

WEB CACHE DECEPTION ATTACK

Omer Gil

Request

Raw Headers Hex

```
GET /myaccount/home/attack.css HTTP/1.1
Host: www.paypal.com
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/52.0.2743.116 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,
image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch, br
Accept-Language: en-US,en;q=0.8,he;q=0.6
```

No SID

Response

Raw Headers Hex HTML Render

```
iv id="js_toggleProfileStatus" class="welcomeMessage
js_selectModule selectModule " data-module-number=""><p
class="vx_h2 engagementWelcomeMessage
nemo_welcomeMessageHeader">Hi Omer.
class="toggleProfileStatus"><button
id="js_engagementActionTrigger" class="vx_btn-link
engagement-actionText vx_small-text js_emTrigger
nemo_engagementActionTrigger"
aria-controls="js_emSlideDownContainer"
name="EM_AcctSetup_Open"
data-pagename="main:walletweb:summary::main"
data-pagename2="main:walletweb:summary::main::"
data-track-type="link"><span class="profileStatusText">Get
even more out of your PayPal account</span></button><span
class="icon icon-small icon-arrow-down-small
nemo_profileStatusDownArrow"
aria-hidden="true"></span></p></div></div><div
id="js_engagementActions" class="col-sm-5
engagementActions"><ul class="actionsContainer
nemo_actionsContainer"><li class="actionItem"><a
href="/myaccount/transfer/buy" role="button" target="_top"
data-module-number="" name="EM_GoodsServices"
```

About me

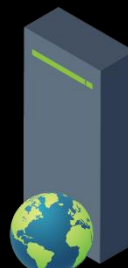
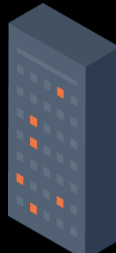
 @omer_gil

