



Design and build secure file transfer service with Laravel and Heroku

by Mykola Bubelich # Vienna PHP 04/2017

Mykola Bubelich

Experienced full stack software developer

JavaScript/Python/PHP/HTML/CSS/Linux/Networking

fb.com/thesimj

github.com/thesimj

www.bubelich.com

** This is my first talk on meetup, especially in English.*

Please, keep calm and do not throw tomatoes on me



I have a dream...

- Martin Luther King, Jr.

Now everyone tries to get as much information about users as possible and then sell it or use it to sell you goods / services / etc.



Requirement:

- Transfer up to 500 Mb
- Client-side encryption/decryption and integrity check
- Store limited time, up to 7 days
- Provide link only for one/two download
- Server and owner have zero knowledge about files
- Pass all security tests with highest rank
- FAST, REALLY FAST
- Cheap and easy maintenance



CryptoEsel

only he can do this

our savior from nsa, mi6, fsb and others

Why CryptoEsel?

Donkeys are used by people on scale of thousands of years and never fail

And now, when we have such strong machines, but in some cases we can rely only on donkeys

Donkey are triple S

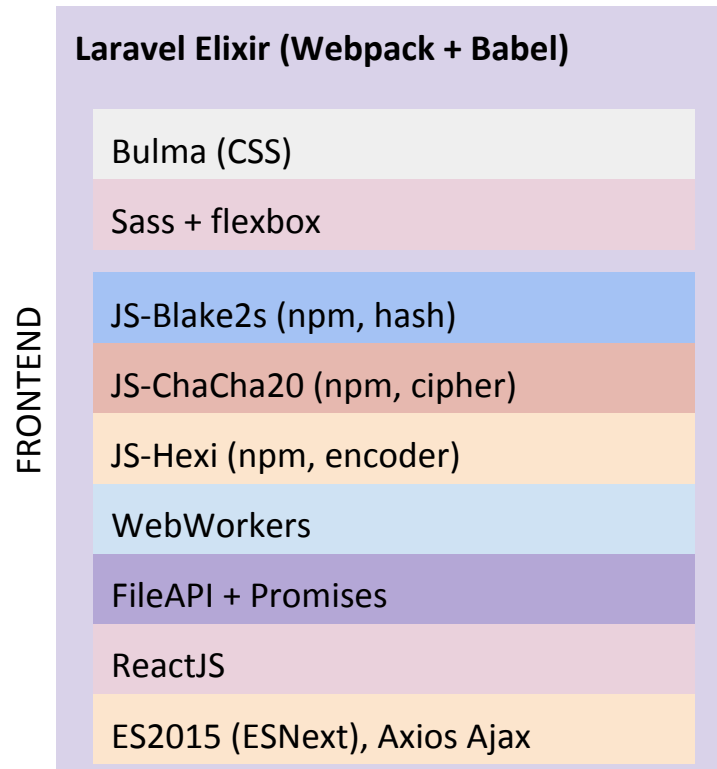
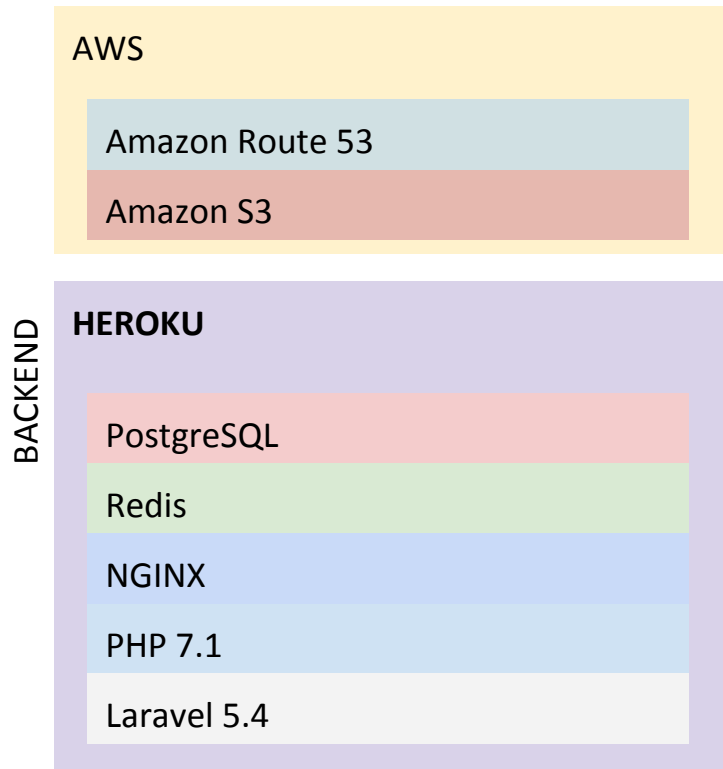
- Strong
- Smart
- Small

and of course they are perfect transport for any kind of stuff and they don't care about what exactly do they deliver

