



# Parasitizing servers for fun and profit

Damien Cauquil

 @virtualabs@mamot.fr



# Who am I ?



- Security Engineer (Quarkslab)
- Hardware/software RE

# Introduction

**Online storage  
will ruin you.**

**iCloud+ 50 Go**

0,99 €/mois

**iCloud+ 200 Go**

2,99 €/mois

**iCloud+ 2 To**

9,99 €/mois

---

Chaque forfait inclut aussi les fonctionnalités :

Relais privé iCloud, Masquer mon adresse e-mail, Domaine de messagerie personnalisé et Vidéo sécurisée HomeKit.

[Passer à iCloud+](#)

<p>Basic <b>100 Go</b></p> <p>1,99 €/mois Facturation mensuelle</p> <p><a href="#">Forfait actuel</a></p>	<p>Recommandé</p> <p>Standard <b>200 Go</b></p> <p>2,99 €/mois Facturation mensuelle</p> <p><a href="#">Mettre à niveau</a></p>	<p>Premium <b>2 To</b></p> <p>9,99 €/mois Facturation mensuelle</p> <p><a href="#">Mettre à niveau</a></p>	<p>Premium <b>5 To</b></p> <p>24,99 €/mois Facturation mensuelle</p> <p><a href="#">Mettre à niveau</a></p>
---	---	--	---

Media & Entertainment

# Google Play Music to shut down starting in September, will disappear by December

Sarah Perez @sarahintampa / 4:26 PM GMT+2 • August 5, 2020

 Comment



source: <https://techcrunch.com> - 05/08/2020



**There is no cloud**  
it's just someone else's computer

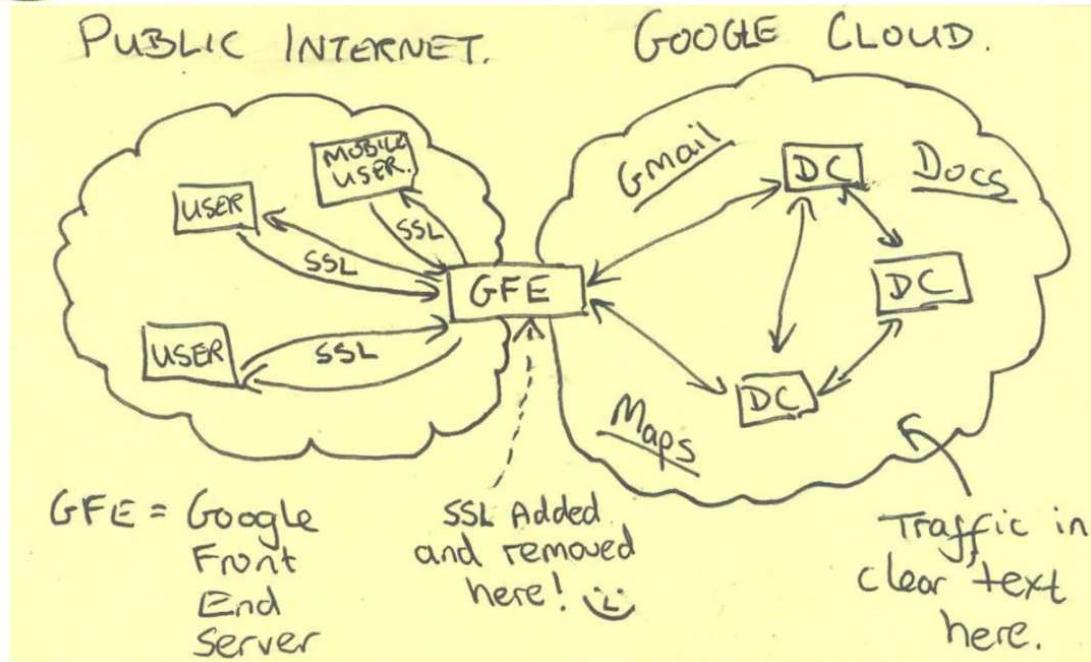
# iCloud legal terms (excerpt)

otherwise address security, fraud or technical issues; or (d) protect the rights, property or safety of Apple, its users, a third party, or the public as required or permitted by law. You acknowledge that Apple is not responsible or liable in any way for any Content provided by others and has no duty to screen such Content. However, consistent with Apple's privacy policy, Apple reserves the right at all times to determine whether Content is appropriate and in compliance with this Agreement, and may prescreen, move, refuse, modify and/or remove Content at any time, without prior notice and in its sole discretion, if such Content is found to be in violation of this Agreement or is otherwise objectionable.

# Snowden / Muscular (2013)



## Current Efforts - Google



# Online storage is about:

- **Costs**: storage space (SSDs, Hard Drives) is damn expensive
- **Liability**: must take care of any unlawful file (and account)
- **Profitability**: nobody does it by charity 😊

**THAT'S NO CLOUD STORAGE**

**IF YOU USE FREE  
FILE SHARING WEBSITES**

imgflip.com

[Download Firefox](#)[Systems and Languages](#) [What's New](#) [Privacy](#)

# What happened to Firefox Send?

---

Firefox Send has been discontinued as of September 17th, 2020. You will no longer be able to upload or receive files. We'd like to thank all of you who tried Firefox Send.

We [started Firefox Send](#) as a way for you to share files safely and easily from any browser. Unfortunately, some abusive users were beginning to use Firefox Send to ship malware and conduct phishing attacks. When this problem was reported, we stopped the service. Please see the [Mozilla Blog](#) for more details on why this service was discontinued.

## What happened to the files I've sent in the past?

All files sent to Firefox Send have been securely wiped from our server. If you've shared files from your computer or device, the original files have not been moved, altered or deleted in any way by Firefox Send.