 omergil.blogspot.com

- Omer Gil
- 28
- Married + Java
- PT team leader at EY
- Student



About caching

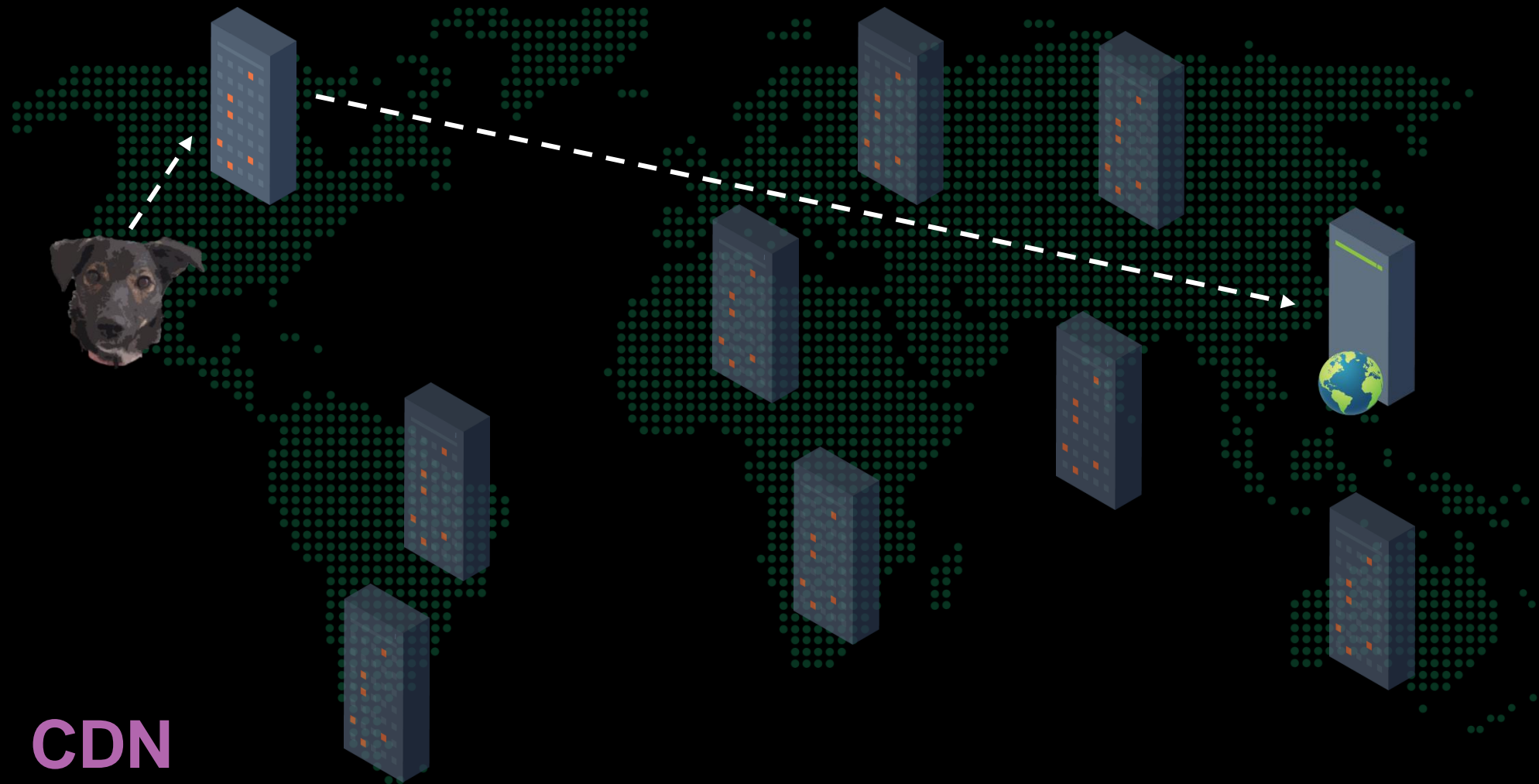


About caching



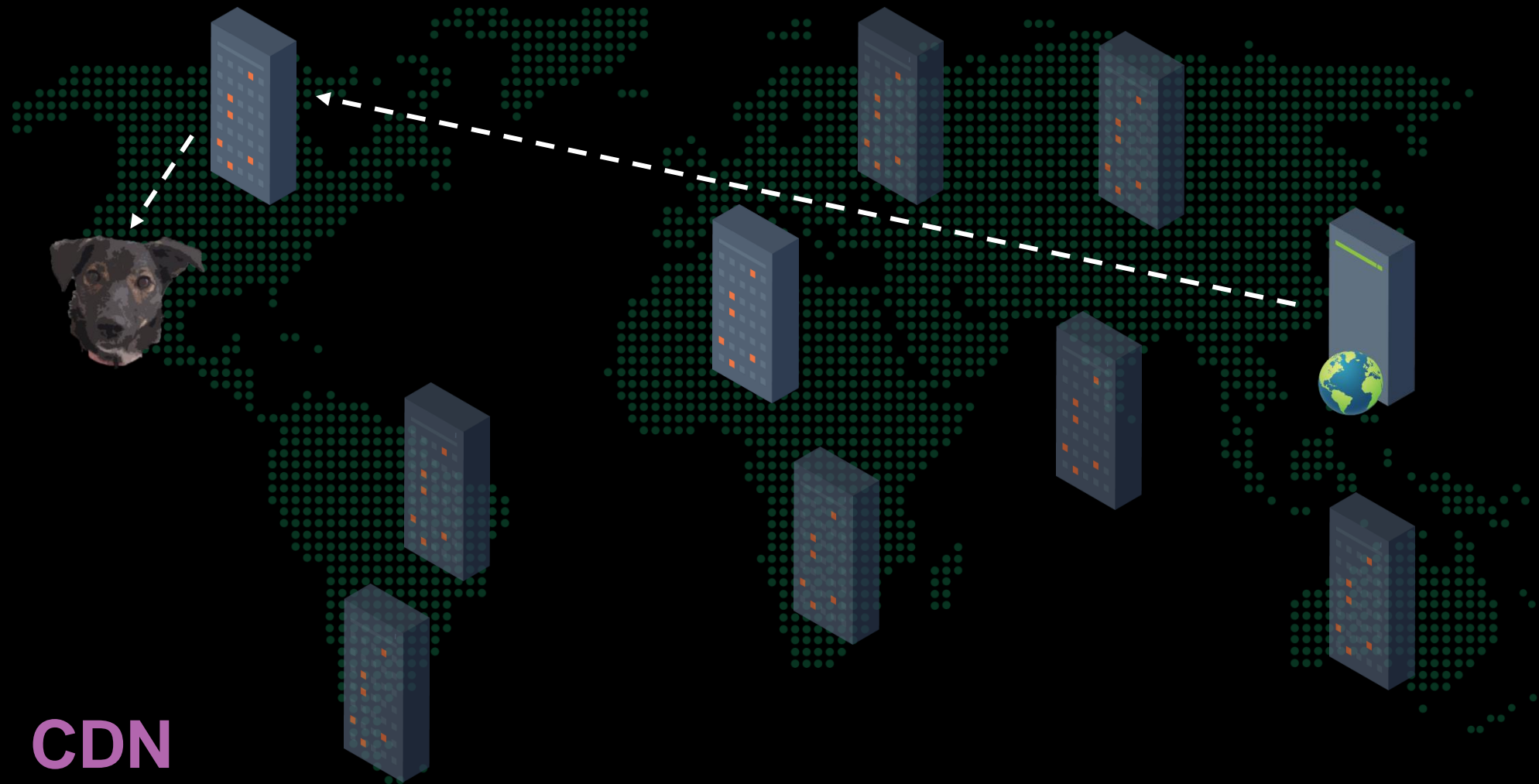
CDN

About caching



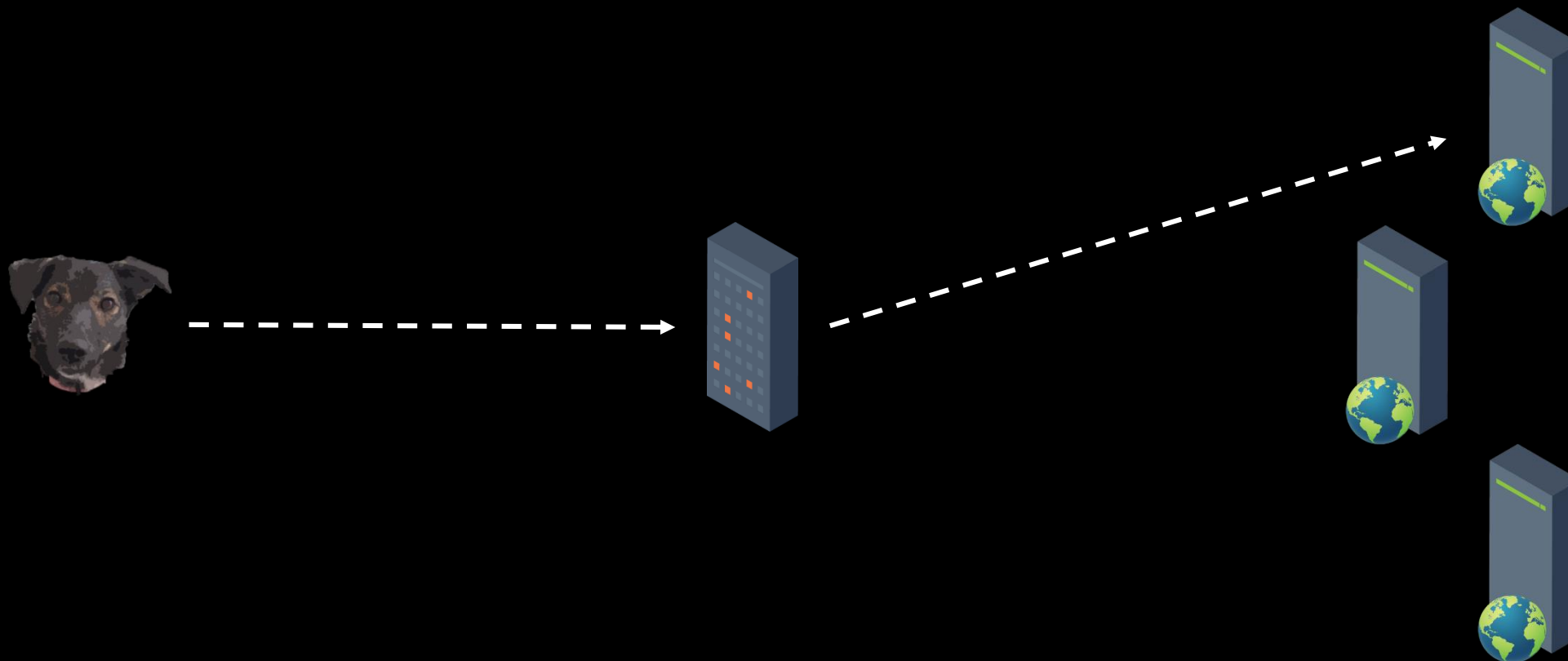
CDN

About caching



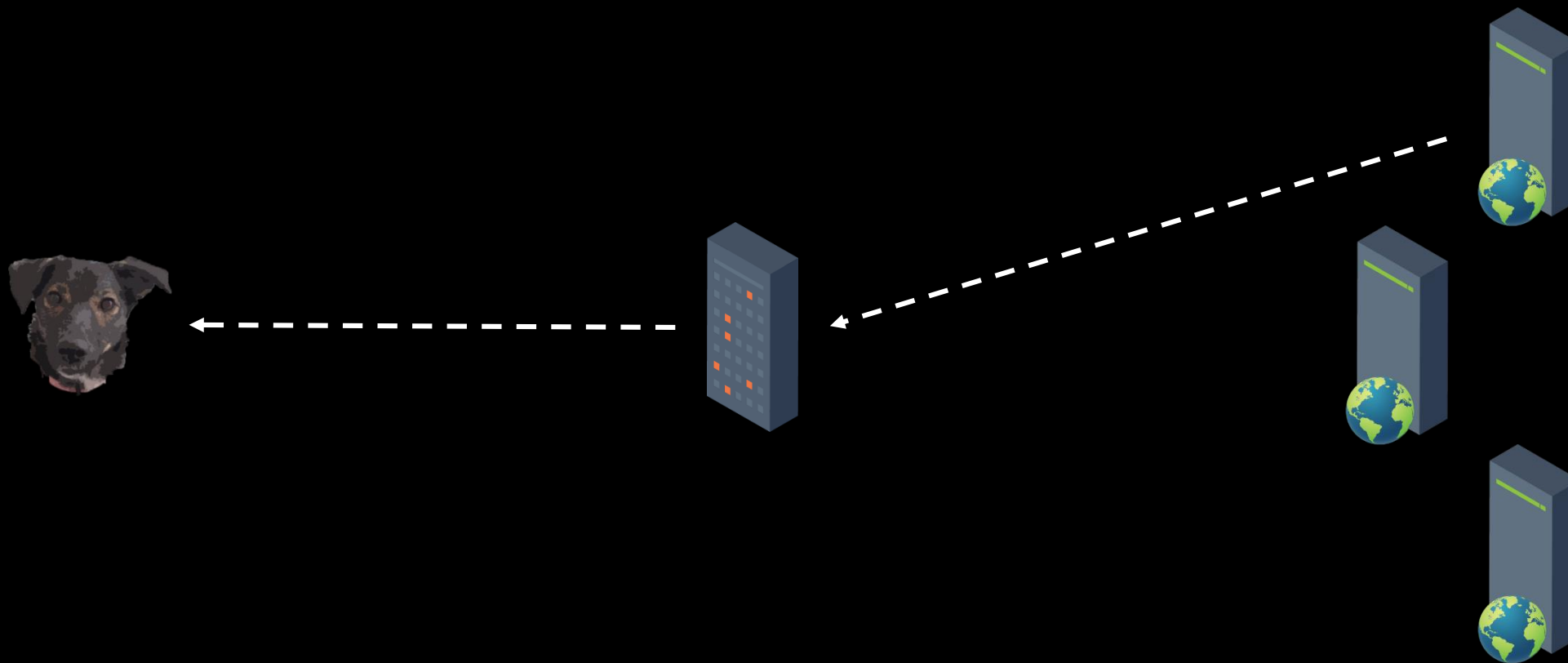
