2015 RuCTFE

ON

2015 ZERO NIGHTS

SERVICES WRITE-UPS

and more

Mikhail Vyatskov aka Tris

MOTIVATION

“The main goal of RuCTFE is to share experience and knowledge in the computer security and to have some fun together.”

— RuCTFE Rules

RULES

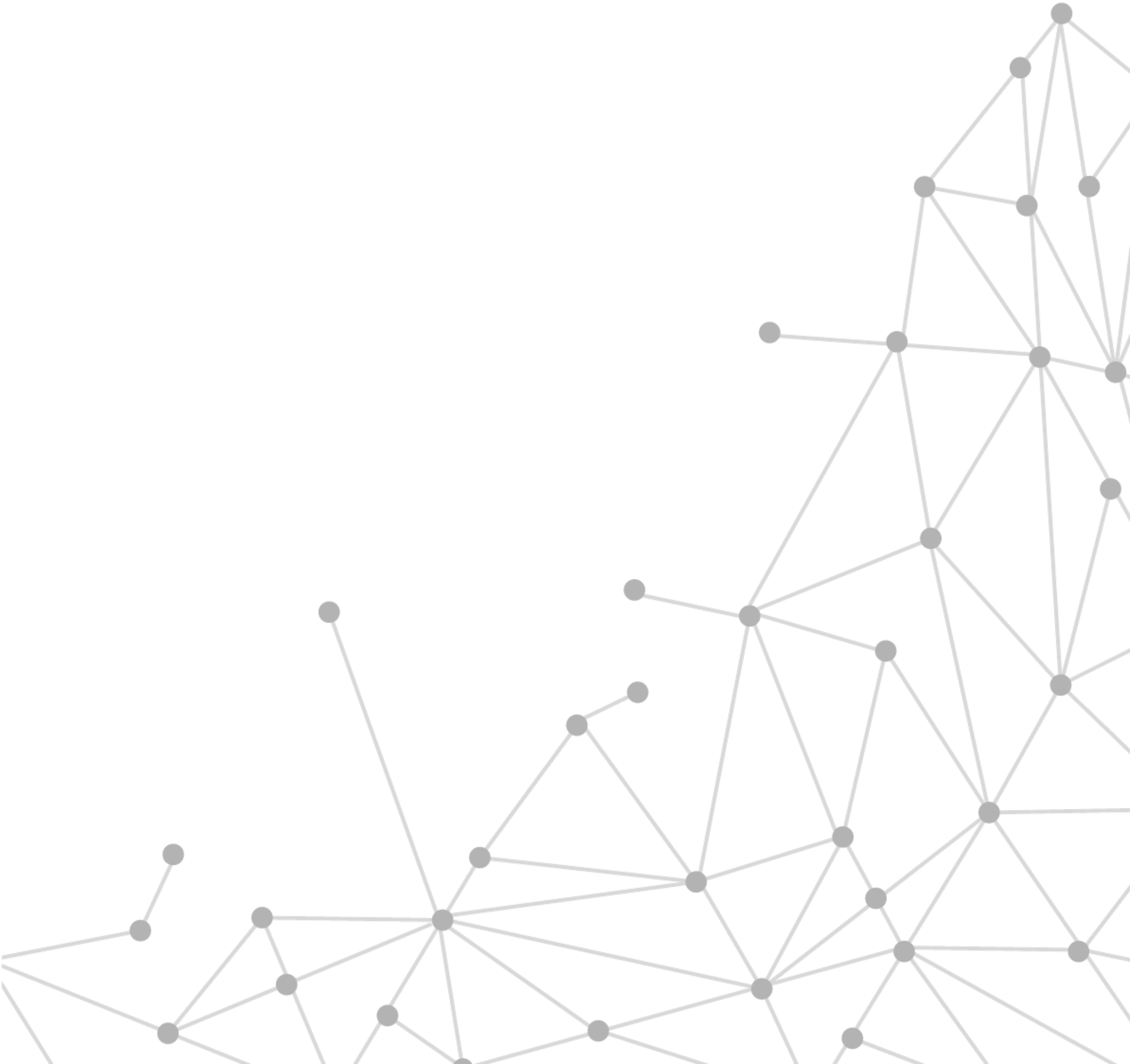
- Each team has an image
- There are some services on this image
- There are some vulnerabilities
- Hack em’ all!

MINISTRY OF LOVE

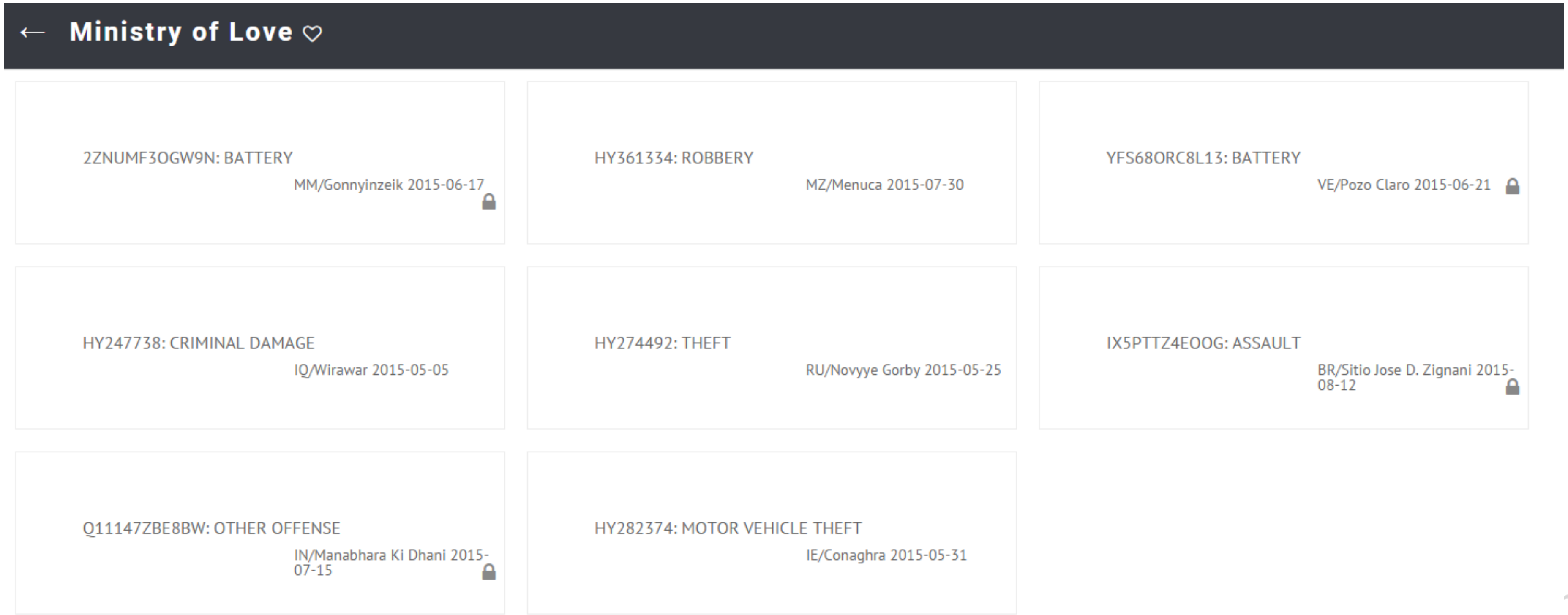
Maxim Muzafarov aka m_messiah

ABOUT SERVICE

- Python
- Tornado web server
- Momoko
- WebSockets



WATCH CRIMES



← Ministry of Love ♡

2ZNUMF3OGW9N: BATTERY
MM/Gonnyinzeik 2015-06-17 🔒

HY361334: ROBBERY
MZ/Menuca 2015-07-30

YFS68ORC8L13: BATTERY
VE/Pozo Claro 2015-06-21 🔒

HY247738: CRIMINAL DAMAGE
IQ/Wirawar 2015-05-05

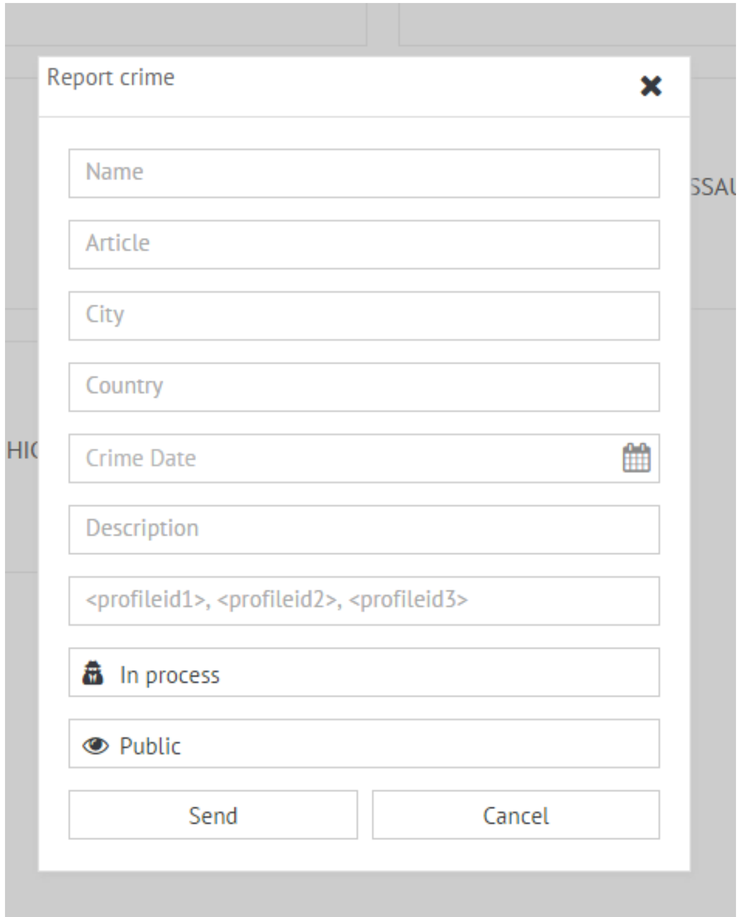
HY274492: THEFT
RU/Novyye Gorby 2015-05-25

IX5PTTZ4EOOG: ASSAULT
BR/Sitio Jose D. Zignani 2015-08-12 🔒

Q11147ZBE8BW: OTHER OFFENSE
IN/Manabhara Ki Dhani 2015-07-15 🔒

HY282374: MOTOR VEHICLE THEFT
IE/Conaghra 2015-05-31

REPORT A CRIME



Report crime ✖

Name

Article

City

Country

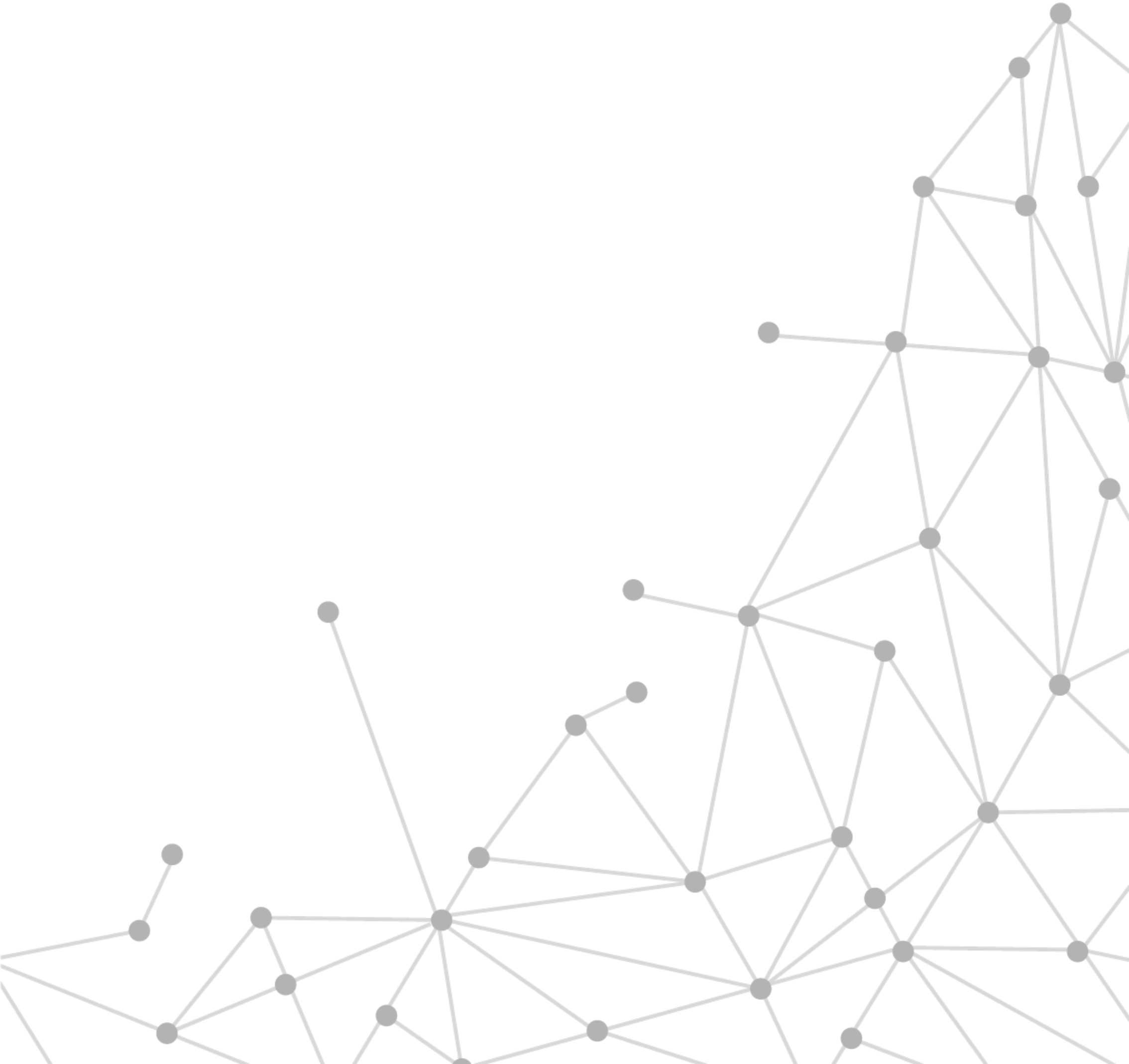
Crime Date

Description

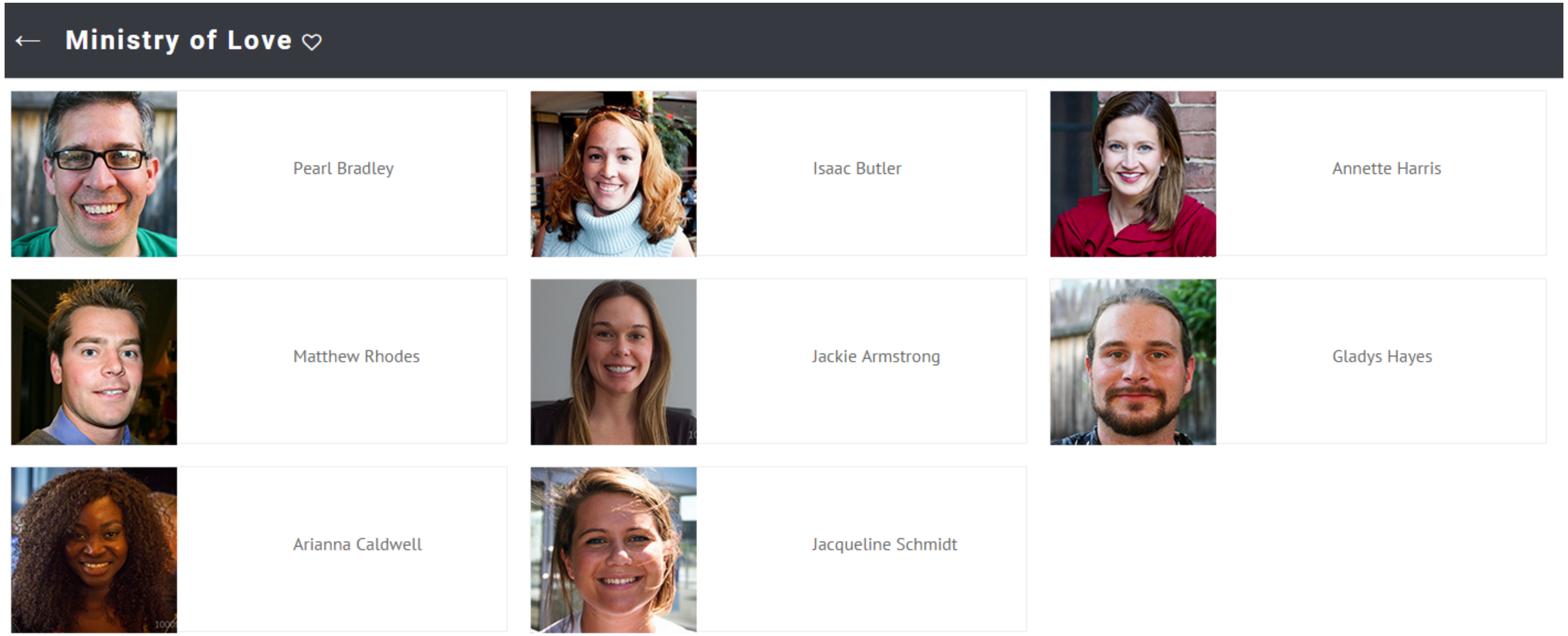
<profileid1>, <profileid2>, <profileid3>

