SAME ORIGIN METHOD EXECUTION (SOME)

Ben Hayak
Security Researcher
Ben.Hayak@gmail.com
Twitter: @BenHayak

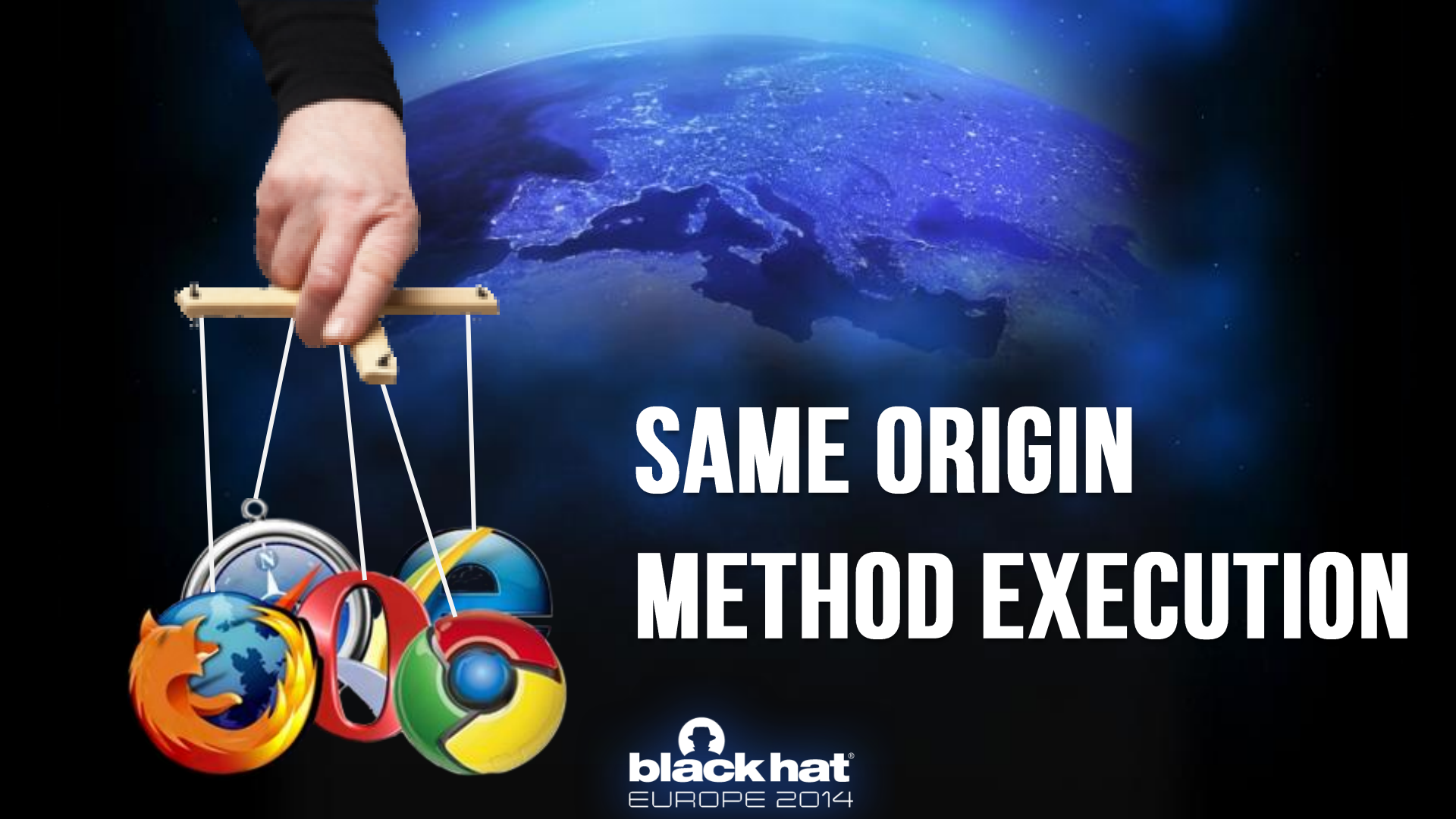
ADVANCE YOUR WEB APPLICATION KNOWLEDGE.

BOOST YOUR INCOME BUG BOUNTY PROGRAMS

PROVIDE YOUR CUSTOMERS WITH A BETTER PROTECTION


CHALLENGE
YOURSELVES


CRITICAL
black hat
EUROPE 2014


SAME ORIGIN
METHOD EXECUTION
black hat
EUROPE 2014

black hat EUROPE 2014

BUG BOUNTIES

Facebook WhiteHats (Thank you list):
http://www.facebook.com/whitehat

eBay Security Acknowledgment (Thank you list):
http://pages.ebay.com/securitycenter/ResearchersAcknowledgement.html

PayPal Wall of fame (Thank you list):
https://www.paypal.com/us/webapps/mpp/security-tools/wall-of-fame-honorable-mention

Twitter White Hats:
https://twitter.com/about/security

DropBox Special_thanks page:
https://www.dropbox.com/special_thanks

Adobe Security Acknowledgments page:
http://www.adobe.com/support/
security/bulletins/securityacknowledgments.html