CDN

About caching



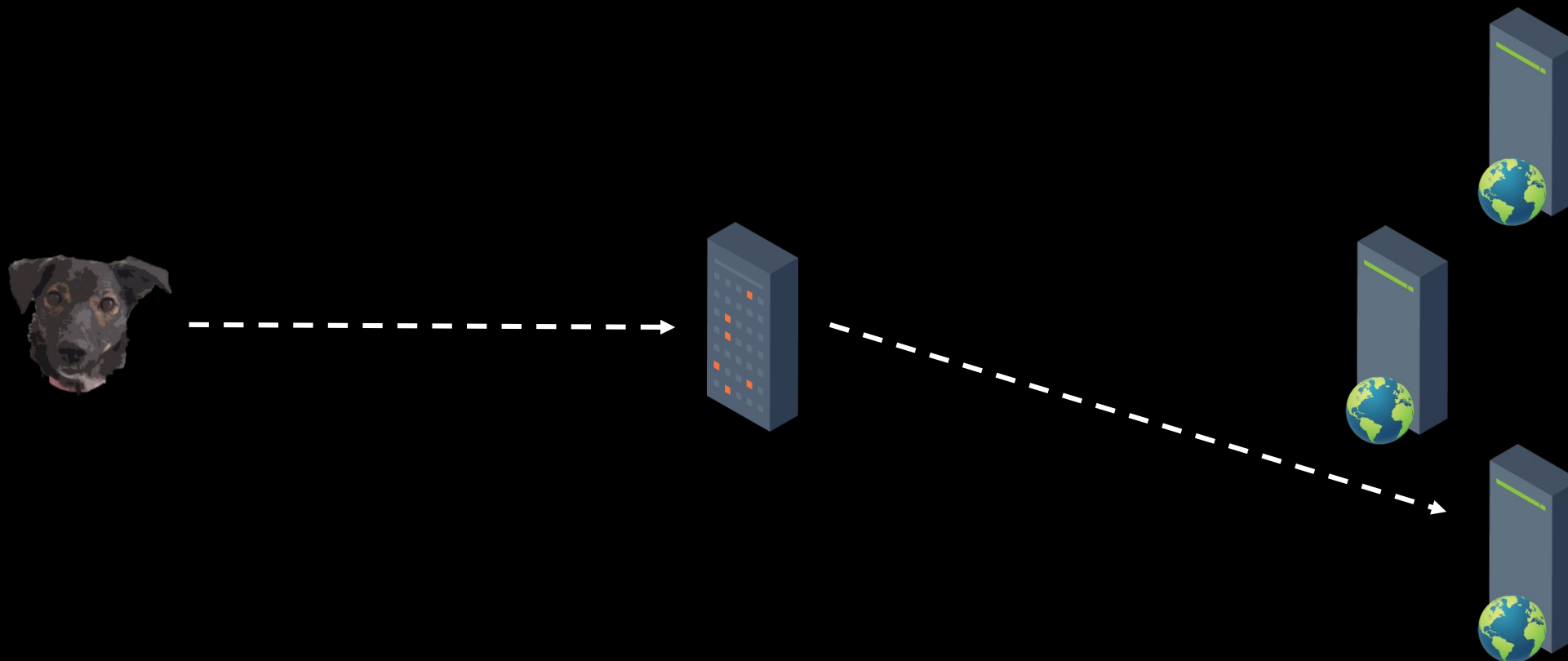
Load Balancer

About caching



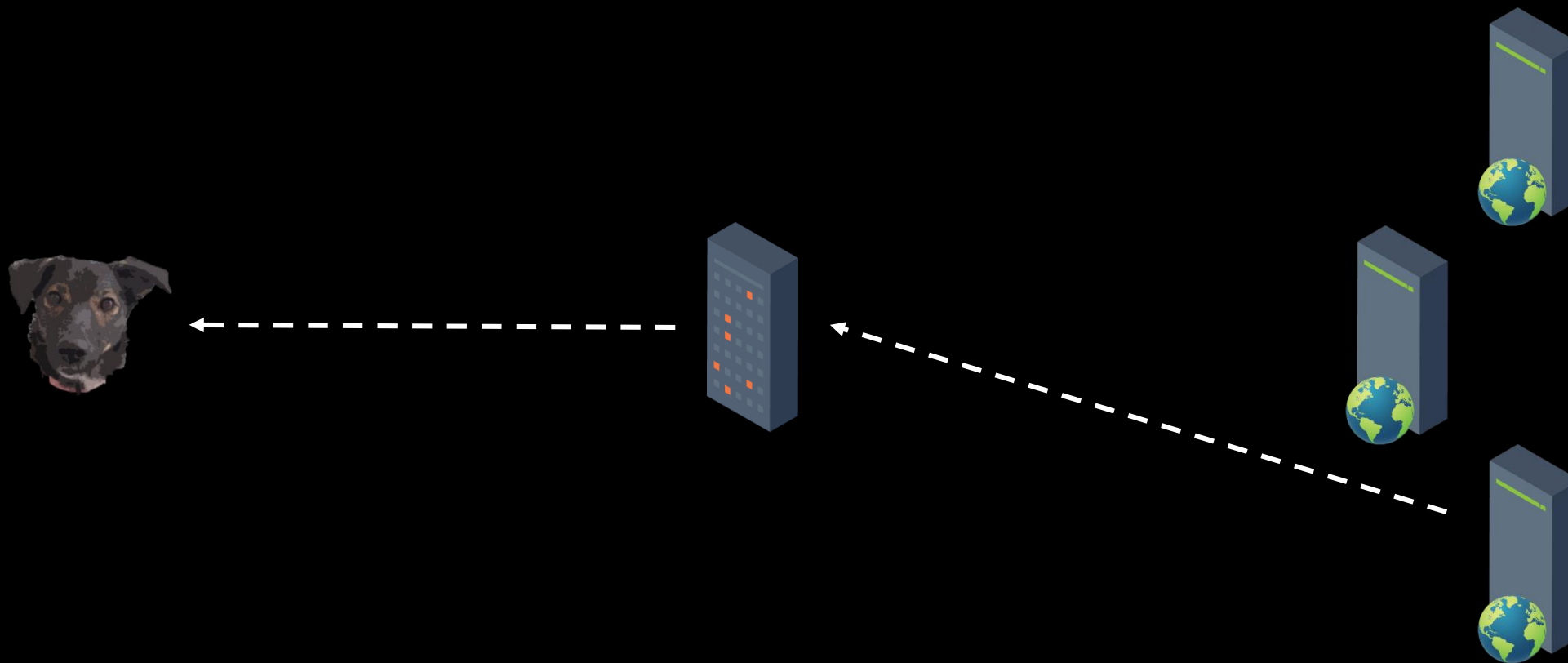
Load Balancer

About caching



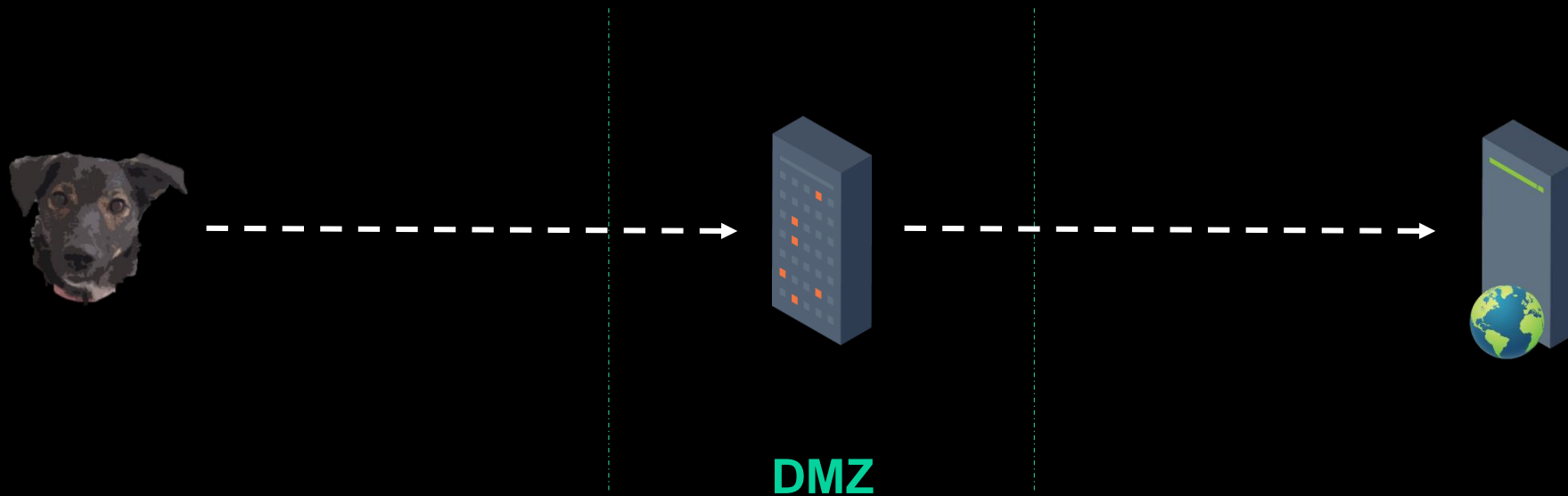
Load Balancer

About caching



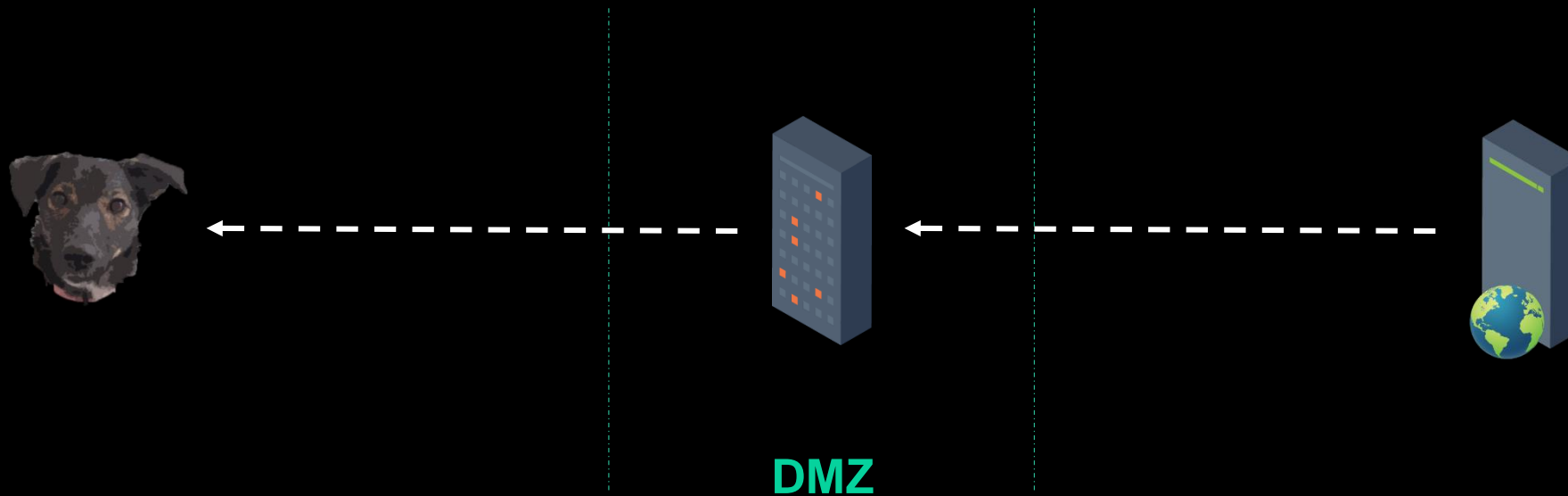
Load Balancer