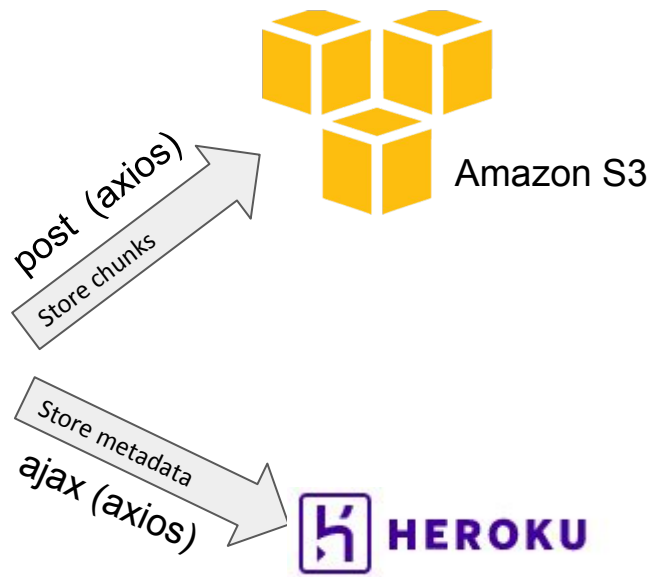
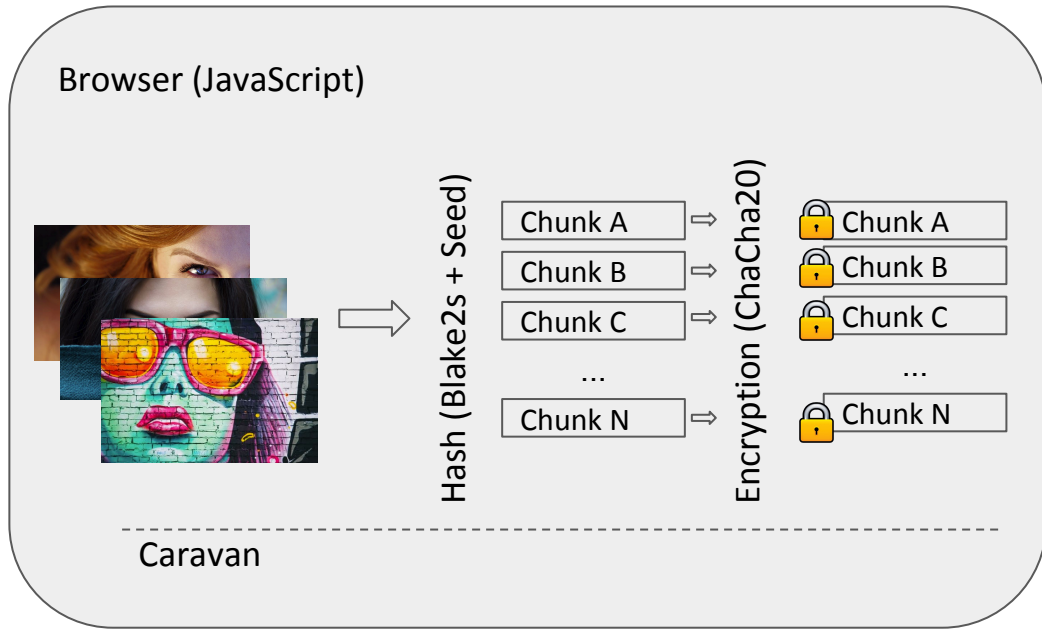
Make Donkey Great Again!