Google | Application Security

Home Tools Vulnerability Reward Program **Hall of Fame** Research

The 0x0A List Reward Recipients Honorable Mention Prior to Reward Program

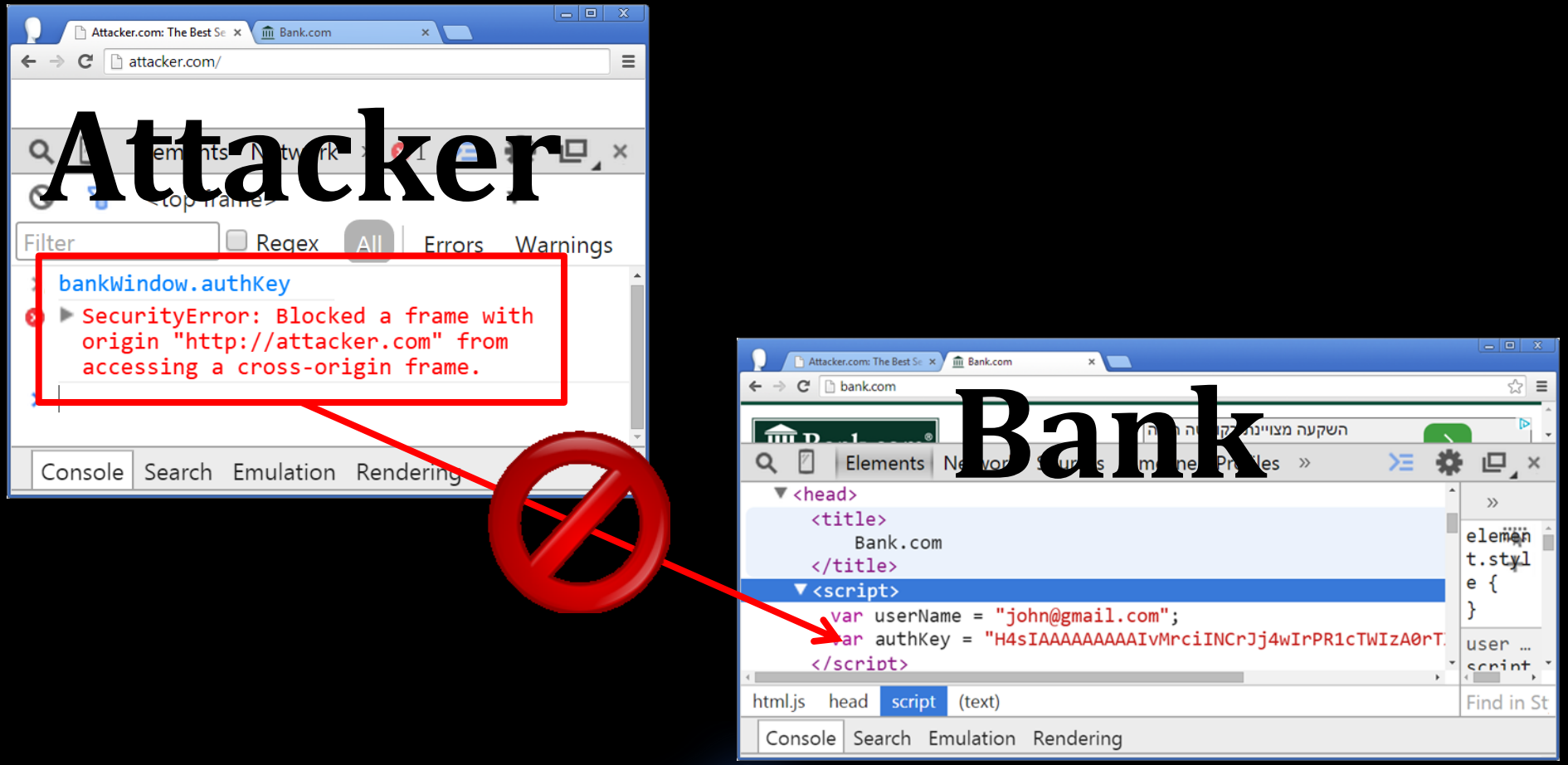
The "0x0A List"

The table below lists our best bug reporters since we launched Google's vulnerability reward program back in November 2010. We will u
per year.

black hat
EUROPE 2014

SAME ORIGIN POLICY (SOP)

SAME ORIGIN POLICY



SAME ORIGIN POLICY

- Document Access
- Object Access
- Ajax Requests
- Data Leakage

SAME ORIGIN POLICY

- <img src="[[URL]]">
- <link rel href="[[URL]]">
- <script src="[[URL]]">

[[External resources]]

JSON WITH PADDING

JSONP

JSON

LIGHTWEIGHT DATA EXCHANGE FORMAT

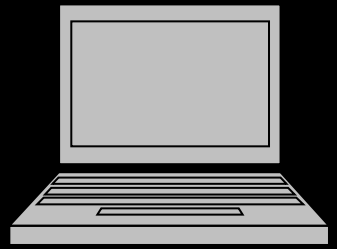
//XML..

```
<xml>
<person>
      <name>john</name>
      <credit>34</credit>
</person>
</xml>
```