About caching



Reverse Proxy

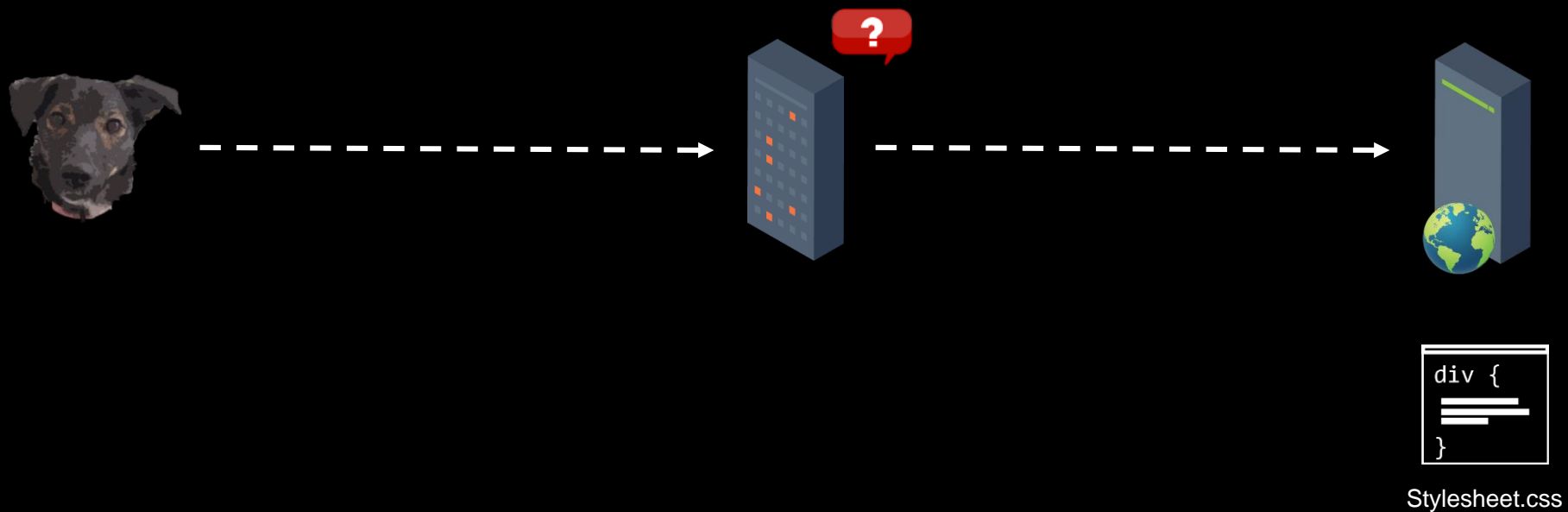
About caching



Reverse Proxy

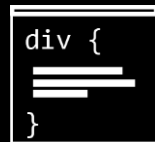
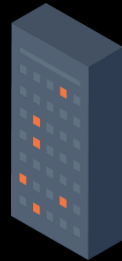
About caching

<https://www.example.com/styleSheet.css>

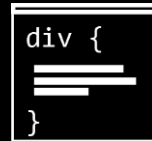
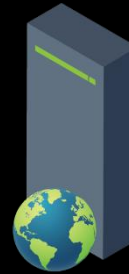