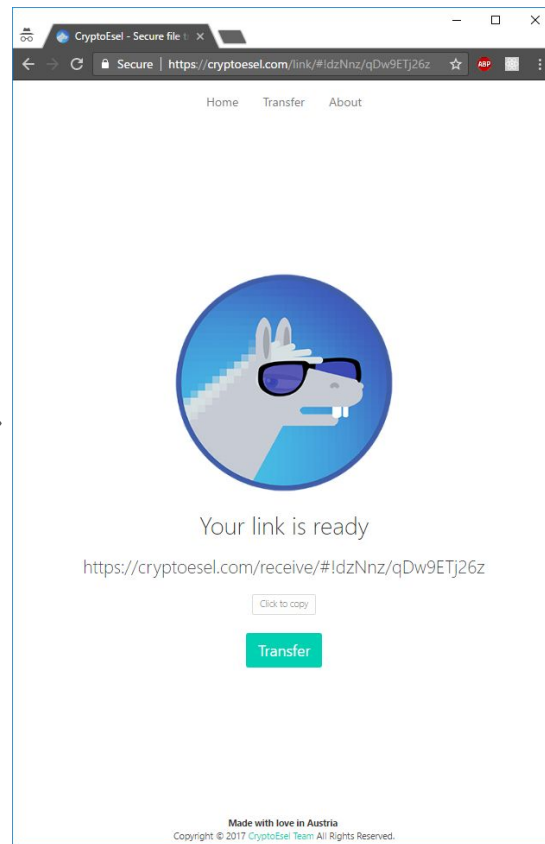
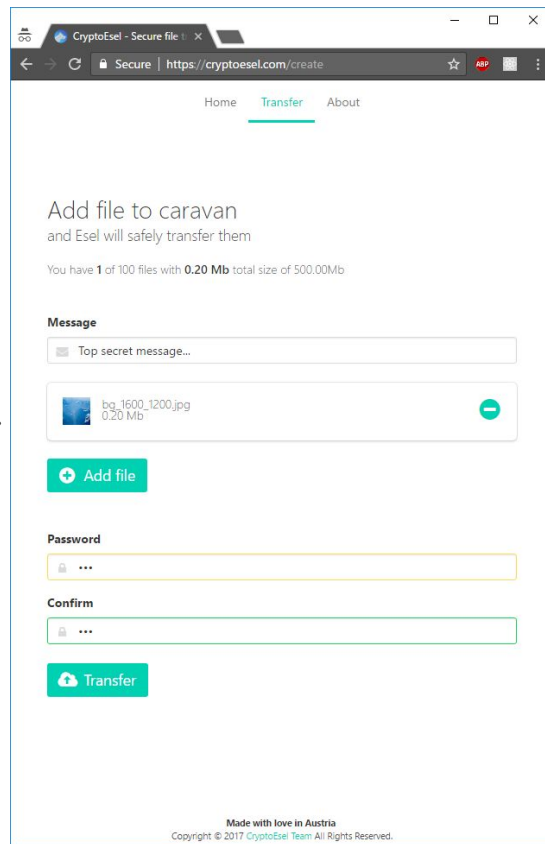
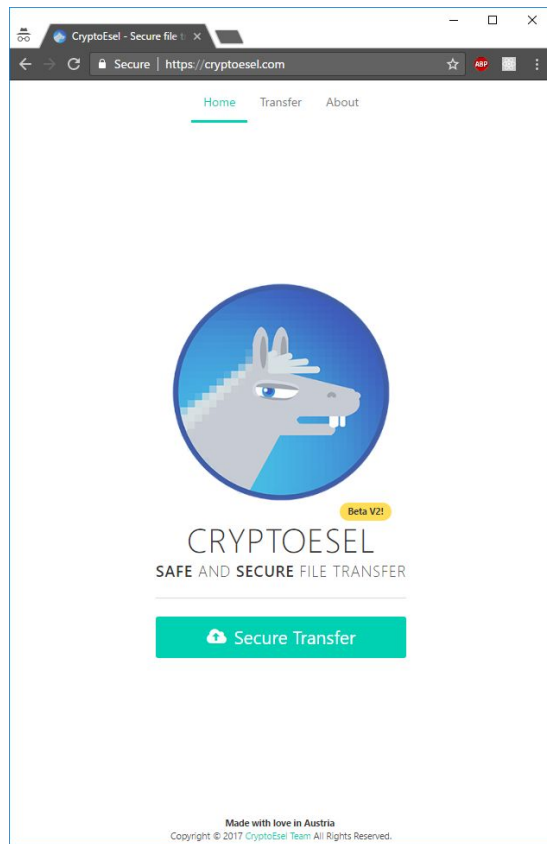
Technology stack



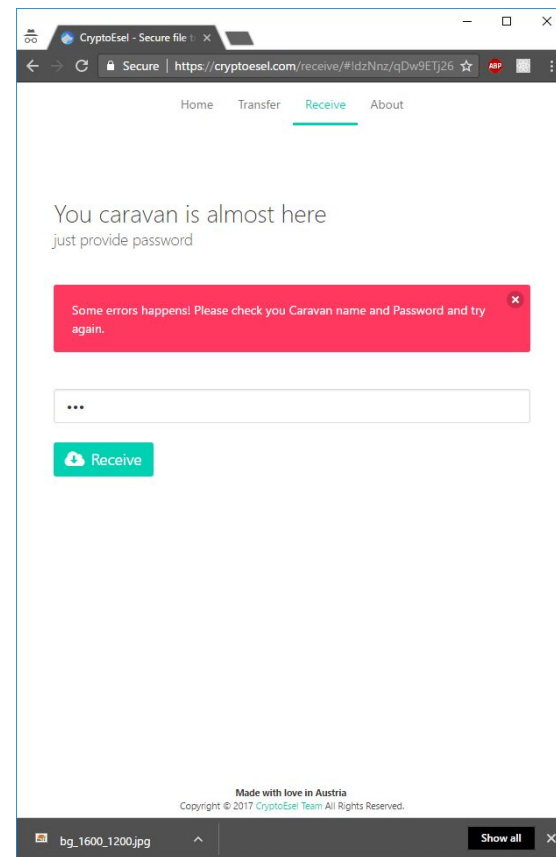
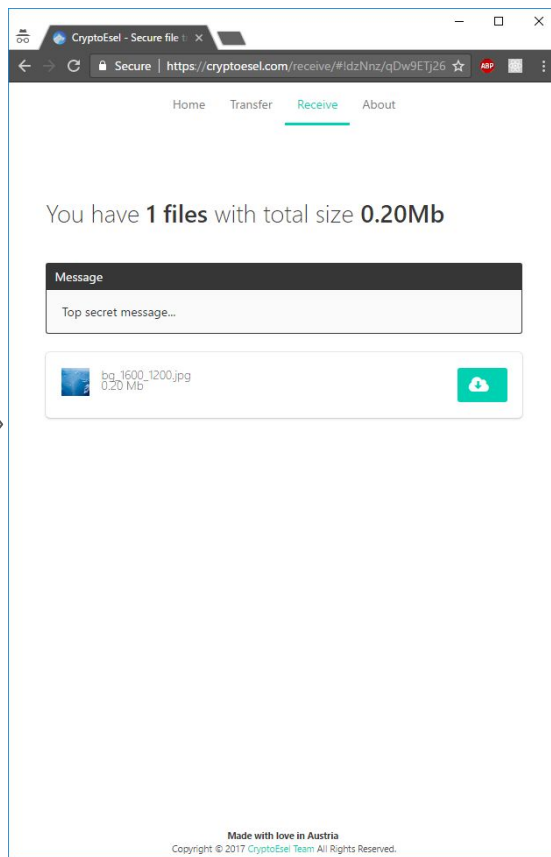
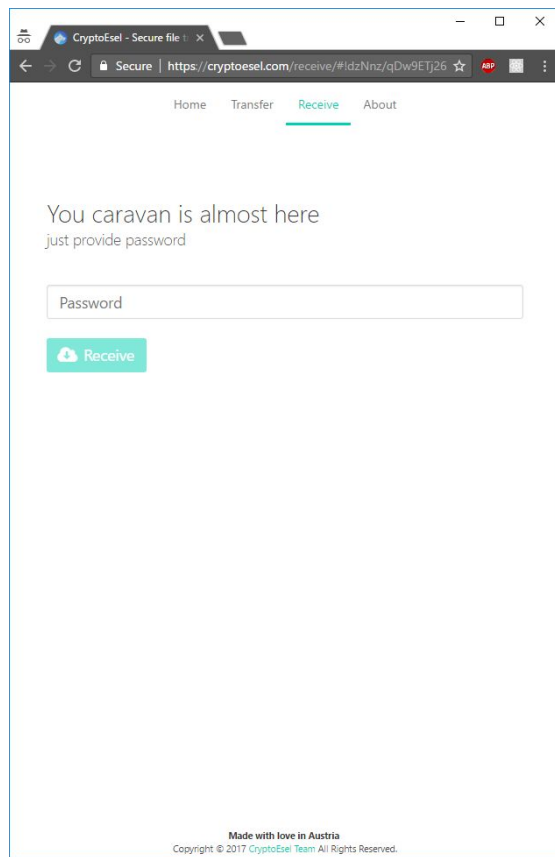
How it works (very simple)