In process

Public



AUTHENTICATE



← Ministry of Love ♡

Pearl Bradley

Isaac Butler

Annette Harris

Matthew Rhodes

Jackie Armstrong

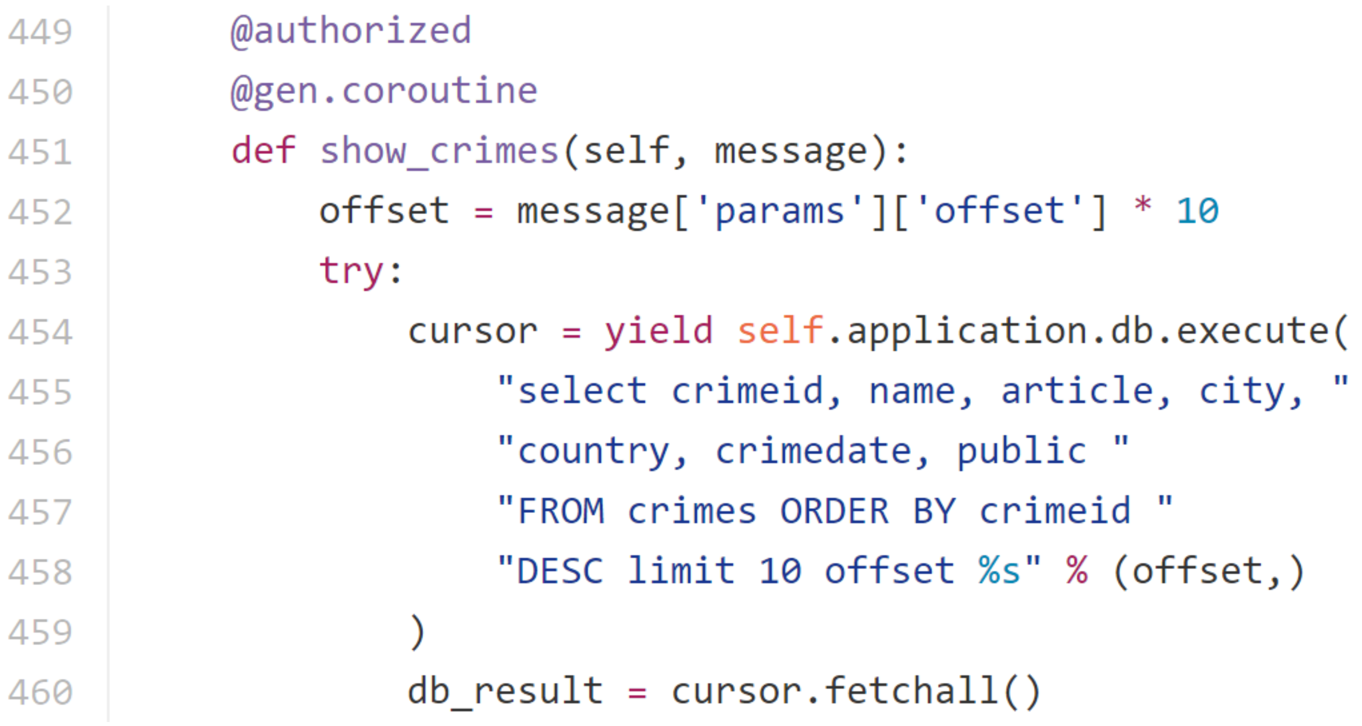
Gladys Hayes

Arianna Caldwell

Jacqueline Schmidt

HACK IT!

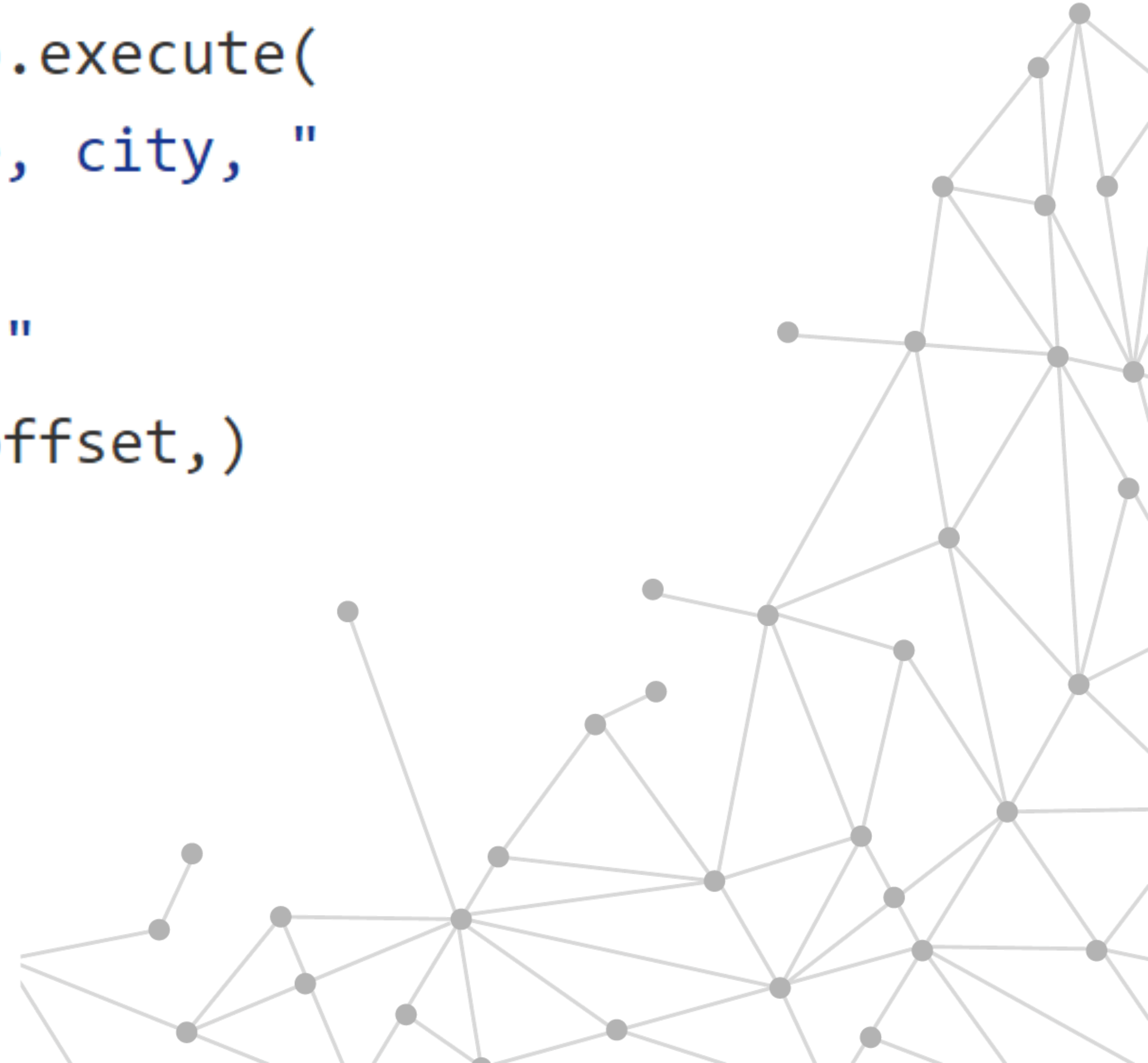
SQL INJECTION



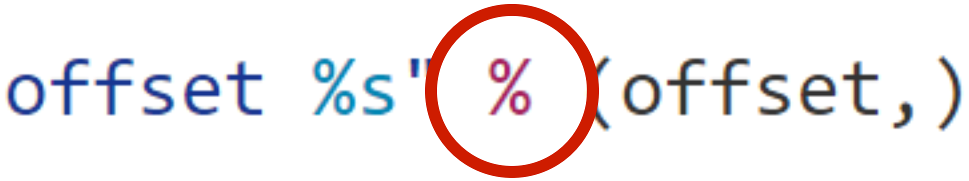
```
@authorized
@gen.coroutine
def show_crimes(self, message):
    offset = message['params']['offset'] * 10
    try:
        cursor = yield self.application.db.execute(
            "select crimeid, name, article, city, "
            "country, crimedate, public "
            "FROM crimes ORDER BY crimeid "
            "DESC limit 10 offset %s" % (offset,)
        )
        db_result = cursor.fetchall()
```

SQL INJECTION

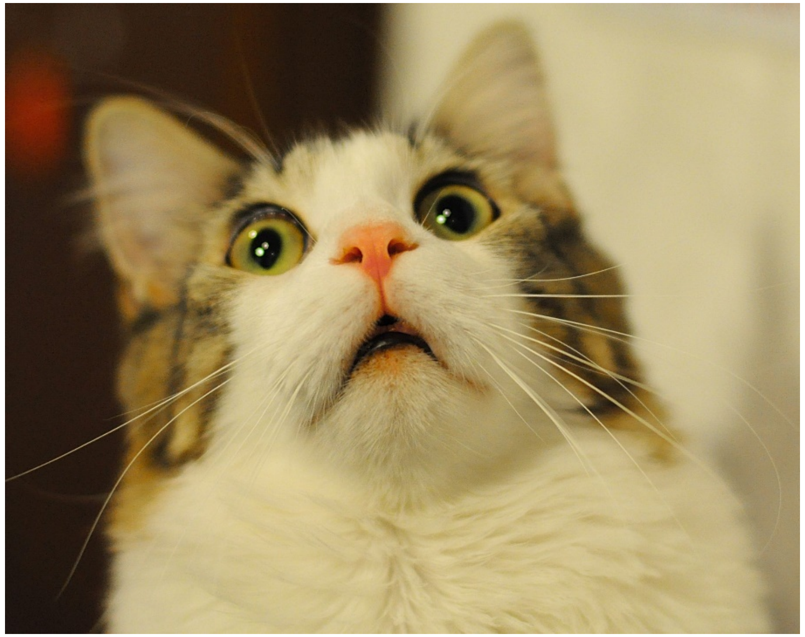
```
cursor = yield self.application.db.execute(
    "select crimeid, name, article, city, "
    "country, crimedate, public "
    "FROM crimes ORDER BY crimeid "
    "DESC limit 10 offset %s" % (offset,)
)
```



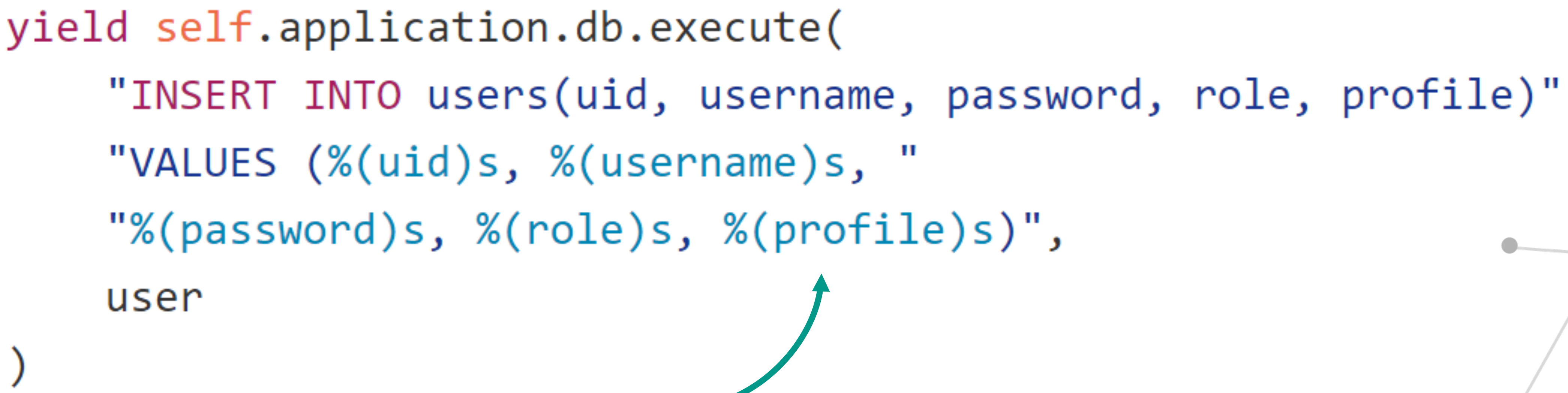
SQL INJECTION



```
offset %s" % (offset,)
```



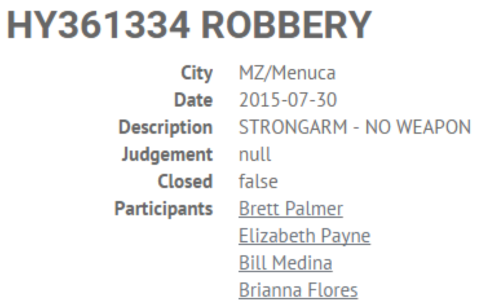
PROFILE SPOOFING



```
yield self.application.db.execute(
    "INSERT INTO users(uid, username, password, role, profile)"
    "VALUES (%(uid)s, %(username)s, "
    "%(password)s, %(role)s, %(profile)s)",
    user
)
```

Bind profile
without authentication

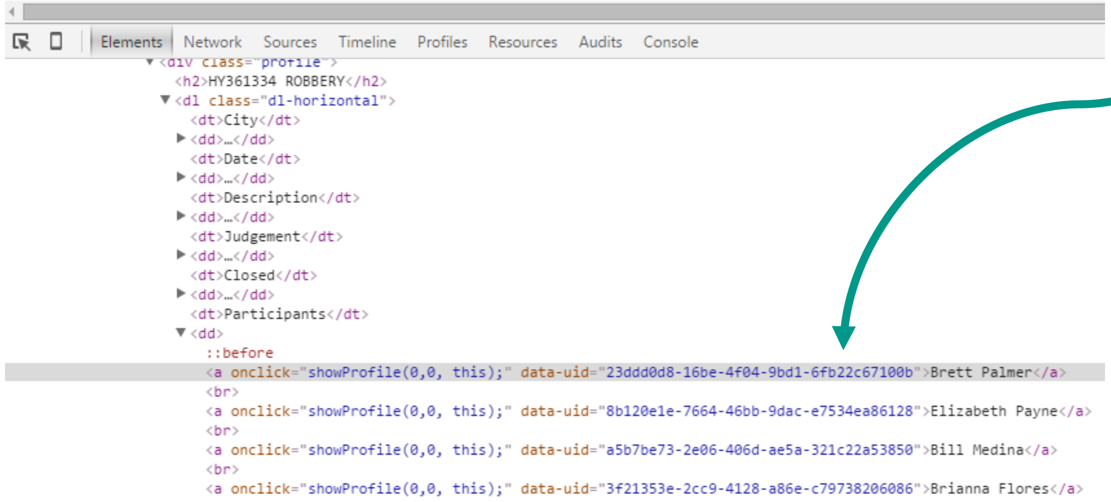
PROFILE SPOOFING



HY361334 ROBBERY

City	MZ/Menuca
Date	2015-07-30
Description	STRONGARM - NO WEAPON
Judgement	null
Closed	false
Participants	Brett Palmer Elizabeth Payne Bill Medina Brianna Flores