About caching

<https://www.example.com/styleSheet.css>



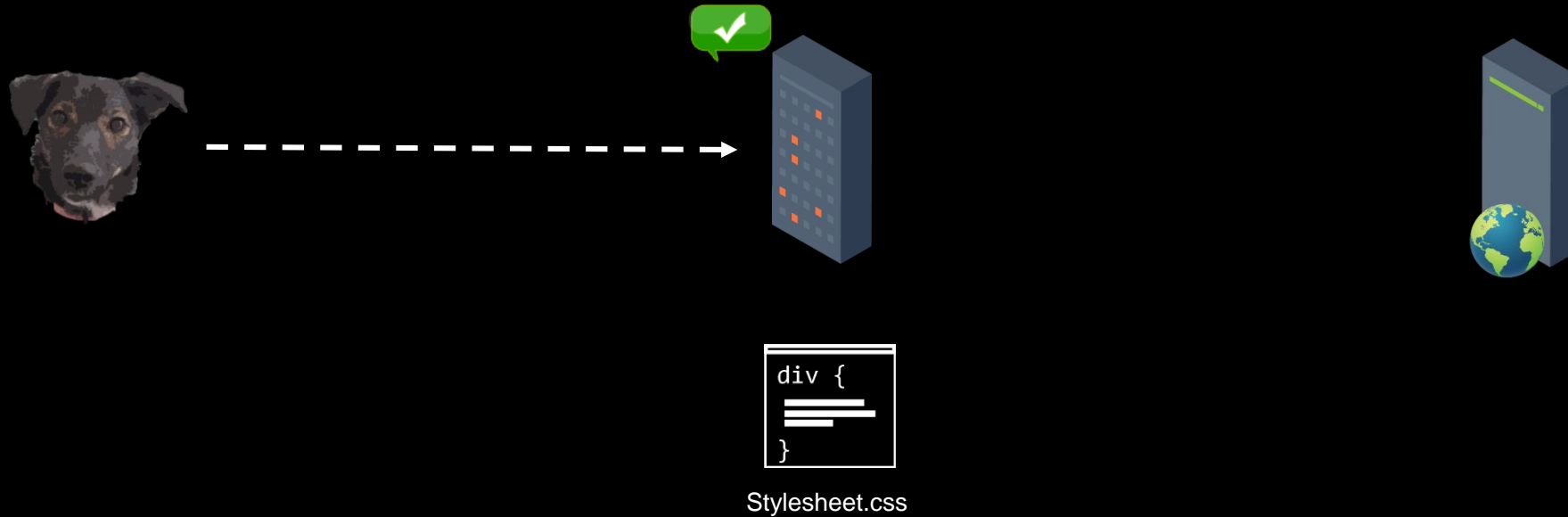
Stylesheet.css



Stylesheet.css

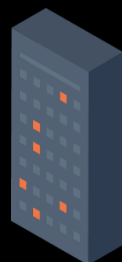
About caching

<https://www.example.com/styleSheet.css>



About caching

<https://www.example.com/styleSheet.css>



Stylesheet.css

Servers' reactions

<http://www.example.com/account.php/nonexistent.css>



account.php

The Spanner: <http://www.thespanner.co.uk/2014/03/21/rpo/>
XSS Jigsaw: <http://blog.innerht.ml/page/2/>

Servers' reactions

<http://www.example.com/account.php/nonexistent.css>



Response from <http://www.example.com:80/account.php/nonexistent.css> [127.0.0.1]

Forward Drop Intercept is on Action

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Thu, 15 Jun 2017 18:47:53 GMT
Server: Apache/2.4.4 (Win32) OpenSSL/0.9.8y PHP/5.4.16
X-Powered-By: PHP/5.4.16
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 1330
Connection: close
Content-Type: text/html

<html>

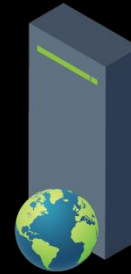
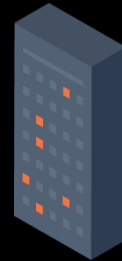
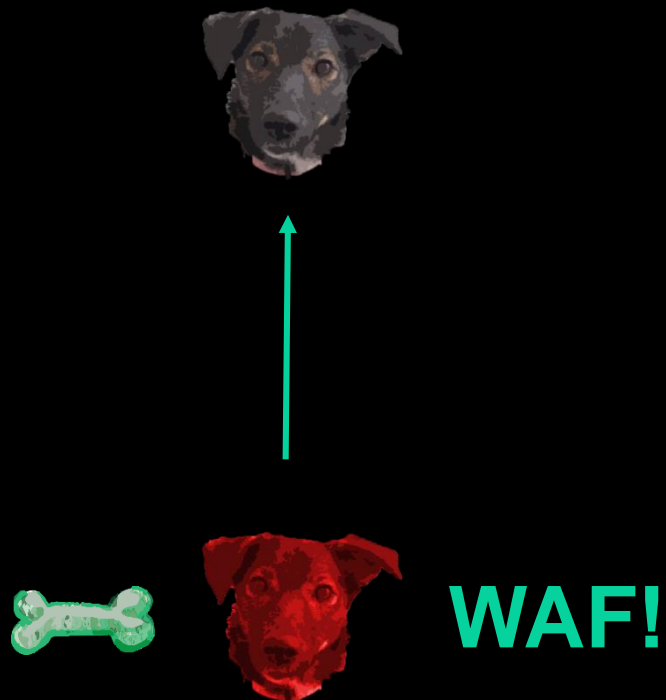
  <head>
    <title>Account</title>
```



account.php

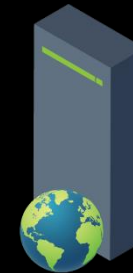
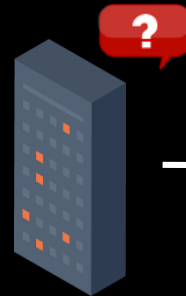
Getting down to business

“Hey, access
<https://www.bank.com/account.do/stylesheet.css>”



Getting down to business

The user browses to
<https://www.bank.com/account.do>/*stylesheet.css*

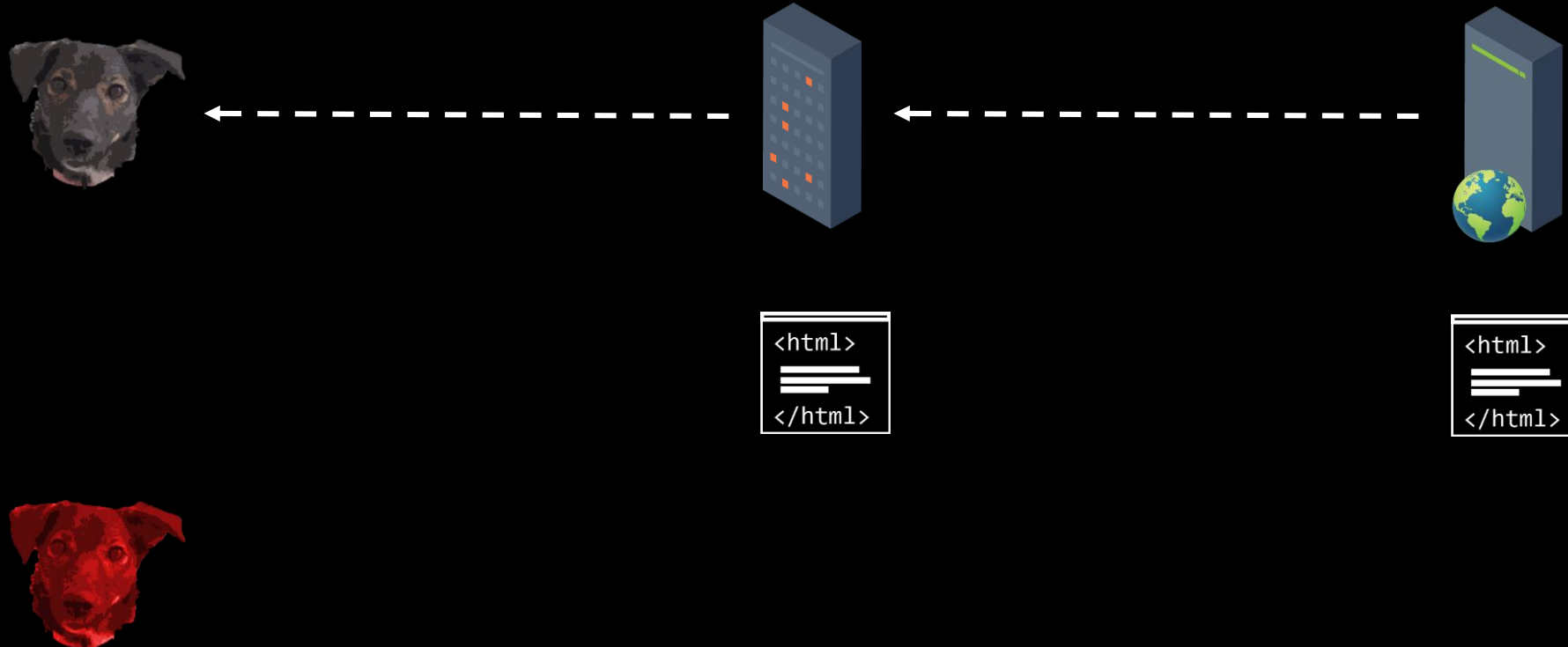


```
<html>  
_____  
</html>
```



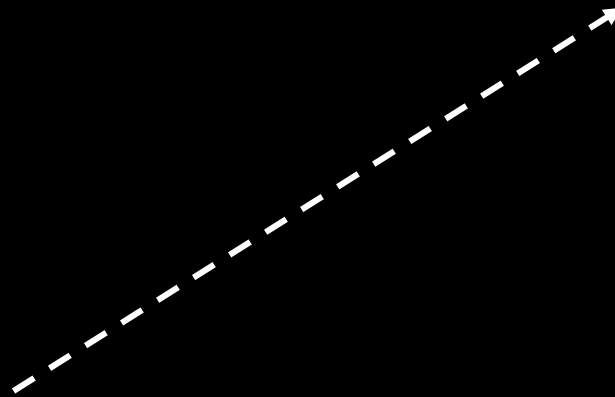
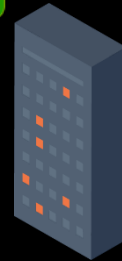
Getting down to business

`https://www.bank.com/account.do`
returns with the content of `account.do`
and the private page is cached



Getting down to business

The attacker browses to
<https://www.bank.com/account.do>/*stylesheet.css*
and gets the content of the user's account.do page

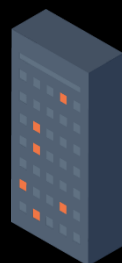


