Super file(s) transfert !!

Web project / Crypto

> *by gpouyat* 🛸 👓

Summary:

Are you lost ? It's not a big subject.

Mandatory

New BOSS: - "Welcome to our secure company ! We are super secure! We have forbidden USB keys. We have blocked all websites for file(s) transfer. Yes, indeed we don't want to lose confidential document"

You: - "Ok nice, but how to send file(s) ? by mail ?"

New BOSS: - "No, never, because we could lose control of the file(s), and often the size limit of mails blocks us"

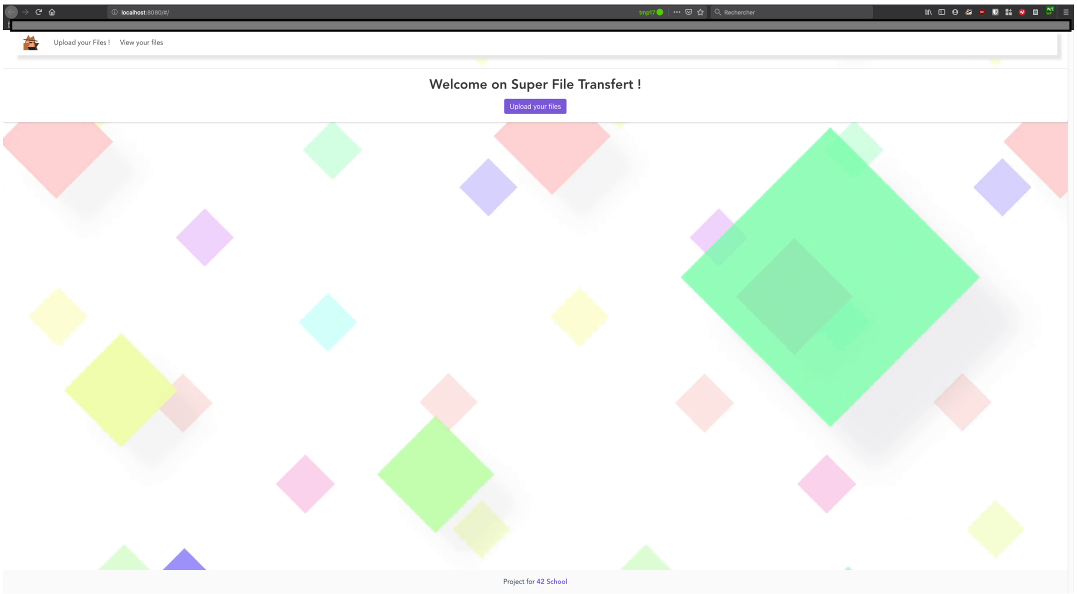
You: "- So, how do we exchange file(s) with your clients? How do you transfer my work contract ? How can I send files to co-workers ?"

BOSS: - "Very good questions! I hired you to answer these questions!"

Instructions

We need a file transfer platform wich:

1. We can access with the web navigator



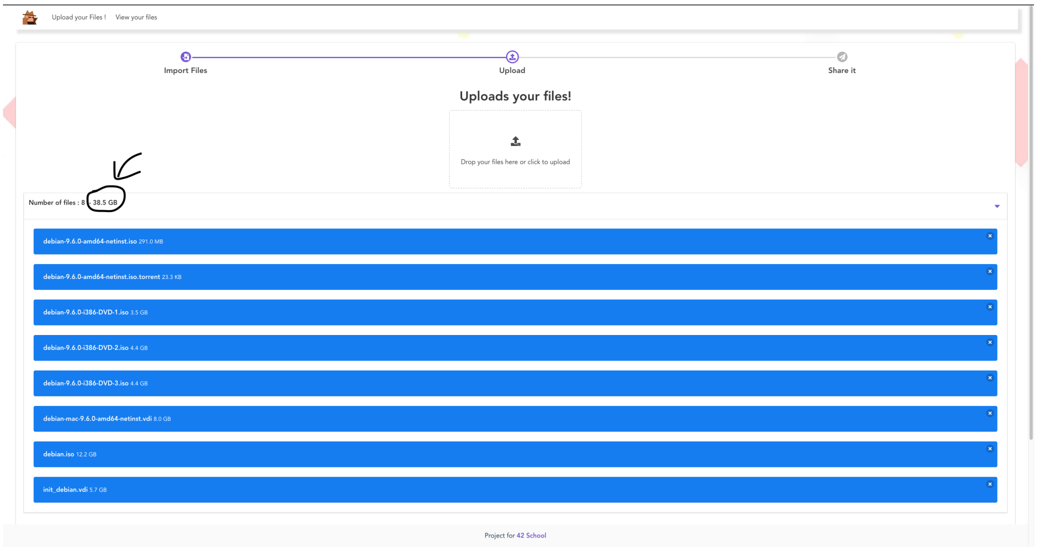
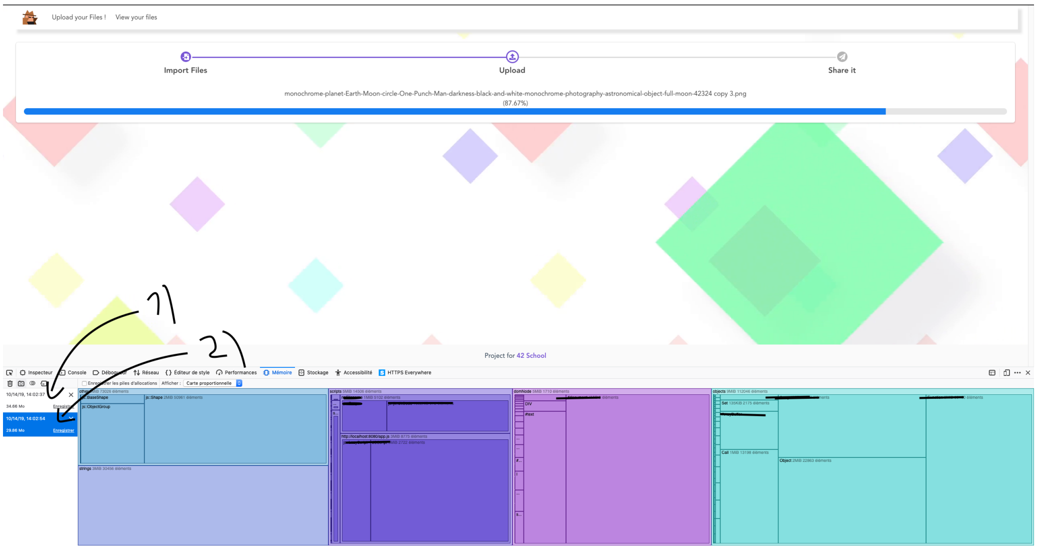
Welcome on Super File Transfert !

Project for 42 School

2. The server, if there is any, must not be able to access the files wich are being sent.

> *If there is a server, the file(s) must be encrypted and the secret key should not be stored on the server or accessible in logs*