HEAVY FORMAT

black hat®
EUROPE 2014

```
var person =
{“name”:”John”,”credit”:34}
```



1. person = RequestData

2. {“name”:”John”,”credit”:34}

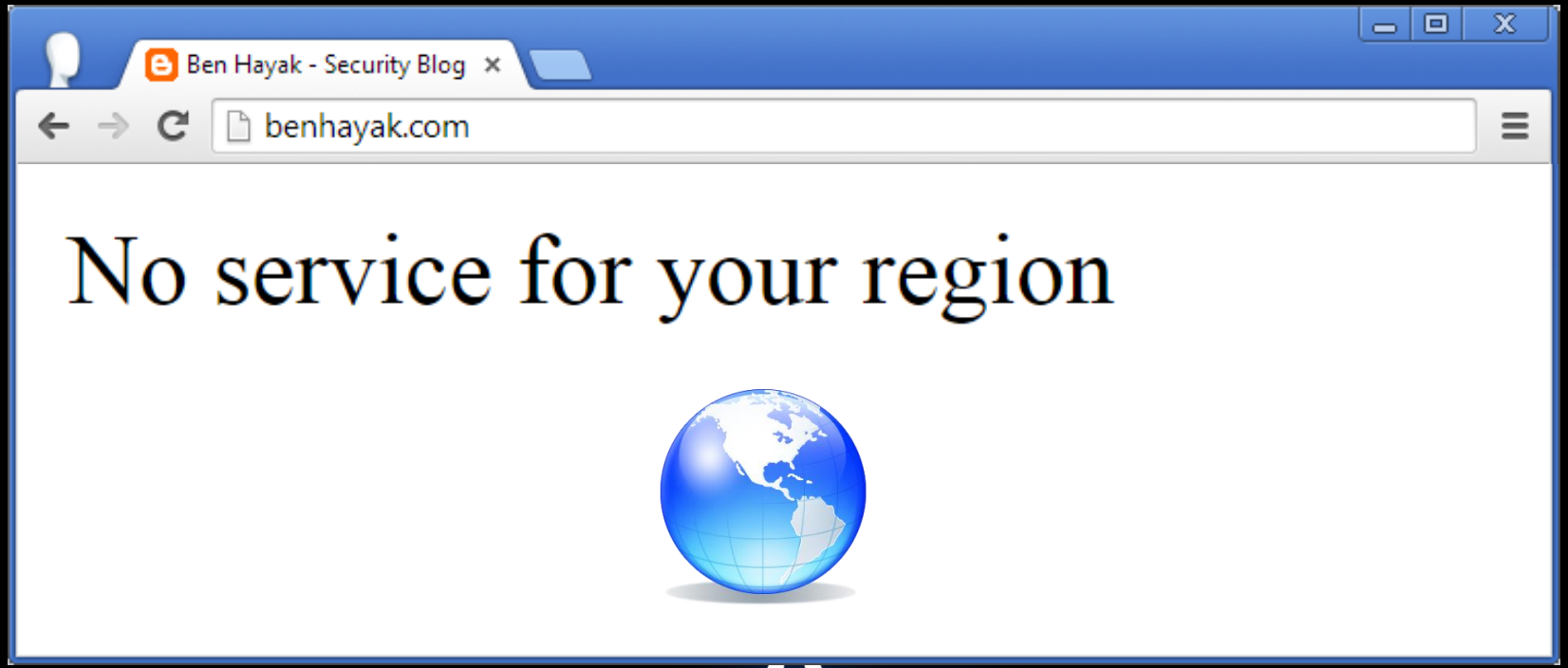
```
person.name   == “John”
person.credit   == 34
```


Light
Fast
Easy
black hat
EUROPE 2014

www.telize.com/geoip?callback=**getgeoip**

http://benhayak.com

http://benhayak.com



http://benhayak.com

```
<script type="application/javascript">
    function getgeoip(json){
        document.write("Geolocation information for IP address : ",
        json.ip);
        document.write("Country : ", json.country);
        document.write("Latitude : ", json.latitude);
        document.write("Longitude : ", json.longitude);
    }
</script>

<script type="application/javascript" src=
"http://www.telize.com/geoip?callback=getgeoip"></script>
```

SAME ORIGIN POLICY

- <img src="[[URL]]">
- <link rel href="[[URL]]">
- <script src="[[URL]]">

[[External resources]]

JSON WITH PADDING

<script src=

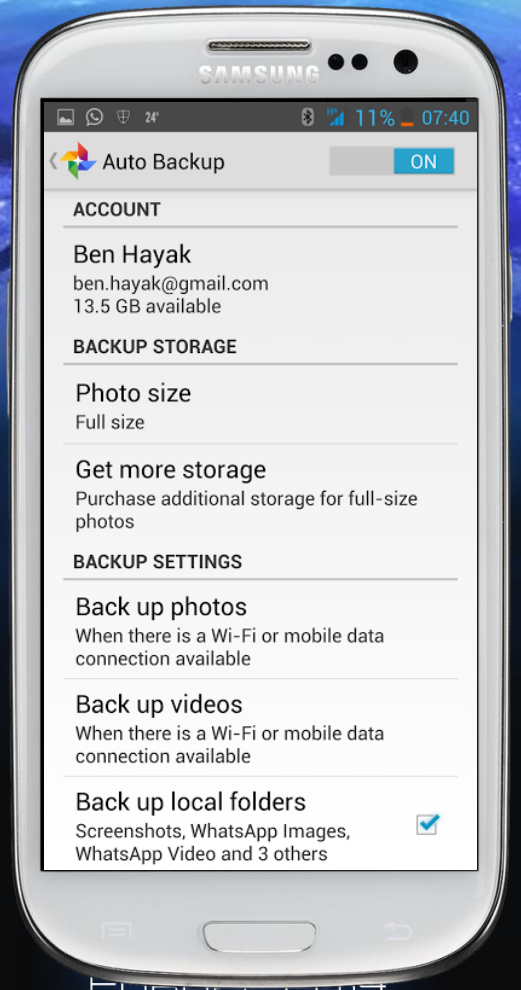
“http://external/geo?**callback=getgeoip**”>

USE CROSS ORIGIN DYNAMIC DATA


READY FOR SOME ?
black hat
EUROPE 2014

LET ME TAKE A #SELFIE

AUTO BACKUP


SAMSUNG
11% 07:40
Auto Backup
ON
ACCOUNT
Ben Hayak
ben.hayak@gmail.com
13.5 GB available
BACKUP STORAGE
Photo size
Full size
Get more storage
Purchase additional storage for full-size photos
BACKUP SETTINGS
Back up photos
When there is a Wi-Fi or mobile data connection available
Back up videos
When there is a Wi-Fi or mobile data connection available
Back up local folders
Screenshots, WhatsApp Images, WhatsApp Video and 3 others

AUTO

BACK

Back up photos & videos

https://support.google.com/plus/answer/1647509?hl=en

Help

Help forum

Back up photos & videos automatically

Automatically back up your photos and videos to Google+ by turning on Auto Backup. This can include photos you take with your device's camera, photos you download onto your phone or computer, and photos saved by other apps, like WhatsApp and Hangouts.

Private

Your automatically backed up photos are private unless you choose to share them.