```
<html>  
_____  
</html>
```

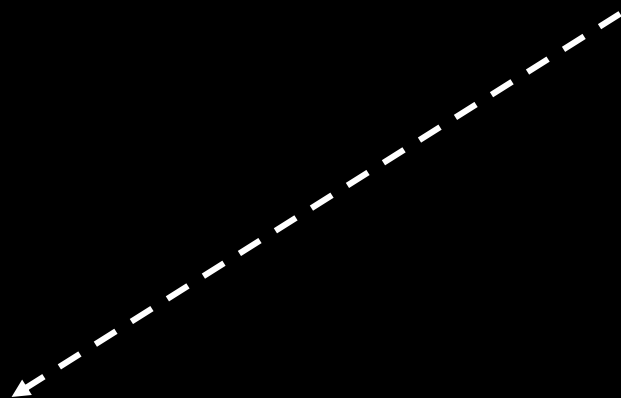


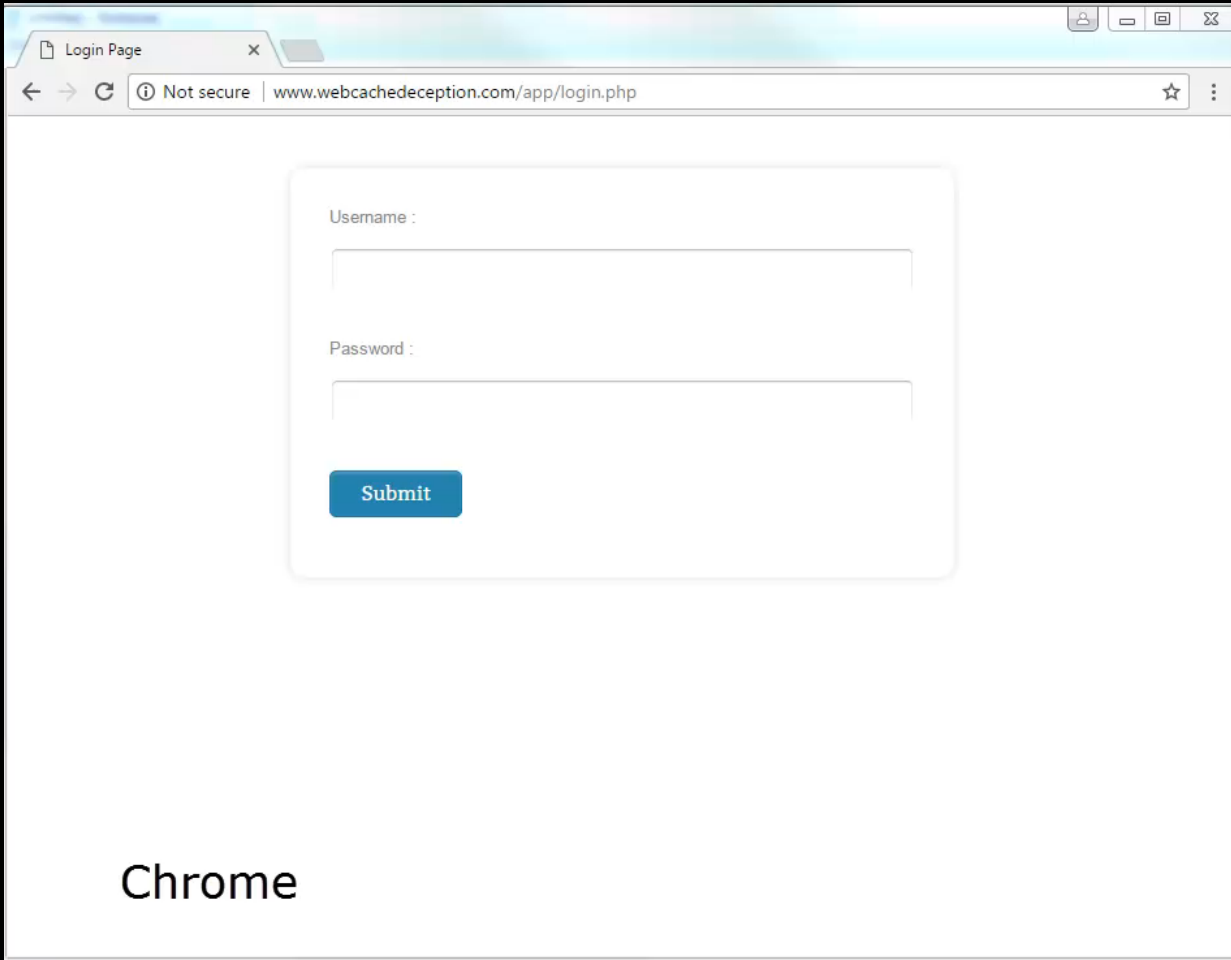
Getting down to business

The attacker browses to
<https://www.bank.com/account.do>/*stylesheet.css*
and gets the content of the user's account.do page

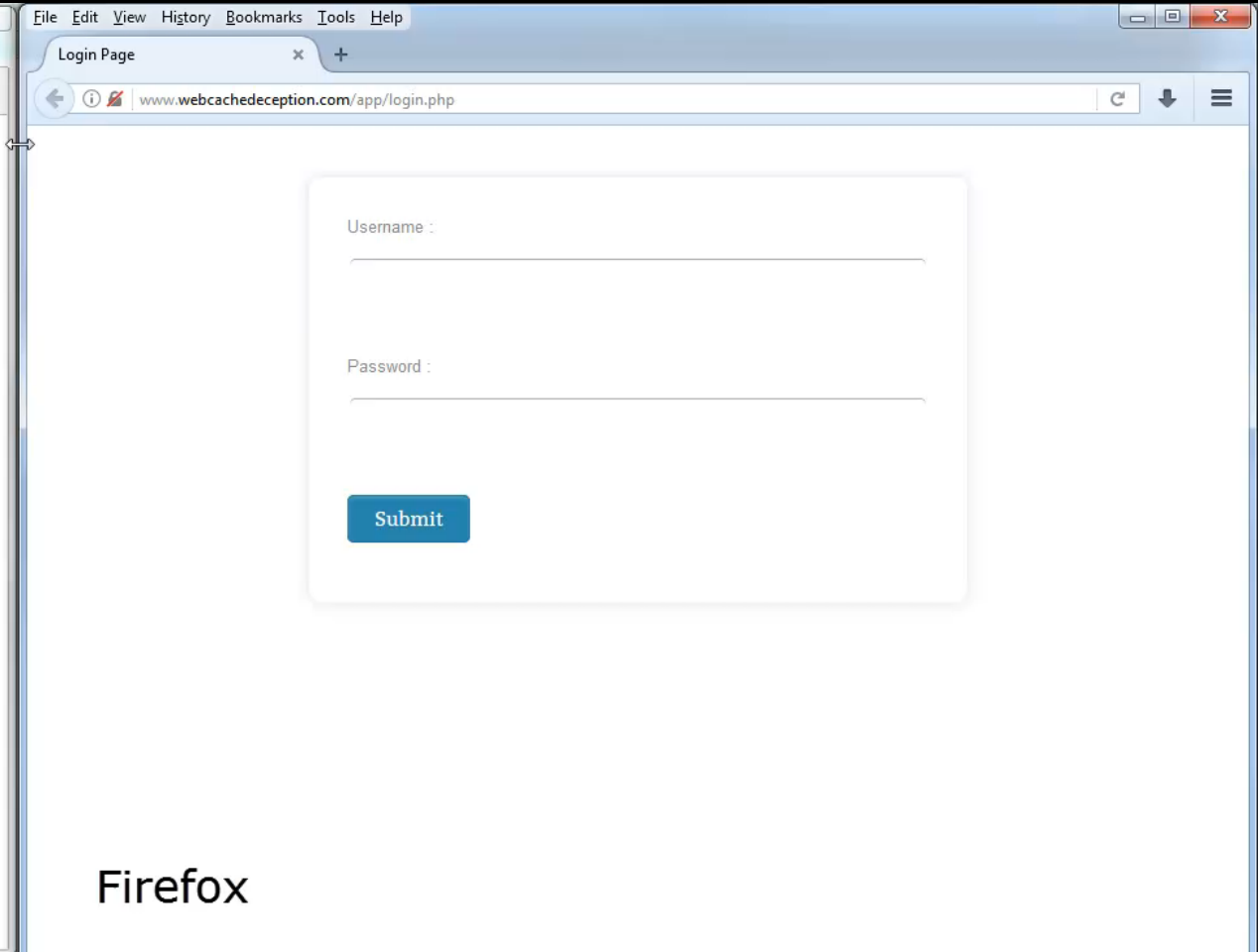