Look and feel (Send file)



Look and feel (Receive file)



Laravel Routes

Simple API

/caravan/request

- send request for storing caravan (files)

/caravan/

- get information about caravan

/chunk/confirm/

- confirmation about storing files in AWS S3

/chunk/

- get chunk information

```
public function request(Request $request)
{
    $this->validate($request, [
        'caravan' => 'required|max:24',
        'data' => 'required|max:1048576',
        'mac' => 'required|max:64',
        'nonce' => 'required|max:16',
    ]);

    $hash = base64_encode(base64_decode($request->get('caravan')) . random_bytes(6));

    $caravan = new Caravan([
        'hash' => $hash,
        'data' => $request->get('data'),
        'mac' => $request->get('mac'),
        'nonce' => $request->get('nonce'),
    ]);

    $request = (new BucketController())->request($request->get('files'));

    $caravan->save();

    return json_encode([
        'hash' => $hash,
        'chunks' => $request
    ]);
}
```



PHP Laravel app directory

Models:

- Caravan

represents single caravan, stores metadata

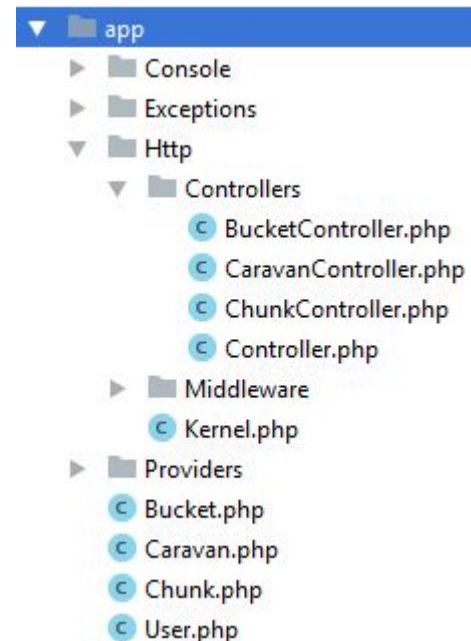
encrypted

- Bucket

represents single file, stores file chunks description

- Chunk

store information about chunk, nonce, and S3 link,
status and attempt counter



There is no way to find out a relation between a Caravan and a Bucket. Whole metadata is encrypted!



PHP Laravel app directory

Controllers:

- Caravan

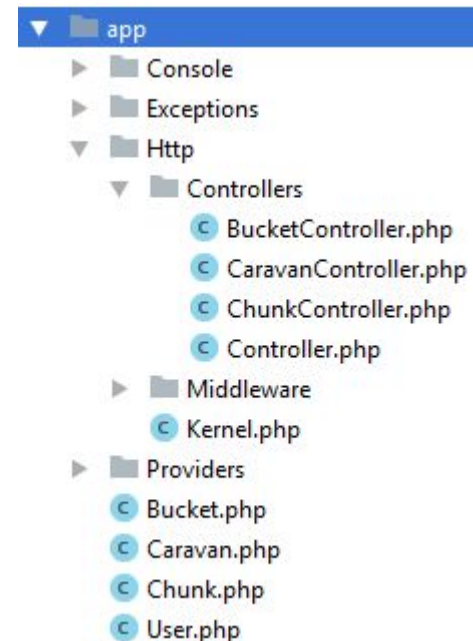
Controls request for caravan creation

- Bucket

Prepares chunks identifier for each chunk of file

- Chunk

Generates random ID for chunks and create signed request for storing file on Amazon S3