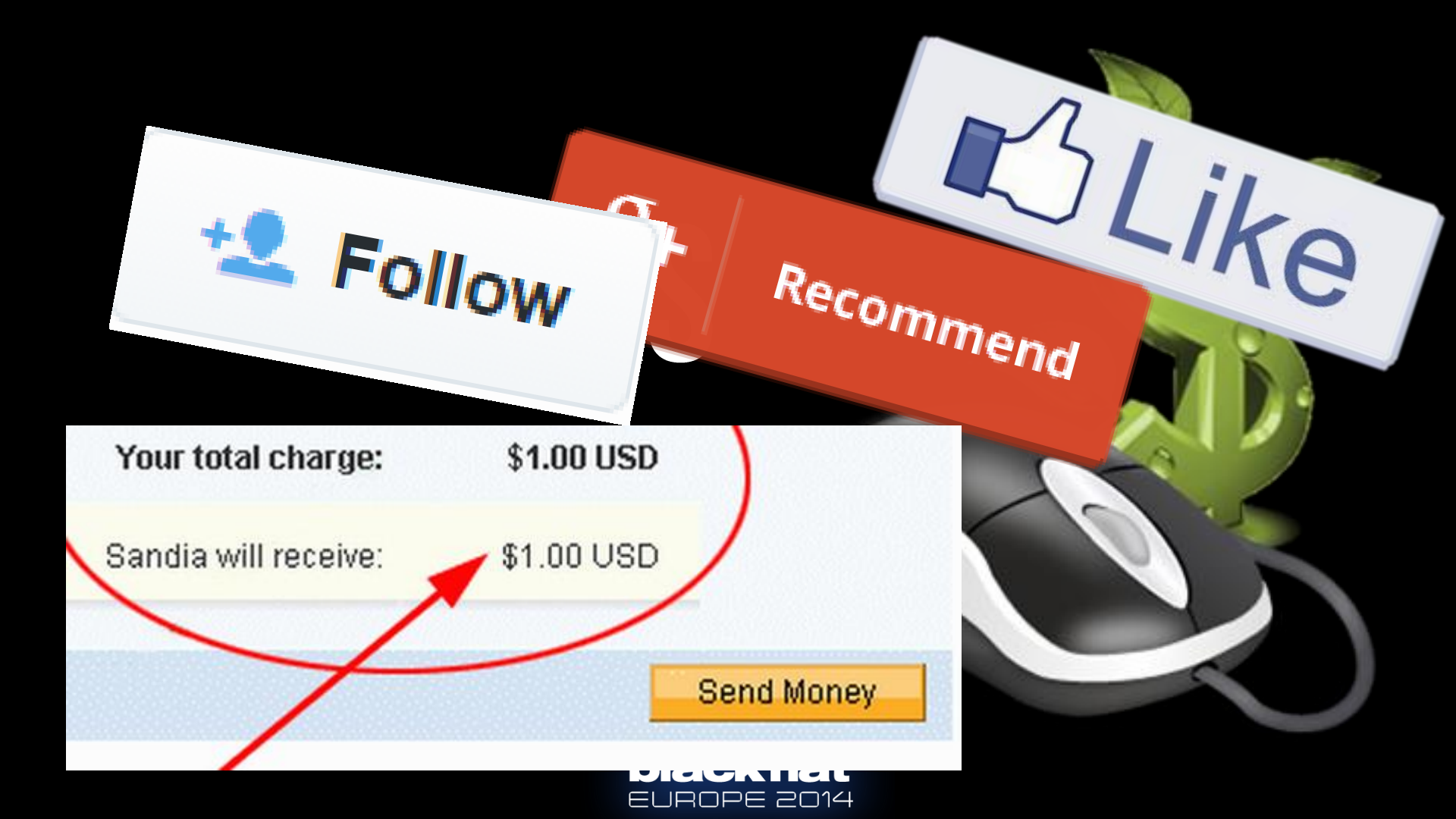

SOME ACTION
black hat
EUROPE 2014


SOME DEMO
black hat
EUROPE 2014


SAME ORIGIN METHOD
EXECUTION
black hat
EUROPE 2014

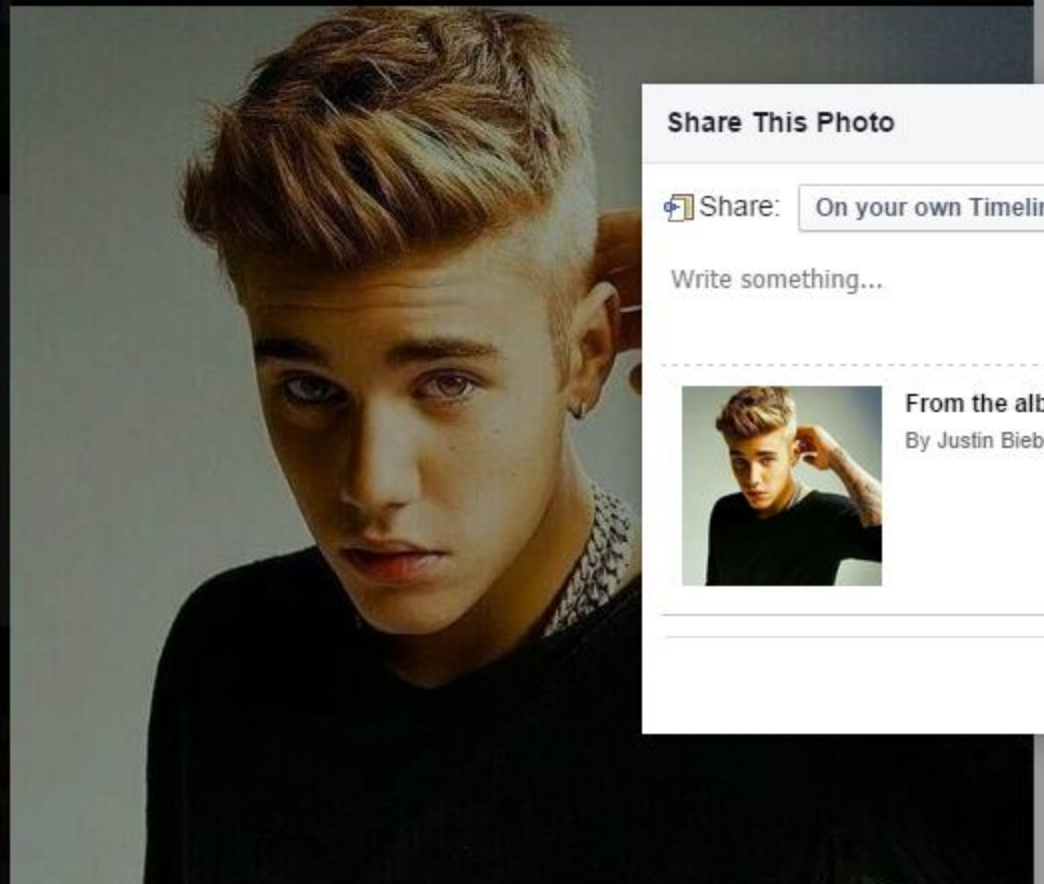
WHAT CAN WE DO WITH IT?

