WHY DO WE NEED SECURITY HEADERS?

JACEK MARMUSZEWSKI
DEVOPS @ AIRHELP

- 19:30 - Why do we need security headers? - Jacek Marmuszewski [EN/EN]

AGENDA!

1. WHY DO WE EVEN TALK ABOUT IT?
2. HOW EASY IT IS TO HACK YOUR SIDE?
    A. ATTACK VECTOR
    B. PREVENTION
3. RANDOM THOUGHTS


WHY?

WHY?

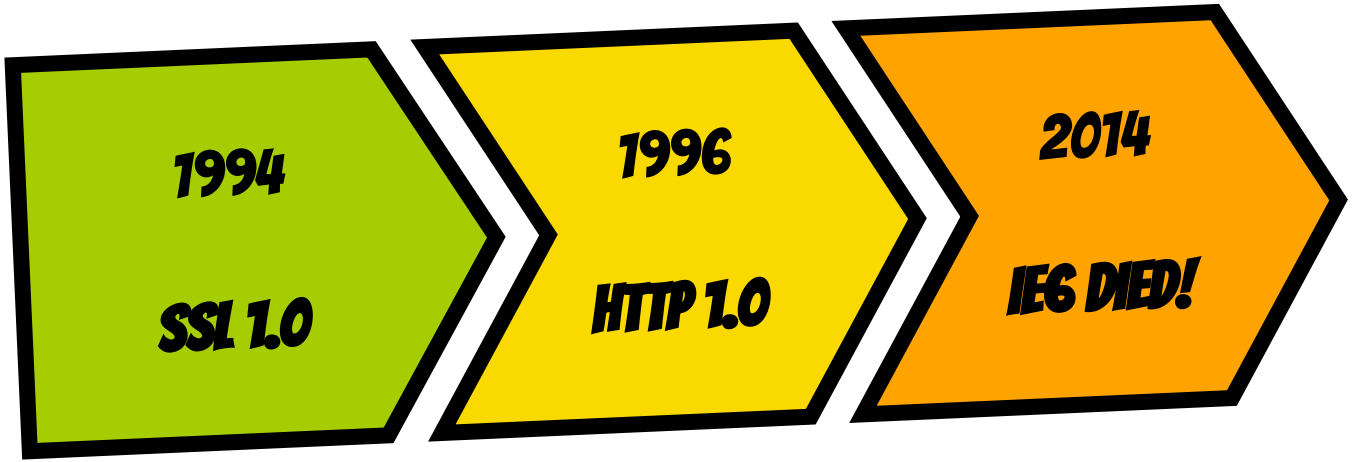
A. IT'S EASY!
B. "MY BACKEND IS SUPER SECURED, I DON'T NEED THIS SH*T"
C. "MODERN BROWSERS ARE SECURE ..."

WHY?

... you should care

A LONG TIME AGO ...

NOT SO LONG AGO ...



FUN FACTS!

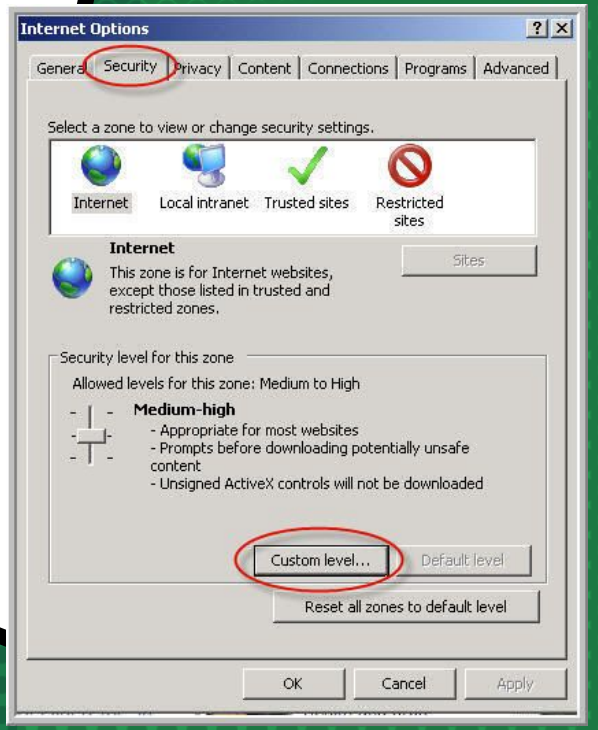

NO ENCRYPTION STANDARD
UNTIL 1994!

SSL 1.0 COULD BE HACKED WITH PEN AND PAPER


FIRST UNIX SERVERS USED
ONLY LOGIN ... NO
PASSWORD!

FIRST SERVERS HAD PUBLIC PUT METHOD!

IT'S EXTREMELY HARD TO CHANGE SECURITY STANDARD




SCARED?
YOU SHOULD BE!

BEST ATTACK SURFACE: USERS!

HOW?

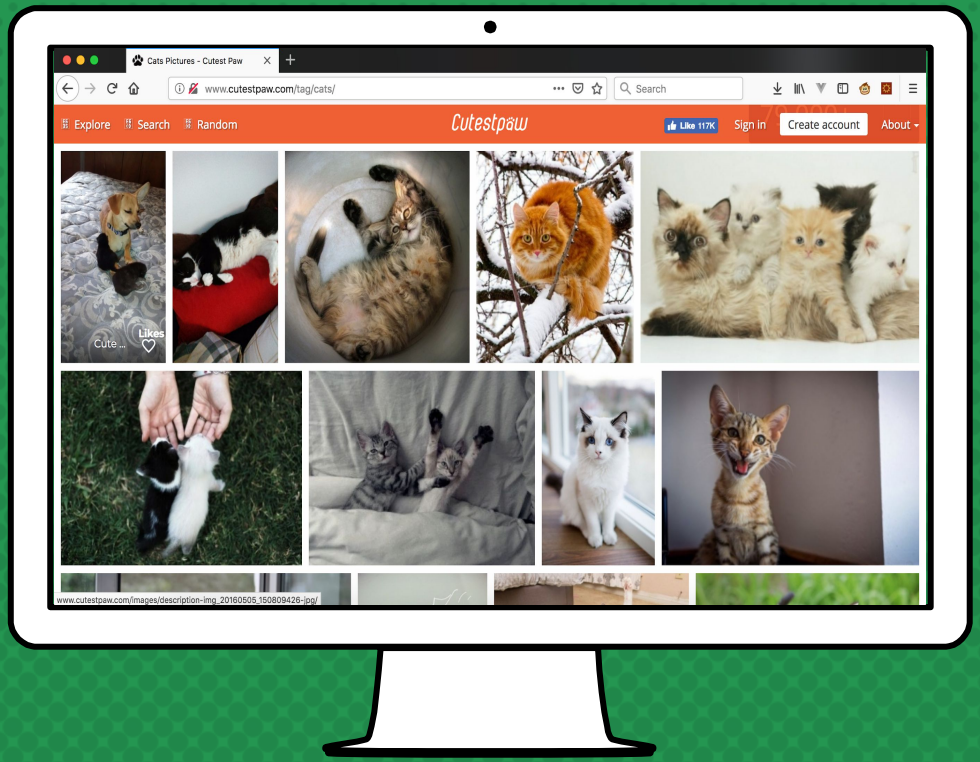
Day 1

What do we need

1. HTML + JS (Stack Overflow)
2. Free Hosting
3. Hardcore Social Engineering Skills

EVIL SITE!