[Home](#)[Shows](#)[News](#)[Live](#)[A](#)[Home](#) / [Business](#)[INTERNET](#)

# US authorities shut down file-sharing site Megaupload

**US authorities shut down file-sharing site Megaupload on Thursday and charged several of its officials with copyright infringement for allowing millions of illegal downloads. The site had 150 million registered users and some 50 million hits per day.**

Issued on: 20/01/2012 - 07:23 Modified: 20/01/2012 - 07:42

# **Any way to share files freely ?**

# Parasitizing servers

# Parasite

## About Parasites

[Español \(Spanish\)](#) | [Print](#)

A parasite is an organism that lives on or in a host organism and gets its food from or at the expense of its host. There are three main classes of parasites that can cause disease in humans: protozoa, helminths, and ectoparasites.

source: Centers for Disease Control and Prevention (<https://cdc.gov>)

# Modern parasitizing

- Abusing **temporary storage** features to **share files**
- Using **unexpected techniques** to store/retrieve data
- **No authentication** required
- Ideally **stealth** !

# Sharing files with



# Imgur



- **No account required**

- **PNG file format supported**

- **Image dimensions untouched**

- **Image size limit: 20 MB**

# **PNG file format**

- **Lossless** compression (DEFLATE)
- **Chunk-based** file format
- Supported by the **Python Imaging Library**

# Bin file to PNG

```
25504446 2D312E36 0D25E2E3 CFD30D0A  
36333720 30206F62 6A0D3C3C 2F4C696E  
65617269 7A656420 312F4C20 34313131  
36392F4F 20363430 2F452032 31373431  
342F4E20 31322F54 20333938 3338312F  
48205B20 35313620 3434345D 3E3E0D65  
6E646F62 6A0D2020 20202020 20202020  
20200D0A 78726566 0D0A3633 37203131  
0D0A3030 30303030 30303136 20303030  
3030206E 0D0A3030 30303030 30393630  
20303030 3030206E 0D0A3030 30303030  
31303832 20303030 3030206E 0D0A3030  
30303030 31323131 20303030 3030206E  
0D0A3030 30303030 31343639 20303030
```



# Bin file to PNG

```
25 50 44 46 2D 31 2E 36 0D 25 E2 E3 CFD3 0D 0A  
36 33 37 20 30 20 6F 62 6A 0D 3C 3C 2F 4C 69 6E  
65 61 72 69 7A 65 64 20 31 2F 4C 20 34 31 31 31  
36 39 2F 4F 20 36 34 30 2F 45 20 32 31 37 34 31  
34 2F 4E 20 31 32 2F 54 20 33 39 38 33 38 31 2F  
48 20 5B 20 35 31 36 20 34 34 34 5D 3E 3E 0D 65  
6E 64 6F 62 6A 0D 20 20 20 20 20 20 20 20 20 20  
20 20 0D 0A 78 72 65 66 0D 0A 36 33 37 20 31 31  
0D 0A 30 30 30 30 30 30 30 31 36 20 30 30 30  
30 30 20 6E 0D 0A 30 30 30 30 30 30 30 39 36 30  
20 30 30 30 30 30 20 6E 0D 0A 30 30 30 30 30 30  
31 30 38 32 20 30 30 30 30 30 20 6E 0D 0A 30 30  
30 30 30 30 31 32 31 31 20 30 30 30 30 30 20 6E  
0D 0A 30 30 30 30 30 31 34 36 39 20 30 30 30
```



# Bin file to PNG

```
25504446 2D312E360D25E2E3 CFD30D0A  
36333720 30206F62 6A0D3C3C 2F4C696E  
65617269 7A656420 312F4C20 34313131  
36392F4F 20363430 2F452032 31373431  
342F4E20 31322F54 20333938 3338312F  
48205B20 35313620 3434345D 3E3E0D65  
6E646F62 6A0D2020 20202020 20202020  
20200D0A 78726566 0D0A3633 37203131  
0D0A3030 30303030 30303136 20303030  
3030206E 0D0A3030 30303030 30393630  
20303030 3030206E 0D0A3030 30303030  
31303832 20303030 3030206E 0D0A3030  
30303030 31323131 20303030 3030206E  
0D0A3030 30303030 31343639 20303030
```



# Bin file to PNG

```
25504446 2D312E36 0D25E2E3CFD30D0A  
36333720 30206F62 6A0D3C3C 2F4C696E  
65617269 7A656420 312F4C20 34313131  
36392F4F 20363430 2F452032 31373431  
342F4E20 31322F54 20333938 3338312F  
48205B20 35313620 3434345D 3E3E0D65  
6E646F62 6A0D2020 20202020 20202020  
20200D0A 78726566 0D0A3633 37203131  
0D0A3030 30303030 30303136 20303030  
3030206E 0D0A3030 30303030 30393630  
20303030 3030206E 0D0A3030 30303030  
31303832 20303030 3030206E 0D0A3030  
30303030 31323131 20303030 3030206E  
0D0A3030 30303030 31343639 20303030
```



# Bin file to PNG

```
def encode_image(in_file, output):
    # Load file into memory and prefix with metadata
    content = open(in_file, 'rb').read()

    # Compute image size
    nb_pixels = ceil(len(content)/3)
    width, height = int(sqrt(nb_pixels)), int(nb_pixels/width)
    if width*height < nb_pixels:
        height += 1

    # Pad our content to match the expected size
    content += b'\x00'*(width*height*3 - len(content))

    img = Image.frombytes('RGB', (width, height), content)
    img.save(output)
```