CLICKS


Follow
Recommend
Like
Your total charge: $1.00 USD
Sandia will receive: $1.00 USD
Send Money

Justin Bieber

https://www.facebook.com/JustinBieber/photos/pb.67253243887.-2207520000.1411994860./1015258555814



Justin Bieber

Share This Photo

Share: On your own Timeline

Write something...

From the album: Profile Pictures

By Justin Bieber

Friends Cancel **Share Photo**

I Love Justin Bieber <--- Please like my page nobody like it i feel so sad please help me to get more likes on my page&pictures nobody help me to get the likes can you help me? .. Thank you

1970 Ford Mustang COUPE

COBRA JET REPLICA 1000 MILES SINCE FULL RESOTR

6 viewed per hour.

Condition: **Used**

Time left: 19d 23h (Oct 19, 2014 08:26:04 PDT)

US $29,999.00

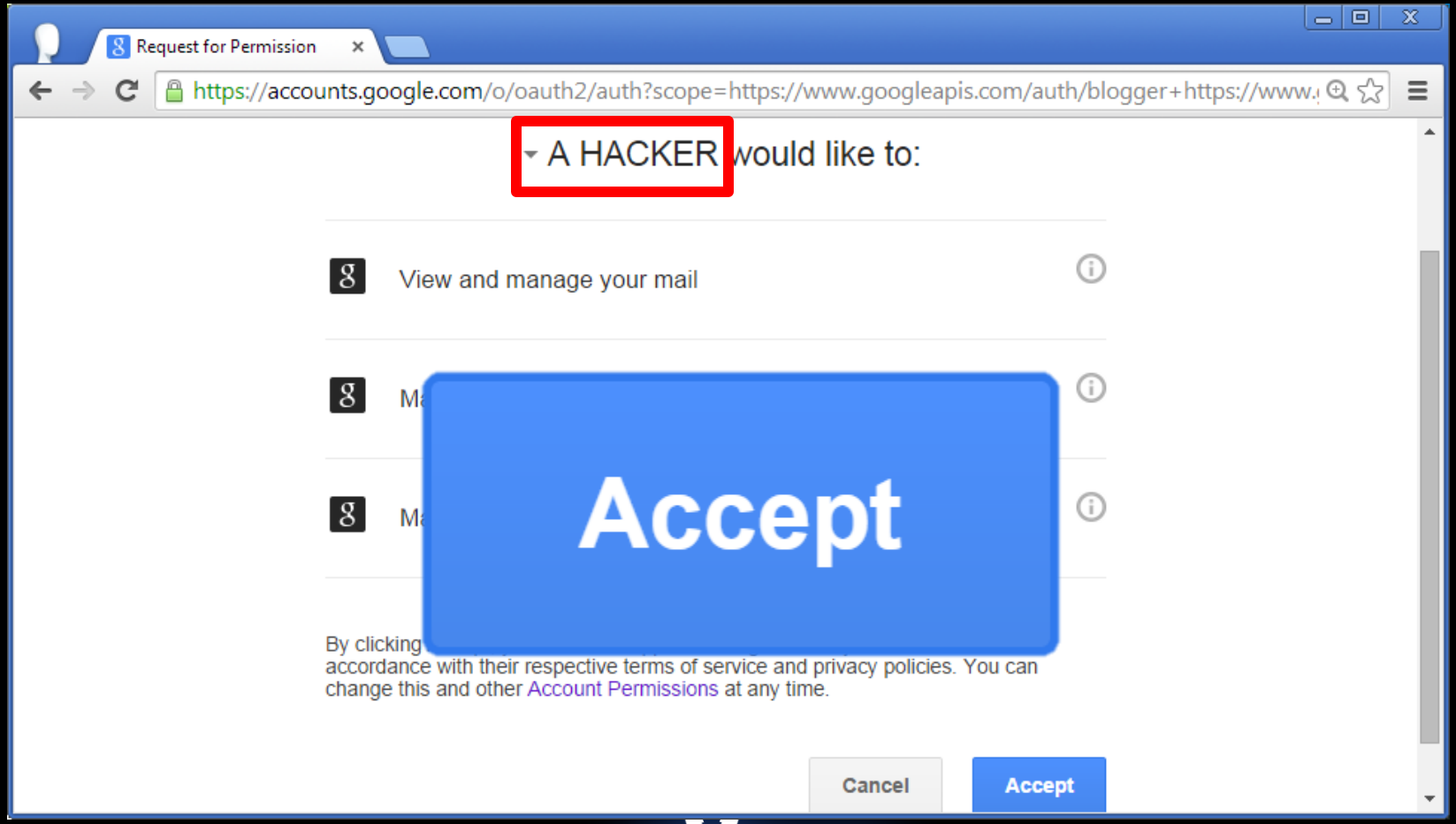
Approximately **ILS 110,300.17**

Buy It Now

Immediate payment of US $500.00 is required.