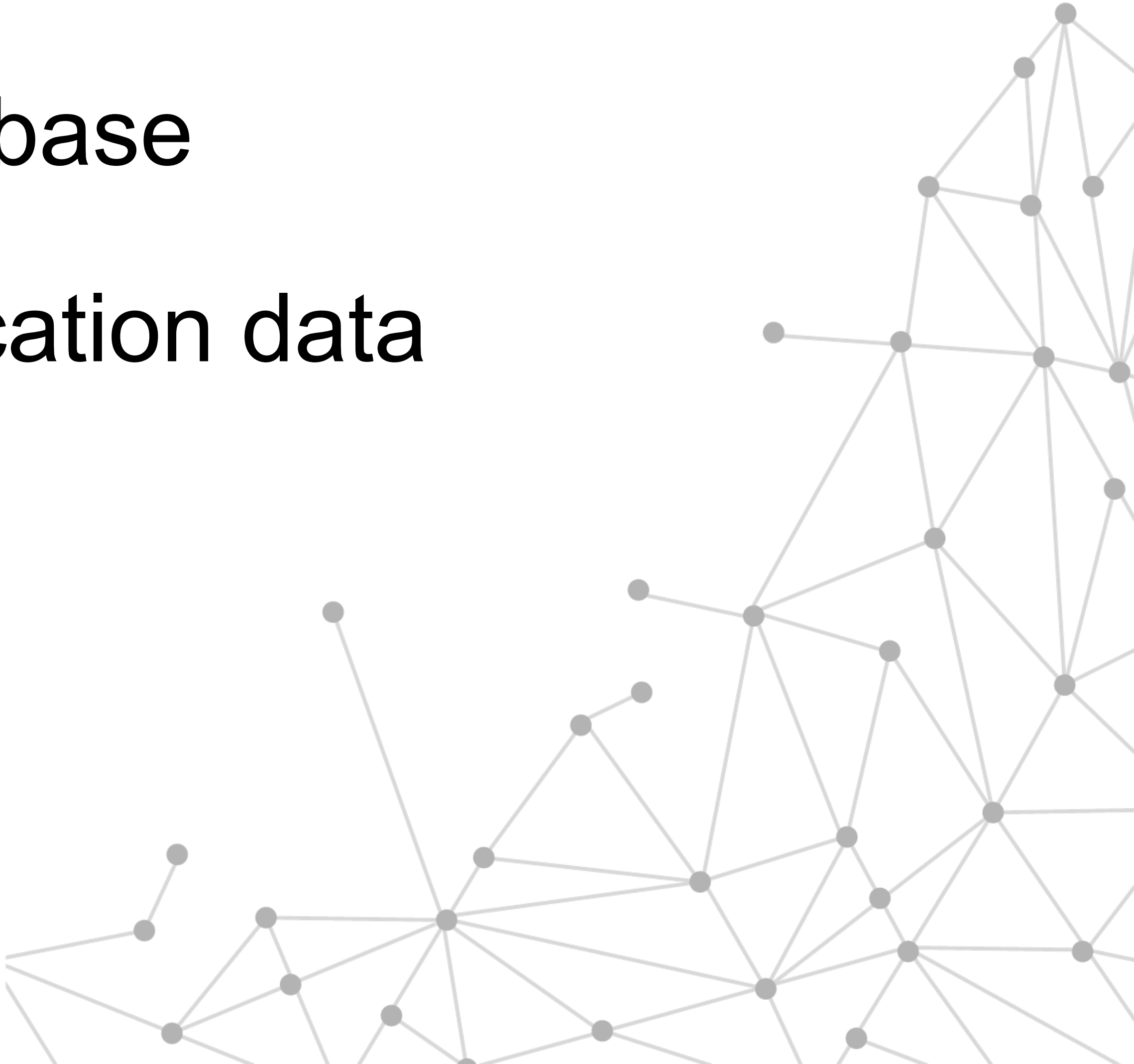
Profile ids are visible in open crimes



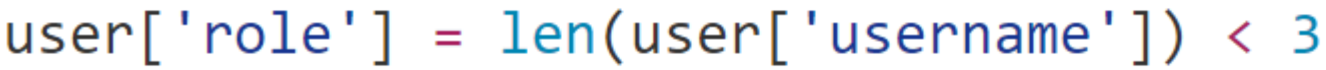
```
▼<div class="profile">
   <h2>HY361334 ROBBERY</h2>
  ▼<dl class="dl-horizontal">
     <dt>City</dt>
    ▶<dd>…</dd>
     <dt>Date</dt>
    ▶<dd>…</dd>
     <dt>Description</dt>
    ▶<dd>…</dd>
     <dt>Judgement</dt>
    ▶<dd>…</dd>
     <dt>Closed</dt>
    ▶<dd>…</dd>
     <dt>Participants</dt>
    ▼<dd>
       ::before
       <a onclick="showProfile(0,0, this);" data-uid="23ddd0d8-16be-4f04-9bd1-6fb22c67100b">Brett Palmer</a>
       <br>
       <a onclick="showProfile(0,0, this);" data-uid="8b120e1e-7664-46bb-9dac-e7534ea86128">Elizabeth Payne</a>
       <br>
       <a onclick="showProfile(0,0, this);" data-uid="a5b7be73-2e06-406d-ae5a-321c22a53850">Bill Medina</a>
       <br>
       <a onclick="showProfile(0,0, this);" data-uid="3f21353e-2cc9-4128-a86e-c79738206086">Brianna Flores</a>
```

SAME DATABASE

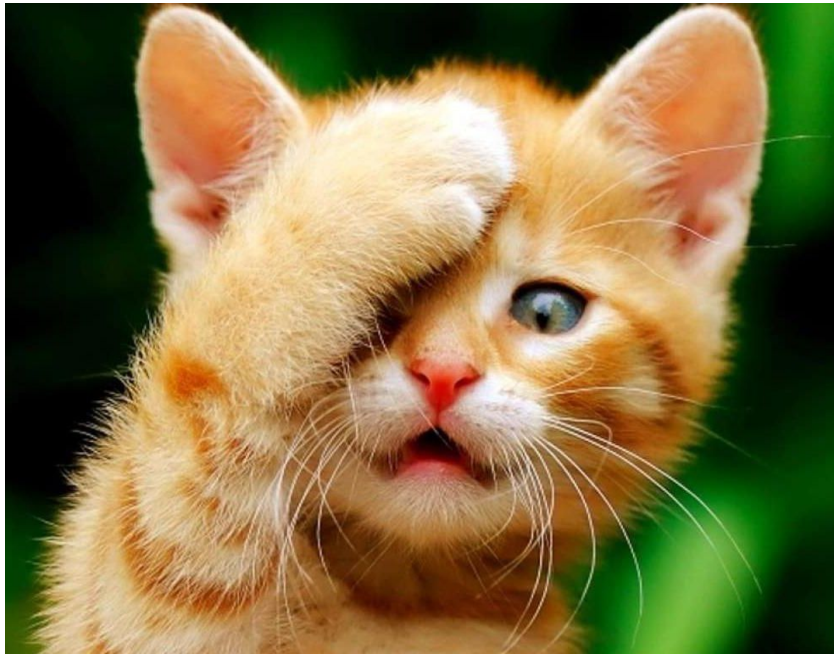
- Each team has similar database
- Each team has all authentication data



