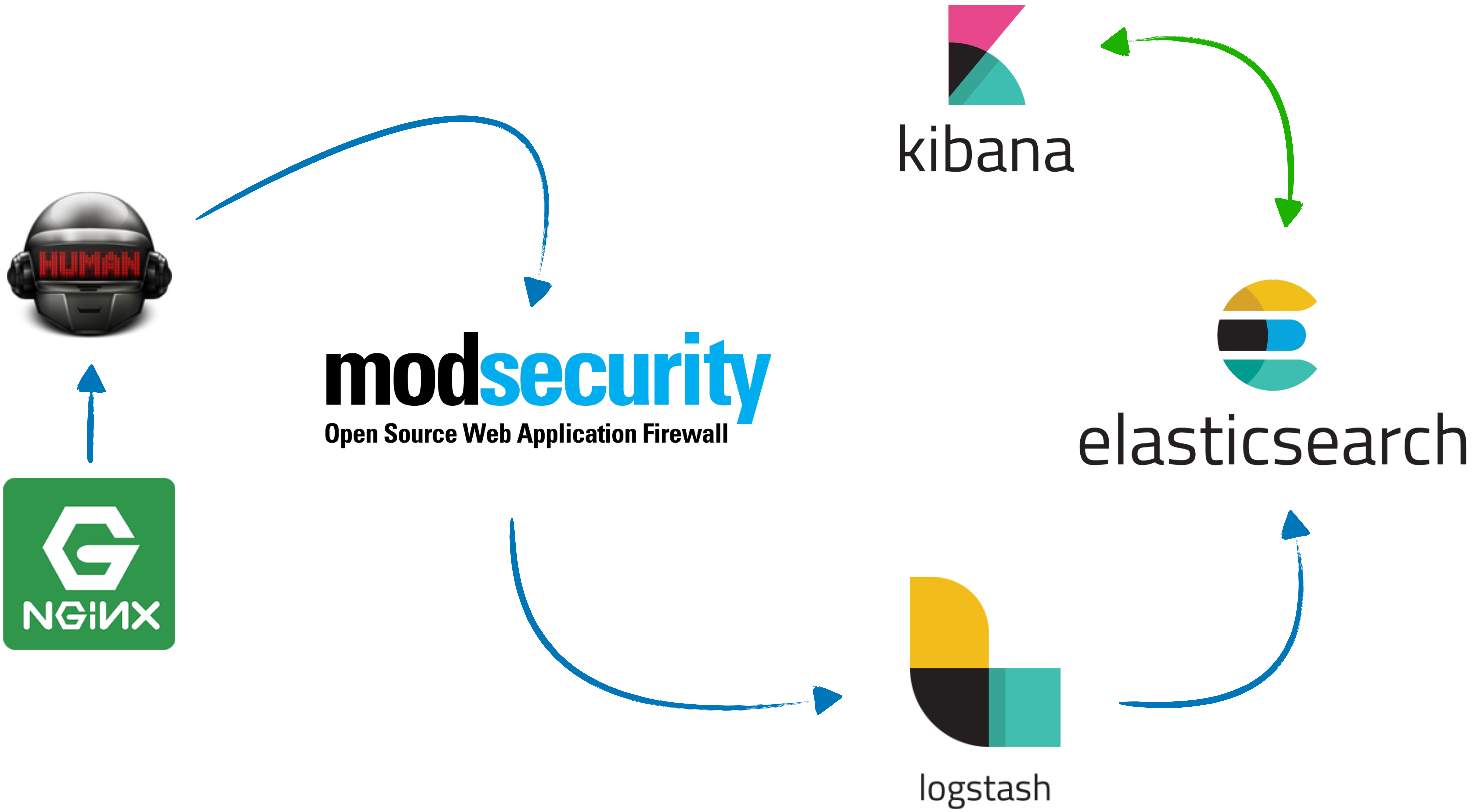
Total Requests

294,277

Total Requests

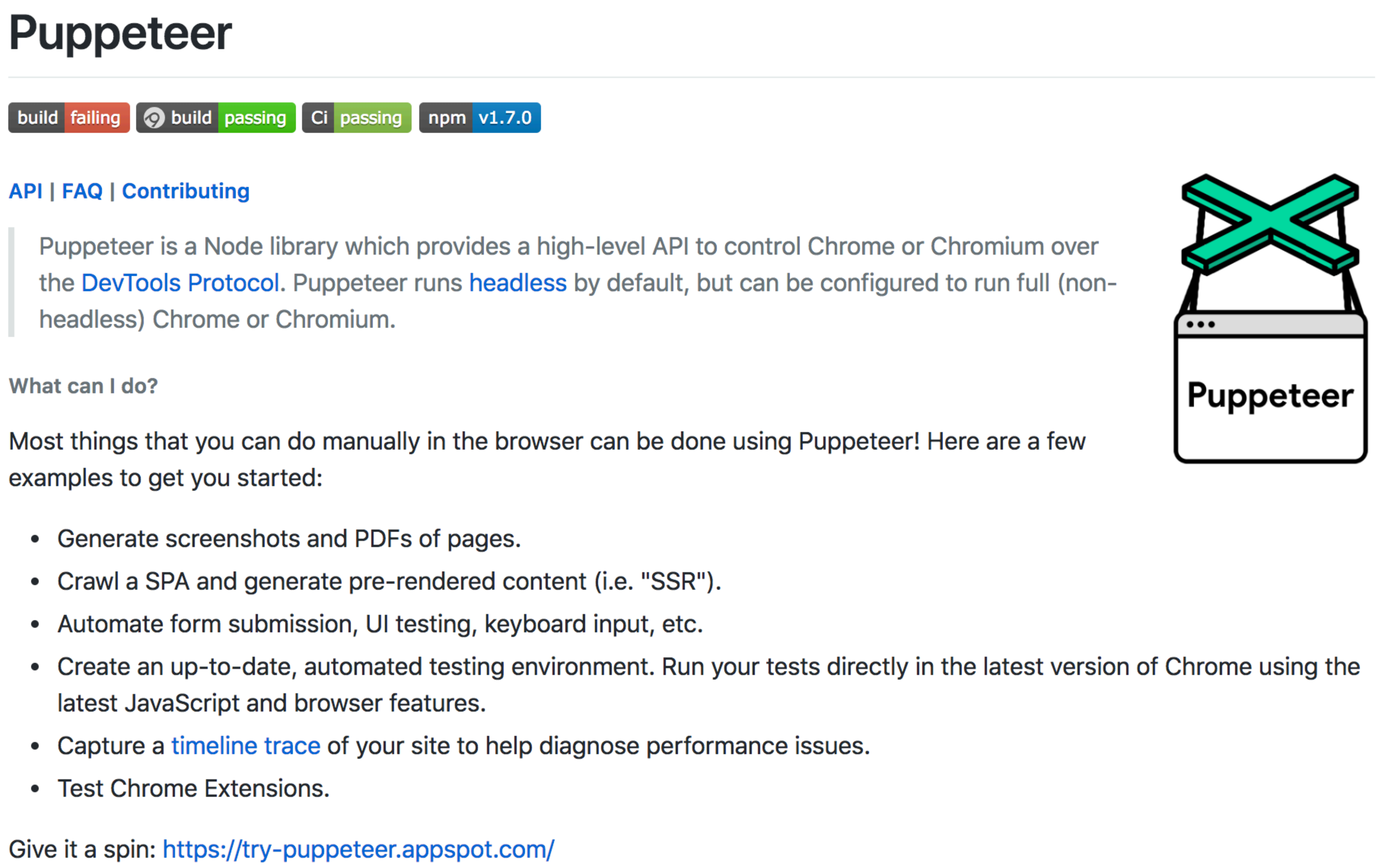
500
400
300
200
100
0
Count
2018-08-03 02:00
2018-08-07 02:00
2018-08-11 02:00
2018-08-15 02:00
2018-08-19 02:00
2018-08-23 02:00
2018-08-27 02:00
2018-08-31 02:00
2018-09-05 02:00
@timestamp per 12 hours
● Human Detection: Mi...
● Human Detection: Bl...
● Human Detection: Bl...
● DNSBL: Tor Exit Node
● DNSBL: IP Address wi...
● DNSBL: Suspicious / ...
16,000
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
Detects MSSQL code execution and information gathering at
Detects concatenated basic SQL injection and SQLLFI attem
File extension not allowed
Human Detection: Missing Cookie
Inbound Anomaly Score Exceeded (Total Score: 15)
Inbound Anomaly Score Exceeded (Total Score: 5)
SQL Injection Attack Detected via libinjection
WordPress Login Harvester
[redacted].it
[redacted].it
Source
Destination

ROMHACK
CYBERSECURITY CONVENTION
romhack.io


HUMAN
NGINX
modsecurity
Open Source Web Application Firewall
logstash
elasticsearch
kibana