Fluffy.com



THE HARD PART - SOCIAL ENGINEERING

114k

When you want a Golden Retriever but are only allowed to get a **cat**

r/aww · Posted by u/jenpriester 14 days ago

1.6k Comments Share Save ...

1170

wykop

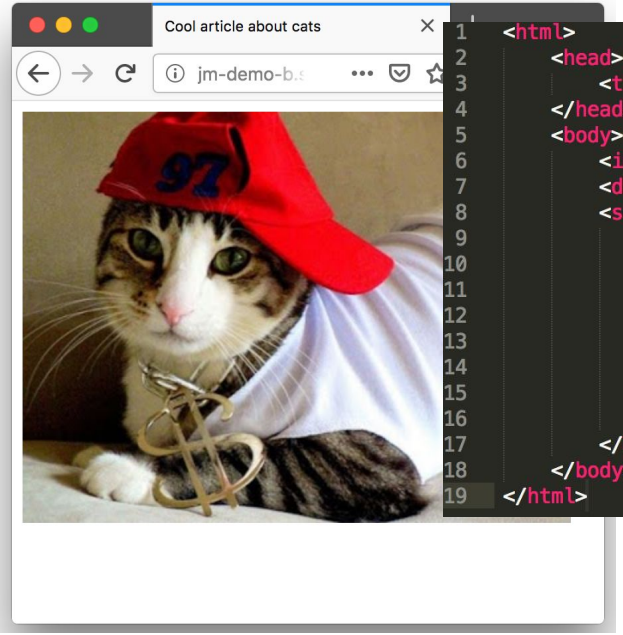
Niebezpieczny kot

@cornholio youtube.com #wykop #youtube +4 inne

Niebezpieczny kot

117 komentarzy opublikowany 9 mies. temu

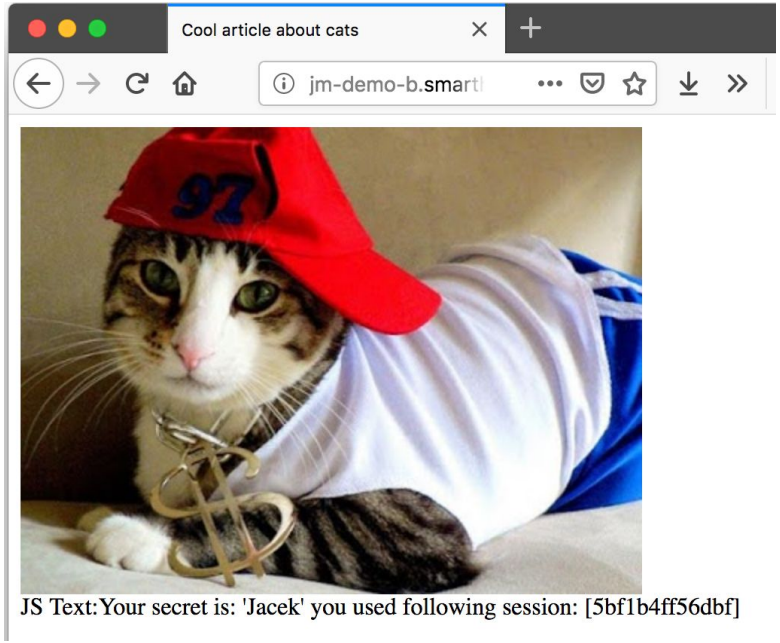
CLICK!



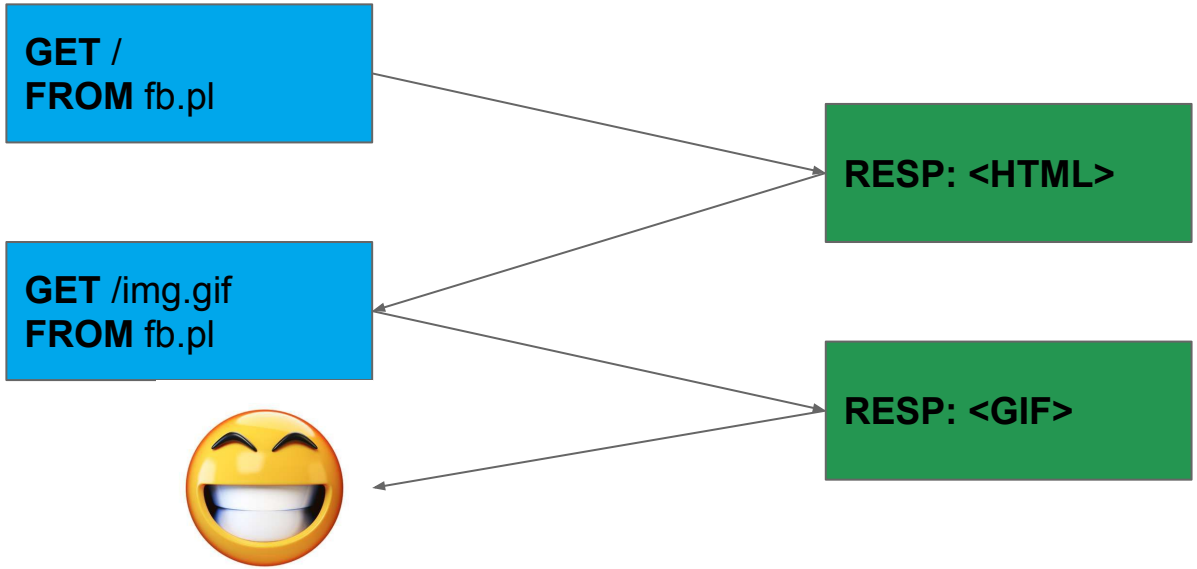

```
<html>
    <head>
        <title>Cool article about cats</title>
    </head>
    <body>
        <img src="<URL>" /></br>
        <div id="js" />
        <script>
            var url = 'https://facebook.com/api/get-all-my-data.'
            var xmlHttp = new XMLHttpRequest();
            xmlHttp.open( "GET", url, false );
            xmlHttp.withCredentials = true;
            xmlHttp.send( null );

            var div = document.getElementById('js');
            div.innerHTML = div.innerHTML + 'JS Text:' + xmlHttp.responseText;
        </script>
    </body>
</html>
```