“BACKDOOR”



```
user['role'] = len(user['username']) < 3
```



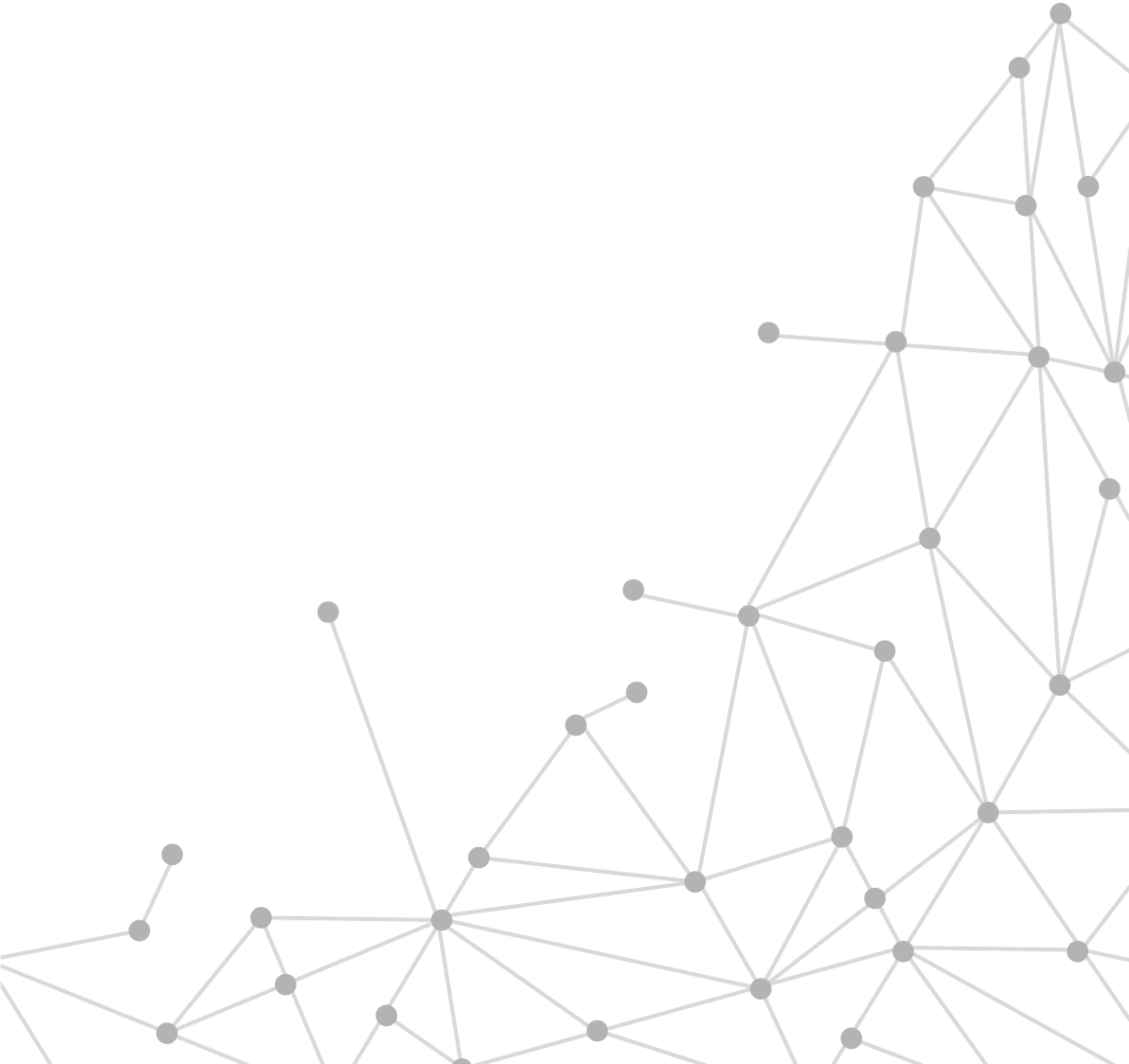
bit.ly/ructfe_mol_sploit

MINISTRY OF TAXES

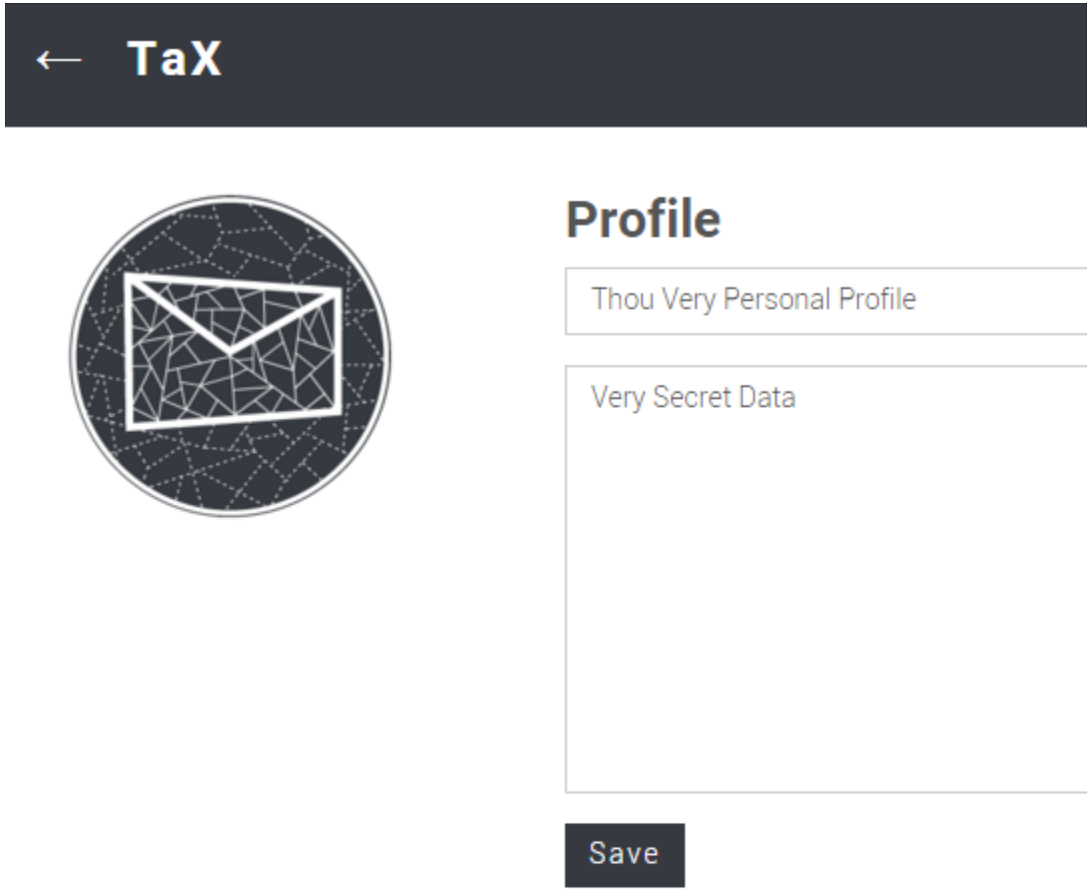
Pavel Blinov aka pahaz

ABOUT SERVICE

- Node.js
- Koa web framework
- Custom router



ADD PERSONAL DATA

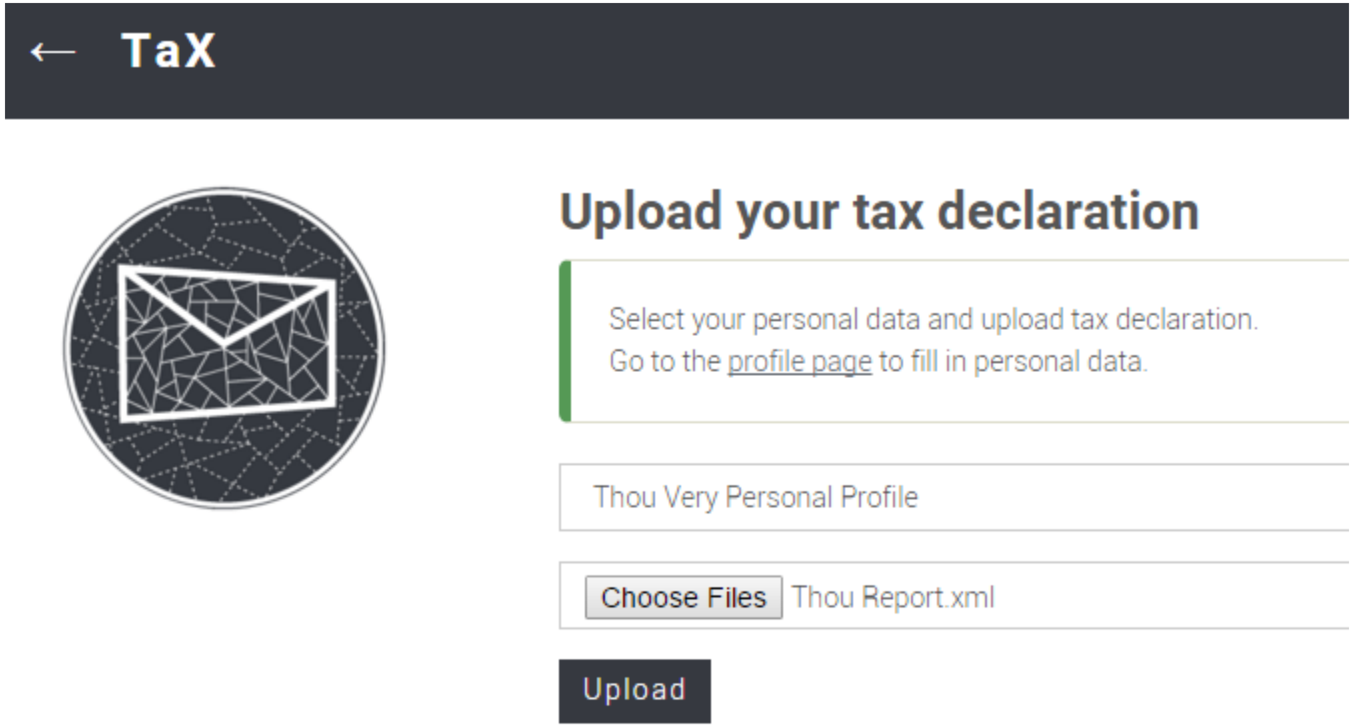


Profile

Thou Very Personal Profile

Very Secret Data

UPLOAD REPORT



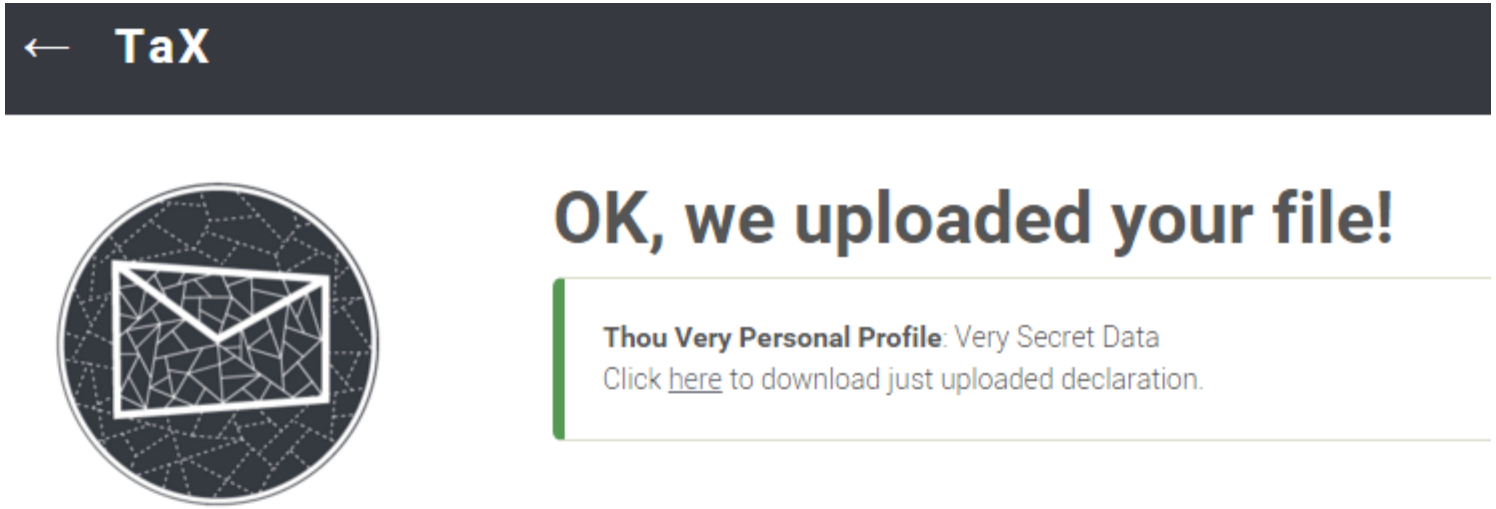
Upload your tax declaration

Select your personal data and upload tax declaration.
Go to the profile page to fill in personal data.

Thou Very Personal Profile

Thou Report.xml

UPLOAD REPORT

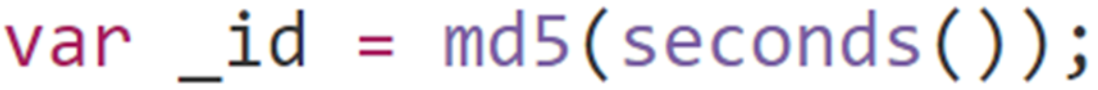


OK, we uploaded your file!

Thou Very Personal Profile: Very Secret Data
Click here to download just uploaded declaration.

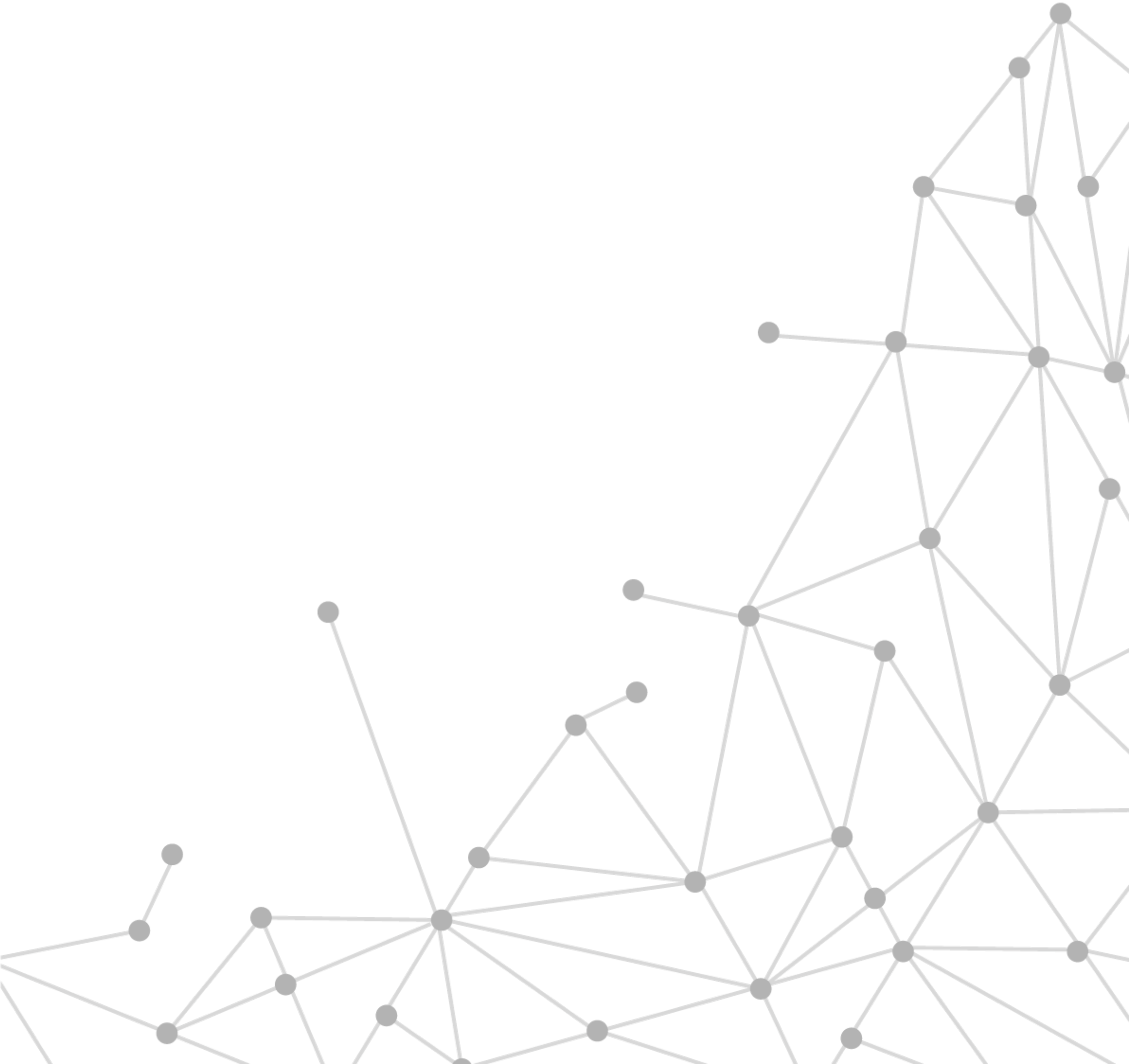
HACK IT!

WEAK ID GENERATION

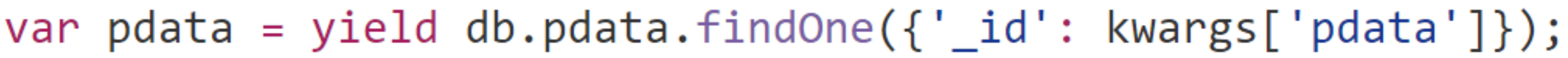


```
var _id = md5(seconds());
```

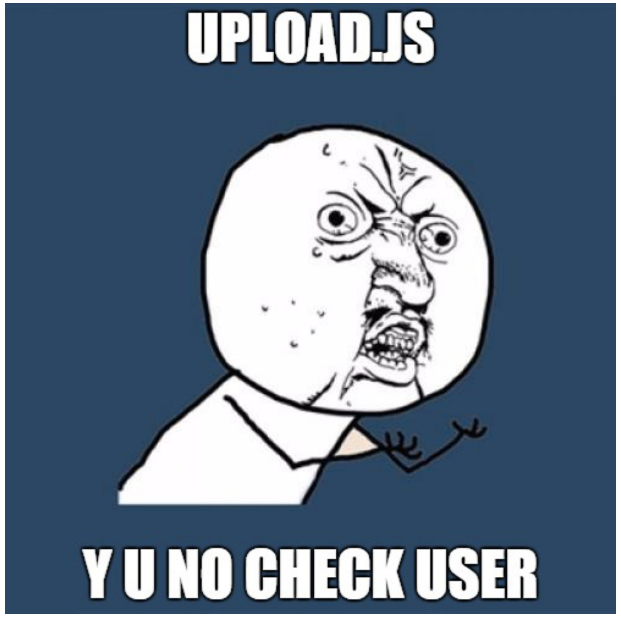
So what?



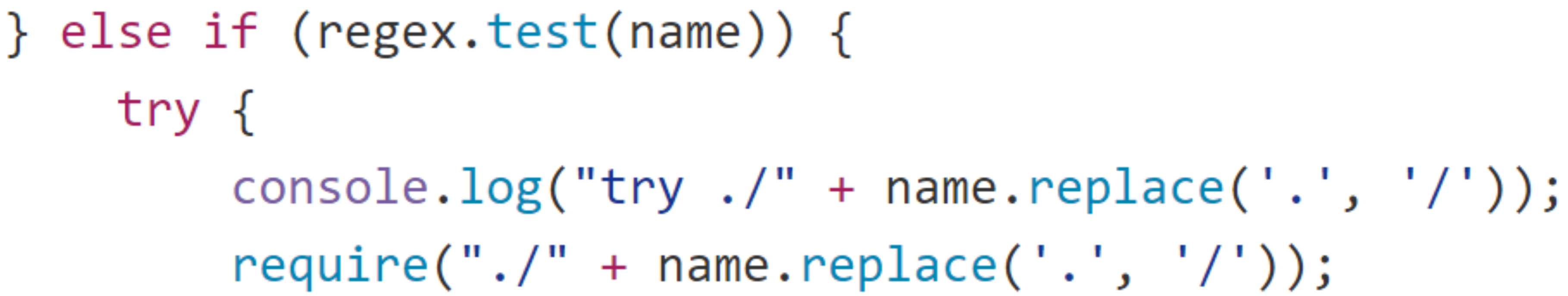
WEAK ID GENERATION



```
var pdata = yield db.pdata.findOne({'_id': kwargs['pdata']});
```

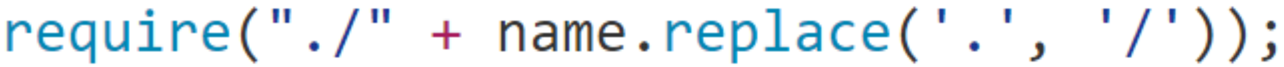


REMOTE CODE EXECUTION



```
} else if (regex.test(name)) {
    try {
        console.log("try ./" + name.replace('.', '/'));
        require("./" + name.replace('.', '/'));
```