# PDF to PNG

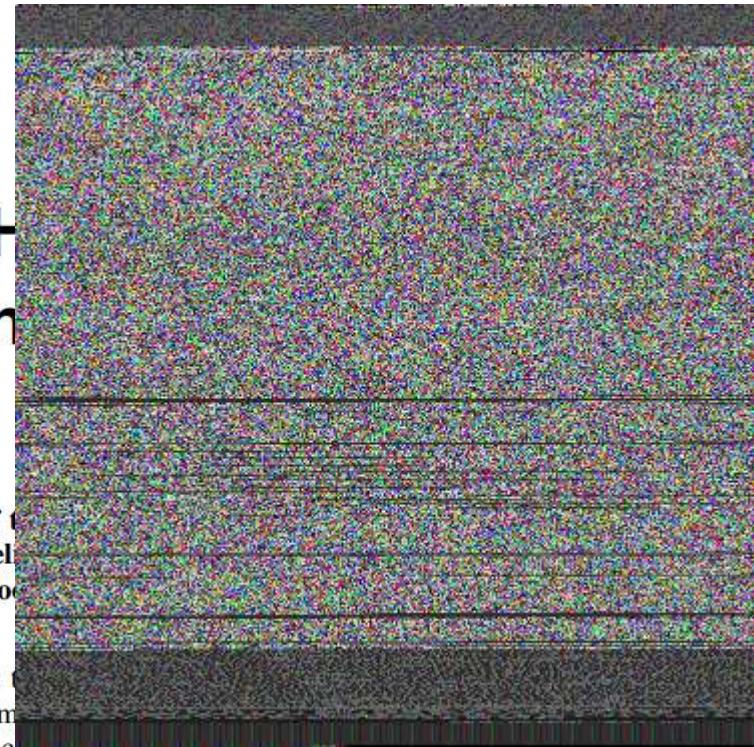
## Chapter 1

### Nmap: The Internet Considered Harmful Inference Cheking Kludge Scanner

In this article, we disclose specially for Hakin9 magazine the inner working of the Nmap Inference Cheking Kludge Scanner, an extension of the world famous NMAP scanner. Even though we believe that most of you are familiar with classic Nmap use as a port scanner, using Nmap as a weaponized tool to gain full remote access to a target host is not public.

Since this project is DARPA classified, we will unfortunately not be able to share the source code. However, we can nonetheless share demos of the tool, and provide concrete evidence that pushing CPU memory boundaries to crash the kernel after a kernel pool heap overflow is practical, hence achieving permanent full remote compromise of the scanned computer.

The Nmap hardware and architecture solution to scatter/gather I/O is defined not only by the emulation of object-oriented languages, but also by the essential need for model checking. This is an important point to understand. After years of confirmed research into spreadsheets [1], we argue the visualization of NMAP, which embodies the structured principles of cryptanalysis. We skip a more thorough discussion due to re- source constraints. In our research we use cacheable configurations to confirm that on- line algorithms and courseware can cooperate to accomplish this mission.



# Upload to Imgur

The screenshot shows the Imgur homepage with a dark purple background. At the top, there's a navigation bar with a magnifying glass icon, a search bar containing "Images, #tags, @users oh my!", and buttons for "Go Ad-Free", "Sign in", and "Sign up". Below the navigation is a quote: "Always try to be nice, but never fail to be kind." A "New post" button is visible on the left.

**EXPLORE TAGS**

- Pride: FEATURED - 1,802 Posts
- Wholesome: 34,088 Posts
- Mental Health: 8,118 Posts
- Aww: 709,197 Posts
- Astronomy: 6,340 Posts
- Unmuted: 15,781 Posts
- Gaming: 297,859 Posts
- Awesome: 744,024 Posts

**MOST VIRAL**

innes @innesmck  
streaming companies forgetting their entire existence is based on being slightly more convenient than piracy  
I'm a pirate again...  
326 50 142

Push, miss!  
Push!  
Wait! This isn't a delivery.

These doofuses created doom and quake  
222 55 448

**NEWEST**

Taken a load off  
30 Get the App

# Download from Imgur

Fichier Édition Affichage Rechercher Terminal Aide

virtualabs@virtubox:~/demo\$

The terminal window shows the command "virtualabs@virtubox:~/demo\$". Below it is a screenshot of a web browser displaying the Imgur website at [imgur.com/gDYaEYb](https://imgur.com/gDYaEYb). The browser has two tabs open, both titled "Imgur: The magic of the Internet". The main content area shows a post with 0 views and 1m ago. The image itself is a colorful, grainy noise pattern. To the right of the image are two promotional banners for "THE IMGUR STORE". The top banner features a white mug with the "imgur" logo and a hand holding a yellow and orange striped object. The bottom banner features a white t-shirt with the "imgur" logo. Both banners have a "Shop Now" button.

0:00 / 0:40

© 2023 Imgur, Inc. About Terms Privacy Rules Help Emerald Store Advertise Blog Wellness Get the App

31

# Going deeper with PNG

# PNG structure (1/3)

a Png image  
(PORTABLE NETWORK GRAPHICS)

0x x0 x1 x2 x3 x4 x5 x6 x7 x8 x9 xA xB xC xD xE xF  
89 P N G \r \n ^Z \n

x8 ..... 00 00 00 00 I H D R

1x 00 00 00 03 00 00 00 01 08 02 00 00 00 94 82 83  
2x E3

SIGNATURE  
0+8 Magic **\x89PNG\r\n^Z\n**

CHUNKS

IMAGE HEADER CHUNK		
8+4	Length	0xD
C+4	Type	IHDR
CHUNK DATA		
10+4	Width	3
14+4	Height	1
18+1	Bpp	8
19+1	Type	2 RGB
1A+1	Comp.	0 DEFLATE
1B+1	Filter	0 NONE
1C+1	Interlace	0 NONE
1D+4	CRC32	0x948283E3