Database structure

Should be simple, fast and small. Use primary key, indexes and **no foreign keys**

	Caravan <ul style="list-style-type: none">- hash (id in link)- nonce- mac (integrity)- metadata (encrypted)- attempt

	Bucket <ul style="list-style-type: none">- hash- size- hashes [chunks...]- attempt

	Chunks <ul style="list-style-type: none">- hash- nonce- request (ID)- key (S3 path)- attempt- status

The no connection in databases. Information about a relation users can get only when decrypt metadata of the Caravan with proper ID and password



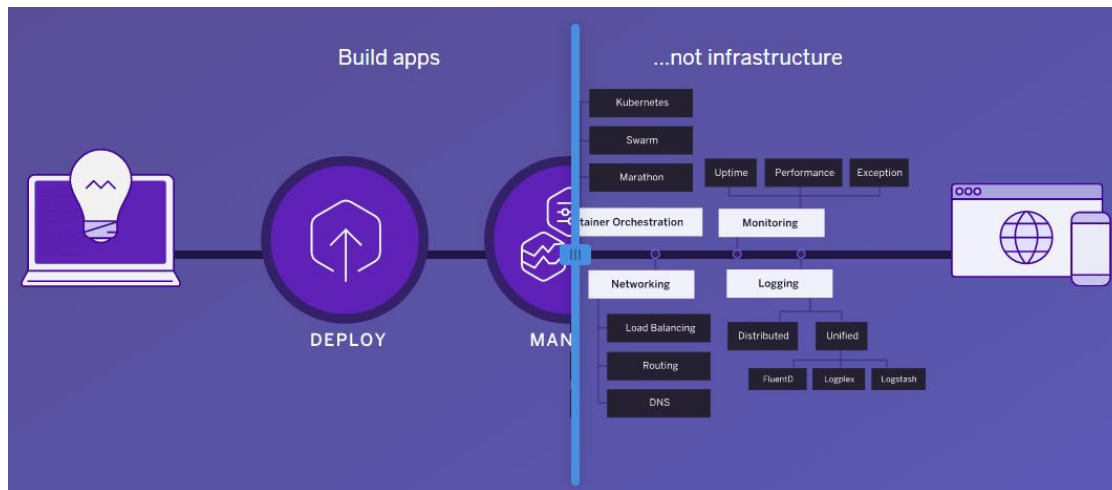
Database example (Chunks table)