```
<html>  
_____  
</html>
```





Chrome



Firefox



`http://www.webcachedeception.com/app/private.php/logo.png`



Summary

Activity

Send & Request Payments

Wallet

Shopping



Log out



Hi Omer.

Get even more out of your PayPal account



Pay for goods or services



Great shopping deals



Download our app

PayPal balance

No balance needed to shop or send payments

Currencies

[Add funds](#)
[Withdraw funds](#)

Completed

JUN 28

Purchase

-\$ AUD

MAY 26

Canceled - Request received \$10.00 USD

~~\$10.00~~ USD

[View all](#)

Bank accounts and cards

MasterCard x-

AMEX American Express x-

When you [add your local bank account](#), you can

Conditions

- Web cache functionality is set for the web application to cache static files based on their extensions, disregarding any caching header.
- When accessing a page like *http://www.example.com/home.php/nonexistent.css*, the web server will return the content of *home.php* for that URL.
- Victim has to be authenticated while accessing the triggering URL.

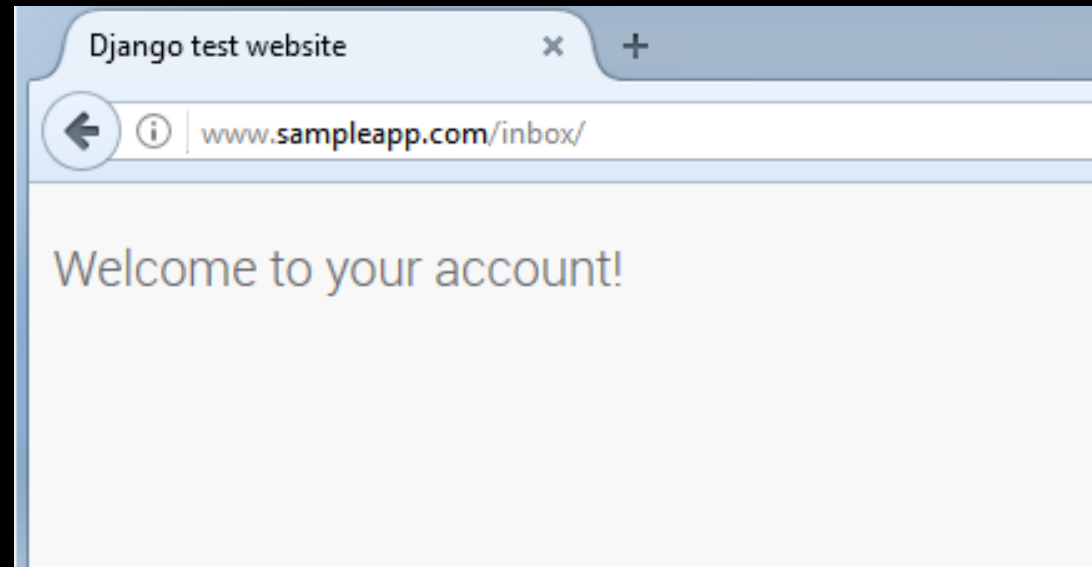
Why the HELL #1

would a web application react like this?

Why the HELL #1

Django:

<http://www.sampleapp.com/inbox/>



Why the HELL #1

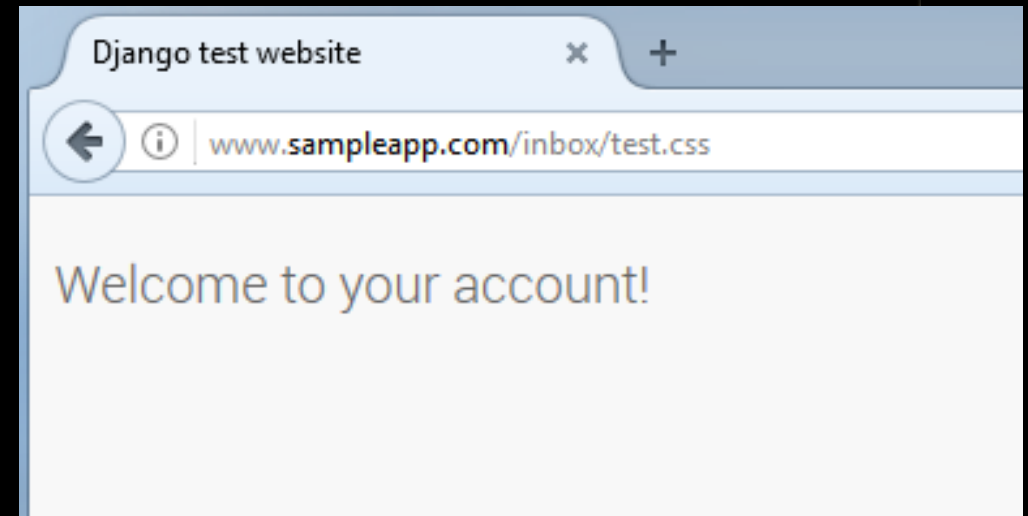
Django:

<http://www.sampleapp.com/inbox/test.css>

```
from django.conf.urls import include, url
from . import views

urlpatterns = [
    url(r'^inbox/', views.index, name='index')
]
```

urls.py



Why the HELL #1

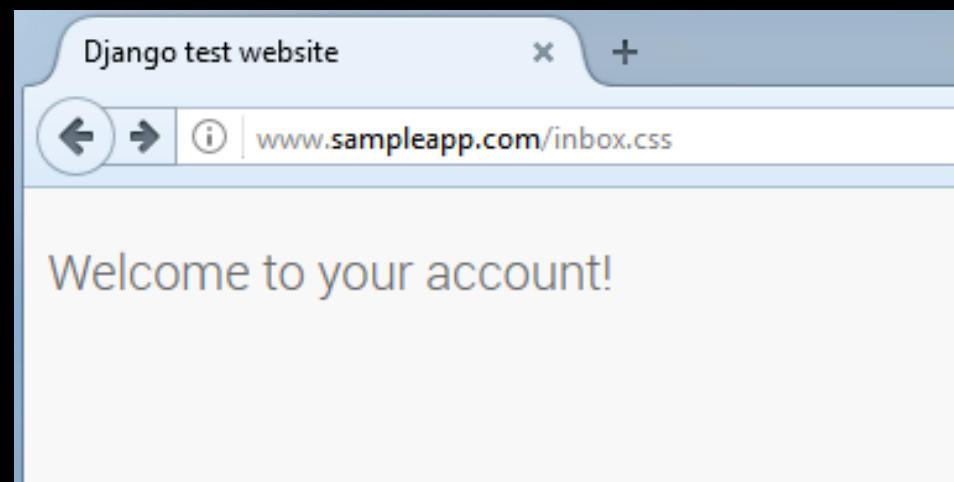
Django:

<http://www.sampleapp.com/inbox.css>

```
from django.conf.urls import include, url
from . import views

urlpatterns = [
    url(r'^inbox', views.index, name='index')
]
```

urls.py



Why the HELL #1

Django:

<http://www.sampleapp.com/inbox/test.css>