3. The files could have any size

> *Don't store all content of file(s) in RAM memory*
>
> 
>
>
> Uploads your files!
>
> Number of files : 8 - 38.5 GB
>
> debian-9.6.0-amd64-netinst.iso 291.0 MB
> debian-9.6.0-amd64-netinst.iso.torrent 23.3 KB
> debian-9.6.0-i386-DVD-1.iso 3.5 GB
> debian-9.6.0-i386-DVD-2.iso 4.4 GB
> debian-9.6.0-i386-DVD-3.iso 4.4 GB
> debian-mac-9.6.0-amd64-netinst.vdi 8.0 GB
> debian.iso 12.2 GB
> init_debian.vdi 5.7 GB
>
> *1 = before download starts*
> *2 = during download*
> *The memory is never full*
>
> 
>
>
> monochrome-planet-Earth-Moon-circle-One-Punch-Man-darkness-black-and-white-monochrome-photography-astronomical-object-full-moon-42324 copy 3.png
> (87.67%)
>
> 10/14/19, 14:02:37 34.66 Mo
> 10/14/19, 14:02:54 29.86 Mo
>
> other 3MiB 73026 éléments; js::BaseShape; js::ObjectGroup; js::Shape 2MiB 50961 éléments; strings 3MiB 30456 éléments; scripts 5MiB 14506 éléments; [redacted] 1MiB 5102 éléments; [redacted]; http://localhost:8080/app.js 3MiB 8775 éléments; [redacted] 2722 éléments; domNode 5MiB 1710 éléments; [redacted] éléments; DIV; #text; objects 9MiB 112046 éléments; [redacted]; Set 135KiB 2175 éléments; [redacted]; Call 1MiB 13198 éléments; Object 2MiB 22863 éléments; [redacted] éléments

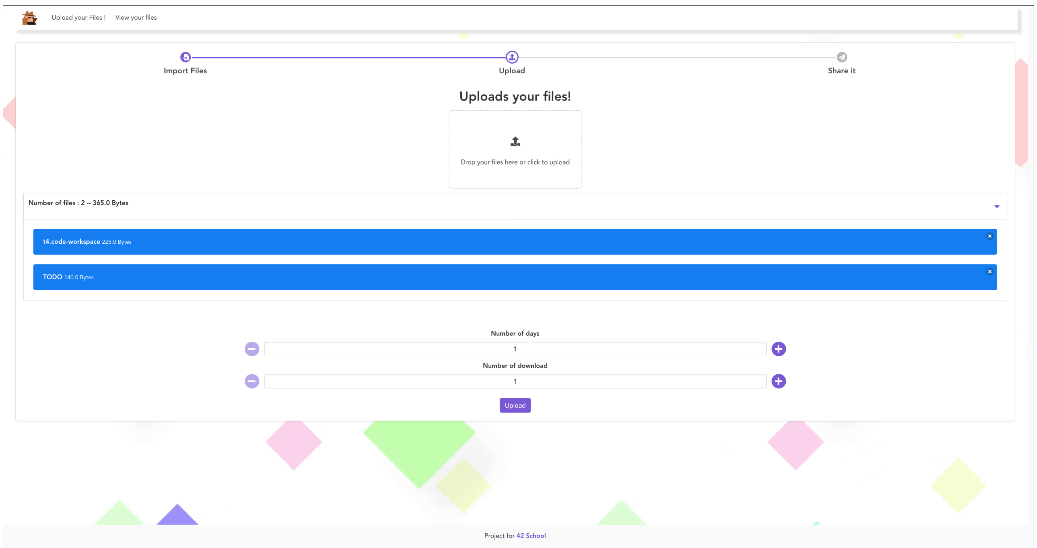
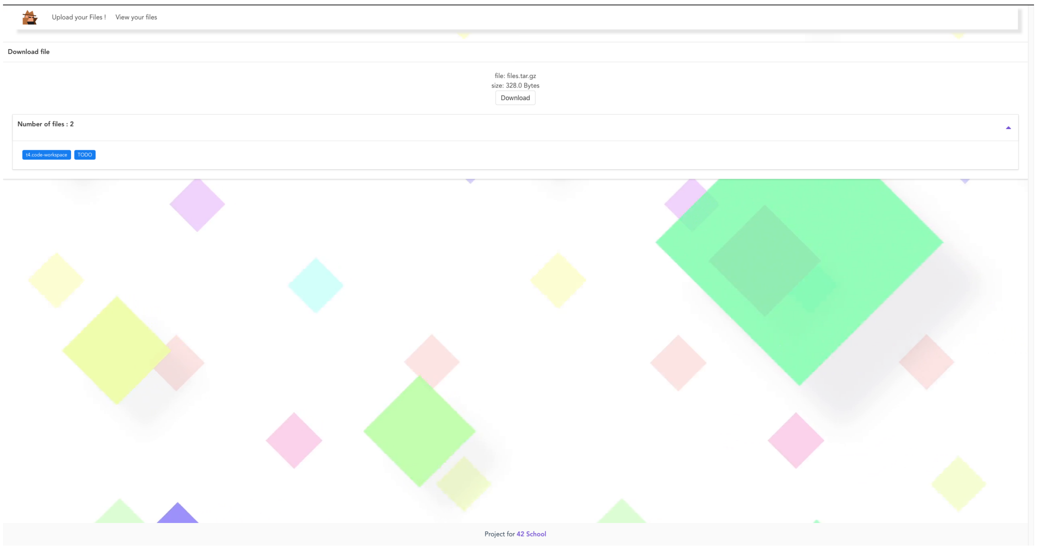
4. The platform should be easy to use