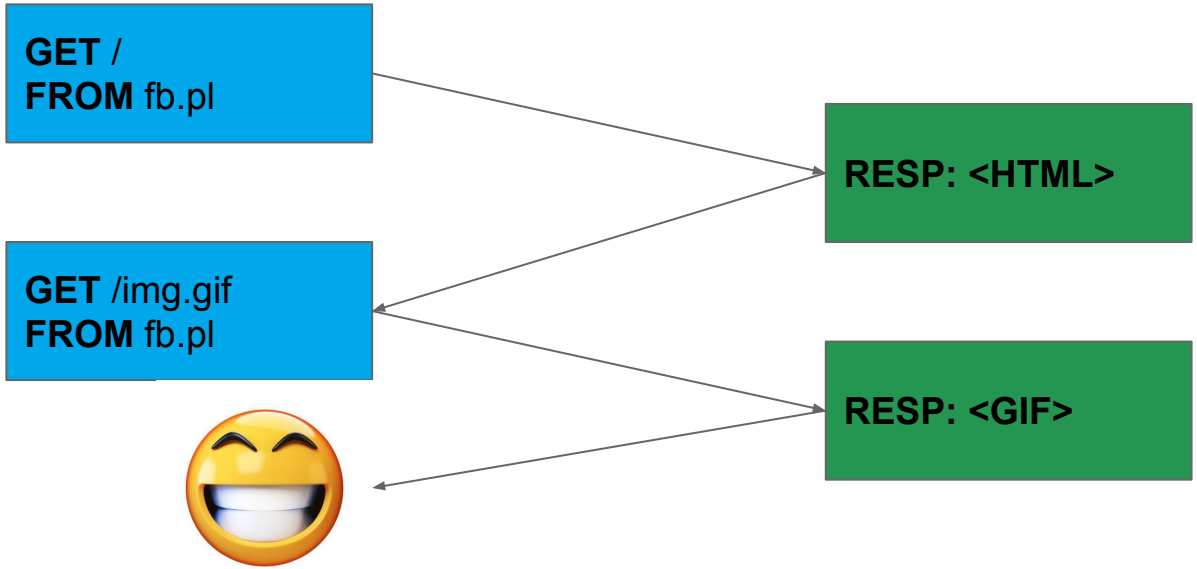
BANG!


Cool article about cats
jm-demo-b.smart
JS Text:Your secret is: 'Jacek' you used following session: [5bf1b4ff56dbf]

HOW BROWSE WORKS



WHAT IF YOU ARE LOGGED IN?



WHAT IF YOU ARE LOGGED IN?