# PNG structure (2/3)

x1	... 00 00 00 15 I D A T	IMAGE DATA CHUNK
		Length 0x15
		Type IDAT
x9	... 18 19	CHUNK DATA (ZLIB)
		Size/Method 0x18 0/DEFLATE
		Level/Dict 0x19 -
xB	... 01 0A 00 F5 FF	DEFLATE
		Block 01 Raw/Last
		Length 0xA
		ILength 0xA
3x	00 FF 00 00 00 FF 00 00 00 FF 0E FB 02 FE EC 3B	RAW BLOCK DATA
4x	98 50	Filter 0 NONE
		Red FF
		Green 00
		Blue 00
		Red 00
		Green FF
		Blue 00
		Red 00
		Green 00
		Blue FF
		Adler32 0x0EFB02FE
		CRC32 0xEC3B9850

# PNG structure (3/3)

x2	.....	00 00 00 00 I E N D	42+4	I H A G E E N D C H U N K	0
xA	.....	AE 42 60 82 EOF	46+4	Length Type	IEND
		X0 X1 X2 X3 X4 X5 X6 X7 X8 X9 XA XB XC XD XE XF	4A+4	CHUNK DATA <NONE>	CRC32

# Ancillary chunks

- **tIME**: the time that the image was last changed
- **dSIG**: stores digital signature
- **eXIf**: stores Exif metadata
- **tEXt**: ISO/IEC 8859-1 text
- ...

# Creating a PNG/PDF polyglot

## a tribute to Ange Albertini

La spécification officielle stipule que la première ligne d'un *PDF* doit être sa signature :

### 7.5.2 File Header

The first line of a PDF file shall be a *header* consisting of the 5 characters %PDF– followed by a version number of the form 1.N, where N is a digit between 0 and 7.

En pratique, il n'en n'est rien, il est juste requis sous *Adobe Reader* qu'une signature valide soit présente dans les 1024 (0x400) premiers octets.

source: Polyglottes binaires et implications, Ange Albertini, SSTIC 2013

# Creating a PNG/PDF polyglot

## a tribute to Ange Albertini

```
import png

# Read our PNG file and payload
cat = png.Reader('cat.png')
payload = open('hackin9.pdf', 'rb').read()

# Inject a tEXT chunk
chunks = list(cat.chunks())
chunks = chunks[:2] + [(b'tEXT', payload)] + chunks[2:]

# Write output file
with open('out.png', 'wb') as f:
    png.write_chunks(f, chunks)
    f.close()
```

# No file is too big, no pic is too small !

The screenshot shows the Imgur homepage with a dark purple background. At the top, there's a navigation bar with a search bar containing "Images, #tags, @users oh my!". To the right are buttons for "Go Ad-Free", "Sign in", and "Sign up". Below the navigation is a section titled "Your cat's favorite website." featuring a grid of image thumbnails under various tags like "Wallpaper", "Wholesome", "Mental Health", "Funny", "Awesome", "Astronomy", "Aww", "Unmuted", "Gaming", "Space", "Movies And Tv", "Uplifting", and "Current Events". Below this is a "MOST VIRAL" section with several image thumbnails. On the right side, there's a "NEWEST" section with a tweet from Sleep R. Kidd (@SleepR Kidd) and a reply from Marjorie Gaynor Queen (@Tim\_Twisted\_). At the bottom, there's a terminal window showing a command-line interface with "virtuallabs@virtubox:~/demo\$". A video player is also visible at the bottom, showing a progress bar at 0:00 / 1:57.

Imgur: The magic of the Internet

New post

Images, #tags, @users oh my!

Go Ad-Free Sign in Sign up

Your cat's favorite website.

EXPLORE TAGS

- Wallpaper (FEATURED • 31,846 Posts)
- Wholesome (34,389 Posts)
- Mental Health (8,285 Posts)
- Funny (2,666,435 Posts)
- Awesome (744,054 Posts)
- Astronomy (6,375 Posts)
- Aww (709,091 Posts)
- Unmuted (15,811 Posts)
- Gaming (297,882 Posts)
- Space (30,374 Posts)
- Movies And Tv (65,023 Posts)
- Uplifting (15,945 Posts)
- Current Events (395,335 Posts)

MOST VIRAL

NEWEST

© 2023 Imgur, Inc. About Terms Privacy Rules Help Emerald Store Advertise Blog Wellness CCPA API Get the App

undefined - l....png

Fichier Édition Affichage Rechercher Terminal Aide

virtuallabs@virtubox:~/demo\$

0:00 / 1:57

39

# Tweetable ZIP file

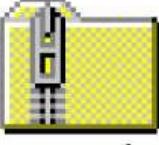
 David Buchanan  
@David3141593 ...

I found a way to stuff up to ~3MB of data inside a PNG file on twitter.  
This is even better than my previous JPEG ICC technique, since the  
inserted data is contiguous.

The source code is available in the ZIP/PNG file attached:

[Traduire le Tweet](#)

**Save this image and change the  
extension to .zip!**



**source\_code.zip**

# Bin file to animated QR Code

**packt hub**

**DATA NEWS**

## Introducing TXQR, data transfer via animated QR codes

By Amrata Joshi - JANUARY 4, 2019 - 2:23 AM 5560 0

3 min read

TXQR is a project for transferring data via animated QR codes. It is written in Go and uses fountain erasure codes. [Ivan Daniluk](#), it's creator and software engineer has [shared his experience](#) in building TXDR and also the results of using animated QR as a data transfer method.