Make Offer


black hat
EUROPE 2014


Request for Permission
https://accounts.google.com/o/oauth2/auth?scope=https://www.googleapis.com/auth/blogger+https://www.
A HACKER would like to:
View and manage your mail
Accept
By clicking
accordance with their respective terms of service and privacy policies. You can
change this and other Account Permissions at any time.
Cancel
Accept


> Access Granted


Vulnerable origin's
DOM & Javascript
SOME
Insert
Home
Page Up
Delete
End
Page Down


black hat
EUROPE 2014

CALLBACKS


<HTML>
/*JAVASCRIPT*/

(PASSIVE) JAVASCRIPT CONTEXT 

(ACTIVE) HTML CONTEXT 

Name	Email
John	John@mail.com
Alice	Alice@mail.com

```
Function initTable(jsondata) {
        //doSomething in www.google.com (example)
}
```

```
<script src=
"http://emailservice/contacts?callback=initTable"
>
```

text/javascript

METHOD EXECUTION

AttackerInput();

WRONG JSONP IMPLEMENTATION

```
<html><head><title>GetContacts</title></head>
<body>
<?php
    if (preg_match('/^[\w.]+$/', $_GET["callback"])) {
        echo '<script src="http://emailservice/contacts?callback=' . $_GET["callback"] .
        '"></script>';
    } else {
        echo '<h1>Server Error 500 </h1>';
    }
?>

...
</body>
</html>
```

HTML CONTEXT (ACTIVE)

VERY WRONG IMPLEMENTATION

```
<html><head><title>GetContacts</title></head>
<body>
<?php
    if (preg_match('/^[\w.]+$/', $_GET["callback"])) {
        $jsonp = '{"contacts":[{"e":"user1@mail.com"},{"e":"user2@mail.com"}]}';
        echo '<script>' . $_GET["callback"] . '(' . $jsonp . ')' . '</script>';
    } else {
        echo '<h1>Server Error 500 </h1>';
    }
?>

</body>
</html>
```

EXPLOITING JSONP

black hat
EUROPE 2014

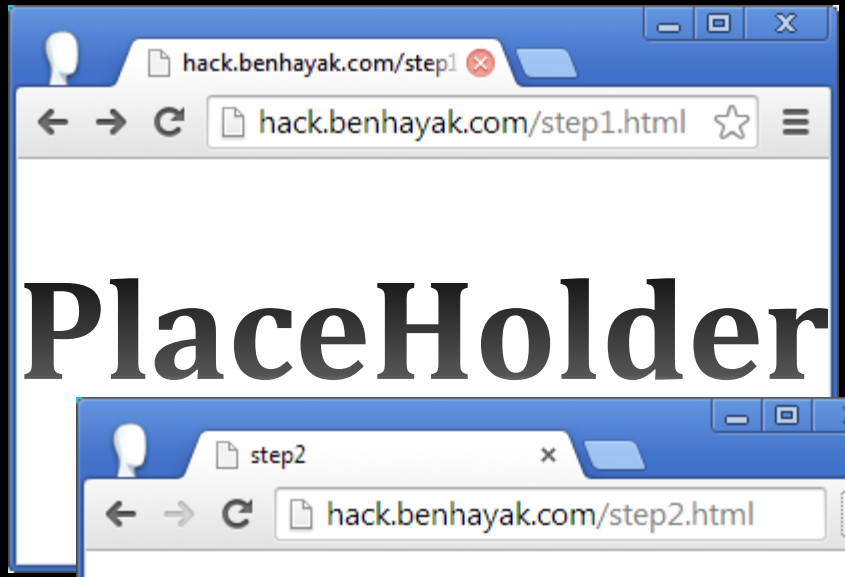
Callback=<XSS>aaa

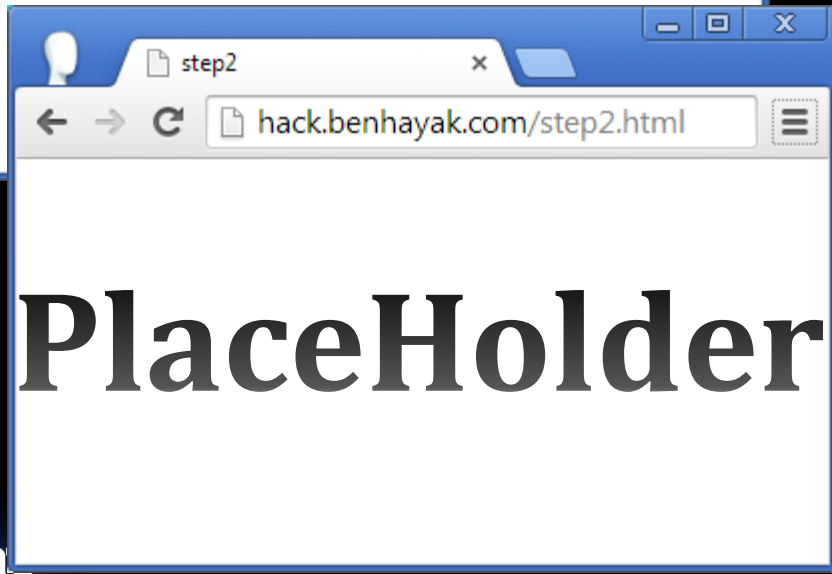
Callback=;alert()