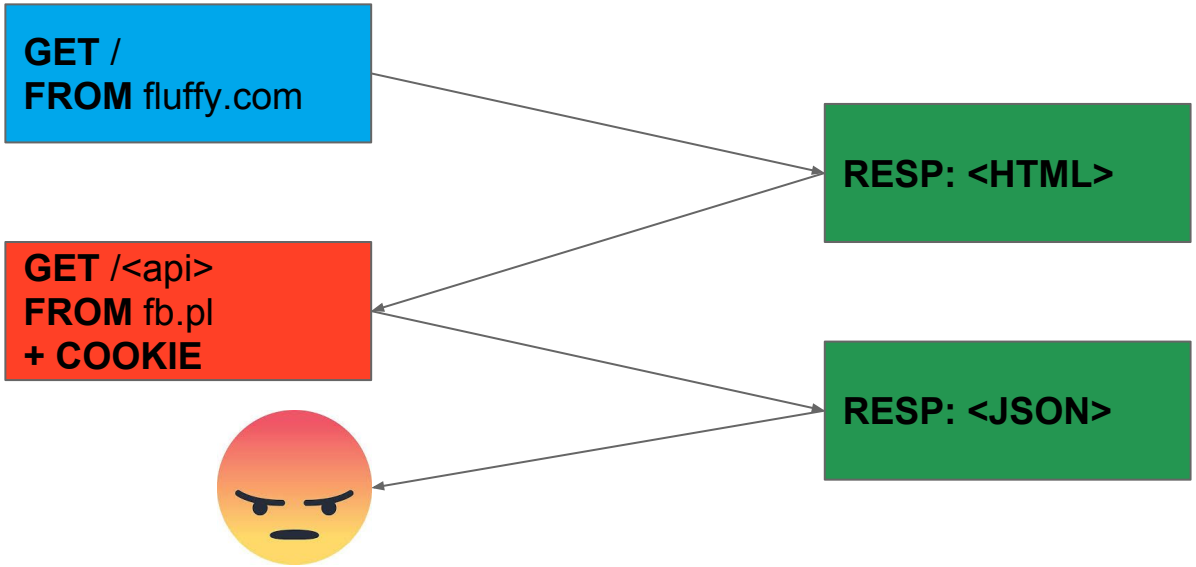
GET /
FROM fb.pl
+ COOKIE

RESP: <HTML>

GET /img.gif
FROM fb.pl
+ COOKIE

RESP: <GIF>

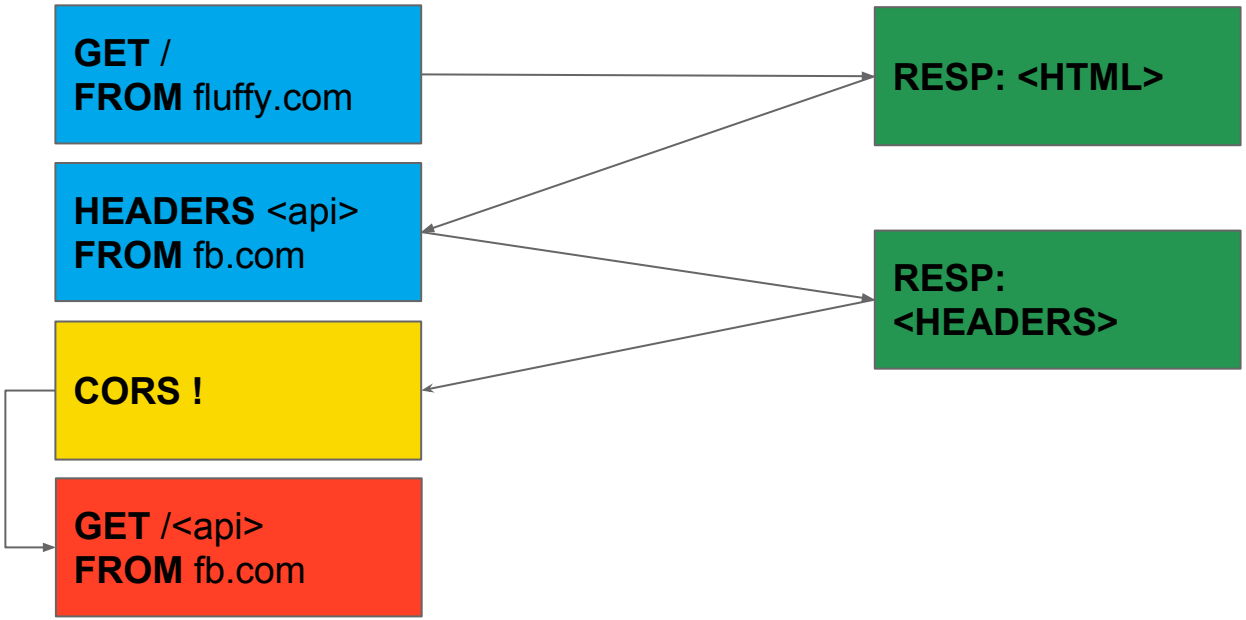
FLUFFY.COM


GET /
FROM fluffy.com
GET /<api>
FROM fb.pl
+ COOKIE
RESP: <HTML>
RESP: <JSON>

Cross-Origin Resource Sharing:
Access-Control-Allow-Origin

X-Permitted-Cross-Domain-Policies

CROSS-ORIGIN RESOURCE SHARING



WHAT IF ... ?

Access-Control-Allow-Origin: *

WHAT IF ... ?

Next

CROSS SITE REQUEST FORGERY

WHAT IF ... ?

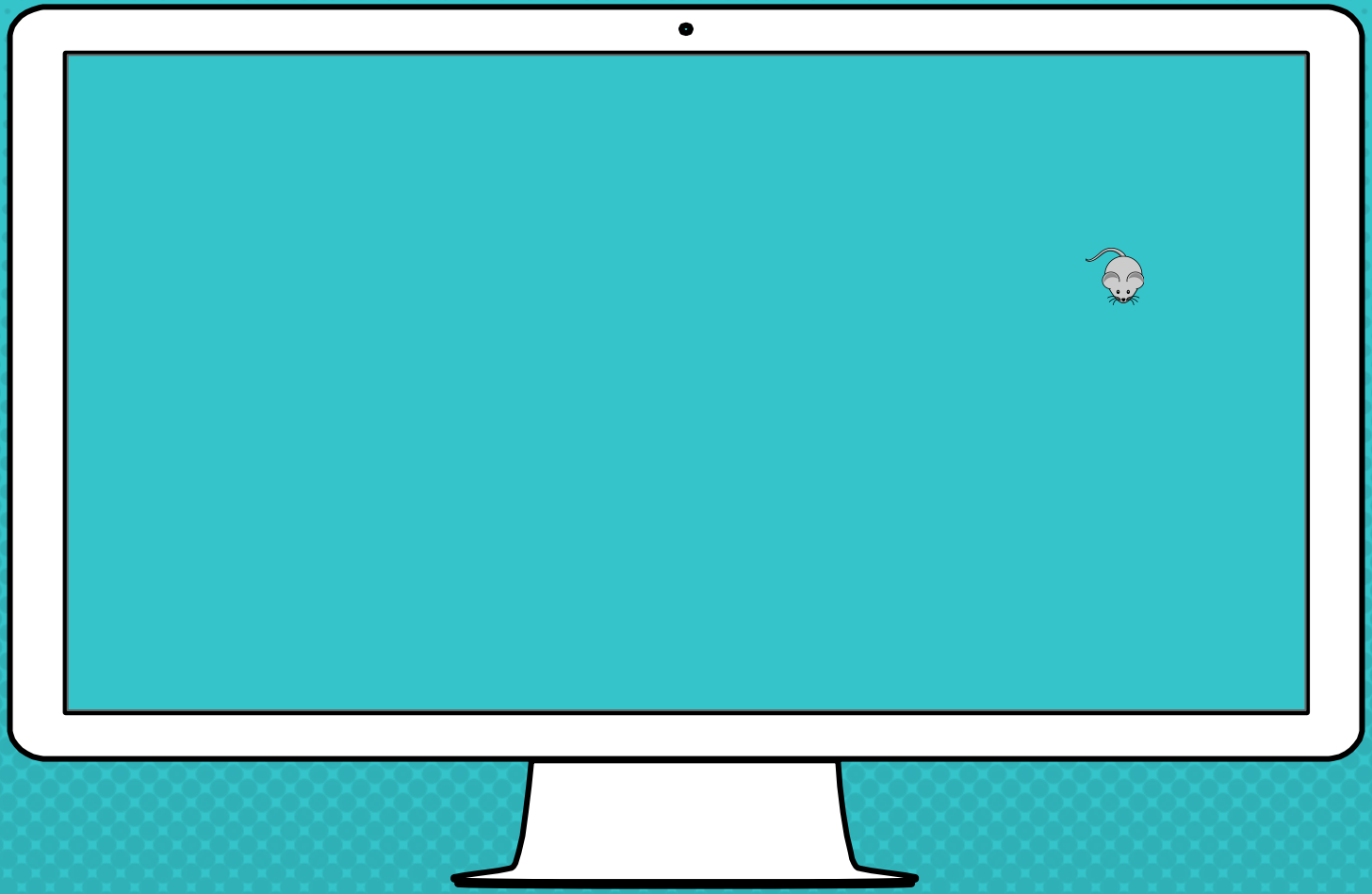
Cross-Origin Resource Sharing:
Access-Control-Allow-Origin

X-Permitted-Cross-Domain-Policies

HOW?

DAY 2


FEED A CAT!