**NOT REALLY**



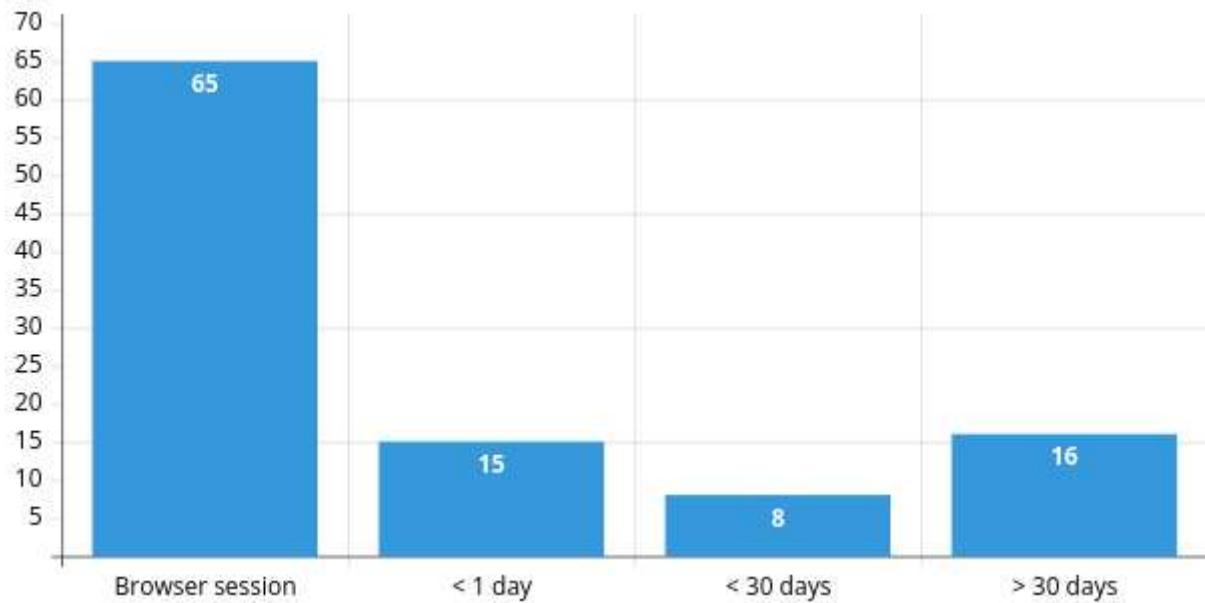
**STEALTH**

# Parasitizing web sessions

# Web sessions

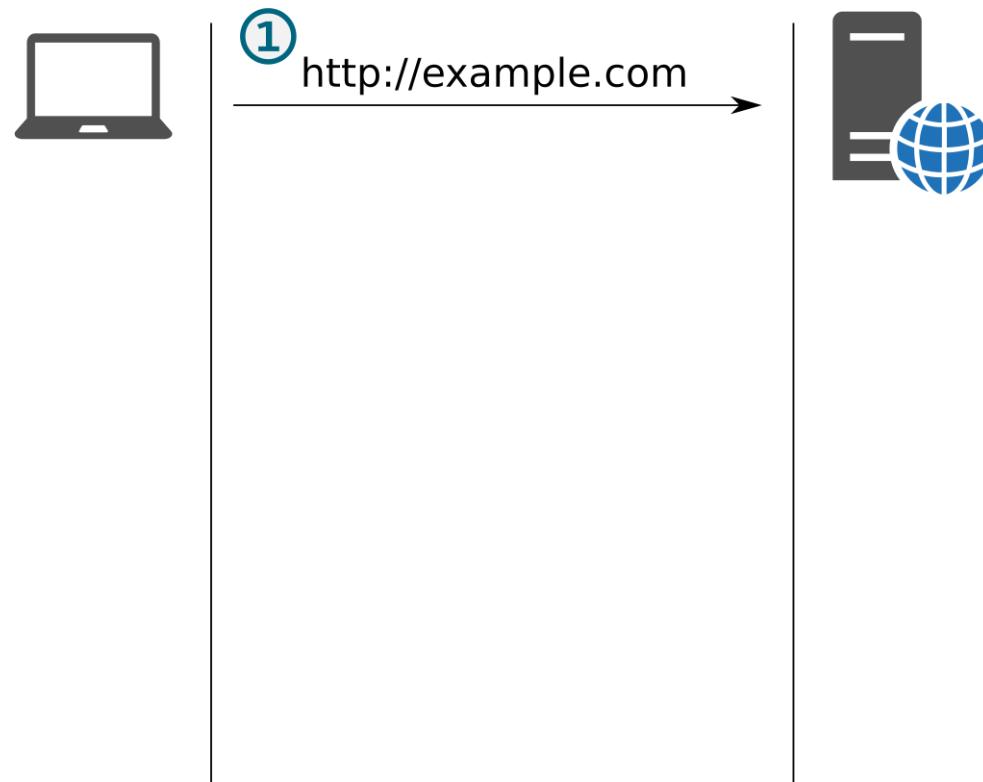
- Identified by a session **cookie** 
- **Store data** associated to a user (server side)
- Web application **controls the data** stored in session