Only [A-Za-z0-9.] allowed

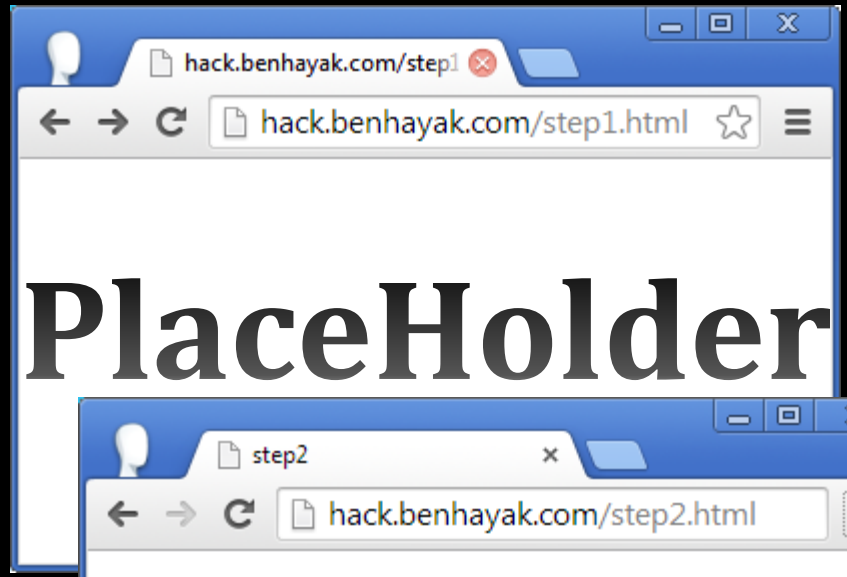
Setup the Environment

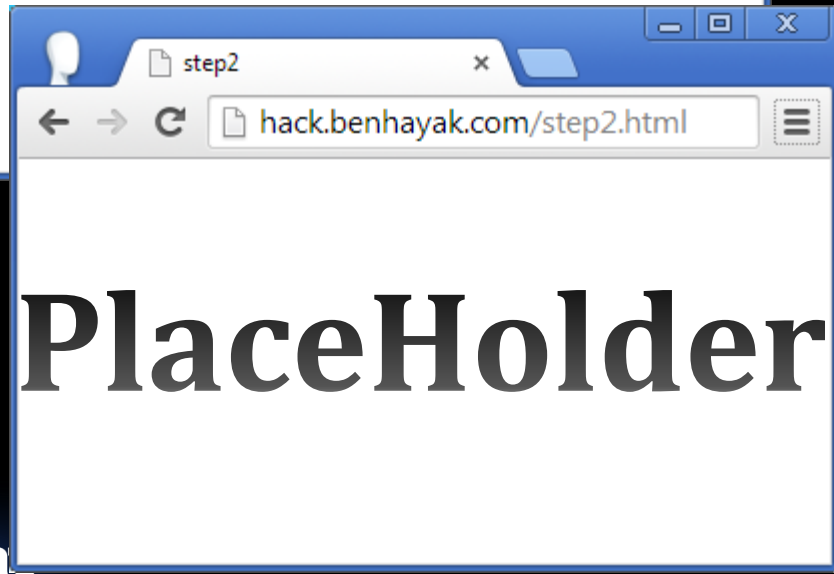
1. Redirect MAIN



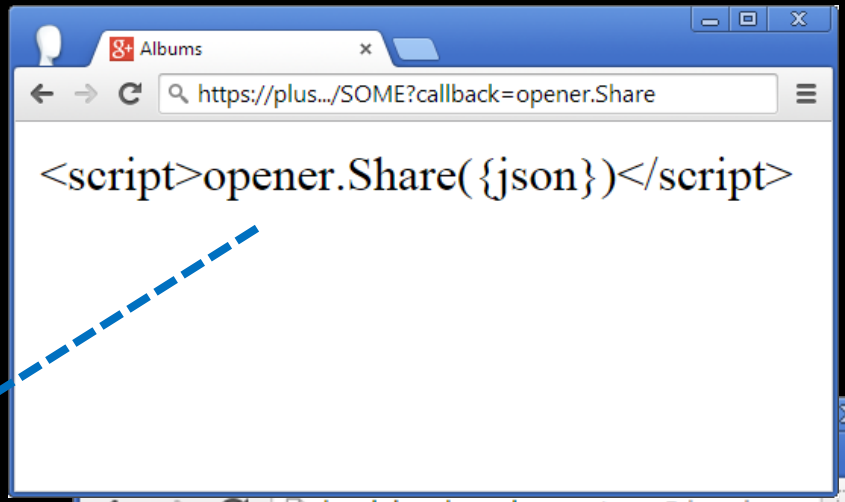


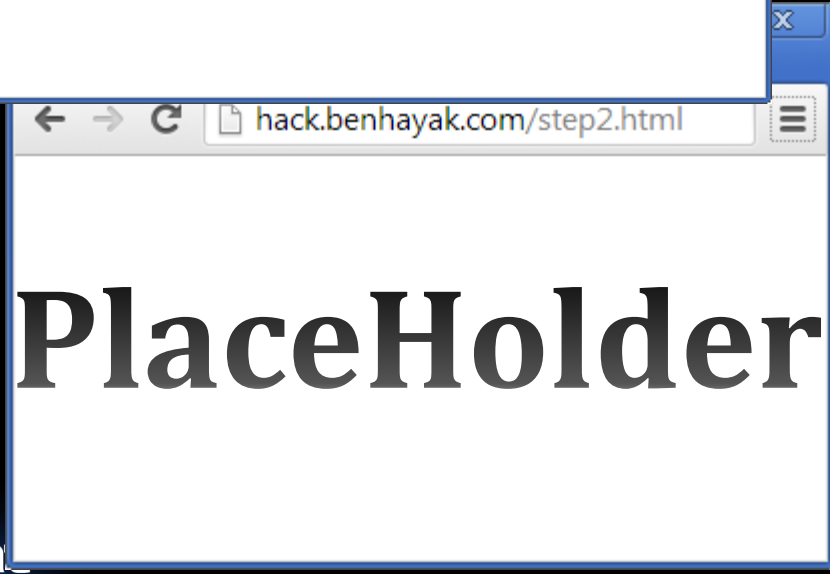
1. Redirect MAIN



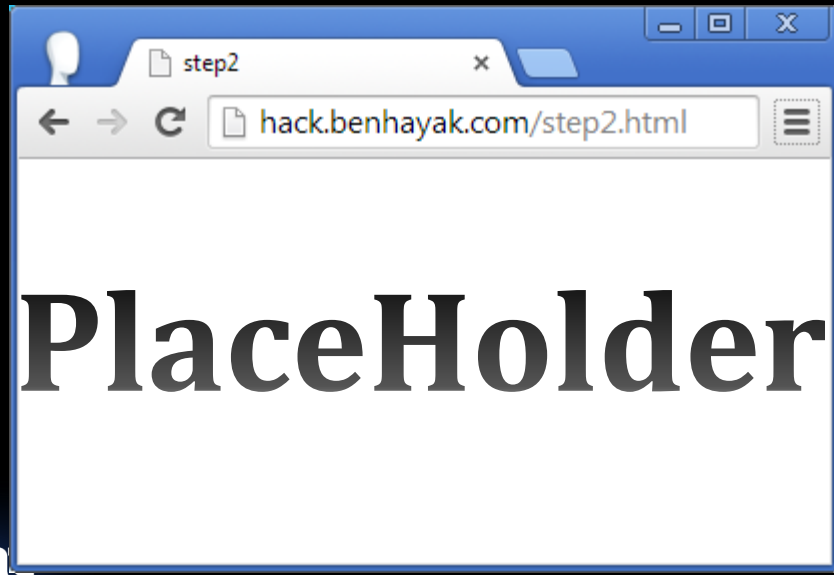


2. Redirect placeholder to SOME



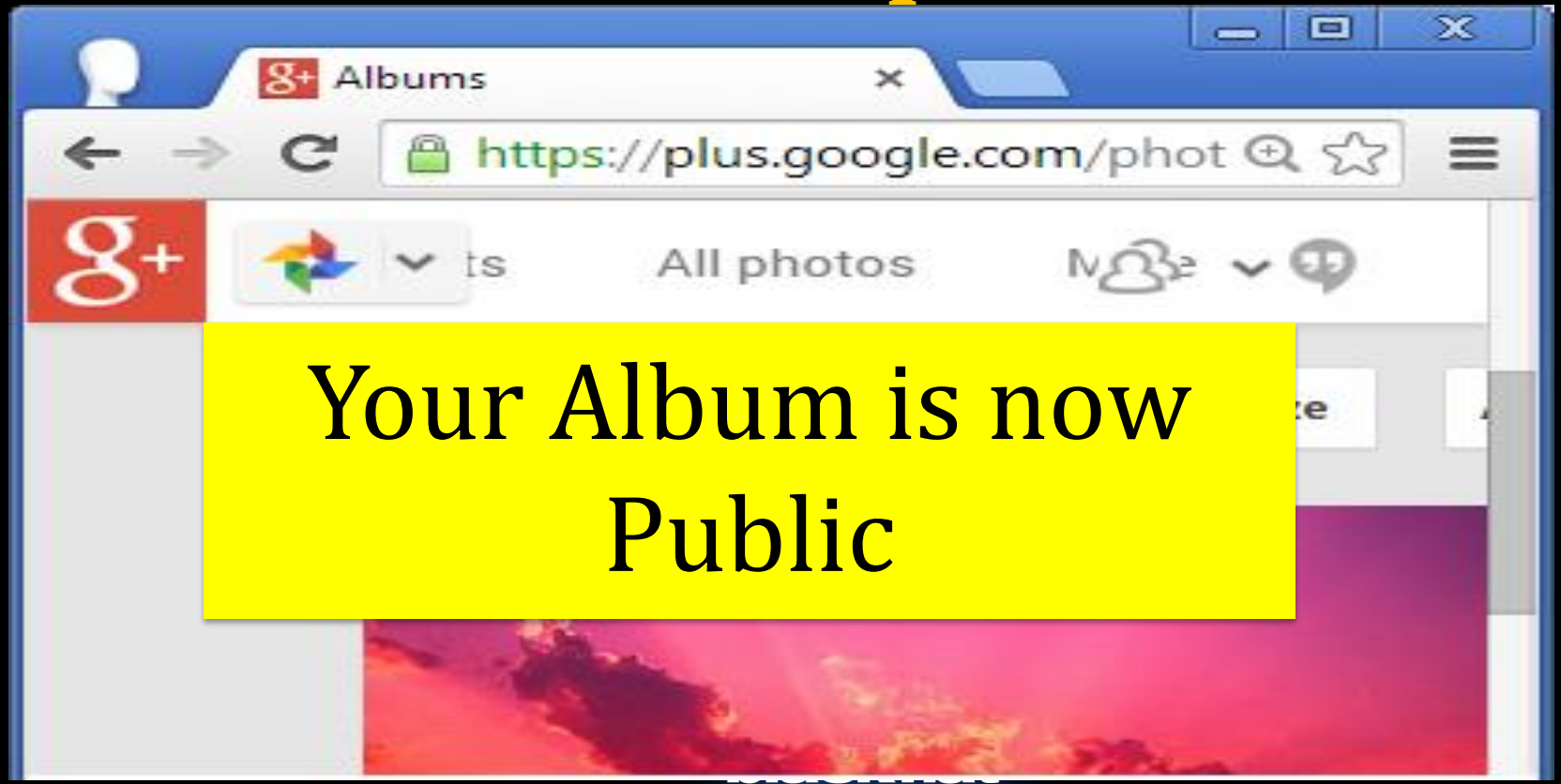


2. Redirect placeholder to SOME



3. Redirect 2nd placeholder to SOME

Mission Accomplished




DEMO


PROTECTIONS?
black hat
EUROPE 2014

CSRF TOKENS?

We don’t need them

XSS FILTERS?

We only need alphanumeric and a dot

FRAME BUSTING?

We can use **Windows**

POPUP BLOCKER?

Use a popup bypass

CONTENT SECURITY POLICY

No restrictions when using windows

HOW CAN I PROTECT MYSELF?

THANK YOU!

Ben Hayak
Security Researcher
Ben.Hayak@gmail.com
Twitter: @BenHayak