reques hash	key	nonce	size	attempt	status	created_at	updated_at
6073 qYG4WCB91ZHNOePLoUAGtfZXmxQm6FTsvnK6fUk8skE=	v2/1d3a909aa6a72c4c195a9ce15384e86ad8999ac9f38f2061506e7bdaa735e496	WcFUvqVib7PwGChl	1048576	1	1	2017-04-11 18:39:31	2017-04-11 18:44:03
6650 tTVgig08Wnjd6PgSHEbfGMLi9OhYjaQx8kg/c1TomTg=	v2/c76616395f0dcdf239757dae375b10acc5f8c378fda5e643a55d2d0c0c2633c	6kfGkcsBPhwnpqXN	1048576	1	1	2017-04-11 18:39:31	2017-04-11 18:44:03
2983 Z7zG4Kzvkcd+ +YdyoCZQ5r2XtFI0HCQqhvKNQc06SYE=	v2/3c85af41fdc56a099a1d8e478e9df0276c7e33a058990a2b2380165fd705505b	Xx85hrlab55EHa0q	1048576	1	1	2017-04-11 18:39:31	2017-04-11 18:44:03
4176 zgVQ8s5F8J1jc6NPPPP2H6cWDY2zqD1oRq3M/1KadKNo=	v2/6b97b94516baf3aa70397ada653f6b8e82c6ff6d960705d8ac1c671f18dccc192	HRrQxLe2l9iFM5UI	1048576	1	1	2017-04-11 18:39:31	2017-04-11 18:44:03
6145 m08Q3l/szNd8ZyZfV6Z42e91ZNQMknFf1kN0xvqE=	v2/d876b8656dbb47f0b07ccde4bd3706bb7b93304b9fb1f65344419269f498ed73	BufhmKK4d2bdbbezO	1048576	1	1	2017-04-11 18:39:31	2017-04-11 18:44:04
5229 2jKDIRPX7FpyYbxfKoE4EYL0NQ3Ty16OGWIFkHeUvm8=	v2/7d3af7563933caf51b2ff64a6fdcad195fe151ac2981822379809beb2bfff6789	iOMhEycvUB7QoHm9	1048576	1	1	2017-04-11 18:39:31	2017-04-11 18:44:04
5520 MSU/HZ54JcN0Eaj/VR8OYDVZmxvL5EgG0Xqk5XWVFnA=	v2/152b760367d973b1e72d34087fdd10324f63e09a4ef4b38dd06aa6342cef234d	wl5+D1OIBgTylqMn	1048576	1	1	2017-04-11 18:39:31	2017-04-11 18:44:04
7134 NI6/sNvTs3umd9XrvUVXHPNPCwCBHRFILSlkMlo5nXc=	v2/b14fe9fc76e5bf9f29911f37a1ac834cd18c5348a2f0afa0268a02a1ab36c126	Tb7Wj3J5bTgtqgMt	1048576	1	1	2017-04-11 18:39:31	2017-04-11 18:44:04
6268 ibROPcnWNzlDouNfdyohWRg53ur4IEOD2HNgr9svtRY=	v2/68049a5c89f7a4e31648077de4e6314927c49d47a52dfdb1d4409dee5da620b6	czCHn+slcDC1TrLE	1048576	1	1	2017-04-11 18:39:31	2017-04-11 18:44:04
6383 WABbdFjWf7rUUXZ7Ex0MVHle0qxVHuoZEDHd6XTCm0c=	v2/4237e08d2debe4e1ce32e887a267832d7b24cb454b1de661e7947da9baff67f7	n5O+7mZmEYJJZazf	1048576	1	1	2017-04-11 18:39:31	2017-04-11 18:44:04
9298 OXioX9EiOximky6HRCrvu8VKd7EzrsxOMpo90TBLKI=	v2/c05facb57d452948ceb94e4cc71d44098300f4e4540bba0b5b273d3315bc2462	E86VkoE87VxHqtzK	1048576	1	1	2017-04-11 18:39:31	2017-04-11 18:44:04
5112 BCoxsJIFRI4mYfK7pd60lPaB/x6UozWnQJOvVcY1+ s=	v2/93cb44f14127240a29f38979ec5d040b13d00a447da80f44640d57dc2b6e	yyXgvpPPxhi3KKFT	1048576	1	1	2017-04-11 18:39:31	2017-04-11 18:44:04
9972 lZY4xMWTSL+ MSLq4Gz0NK4TE2n4lPpdPcDd4A7sMFI=	v2/6c10bb8abfd2b71282441bafce942b11563498e9a36dfe35756b000b6b2ccf25	APFDO+WDqJwQpCzH	1048576	1	1	2017-04-11 18:39:31	2017-04-11 18:44:04
1846 lwgaf6yZjRN5FiuOjCbBUEOZprMwvGWgB0P0akOWZKc=	v2/e8f1a5746b2d37d5897f52103fd3df0fe408d876b3189b73b0eb78a10df73c9d	5HV55w/OiZwLr/A	1048576	1	1	2017-04-11 18:39:31	2017-04-11 18:44:04
8187 GcN8Nq2lGQpqtQ5JjdTMEql6ca0S/HpOfOfRqd4CA+ c=	v2/8c47be9181a3ec8692719e4ab286db2d41537f8b1984ef9f0b99014ccddac08e	h/+Hd79uOXnvVGRO	1048576	1	1	2017-04-11 18:39:31	2017-04-11 18:44:04
3411 UKNXKB503MdVCNmp13DqTb1T1xlkjLNTc9CEzmtw=	v2/6623f297e93fd91895a88e39cf34230fdd112b9ee188f1845e0e74e1d61ae3	OmGFY3g3A89elqXD	1048576	1	1	2017-04-11 18:39:31	2017-04-11 18:44:04
5343 KIKN9xw6mC2YyL9Slo7sMrwkScNCp9yCvNjH0gJNVU=	v2/0704c06e47b7be4454d16e01d94488b25d299067ee271b1b1a659adcd6a1a28a	y0KLsLbu+RLInMAQ	1048576	1	1	2017-04-11 18:39:31	2017-04-11 18:44:04
2162 uBLLOZefzH2Psz49vQVHmHlyACbFD5omuu/rUVV2cco=	v2/4becb190724c43947f246c7783571a7e534f2e0cd3ba89b412b11c2343dea92a	eOrDXdaDUUXEyV2R	1048576	1	1	2017-04-11 18:39:31	2017-04-11 18:44:04
9866 oQ8si3LQJE1BRmP9x7inMadHm4x8OzU/m/mjPlfxWi+Y=	v2/cfd73110e3ea14f2e247ce21a21e95bede9d81218a31531cb52be4db7072b8	+7e2tM0QCrXJSull	1048576	1	1	2017-04-11 18:39:31	2017-04-11 18:44:04
3298 fmUK3DNI5iSVZ9shxTPg8fzKrScqhqPjGo0eOP+w=	v2/4092a4df926a690834f96cef227f1c1de64b814a9d95db1b36e154971df5a3d	+l26/zubnwela98t	1048576	1	1	2017-04-11 18:39:31	2017-04-11 18:44:03

What is Heroku (PaaS)



"Heroku is a cloud platform that lets companies build, deliver, monitor and scale apps — we're the fastest way to go from idea to URL, bypassing all those infrastructure headaches." (C) Heroku





Configure Nginx on Heroku PHP buildpack

Security header

```
add_header Public-Key-Pins 'pin-sha256="....."; max-age=2592000; includeSubDomains' always;  
add_header Strict-Transport-Security "max-age=63072000; includeSubdomains; preload";  
add_header Content-Security-Policy "img-src 'self' data: blob;; default-src https:";  
add_header X-Frame-Options "DENY";  
add_header X-Content-Type-Options "nosniff";  
add_header X-XSS-Protection "1; mode=block" always;  
add_header Referrer-Policy "no-referrer";
```