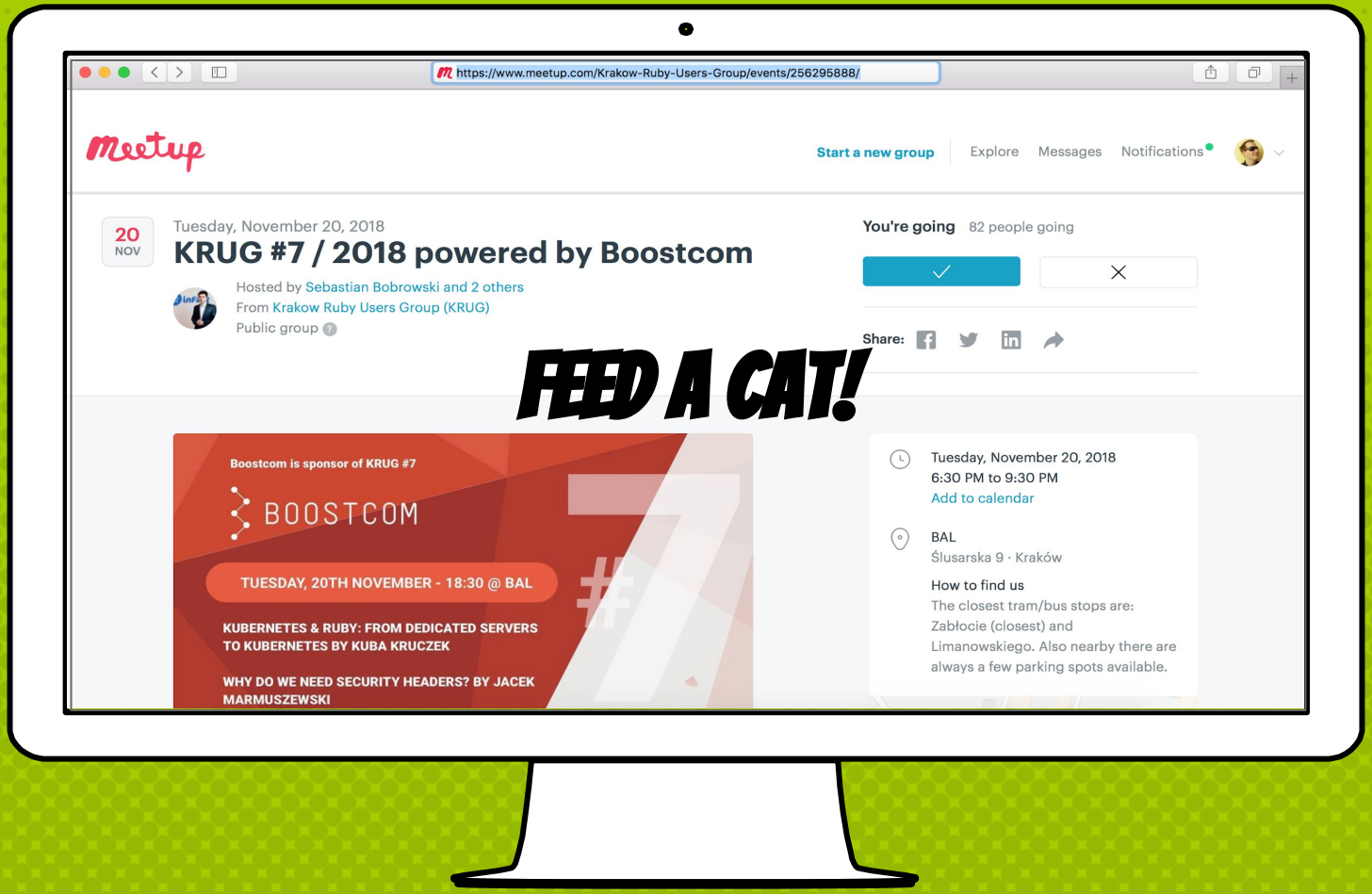


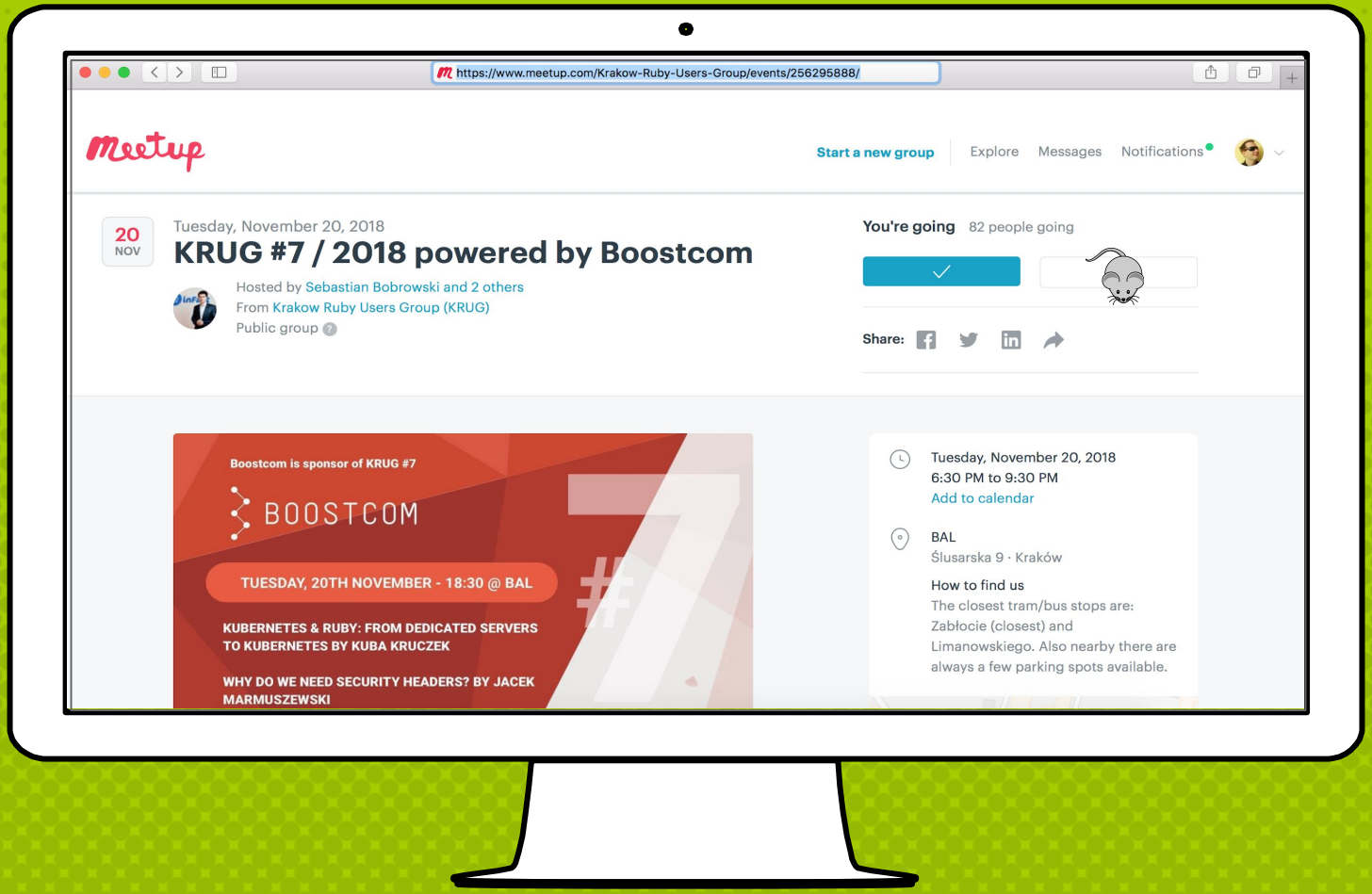

CONGRATS!
FOOD DONATED!