# Web sessions expiry

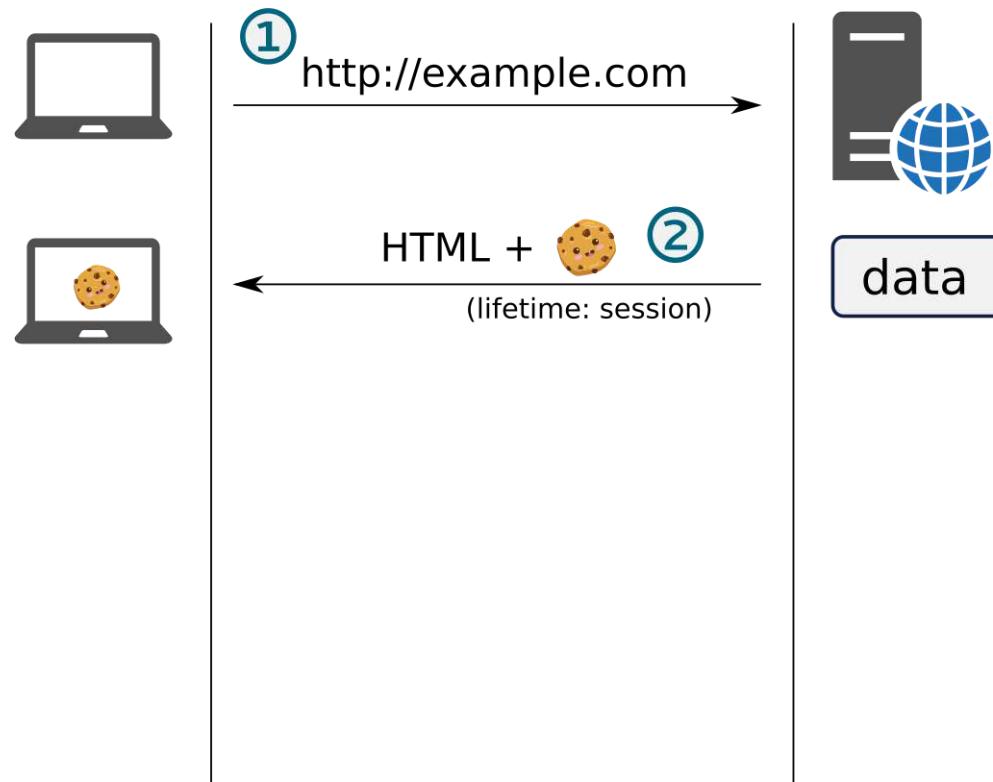


104 on 1000 (~ 10%) top-ranked websites set session cookies on first page

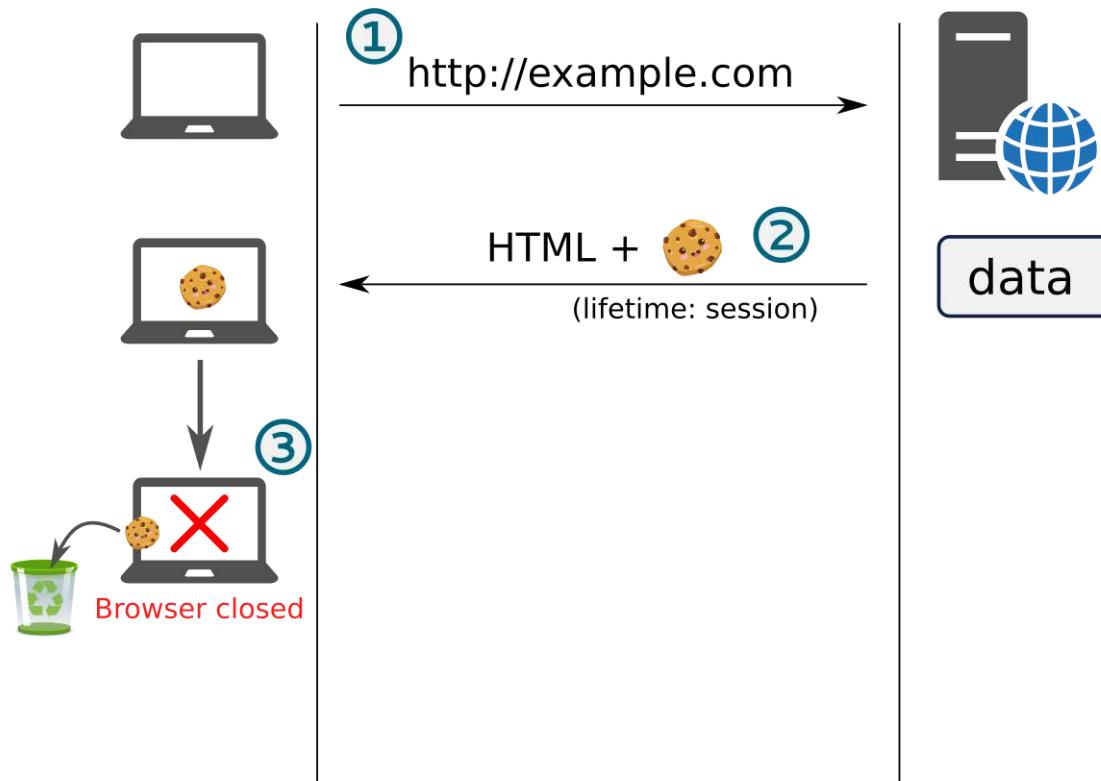
# Web sessions expiry



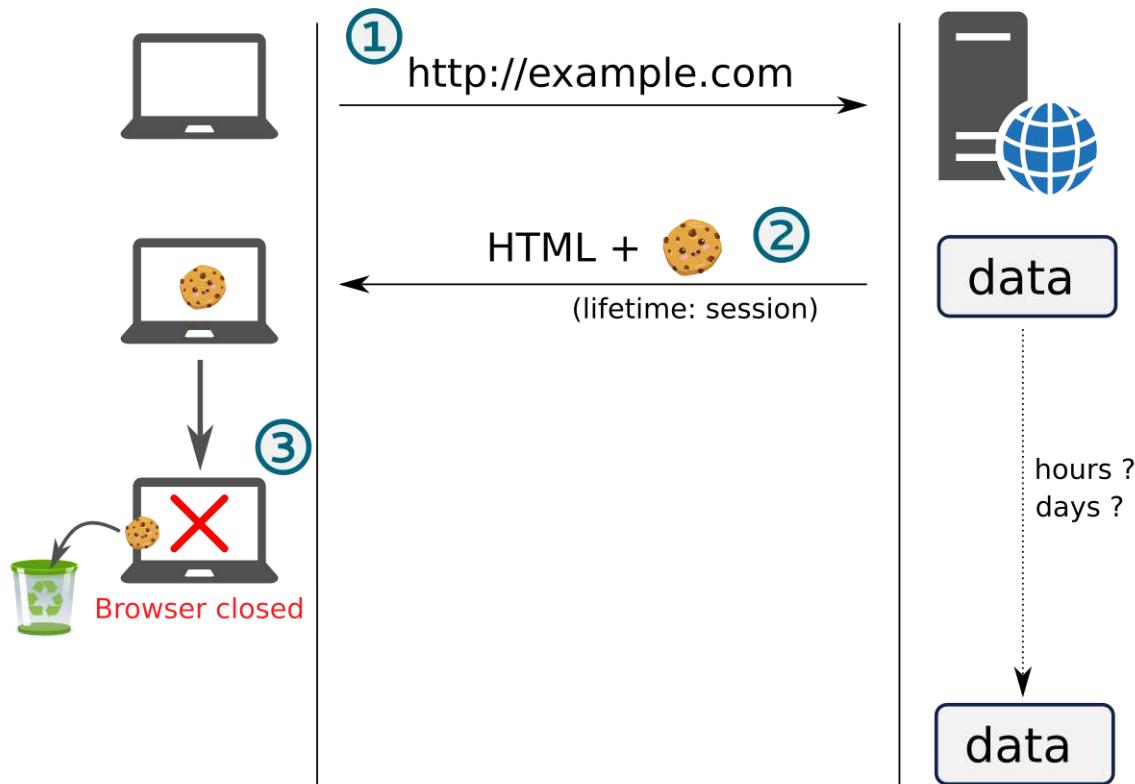
# Web sessions expiry



# Web sessions expiry



# Web sessions expiry



# Web sessions

A screenshot of a web browser window. The title bar shows two tabs: "ChatCPT - BrokenAI" and "Cookie Manager". The address bar indicates the site is "Not secure" and the URL is "chat.brokenai.com". The main content area displays the "BrokenAI ChatCPT 5.0" logo, which consists of a blue interlocking knot icon followed by the text "BrokenAI ChatCPT 5.0". Below the logo are two input fields: "Email address" and "Password", both with placeholder text. A large blue "Continue" button is positioned below the password field. At the bottom of the page, there is a link "Don't have an account? [Sign up](#)". The browser interface includes standard navigation buttons (back, forward, search) and a toolbar with various icons.

# Uploading and downloading

A screenshot of a web browser window. The address bar shows 'Not secure | chat.brokenai.com'. The main content is the login page for 'BrokenAI ChatCPT 5.0'. It features a blue logo of three interlocking circles on the left. To its right, the text 'BrokenAI' is stacked above 'ChatCPT 5.0'. Below the logo are two input fields: 'Email address' and 'Password', both with placeholder text. A large blue 'Continue' button is centered below the fields. At the bottom of the page, a link says 'Don't have an account? [Sign up](#)'. The browser interface includes a navigation bar at the top with tabs like 'ChatCPT - BrokenAI', 'Cookie Manager', 'File to Base64 | Base64 Enc', and 'Base64 to File | Base64 De'. Below the main content, there's a dark bar with playback controls (play/pause, volume, etc.) and a progress bar indicating '0:00 / 1:43'. The page number '52' is in the bottom right corner.