REMOTE CODE EXECUTION



```
require("./" + name.replace('.', '/'));
```

bit.ly/ructfe_tax_sploit

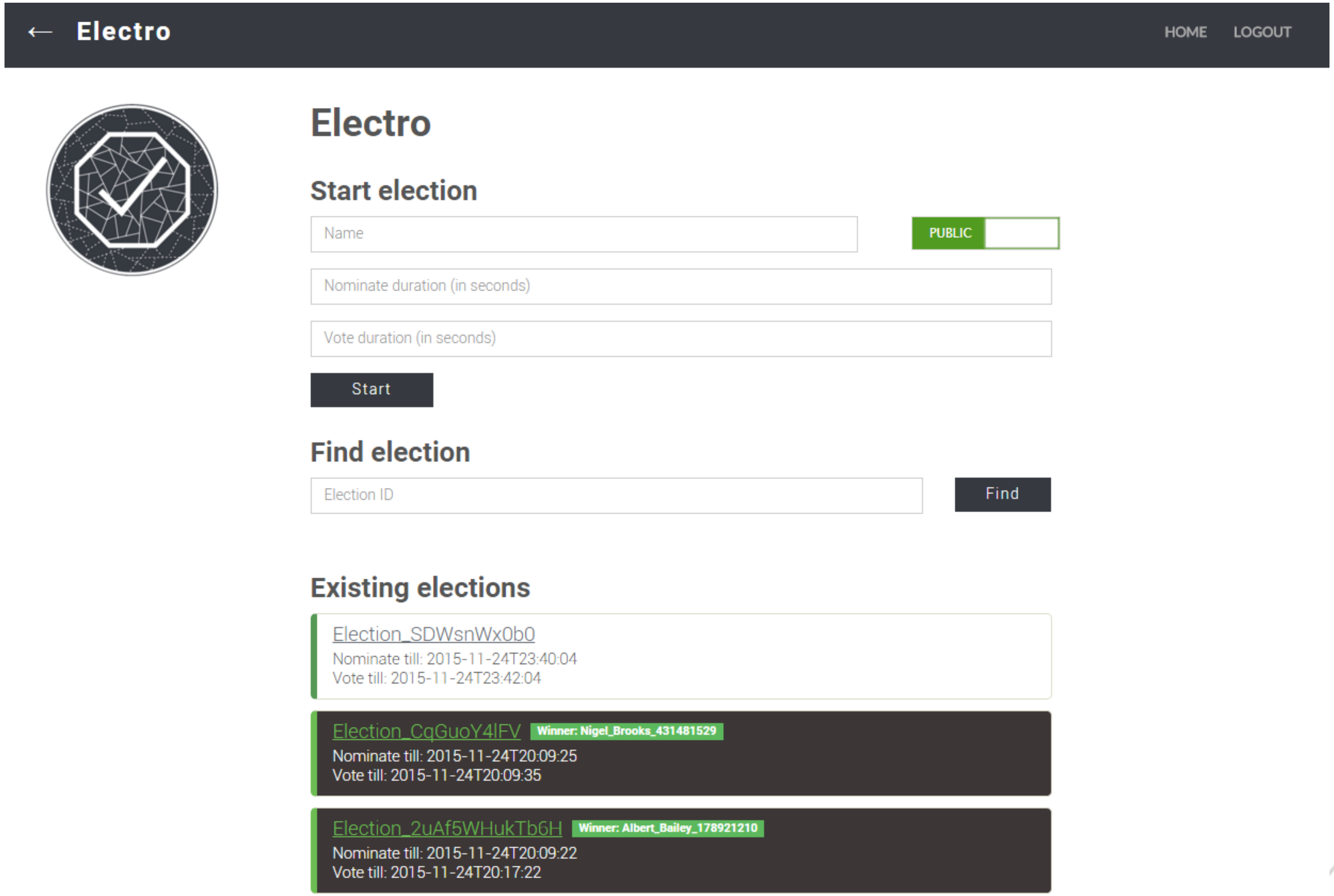
ELECTIONS FOR E-DEMOCRACY

Konstantin Plotnikov aka kost

ABOUT SERVICE

- C# + Mono
- Homomorphic encryption

ELECTIONS



Electro

Start election

Find election

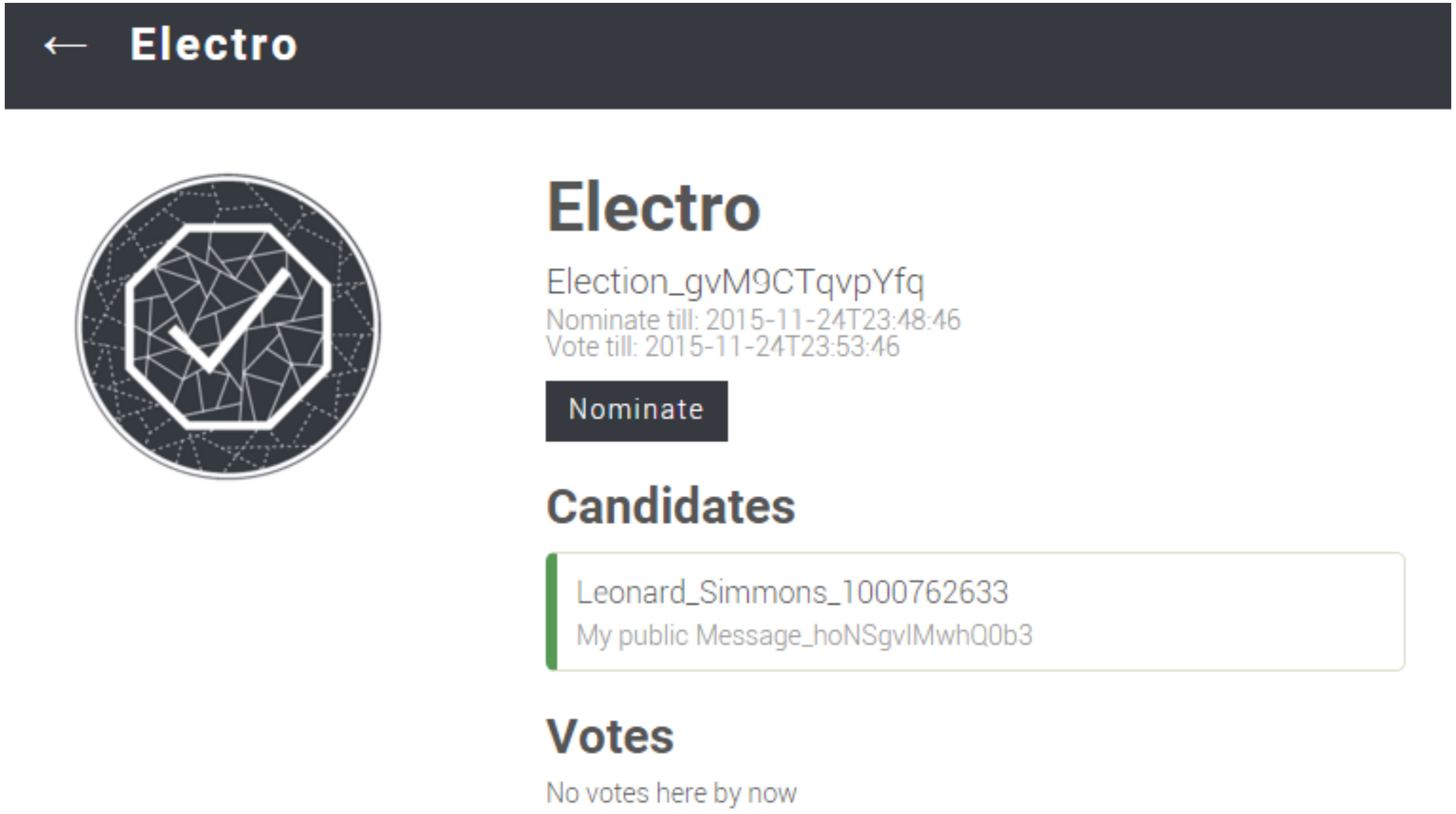
Existing elections

Election_SDWsnWx0b0
Nominate till: 2015-11-24T23:40:04
Vote till: 2015-11-24T23:42:04

Election_CqGuoY4lFV Winner: Nigel_Brooks_431481529
Nominate till: 2015-11-24T20:09:25
Vote till: 2015-11-24T20:09:35

Election_2uAf5WHukTb6H Winner: Albert_Bailey_178921210
Nominate till: 2015-11-24T20:09:22
Vote till: 2015-11-24T20:17:22

NOMINATE



Electro

Election_gvM9CTqvpYfq
Nominate till: 2015-11-24T23:48:46
Vote till: 2015-11-24T23:53:46

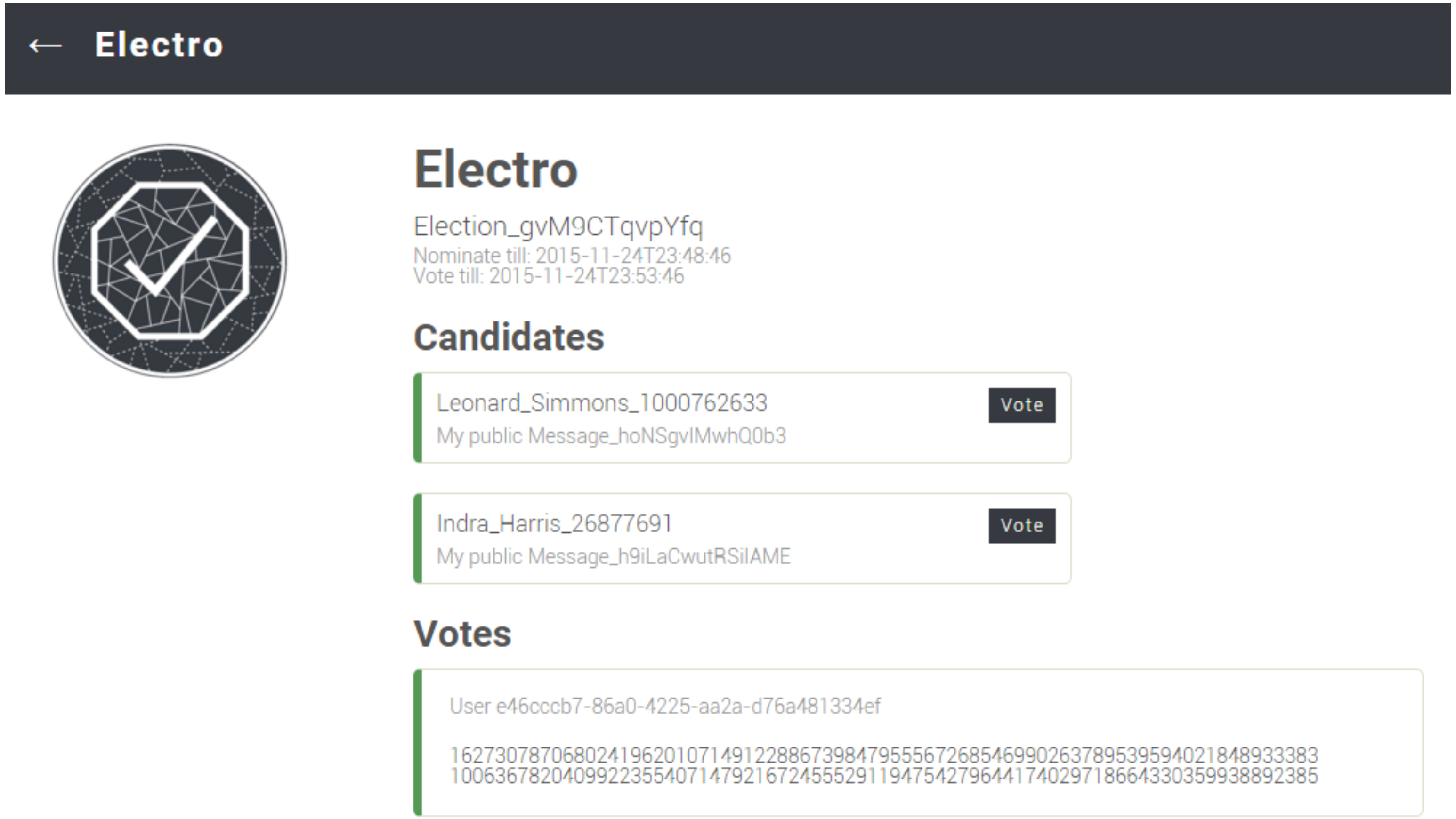
Candidates

Leonard_Simmons_1000762633
My public Message_hoNSgvIMwhQ0b3

Votes

No votes here by now

VOTE



Electro

Election_gvM9CTqvpYfq
Nominate till: 2015-11-24T23:48:46
Vote till: 2015-11-24T23:53:46

Candidates

Leonard_Simmons_1000762633
My public Message_hoNSgvIMwhQ0b3

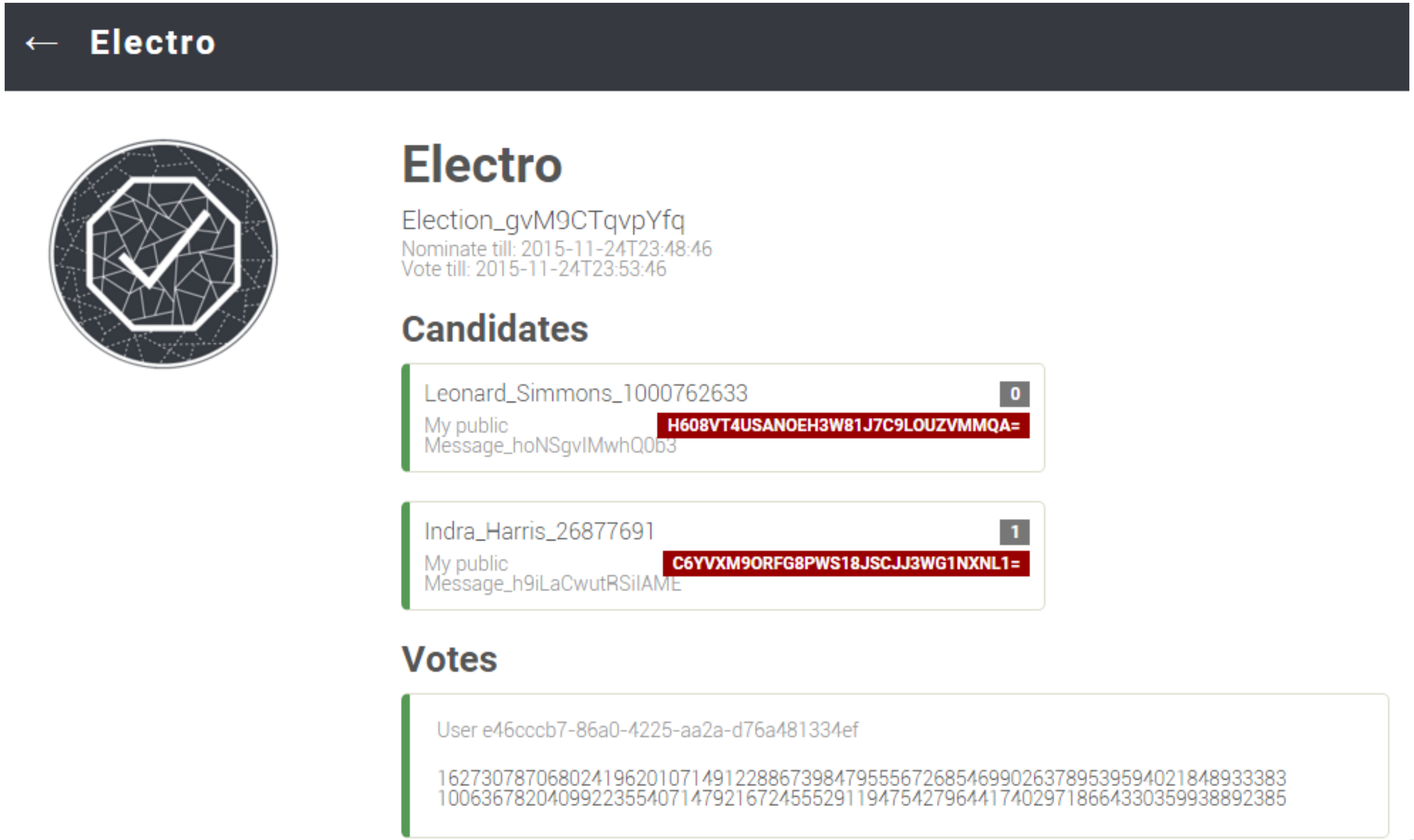
Indra_Harris_26877691
My public Message_h9iLaCwutRSiIAME

Votes

User e46cccb7-86a0-4225-aa2a-d76a481334ef

16273078706802419620107149122886739847955567268546990263789539594021848933383
10063678204099223554071479216724555291194754279644174029718664330359938892385

GET ELECTED



← Electro

Electro

Election_gvM9CTqvpYfq
Nominate till: 2015-11-24T23:48:46
Vote till: 2015-11-24T23:53:46

Candidates

Leonard_Simmons_1000762633 0
My public
Message_hoNSgvIMwhQ0b3
H608VT4USANOEH3W81J7C9LOUZVMMQA=

Indra_Harris_26877691 1
My public
Message_h9iLaCwutRSiIAME
C6YVXM9ORFG8PWS18JSCJJ3WG1NXNL1=

Votes

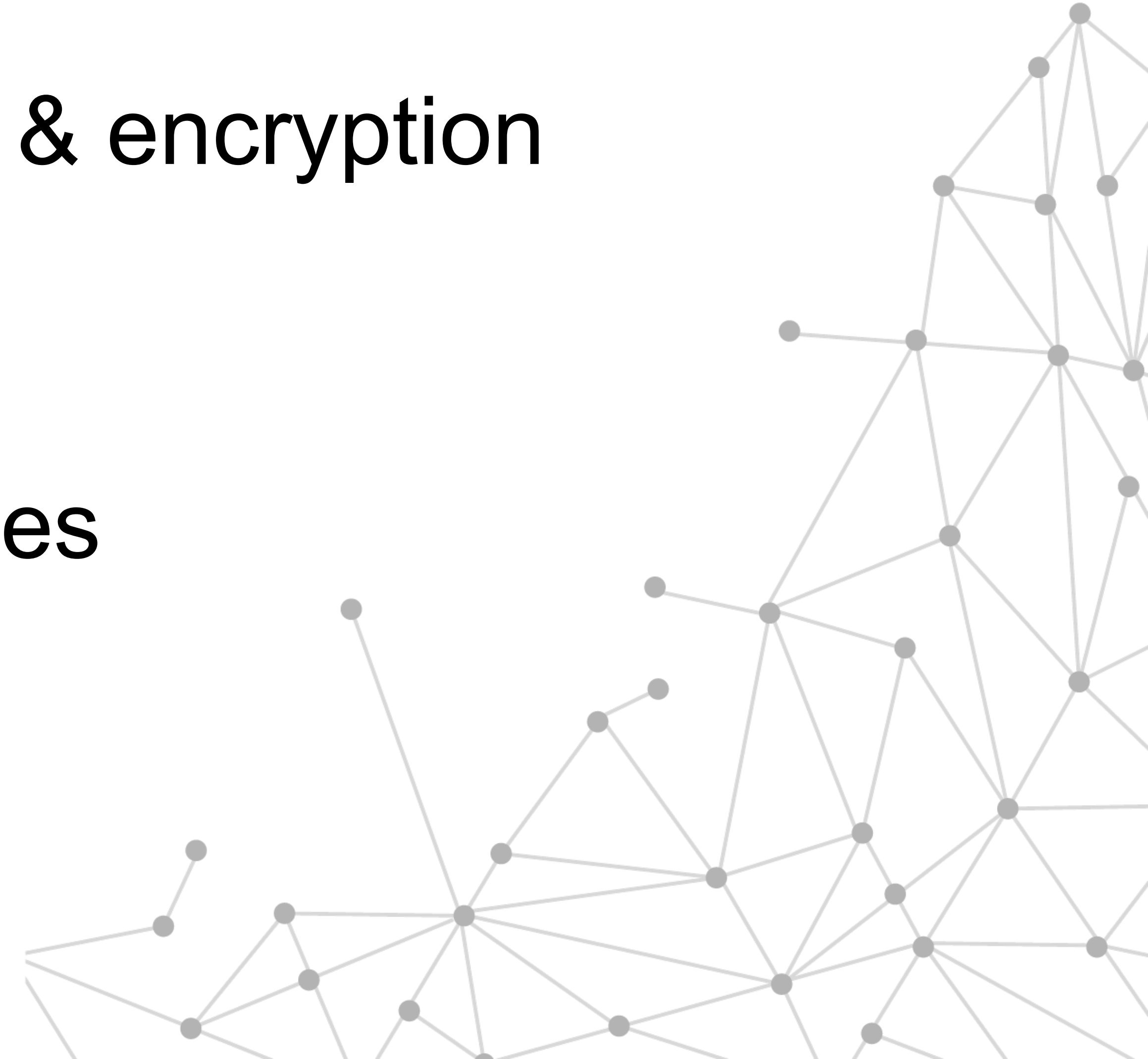
User e46cccb7-86a0-4225-aa2a-d76a481334ef