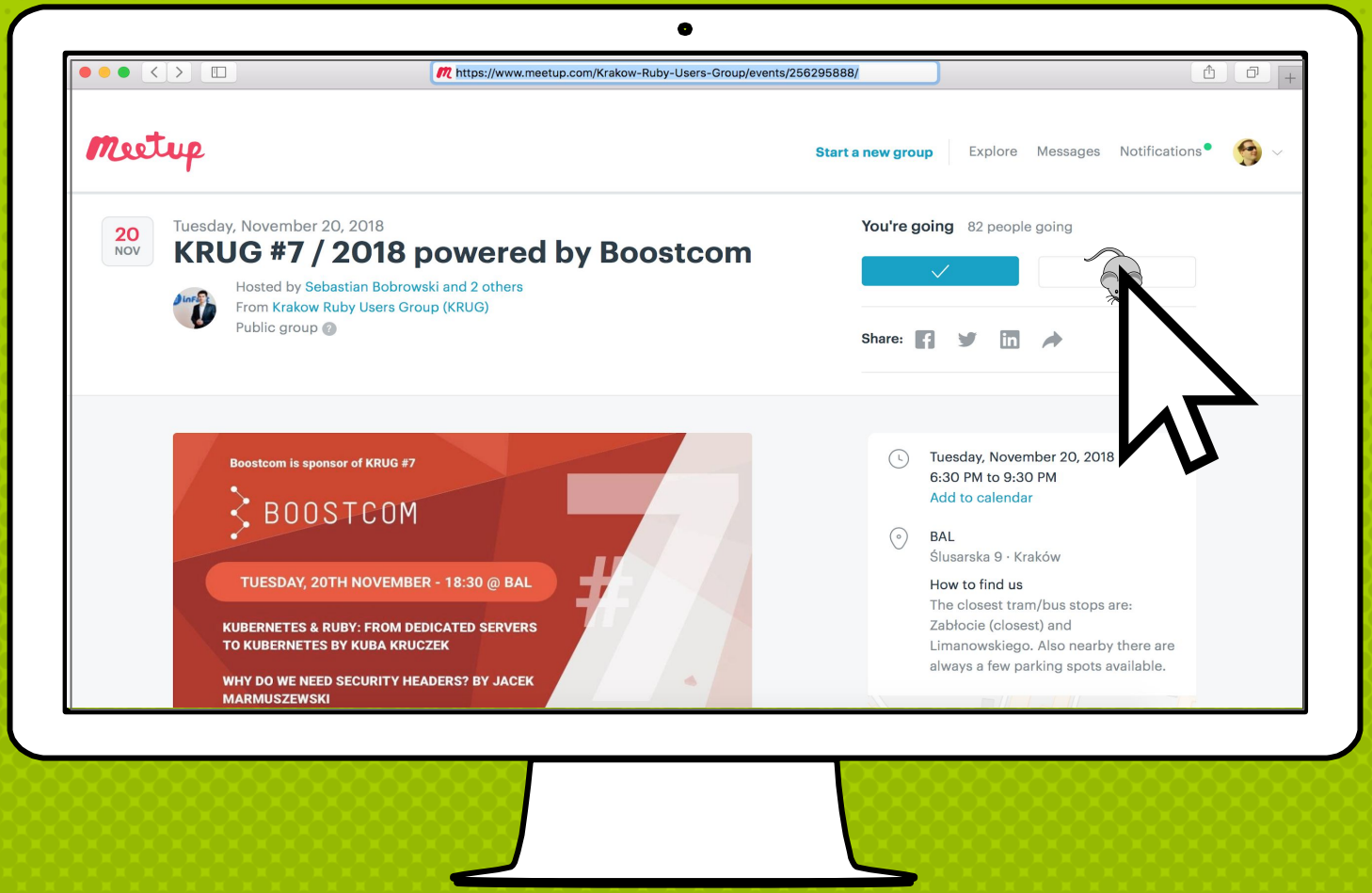
DAY 2

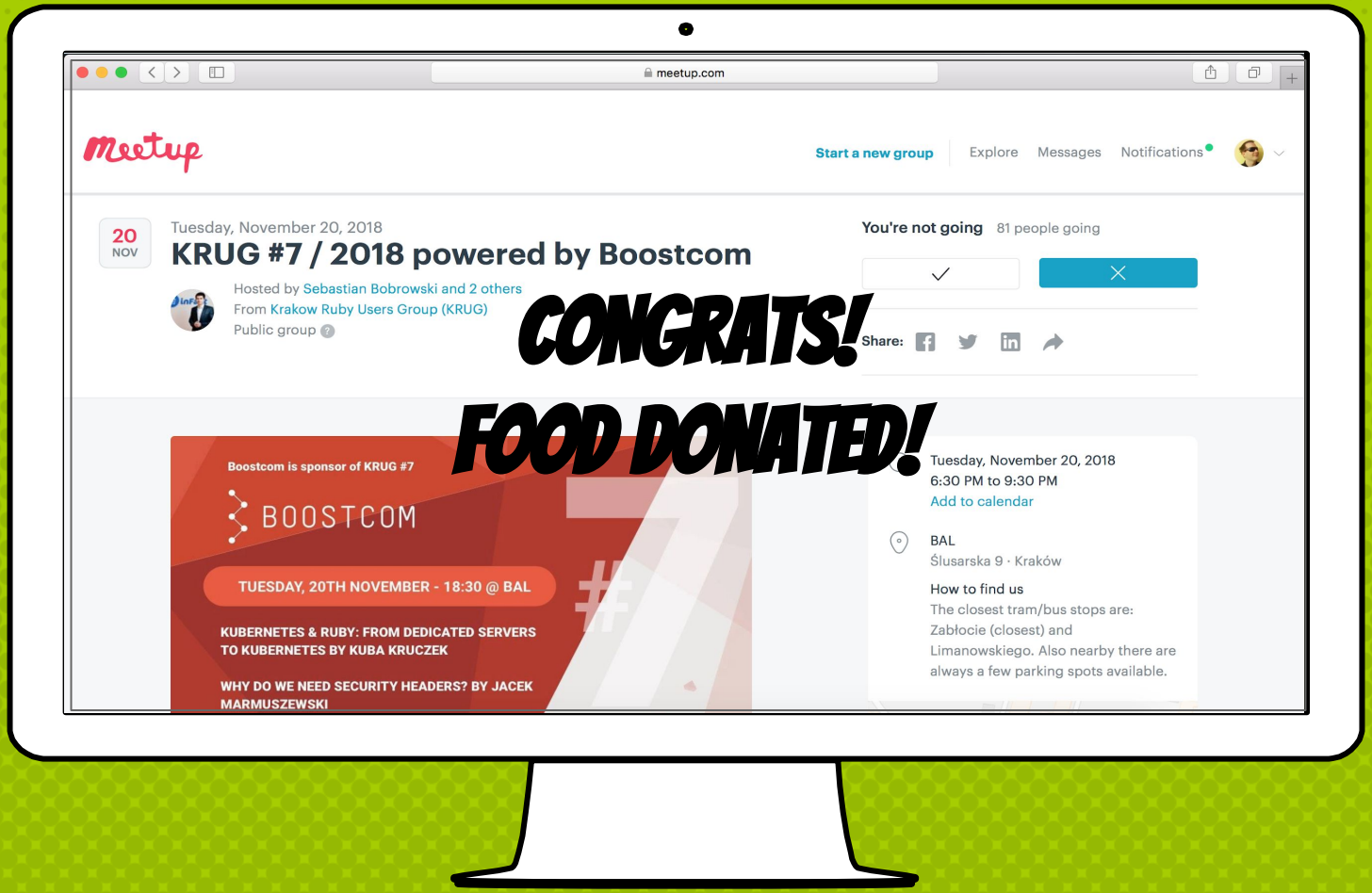
Has just ended ...

CLICK JACK ATTACK!


https://www.meetup.com/Krakow-Ruby-Users-Group/events/256295888/
Meetup
Start a new group
Explore
Messages
Notifications
20
NOV
Tuesday, November 20, 2018
KRUG #7 / 2018 powered by Boostcom
Hosted by Sebastian Bobrowski and 2 others
From Krakow Ruby Users Group (KRUG)
Public group
You're going
82 people going
Share:
FEED A CAT!
Boostcom is sponsor of KRUG #7
BOOSTCOM
TUESDAY, 20TH NOVEMBER - 18:30 @ BAL
KUBERNETES & RUBY: FROM DEDICATED SERVERS TO KUBERNETES BY KUBA KRUCZEK
WHY DO WE NEED SECURITY HEADERS? BY JACEK MARMUSZEWSKI
Tuesday, November 20, 2018
6:30 PM to 9:30 PM
Add to calendar
BAL
Ślusarska 9 · Kraków
How to find us
The closest tram/bus stops are: Zabłocie (closest) and Limanowskiego. Also nearby there are always a few parking spots available.


https://www.meetup.com/Krakow-Ruby-Users-Group/events/256295888/
Meetup
Start a new group
Explore
Messages
Notifications
20
NOV
Tuesday, November 20, 2018
KRUG #7 / 2018 powered by Boostcom
Hosted by Sebastian Bobrowski and 2 others
From Krakow Ruby Users Group (KRUG)
Public group
You're going
82 people going
Share:
Boostcom is sponsor of KRUG #7
BOOSTCOM
TUESDAY, 20TH NOVEMBER - 18:30 @ BAL
KUBERNETES & RUBY: FROM DEDICATED SERVERS TO KUBERNETES BY KUBA KRUCZEK
WHY DO WE NEED SECURITY HEADERS? BY JACEK MARMUSZEWSKI
Tuesday, November 20, 2018
6:30 PM to 9:30 PM
Add to calendar
BAL
Ślusarska 9 · Kraków
How to find us
The closest tram/bus stops are: Zabłocie (closest) and Limanowskiego. Also nearby there are always a few parking spots available.