Force the latest IE version

```
add_header "X-UA-Compatible" "IE=Edge";
```

Set max client body

```
client_max_body_size 2M;
```


Deploy on Heroku

1. git commit -am "update version"

```
[master ef4d17a] update version
```

```
1 file changed, 1 insertion(+)
```

2. git push heroku

```
Counting objects: 4, done.
Delta compression using up to 4 threads.
Compressing objects: 100% (3/3), done.
Writing objects: 100% (4/4), 337 bytes | 0 bytes/s, done.
Total 4 (delta 2), reused 0 (delta 0)
remote: Compressing source files... done.
remote: Building source:
Remote:
remote: -----> PHP app detected
remote: -----> Bootstrapping...
remote: -----> Installing platform packages...
remote:    - php (7.1.3)
remote:    - ext-mbstring (bundled with php)
remote:    - apache (2.4.20)
remote:    - nginx (1.8.1)
remote: -----> Installing dependencies...
remote:    Composer version 1.4.1 2017-03-10 09:29:45
remote:    Loading composer repositories with package information
remote:    Installing dependencies from lock file
remote:    Package operations: 31 installs, 0 updates, 0 removals
.....
```

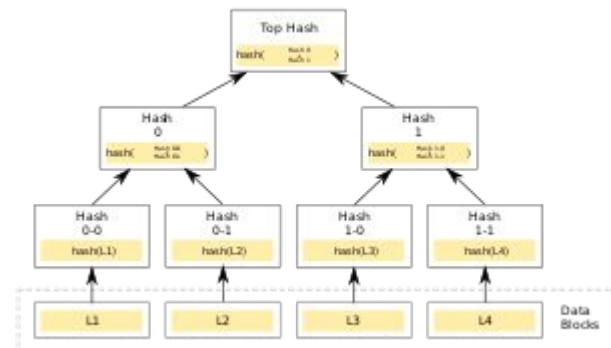
Cryptographic primitives used in client side (JS)

Symmetric cipher - ChaCha20

- ChaCha20 is a stream cipher designed by D. J. Bernstein. It is a refinement of the Salsa20 algorithm, and it uses a 256-bit key.
- 256-bit key, a 64-bit nonce, and a 64-bit stream position to a 512-bit block of the key stream
- Own JavaScript implementation (<https://www.npmjs.com/package/js-chacha20>)

Cryptographic Hash and Message Authentication Code (MAC) - Blake2s

- BLAKE2 is a cryptographic hash function faster than MD5, SHA-1, SHA-2, and SHA-3
- Output max 256-bit, key 256-bit, salt 64-bit and personalization 64-bit long
- Own JavaScript implementation (<https://www.npmjs.com/package/js-blake2s>)



Upcoming in new version v3

Public-Private Elliptic Curve25519

- Curve25519 is an elliptic curve offering 128 bits of security and designed for use with the elliptic curve Diffie–Hellman (ECDH) key agreement scheme designed by D. J. Bernstein.

Merkle tree

- Hash trees allow efficient and secure verification of the contents of large data structures. Will be used to hash chunks of file and files of a Caravan

Pass the tests and show me results

We test our service and get highest rank

- securityheaders.io
- ssllabs.com/ssltest
- gtmetrix.com

Local result for page speed on Chrome (no cache)


Name	Method	Status	Protocol	Scheme	Type	Initiator	Size	Time	Waterfall	400.00 ms	600.00 ms
cryptoesl.com	GET	200	http/1.1	https	document	Other	6.4 KB	58 ms			
style.156be233719bc72f86b9.css	GET	200	http/1.1	https	stylesheet	(index)	135 KB	130 ms			
coolese1.png	GET	200	http/1.1	https	png	(index)	34.4 KB	185 ms			
css?family=Roboto:400,500,700	GET	200	http/2+quic/...	https	stylesheet	(index)	1011 B	80 ms			
fontawesome-webfont.woff2?af7ae505a9eed50...	GET	200	http/1.1	https	font	(index)	76.2 KB	150 ms			
favicon-16x16.png	GET	200	http/1.1	https	png	Other	2.2 KB	55 ms			
favicon-32x32.png	GET	200	http/1.1	https	png	Other	3.2 KB	57 ms			
7 requests 258 KB transferred Finish: 566 ms DOMContentLoaded: 87 ms Load: 443 ms											