```
from django.conf.urls import include, url
from . import views

urlpatterns = [
    url(r'^inbox/$', views.index, name='index')
]
```

urls.py

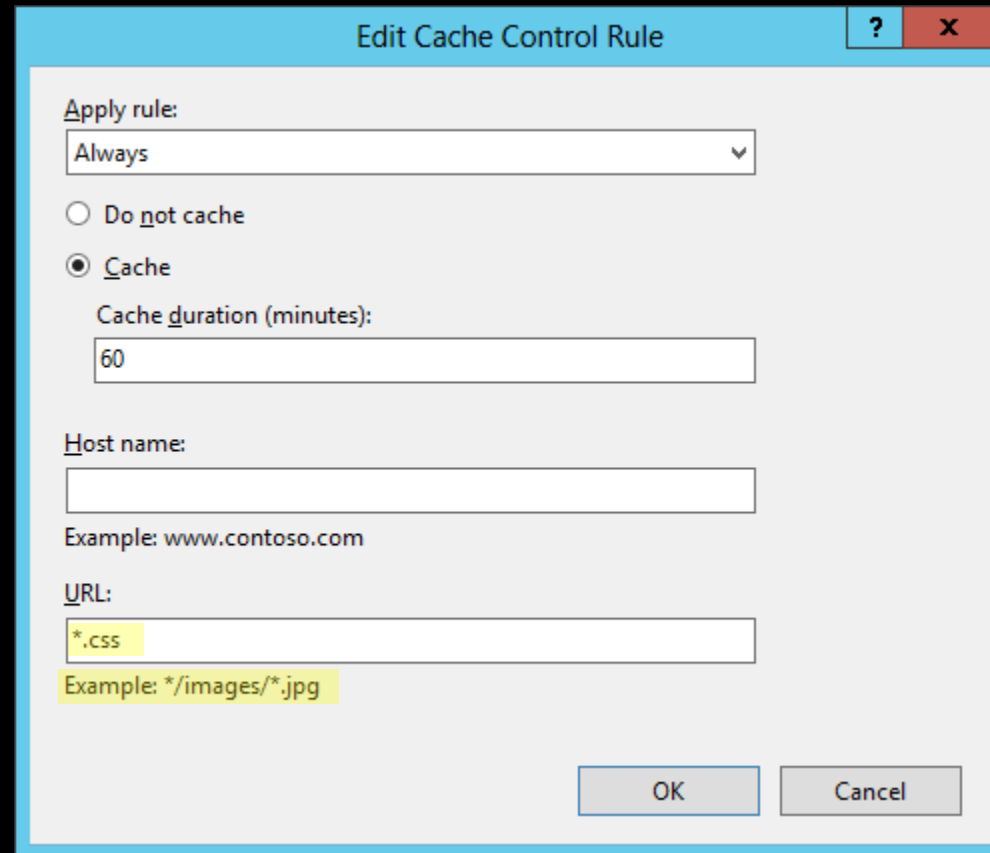


Why the HELL #2

would a caching mechanism react like this?

Why the HELL #2

IIS ARR:



Dialog box titled "Edit Cache Control Rule" with a help icon (?) and a close icon (X).

Apply rule:
Always

Do not cache
 Cache

Cache duration (minutes):
60

Host name:
Example: www.contoso.com

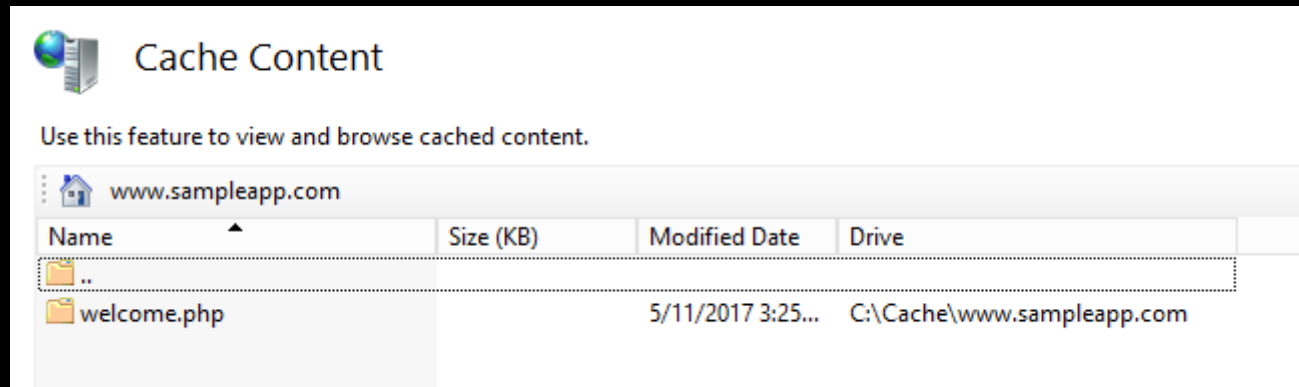
URL:
*.css
Example: */images/*.jpg

OK Cancel

Why the HELL #2

IIS ARR:

<http://www.sampleapp.com/welcome.php/test.css>



Cache Content

Use this feature to view and browse cached content.

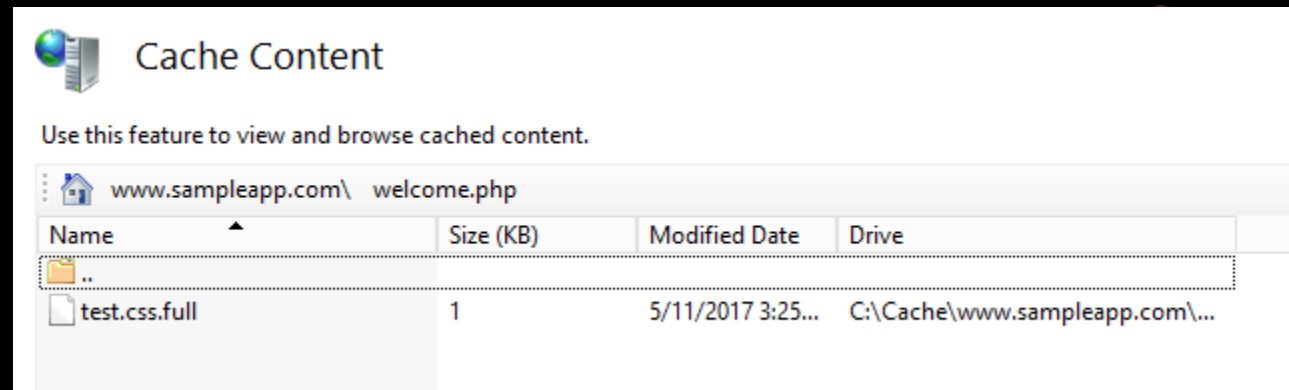
www.sampleapp.com

Name	Size (KB)	Modified Date	Drive
..			
welcome.php		5/11/2017 3:25...	C:\Cache\www.sampleapp.com

Why the HELL #2

IIS ARR:

<http://www.sampleapp.com/welcome.php/test.css>



Why the HELL #2

Cloudflare:

- Eligibility phase

class, css, jar, js, jpg, jpeg, gif, ico, png, bmp, pict, csv, doc, docx, xls, xlsx, ps, pdf, pls, ppt, pptx, tif, tiff, ttf, otf, webp, woff, woff2, svg, svgz, eot, eps, ejs, swf, torrent, midi, mid

<https://blog.cloudflare.com/understanding-our-cache-and-the-web-cache-deception-attack/>
<https://blogs.akamai.com/2017/03/on-web-cache-deception-attacks.html>

Why the HELL #2

Cloudflare:

- Disqualification phase

‘Edge cache expire TTL’ to the rescue!

Create a Page Rule for webcachedeception.com ✕

If the URL matches: By using the asterisk (*) character, you can create dynamic patterns that can match many URLs, rather than just one. [Learn more here](#)

Then the settings are:

Cache Level	Standard	✕
Edge Cache TTL	2 hours	✕

[+ Add a Setting](#)

Cancel Save as Draft Save and Deploy

Why the HELL #2

Cloudflare:

Edge Cache Expire TTL: Easiest way to override any existing headers

With Cache Everything, we respect all headers. If there is any header in place from the server or a CMS solution like WordPress, we will respect it. However, we got many requests from customers who wanted an easy way to override any existing headers. Today, we are releasing a new feature called 'Edge cache expire TTL' that does just that.

<https://blog.cloudflare.com/edge-cache-expire-ttl-easiest-way-to-override/>



Mitigation

- Only cache files if their HTTP caching headers allow
- Store all static files in a designated directory
- Cache files by their content type
- Don't accept this! <http://www.example.com/home.php/non-existent.css>.
Return 302 or 404 instead

RESPECT MY



AUTHORITY

THANKS



@omer_gil



omergil.blogspot.com