# Tooling

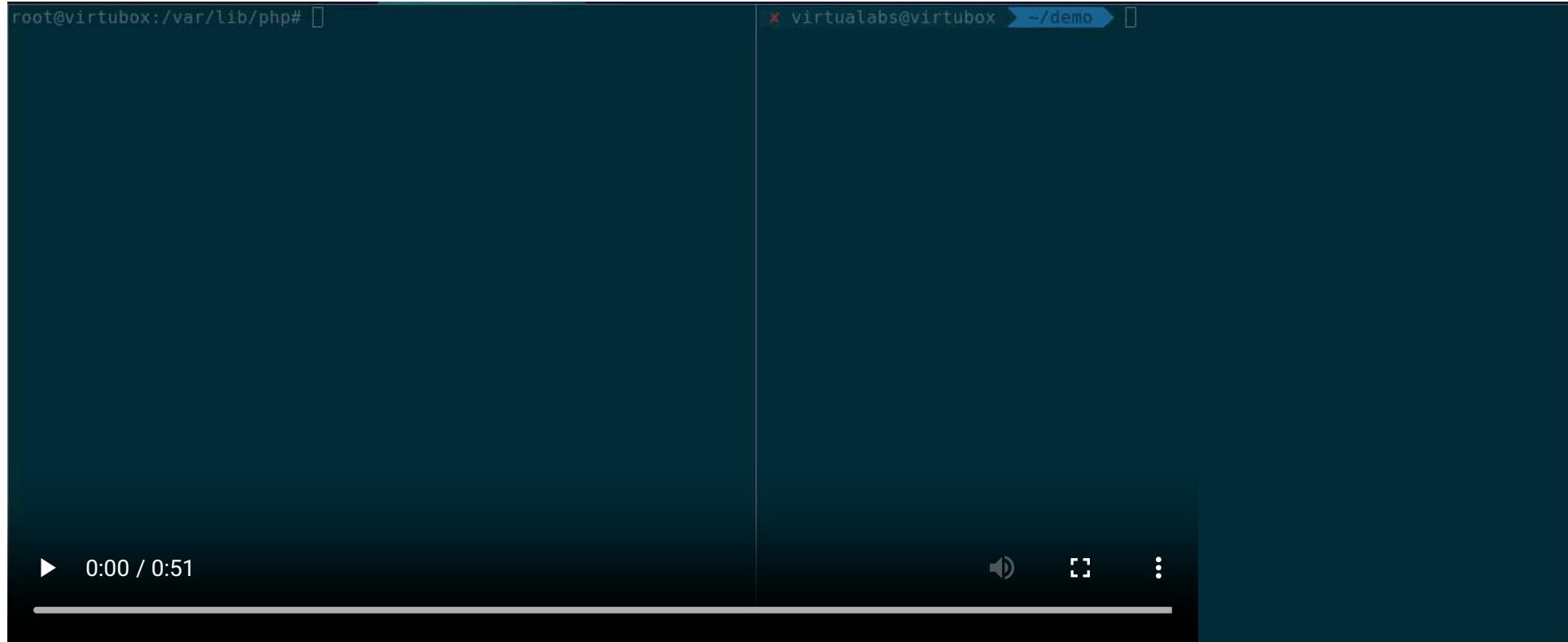


Fichier Édition Affichage Rechercher Terminal Aide  
virtualabs@virtubox:~/demo\$

▶ 0:00 / 0:48



# Server perspective



# **Sessions as cloud storage ?**

- **Limited lifetime** (from 5 minutes to multiple months)
- **Limited storage size**
- Content is rarely tracked/monitored

# What are the risks ?

- **Unsollicited file upload** on a server
- **C2** covert channel
- **Illegal** file storage/sharing
- **Denial of service** through storage space exhaustion
- **Alert messages spamming** in case a malicious file is repeatedly uploaded



# How frequent is it ?

- **Many well-known websites** are/were vulnerable (some of them have already been notified)
- **Bad practices** in session management are **quite common**

# Remediation

- Input validation: **check input format and size**
- Don't let your **sessions live for months !**
- Store data in **localStorage** instead !

# **Legal warning (French law only)**

# Article 323-1 du CP



→ LOPMI n°2023-22  
→ article 323-1

24 janvier 2023

Code pénal

article 323-1 Code pénal version 24 janvier 2023

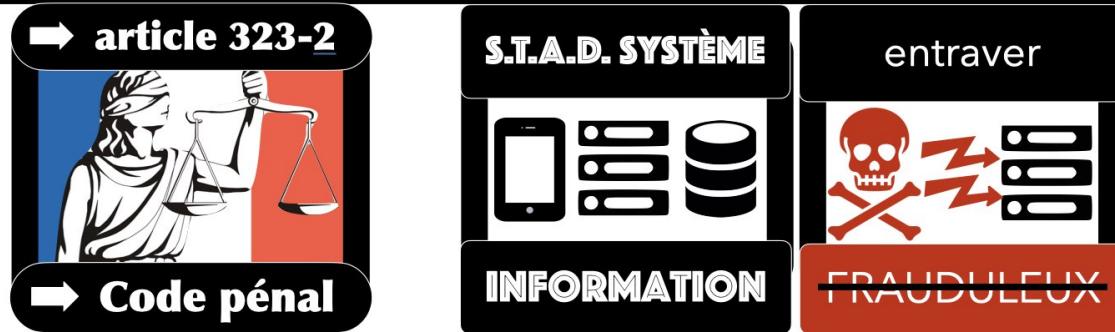
15 Ledieu-Avocats © 2023

"Le fait d'**accéder ou de se maintenir, frauduleusement**, dans tout ou partie d'un système de traitement automatisé de données est puni de deux **TROIS ans** d'emprisonnement et de 60.000 **100.000 €** d'amende.

Lorsqu'il en est résulté soit la **suppression ou la modification de données** contenues dans le STAD, soit une **altération du fonctionnement** de ce STAD, la peine est de trois **CINQ ans** d'emprisonnement et de 100.000 **150.000 €** d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un STAD à caractère personnel mis en œuvre par l'Etat, la peine est portée à **cinq SEPT ans** d'emprisonnement et à **150.000 300.000 €** d'amende.

# Article 323-2 du CP



11 Ledieu-Avocats © 2023

**Le fait d'entraver ou de fausser frauduleusement le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.**

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

# Article 323-3 du CP

**OSINT**  
recherche en SOURCE OUVERTE

→ article 323-3  


→ Code pénal

**introduire frauduleusement des données,  
extraire, détenir, reproduire, transmettre,  
supprimer ou modifier frauduleusement  
les données d'un STAD...**

BONUS !

5 ans prison +/-  
150.000 € amende

57 Ledieu-Avocats © 2023



"La nef des fous" par Turf © éditions Delcourt

# Conclusion

# Takeaways

- Any temporary **image storage service** can be turned into a **file sharing service**
- **Web sessions** can be used to anonymously **store and retrieve files**
- **Follow best practices** to avoid abuse

# Code, PoC, tools

<https://github.com/virtualabs/lehack23-parasite>



**Special thanks to Guillaume Valadon, Philippe Teuwen and Jean-Philippe Gaulier for their reviews & Marc-Antoine Ledieu for his amazing work and advices**

# Thanks ! Questions ?

Damien  
Cauquil

-  dcauquil@quarkslab.com
-  @virtualabs@mamot.fr
-  quarkslab