16273078706802419620107149122886739847955567268546990263789539594021848933383
10063678204099223554071479216724555291194754279644174029718664330359938892385

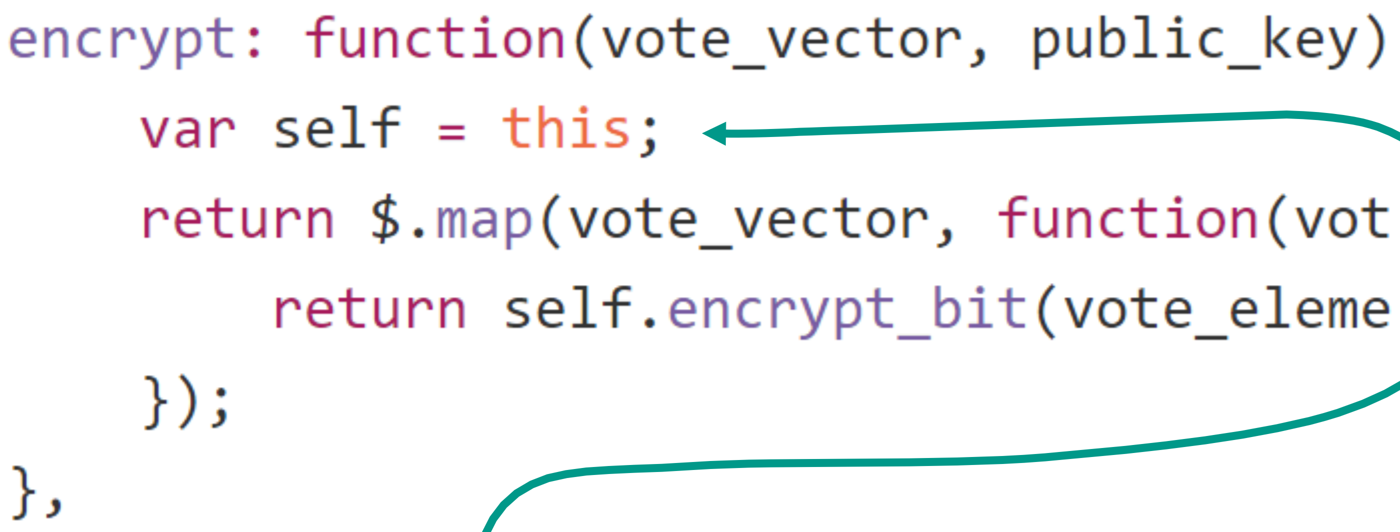
HACK IT!

UNFILTERED INPUT

- Client-side vote generation & encryption
- Vote – vector of integers
- Election result – sum of votes



UNFILTERED INPUT



```
encrypt: function(vote_vector, public_key)
    var self = this;
    return $.map(vote_vector, function(vot
        return self.encrypt_bit(vote_eleme
    });
},
```

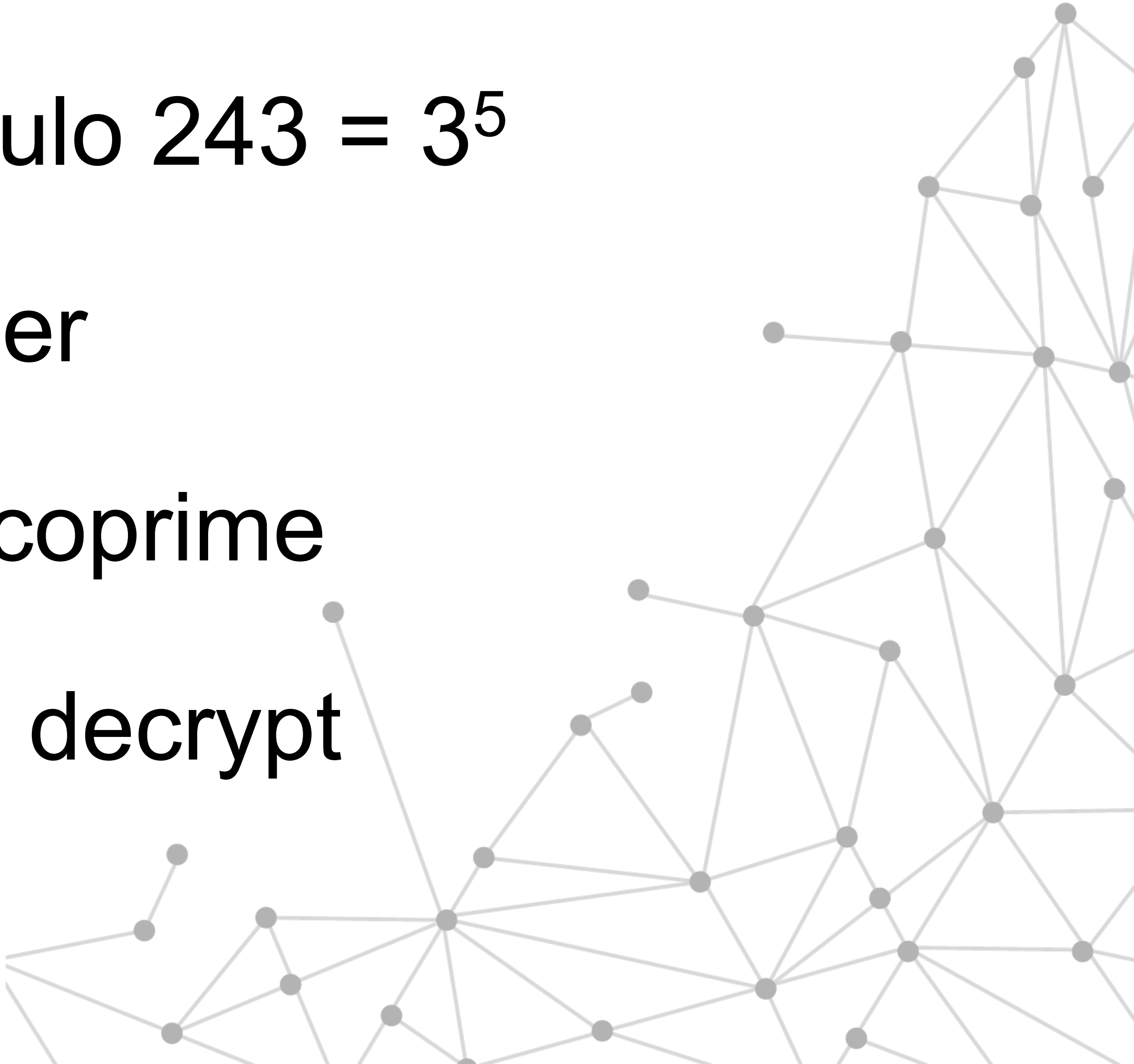
break & hack

UNFILTERED INPUT

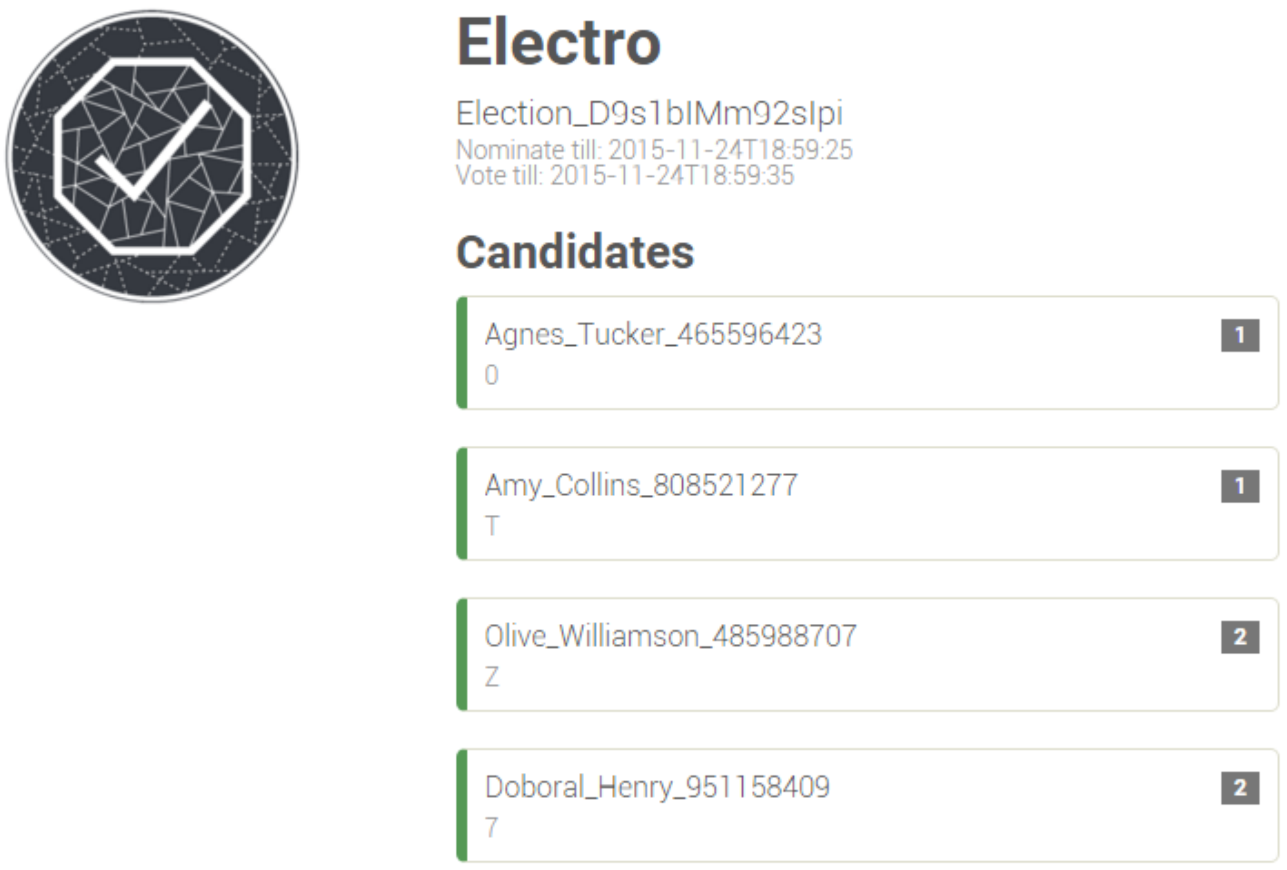
- Calculations are made modulo 243
- Overflow competitor's value
- Let the battle begins!

WEAK PRIVATE KEY GENERATOR

- Calculations are made modulo 243 = 3^5
- Private key – random number
- Chance of them being non-coprime
- 3 divides private key ⇒ can decrypt



WEAK PRIVATE KEY GENERATOR



Electro

Election_D9s1bIMm92sIpi

Nominate till: 2015-11-24T18:59:25
Vote till: 2015-11-24T18:59:35

Candidates

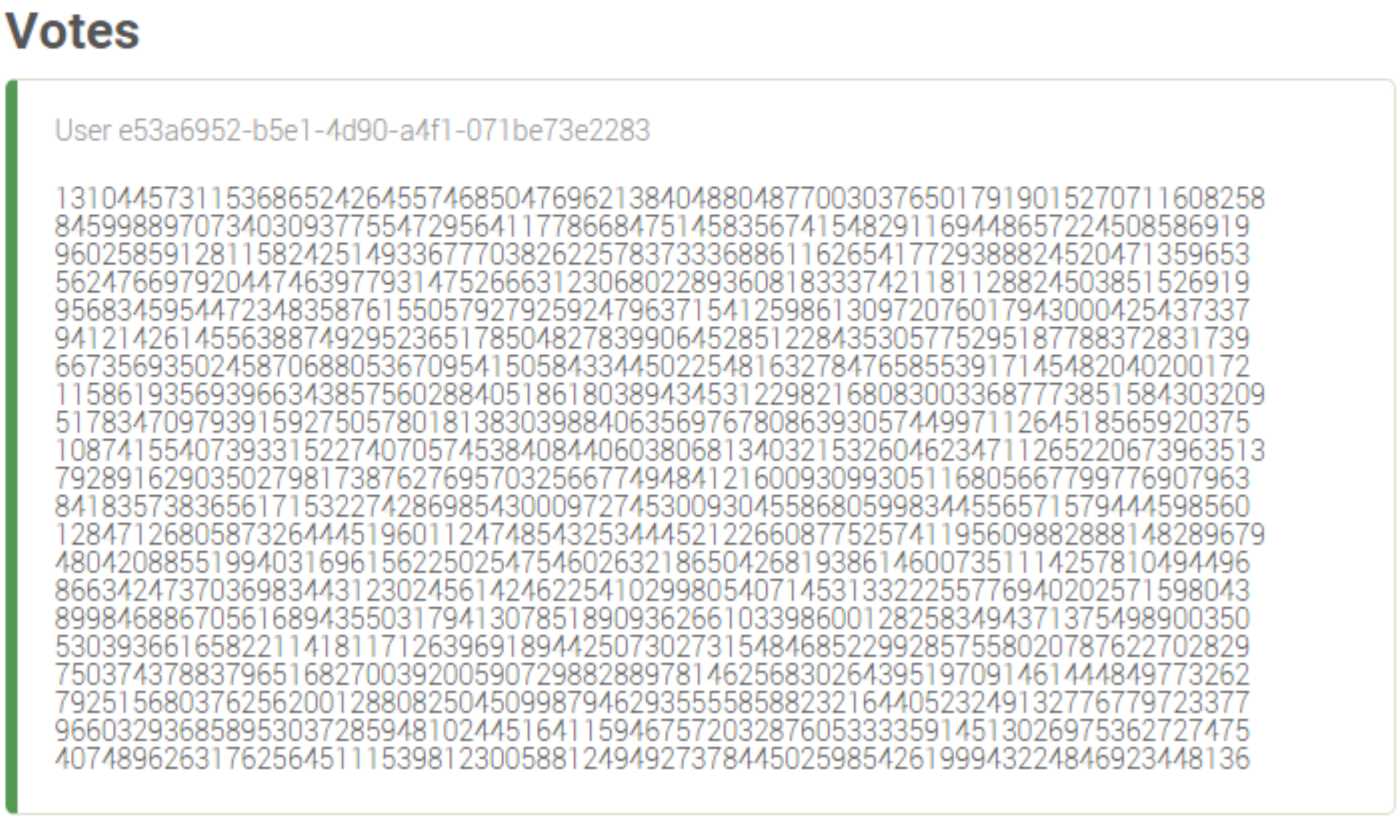
Agnes_Tucker_465596423 **1**
0

Amy_Collins_808521277 **1**
T

Olive_Williamson_485988707 **2**
Z

Doboral_Henry_951158409 **2**
7

WEAK PRIVATE KEY GENERATOR

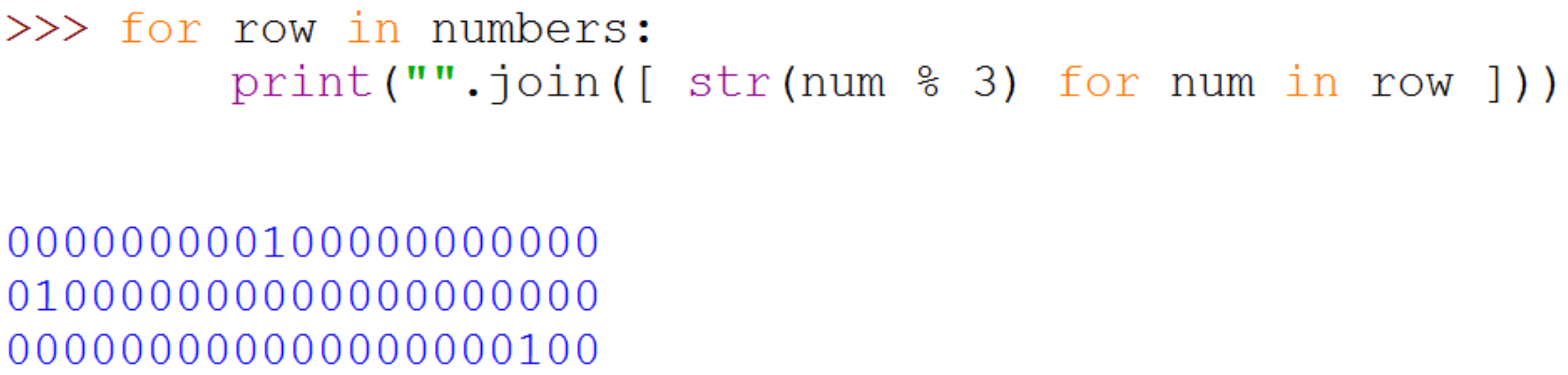


Votes

User e53a6952-b5e1-4d90-a4f1-071be73e2283

```
131044573115368652426455746850476962138404880487700303765017919015270711608258
84599889707340309377554729564117786684751458356741548291169448657224508586919
96025859128115824251493367770382622578373336886116265417729388824520471359653
56247669792044746397793147526663123068022893608183337421181128824503851526919
95683459544723483587615505792792592479637154125986130972076017943000425437337
94121426145563887492952365178504827839906452851228435305775295187788372831739
66735693502458706880536709541505843344502254816327847658553917145482040200172
115861935693966343857560288405186180389434531229821680830033687773851584303209
51783470979391592750578018138303988406356976780863930574499711264518565920375
108741554073933152274070574538408440603806813403215326046234711265220673963513
79289162903502798173876276957032566774948412160093099305116805667799776907963
84183573836561715322742869854300097274530093045586805998344556571579444598560
128471268058732644451960112474854325344452122660877525741195609882888148289679
48042088551994031696156225025475460263218650426819386146007351114257810494496
86634247370369834431230245614246225410299805407145313322255776940202571598043
89984688670561689435503179413078518909362661033986001282583494371375498900350
53039366165822114181171263969189442507302731548468522992857558020787622702829
75037437883796516827003920059072988288978146256830264395197091461444849773262
79251568037625620012880825045099879462935555858823216440523249132776779723377
96603293685895303728594810244516411594675720328760533335914513026975362727475
40748962631762564511153981230058812494927378445025985426199943224846923448136
```