> *We want just a download link. (no password to type)*
> *Warning: The server must not be able to access secret key, never send it to the server*
> *Compatible: firefox 69 / chrome 77 / safari 13.0*

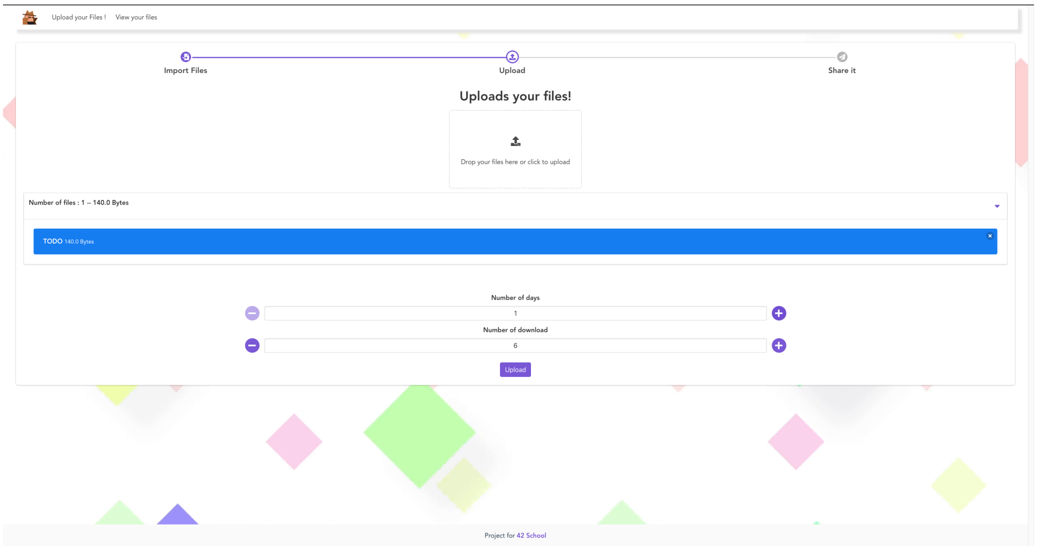
5. The transfer must be encrypted (client side) with good cryptography algorithm and with respect the following specs

> - *Only native crypto library, and polyfill nodeJs native crypto are authorized.*
> - *It is forbidden to re-code crypto algorithm.*
> - *Use good cryptographic practices,*
>   - *Initialization vector must be unique, secret key mut be long and non previsible... (Are they unique and random ?!)*
>   - *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf*
>   - *https://www.w3.org/TR/WebCryptoAPI/*

6. If you send multiple files, you create a TarBall and you compress it, or create a zip file.

> *Warning server must not be able to know the number of files and filenames*
>
> 
>
>
> Uploads your files!
>
> Number of files : 2 -- 365.0 Bytes
>
> t4.code-workspace 225.0 Bytes
>
> TODO 140.0 Bytes
>
> Number of days: 1
>
> Number of download: 1
>
> *Before download, user can view the number of files and filenames*
>
> 
>
>
> Download file
>
> file: files.tar.gz
> size: 328.0 Bytes
>
> Number of files : 2
>
> t4.code-workspace TODO

7. The owner* can set an expiration date and the maximum number of downloads



Uploads your files!