Bypass

come risolvere la challenge con un piccolo script



Puppeteer

API | FAQ | Contributing

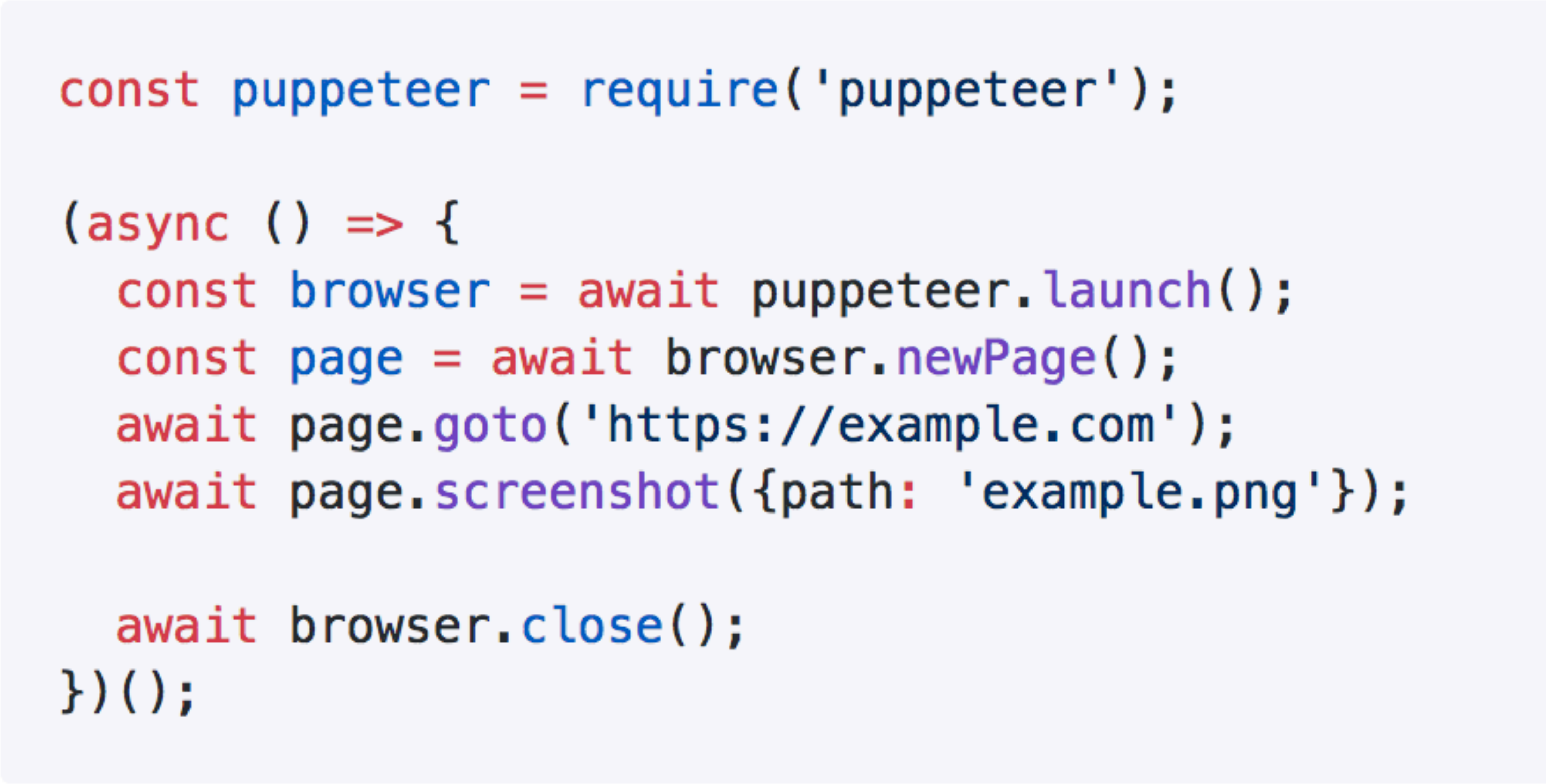
> Puppeteer is a Node library which provides a high-level API to control Chrome or Chromium over the DevTools Protocol. Puppeteer runs headless by default, but can be configured to run full (non-headless) Chrome or Chromium.

What can I do?

Most things that you can do manually in the browser can be done using Puppeteer! Here are a few examples to get you started:

- Generate screenshots and PDFs of pages.
- Crawl a SPA and generate pre-rendered content (i.e. "SSR").
- Automate form submission, UI testing, keyboard input, etc.
- Create an up-to-date, automated testing environment. Run your tests directly in the latest version of Chrome using the latest JavaScript and browser features.
- Capture a timeline trace of your site to help diagnose performance issues.
- Test Chrome Extensions.