WEAK PRIVATE KEY GENERATOR



```
>>> for row in numbers:
        print("".join([ str(num % 3) for num in row ]))


0000000001000000000000
0100000000000000000000
0000000000000000000100
```

⋮

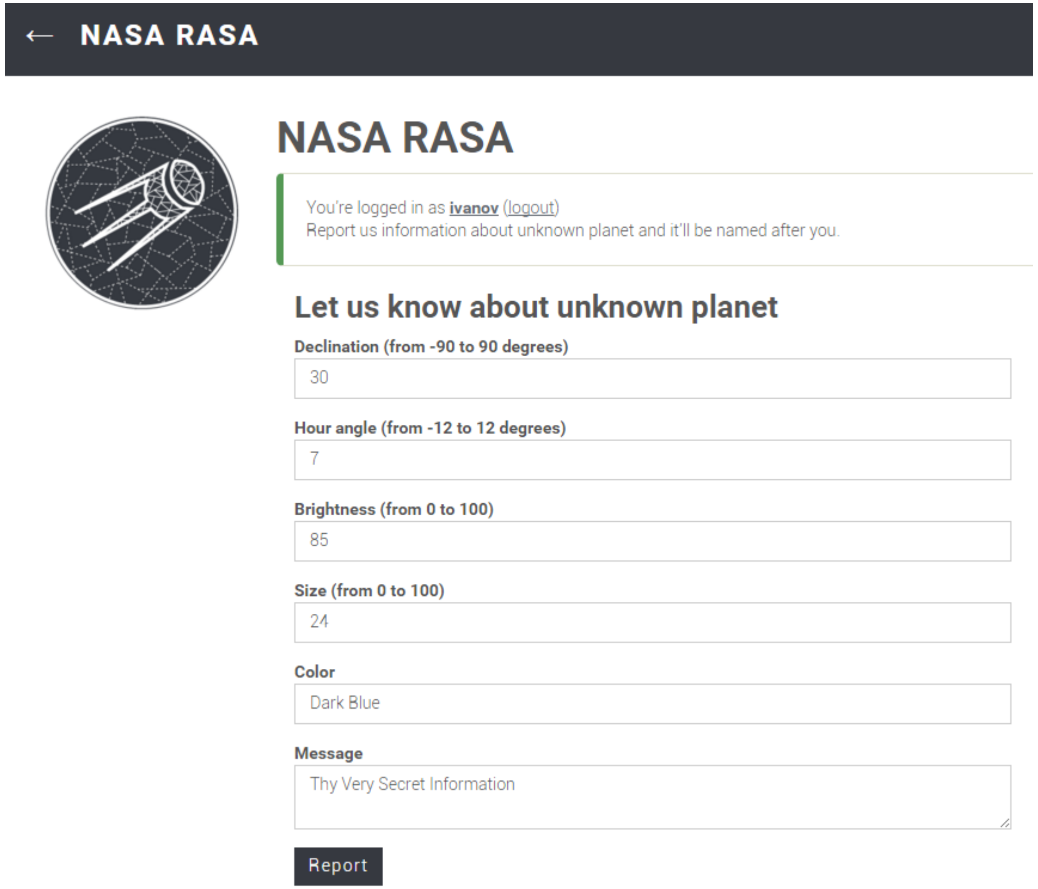
NASA RASA

Andrey Gein aka andgein

ABOUT SERVICE

- PHP
- MySQL

REPORT A PLANET



NASA RASA

You're logged in as **ivanov** (logout)
Report us information about unknown planet and it'll be named after you.

Let us know about unknown planet

Declination (from -90 to 90 degrees)
30

Hour angle (from -12 to 12 degrees)
7

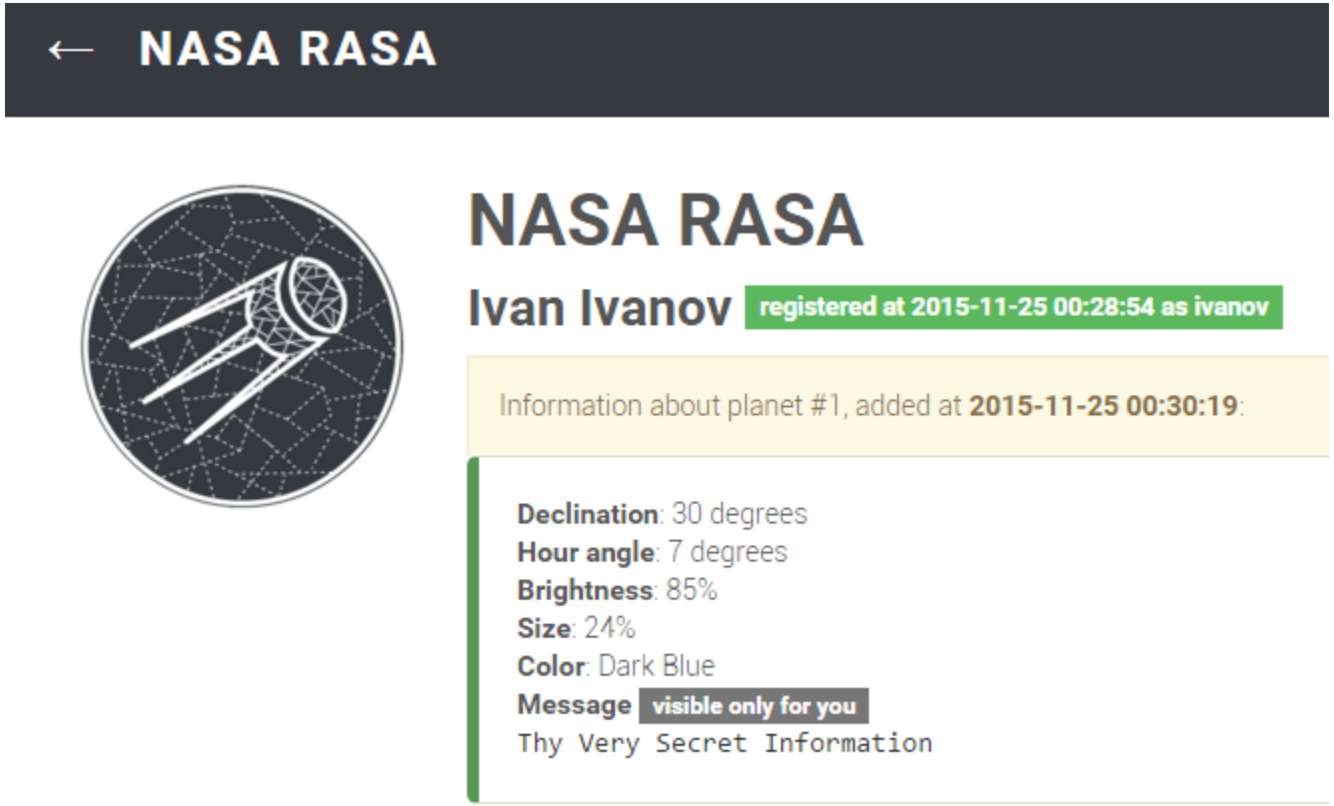
Brightness (from 0 to 100)
85

Size (from 0 to 100)
24

Color
Dark Blue

Message
Thy Very Secret Information

BROWSE DISCOVERED PLANETS



NASA RASA

NASA RASA

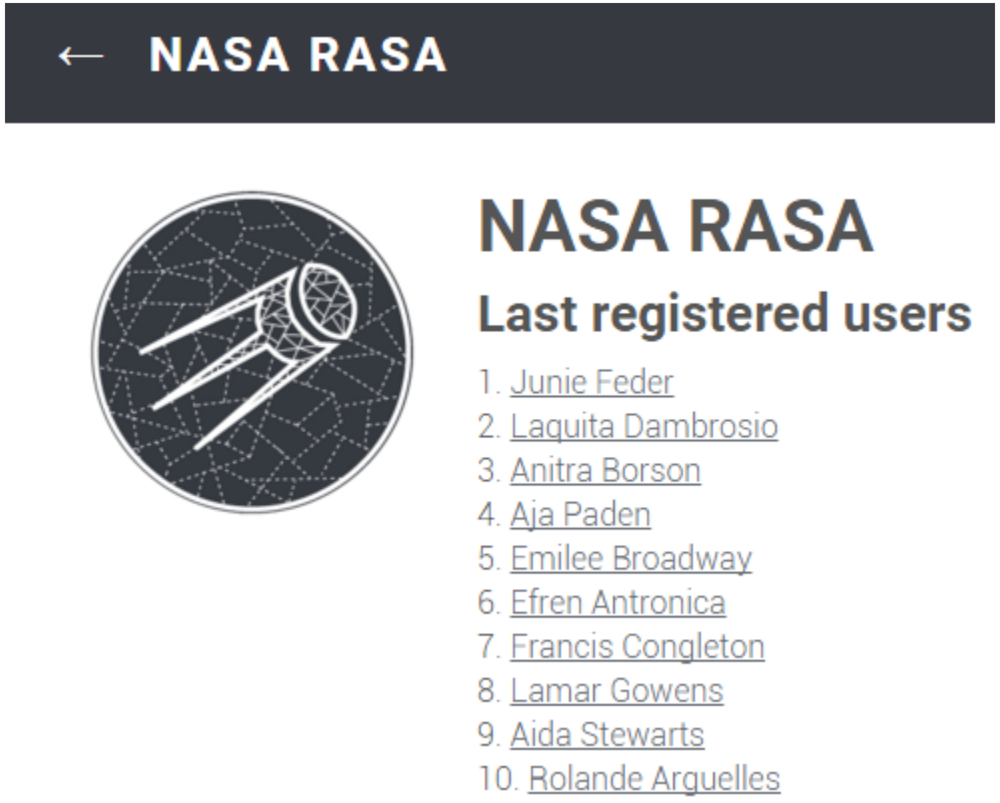
Ivan Ivanov registered at 2015-11-25 00:28:54 as ivanov

Information about planet #1, added at **2015-11-25 00:30:19**:

Declination: 30 degrees
Hour angle: 7 degrees
Brightness: 85%
Size: 24%
Color: Dark Blue
Message visible only for you

```
Thy Very Secret Information
```

BROWSE USERS



← NASA RASA

NASA RASA

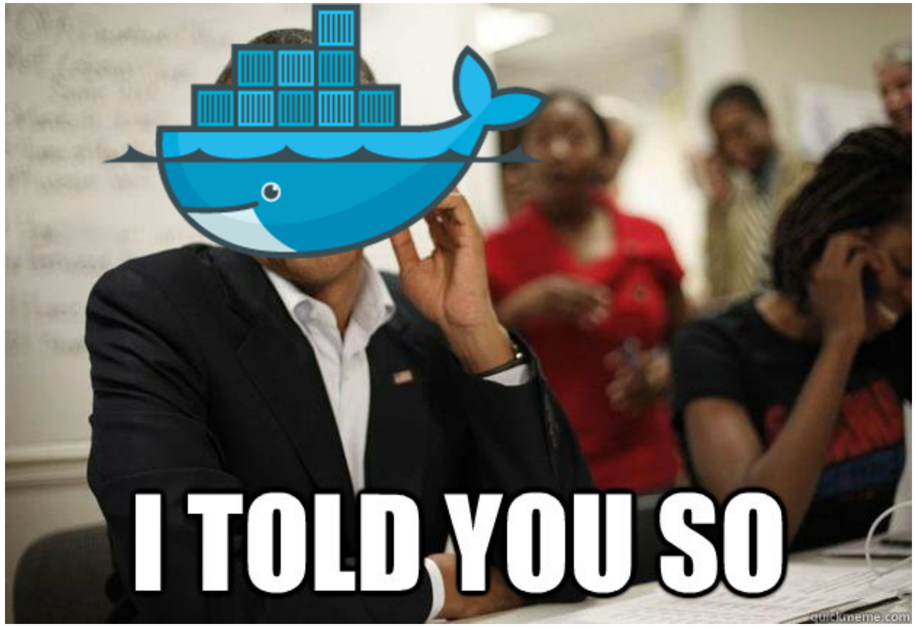
Last registered users

1. Junie Feder
2. Laquita Dambrosio
3. Anitra Borson
4. Aja Paden
5. Emilee Broadway
6. Efren Antronica
7. Francis Congleton
8. Lamar Gowens
9. Aida Stewarts
10. Rolande Arguelles

HACK IT!

HARDCODED DB CREDENTIALS

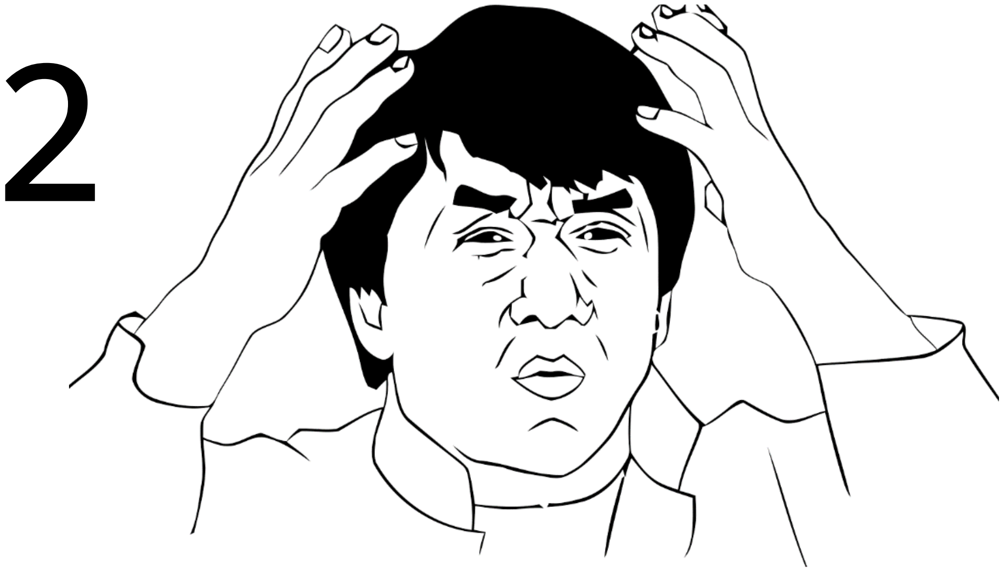
Remember about RCE?