Drop your files here or click to upload

Number of files : 1 -- 140.0 Bytes

TODO 140.0 Bytes

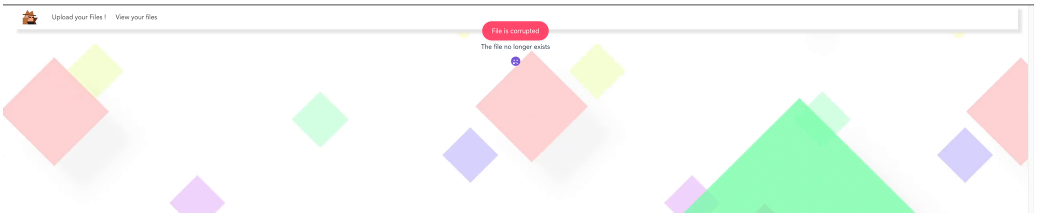
Number of days: 1

Number of download: 6

> *When the download link expires or the number of downloads is 0, the file is removed from the server*

8. If there is a problem with the transfer (corruption of the file's content), the platform must control the file's integrity (client side)

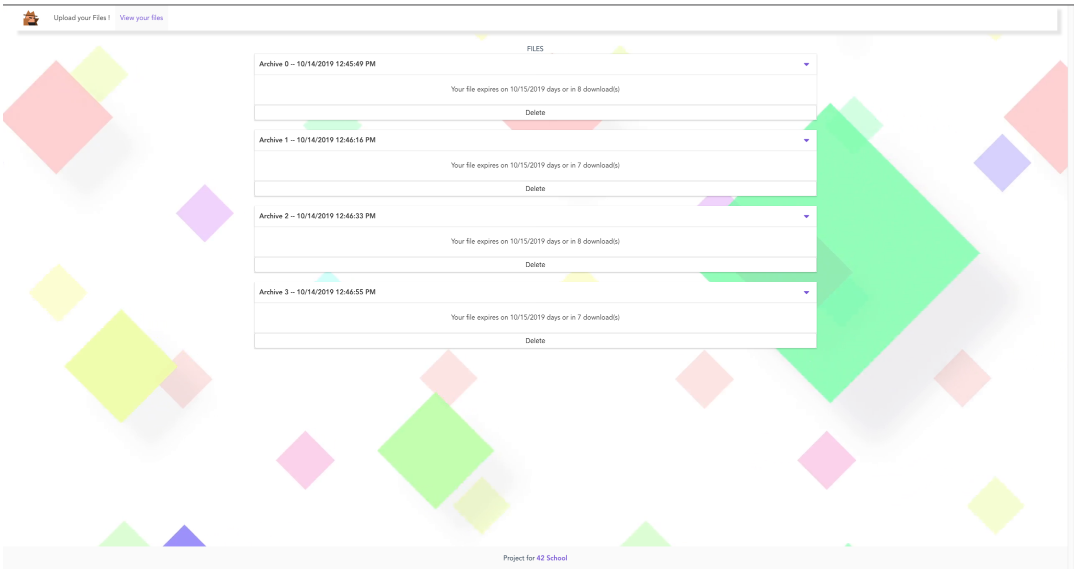
> *If corruption is detected, the client app cancels the ongoing download and shows an error message*



File is corrupted

The file no longer exists

9. The owner* can view his file(s). For each file, show number of downloads left and link's expiry date



FILES

Archive 0 -- 10/14/2019 12:45:49 PM

Your file expires on 10/15/2019 days or in 8 download(s)

Archive 1 -- 10/14/2019 12:46:16 PM

Your file expires on 10/15/2019 days or in 7 download(s)