https://www.meetup.com/Krakow-Ruby-Users-Group/events/256295888/
Meetup
Start a new group
Explore
Messages
Notifications
20
NOV
Tuesday, November 20, 2018
KRUG #7 / 2018 powered by Boostcom
Hosted by Sebastian Bobrowski and 2 others
From Krakow Ruby Users Group (KRUG)
Public group
You're going
82 people going
Share:
Boostcom is sponsor of KRUG #7
BOOSTCOM
TUESDAY, 20TH NOVEMBER - 18:30 @ BAL
KUBERNETES & RUBY: FROM DEDICATED SERVERS TO KUBERNETES BY KUBA KRUCZEK
WHY DO WE NEED SECURITY HEADERS? BY JACEK MARMUSZEWSKI
Tuesday, November 20, 2018
6:30 PM to 9:30 PM
Add to calendar
BAL
Ślusarska 9 · Kraków
How to find us
The closest tram/bus stops are: Zabłocie (closest) and Limanowskiego. Also nearby there are always a few parking spots available.


meetup.com
Meetup
Start a new group
Explore
Messages
Notifications
20
NOV
Tuesday, November 20, 2018
KRUG #7 / 2018 powered by Boostcom
Hosted by Sebastian Bobrowski and 2 others
From Krakow Ruby Users Group (KRUG)
Public group
You're not going
81 people going
Share:
CONGRATS!
FOOD DONATED!
Boostcom is sponsor of KRUG #7
BOOSTCOM
TUESDAY, 20TH NOVEMBER - 18:30 @ BAL
KUBERNETES & RUBY: FROM DEDICATED SERVERS TO KUBERNETES BY KUBA KRUCZEK
WHY DO WE NEED SECURITY HEADERS? BY JACEK MARMUSZEWSKI
Tuesday, November 20, 2018
6:30 PM to 9:30 PM
Add to calendar
BAL
Ślusarska 9 · Kraków
How to find us
The closest tram/bus stops are: Zabłocie (closest) and Limanowskiego. Also nearby there are always a few parking spots available.

X-FRAME-OPTION

HOW?

Day 3

WHAT IS THIS?

JAVASCRIPT!


HACKADAY
HOME
BLOG
HACKADAY.IO
STORE
HACKADAY PRIZE
SUBMIT
ABOUT
HIDING EXECUTABLE JAVASCRIPT IN IMAGES THAT PASS VALIDATION

X-CONTENT-TYPE-OPTION

HOW?