securityheaders.io



Analyse the HTTP response headers

Security Report Summary

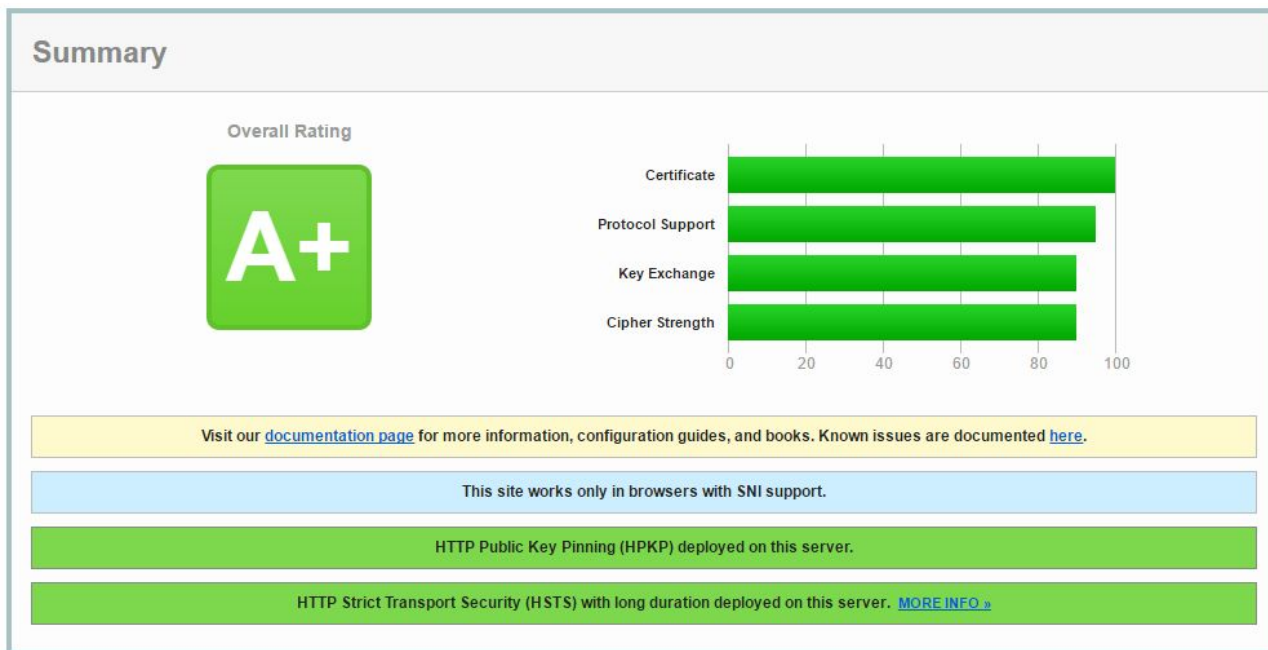


Site:	https://cryptoesel.com/
IP Address:	54.217.215.80
Report Time:	19 Apr 2017 14:14:52 UTC
Report Short URL:	https://schoi.io/NHv
Headers:	<div><div>✓ Public-Key-Pins</div><div>✓ Strict-Transport-Security</div><div>✓ Content-Security-Policy</div><div>✓ X-Frame-Options</div><div>✓ X-Content-Type-Options</div><div>✓ X-XSS-Protection</div><div>✓ Referrer-Policy</div></div>

www.ssllabs.com/ssltest



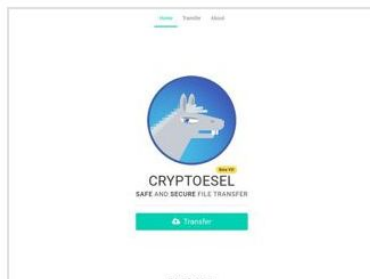
Deep analysis of the configuration of any SSL web server on the public Internet



gtmetrix.com



GTmetrix gives you insight on how well your site loads and provides actionable recommendations on how to optimize it



Latest Performance Report for: <http://cryptoesel.com/>

Report generated: Wed, Apr 19, 2017, 11:56 AM -0700

Test Server Region: 🇨🇦 Vancouver, Canada

Using: 🦊 Firefox (Desktop) 49.0.2, PageSpeed 1.15-gt1, YSlow 3.1.8

Performance Scores

PageSpeed Score

A (98%) ^

YSlow Score

A (93%) ^

Page Details

Fully Loaded Time

2.2s ^

Total Page Size

187KB ^

Requests

9 ^

CryptoEsel Team



Mykola Bubelich

Author of idea and frontend developer

<https://bubelich.com>



Maxi Schramm

Logo and page design

Graphic, web and motion graphics designer with a passion for 2D animation and Open Science.

<http://www.looove-design.com/>

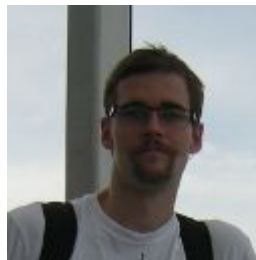


Oleg Rudenko

Architect mentor

Software architect with extensive experience in distributed systems, functional and reactive programming.

<https://www.linkedin.com/in/rudenk0/>



Stepan Grebeniuk

Security Advisor

Information security officer and consultant with 6+ years of experience in corporate security and in security research.

<https://www.linkedin.com/in/stepan-grebeniuk-25b0b955/>

And we are looking for you...

let's make internet private again!

Backend developers

UX/UI specialist

DevOps

Frontend developers

QA

others, with same ideology

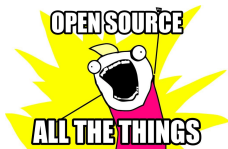
m+searching@bubelich.com

fb.com/thesimj



Thank you for listening

Question & Answers



Please contribute to this open source project

** No donkey was harmed in making of this service.*



<https://cryptoesel.com>
only donkey can keep your secrets...