Archive 2 -- 10/14/2019 12:46:33 PM

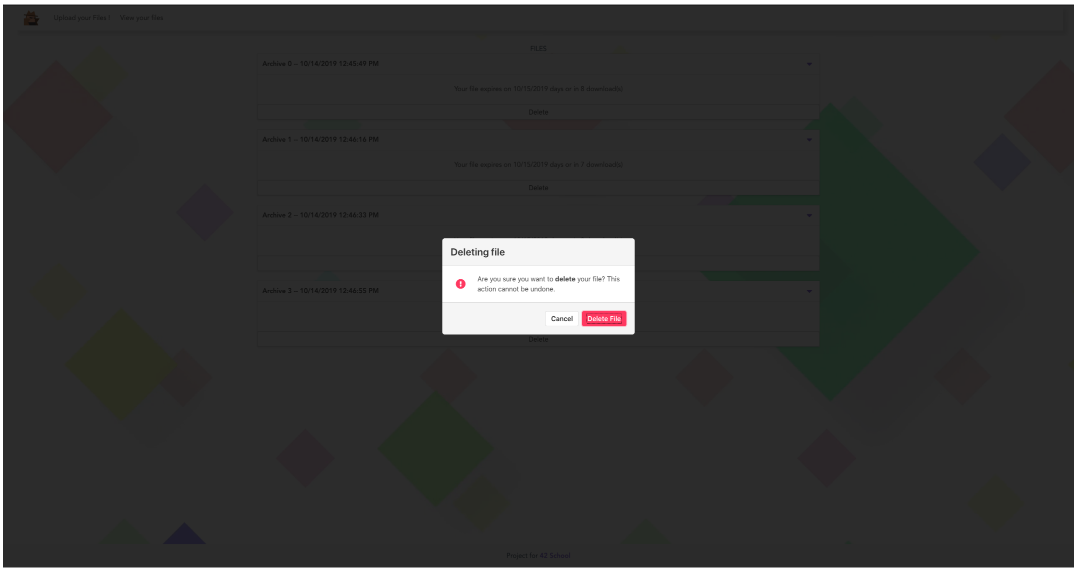
Your file expires on 10/15/2019 days or in 8 download(s)

Archive 3 -- 10/14/2019 12:46:55 PM

Your file expires on 10/15/2019 days or in 7 download(s)

> *When download link expire, the file(s) is removed from server*

10. Only the owner* of the file(s) can delete them



Archive 0 -- 10/14/2019 12:45:49 PM

Your file expires on 10/15/2019 days or in 8 download(s)

Archive 1 -- 10/14/2019 12:46:16 PM

Your file expires on 10/15/2019 days or in 7 download(s)

Archive 2 -- 10/14/2019 12:46:33 PM

Archive 3 -- 10/14/2019 12:46:55 PM

Deleting file

Are you sure you want to **delete** your file? This action cannot be undone.

> *File must not exist anywhere on the server after the delete*

11. The server checks if the client has the secret key before sending metaData or Files

> *Warning! Don't send the secret key to the server*

12. If there is metadata on server. The metadata must be encrypted with another key than the files

13. The content of the file must not be accessible even if a spy sees all the exchanges with the server. or if the server is hacked and all these data are stolen.

**owner: the one who uploaded the file(s)*

Possible bonuses

1. The user can set a password for the uploaded file(s)

   > *It will be prompted when someone tries to download the file(s)*
   > *The download link alone is not enough*

2. Admin page:
   - The admin can:
     - Delete file(s)
     - View number of all file(s) uploaded
   - The admin cannot:
     - View the content of the file(s)
     - View names of the file(s)
     - Know the secret key/ or password
3. Rename file(s)s and archives*
4. Progress bar on download/upload ;)

*archive: is the file that will be downloaded by the client. It contains all the files sent. (archive.zip or archive.tar.gz...)

> *When the site is in production, your very nice* ***Boss*** *will give you an SSL certificate. So all your exchanges will be in HTTPS. For convenience, the project does not need to set the https.*