Day 4

SCRIPT INJECTION

- ✗ SERVER SIDE
- ✗ USER SIDE

Single Page Applications

- my-site.com/page#data
- my-site.com/page#<script>
- goo.gl/CXKUve

CONTENT-SECURITY-POLICY

HOW?

Day 5

PREPARATION

- ✗ HOST LIB
- ✗ HOST FILE
- ✗ EMBED LINK

CHECK SERVER LOGS

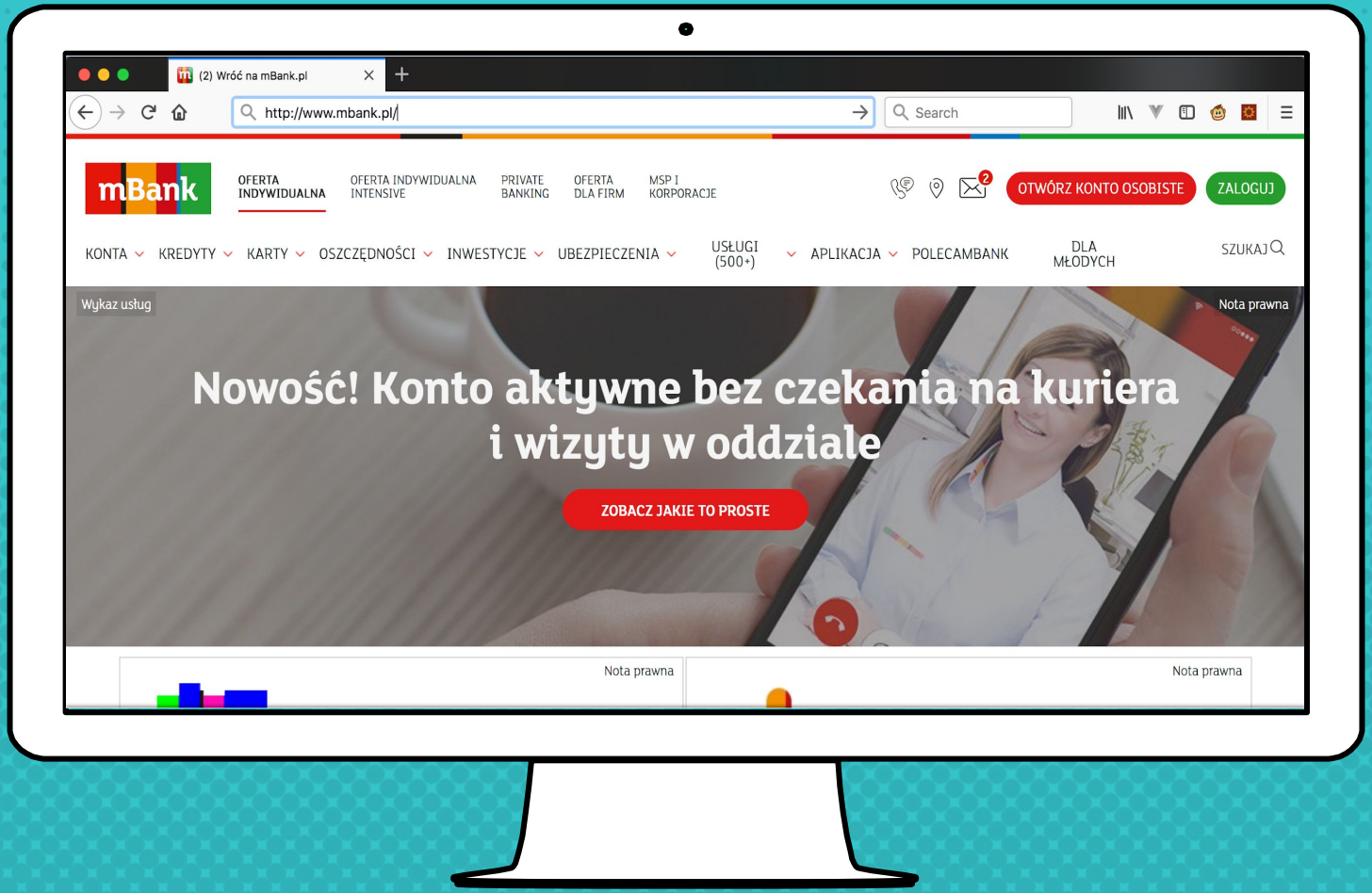
LogFormat "%{Referer}i %U" referer

- ✗ TOKENS
- ✗ MAGIC LINKS
- ✗ APPLICATION INTERNAL STRUCTURE

REFERRER-POLICY

HOW?

Day 6


(2) Wróć na mBank.pl
http://www.mbank.pl/
Search
mBank
OFERTA INDYWIDUALNA
OFERTA INDYWIDUALNA INTENSIVE
PRIVATE BANKING
OFERTA DLA FIRM
MSP I KORPORACJE
OTWÓRZ KONTO OSOBISTE
ZALOGUJ
KONTA
KREDYTY
KARTY
OSZCZĘDNOŚCI
INWESTYCJE
UBEZPIECZENIA
USŁUGI (500+)
APLIKACJA
POLECAMBANK
DLA MŁODYCH
SZUKAJ
Wykaz usług
Nota prawna
Nowość! Konto aktywne bez czekania na kuriera i wizyty w oddziale
ZOBACZ JAKIE TO PROSTE
Nota prawna
Nota prawna


http://www.mbank.pl/

MAN IN THE MIDDLE ... SIMPLE

- 1 MAN
- 1 LAPTOP
- 1 FREE WIFI (STARBUCKS / KRUG / ...)

- E.G. BAL_NA_ZABLOCIU

Man in the Middle ... Advanced

HTTP-STRICT-TRANSPORT-SECURITY

HTTP-PUBLIC-KEY-PINNING

RANDOM

Q & A


AirHelp

THANK YOU!

SOME LINKS

https://www.perpetual-beta.org/weblog/security-headers.html

https://infosec.mozilla.org/guidelines/web_security#cookies

PRESENTATION DESIGN

This presentation uses the following typographies:

- Titles: Bangers
- Body copy: Sniglet

You can download the fonts on this page:

https://www.google.com/fonts#UsePlace:use/Collection:Sniglet|Bangers

Click on the "arrow button" that appears on the top right 

You don't need to keep this slide in your presentation. It's only here to serve you as a design guide if you need to create new slides or download the fonts to edit the presentation in PowerPoint®

DISCLAIMER

- No services were attacked while preparing this presentation
- An similarity to name, logotype, webpage, url of any company is entirely coincidental and unintentional