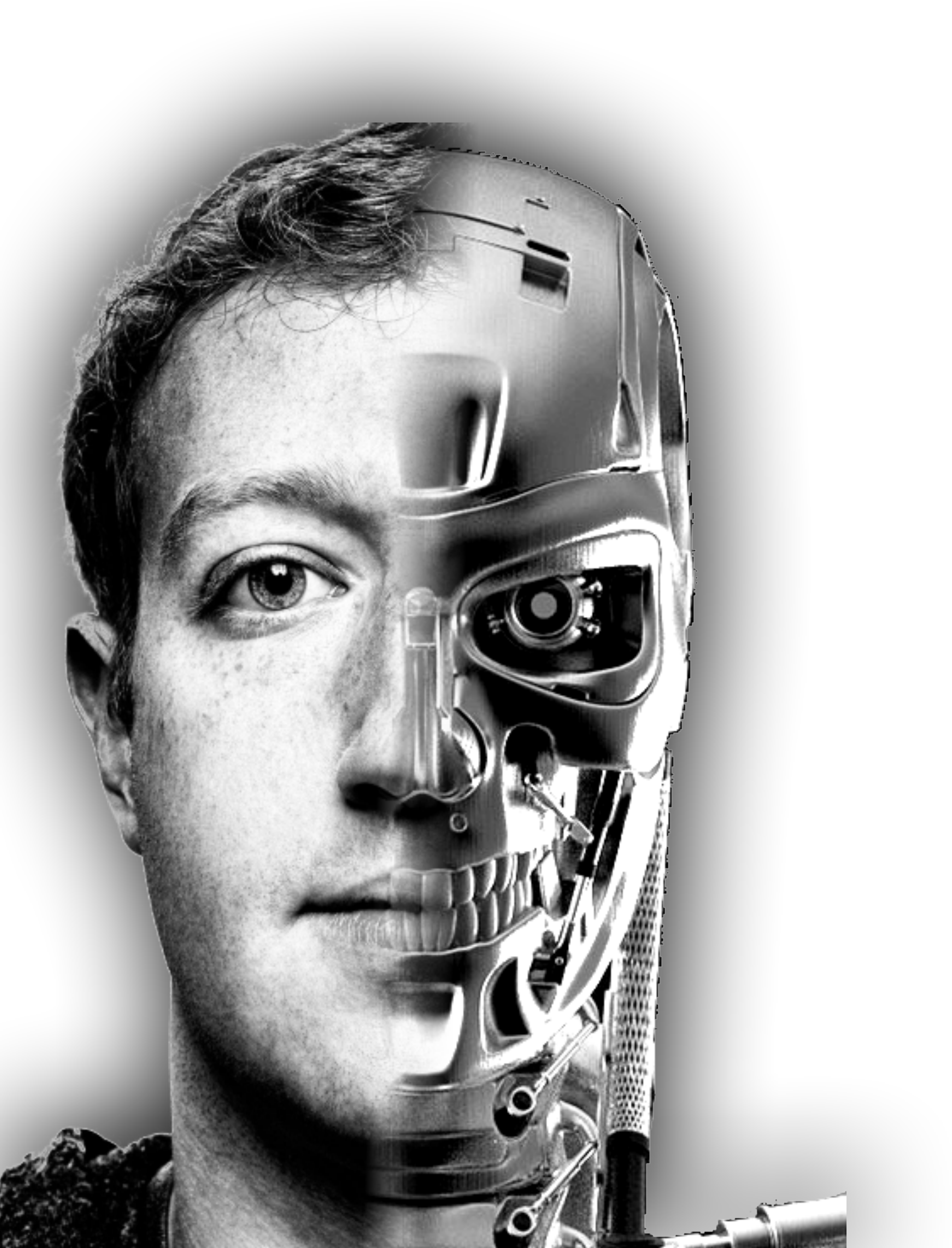
Give it a spin: https://try-puppeteer.appspot.com/



```
const puppeteer = require('puppeteer');

(async () => {
  const browser = await puppeteer.launch();
  const page = await browser.newPage();
  await page.goto('https://example.com');
  await page.screenshot({path: 'example.png'});

  await browser.close();
})();
```



Human Users Detection

stop bots with Nginx + Lua + JavaScript

Grazie!

(per tutto il pesce)

Twitter: **@Menin_TheMiddle**

GitHub: **theMiddleBlue**

youtube.com/rev3rsesecurity

Telegram: **bit.ly/revtele**