PADSPACE COLLATION

```sql
CREATE TABLE test (`name` varchar(10));
INSERT INTO test VALUES ('a'), ('a ');
SELECT COUNT(*) FROM test WHERE name = 'a';
```

⇒2



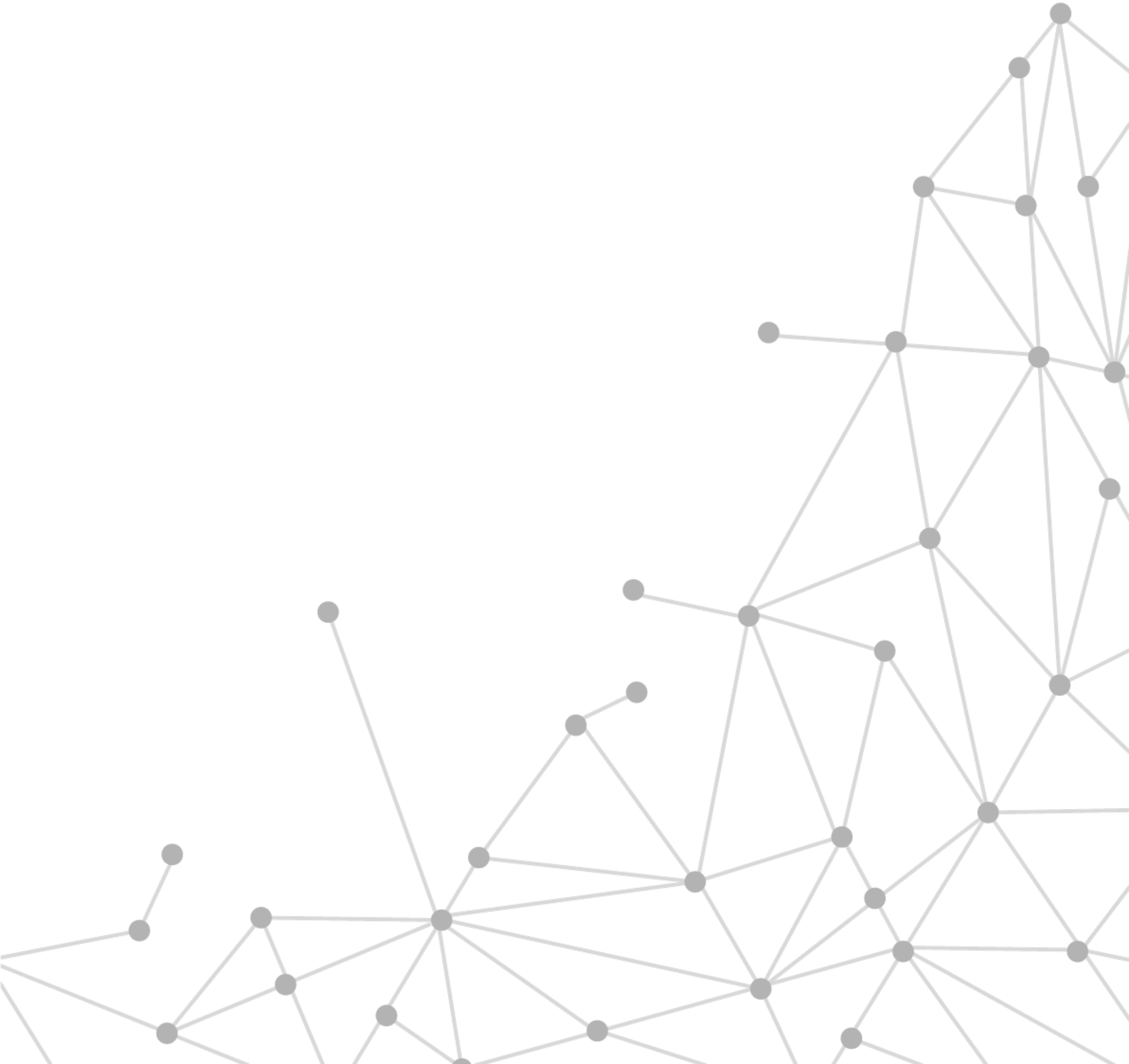
bit.ly/ructfe_collations

HEALTH MONITOR

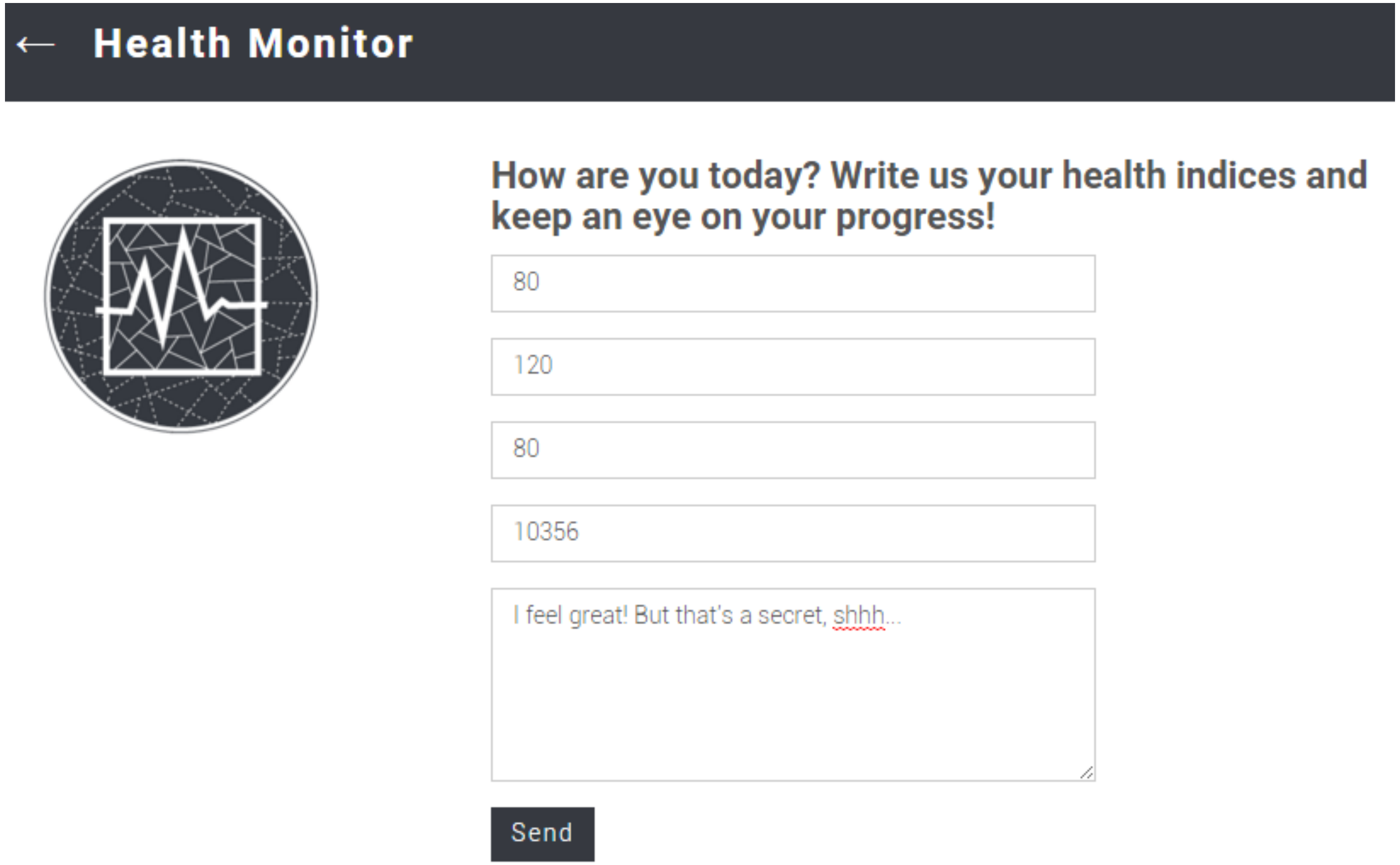
Polina Zonova aka Klyaksa

ABOUT SERVICE

- Go
- SQLite



REPORT YOUR HEALTH



How are you today? Write us your health indices and keep an eye on your progress!

80

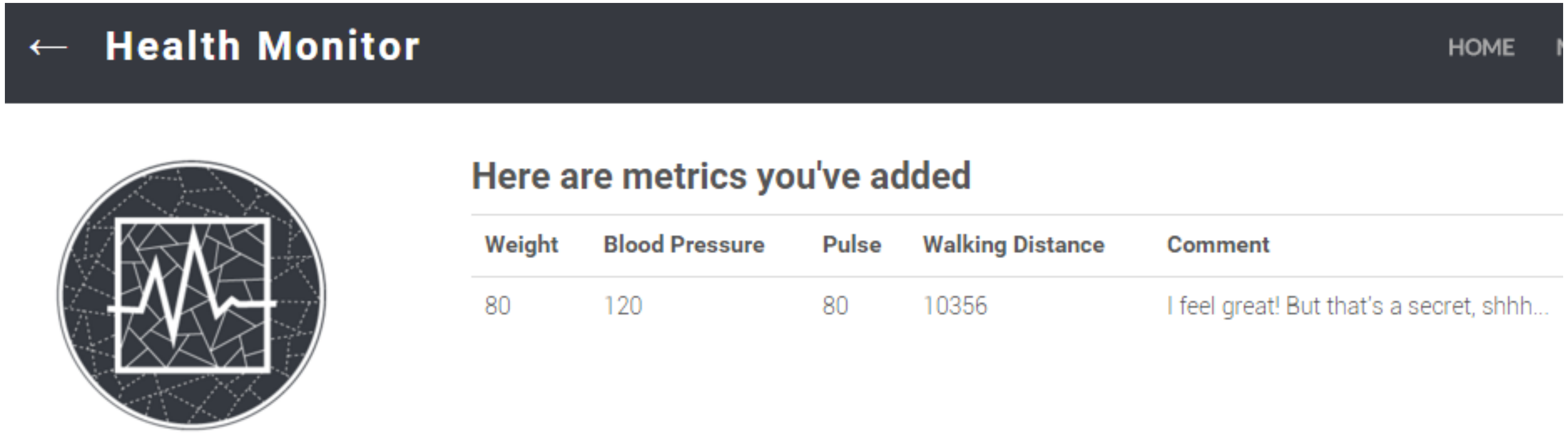
120

80

10356

I feel great! But that's a secret, shhh...

BROWSE YOUR PROGRESS

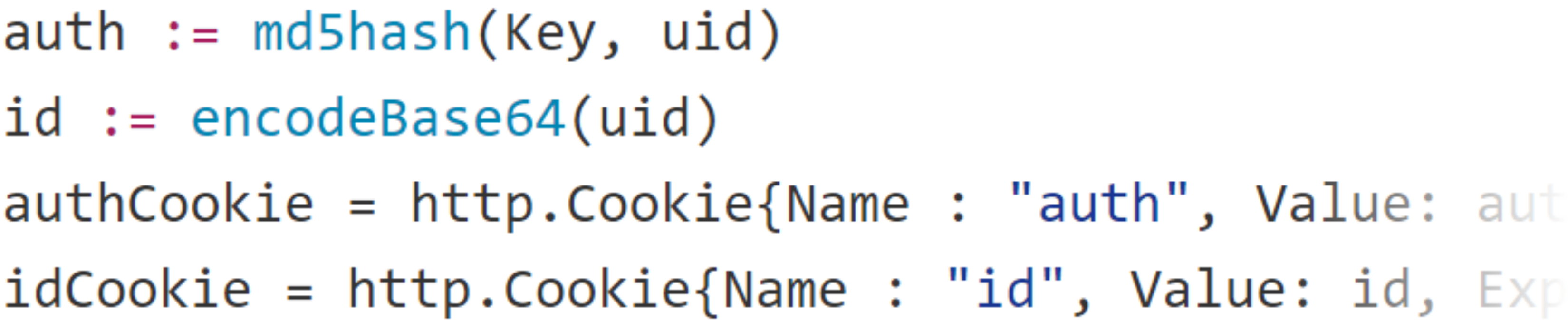


Here are metrics you've added

Weight	Blood Pressure	Pulse	Walking Distance	Comment
80	120	80	10356	I feel great! But that's a secret, shhh...

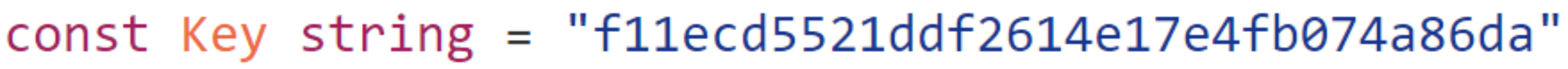
HACK IT!

AUTHENTICATION



```
auth := md5hash(Key, uid)
id := encodeBase64(uid)
authCookie = http.Cookie{Name : "auth", Value: aut
idCookie = http.Cookie{Name : "id", Value: id, Exp
```

HARDCODED SALT



```
const Key string = "f11ecd5521ddf2614e17e4fb074a86da"
```

Plan:

1. Set up vulnbox
2. Change all passwords & keys
3. Win

LENGTH EXTENSION ATTACK

- uids are serial – we can guess
- Over 9k tools to perform MD5 LEA

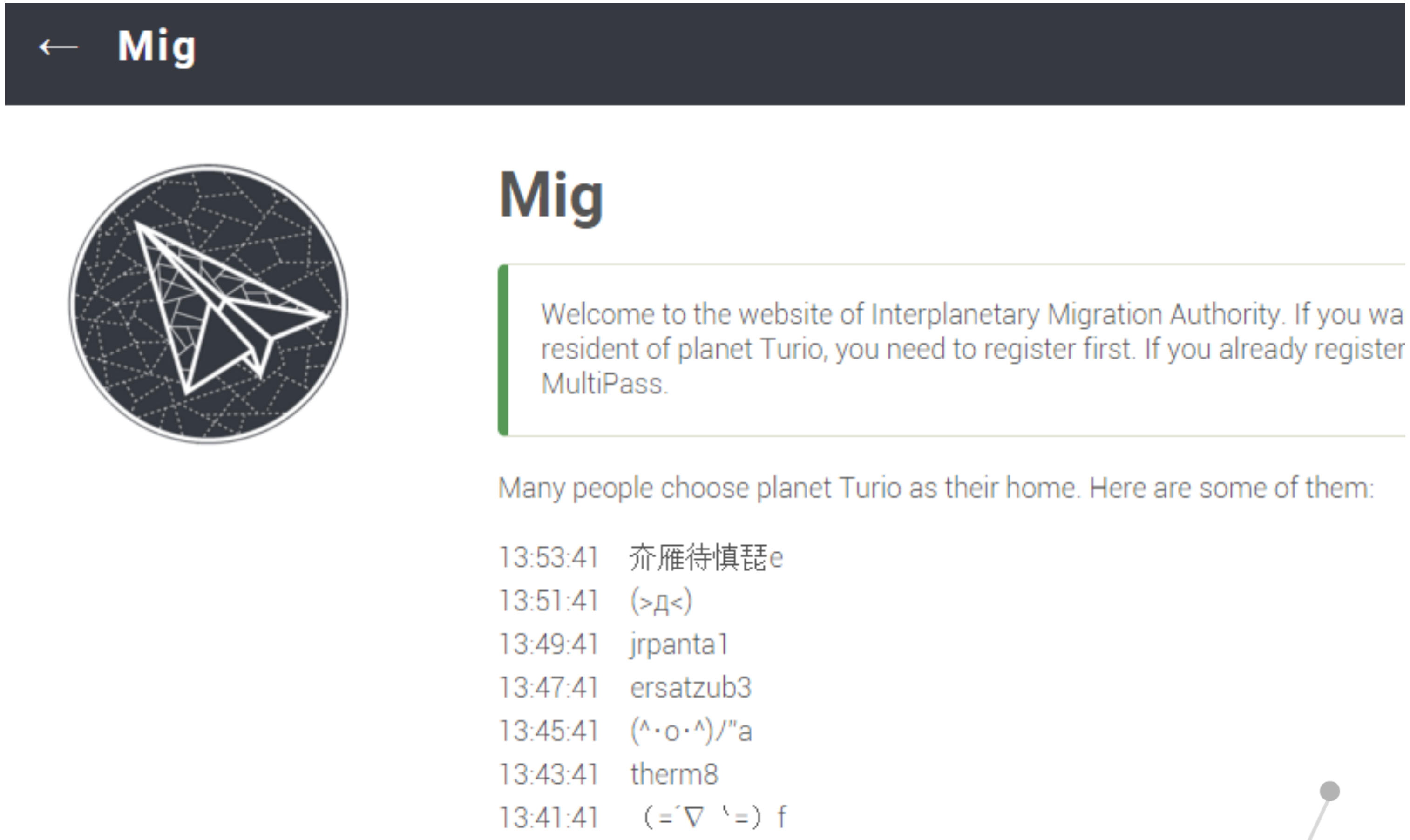
INTERPLANETARY MIGRATION AUTHORITY

Dmitry Titarenko aka dscheg

ABOUT SERVICE

- Nim
- Redis

KNOW CITIZENS



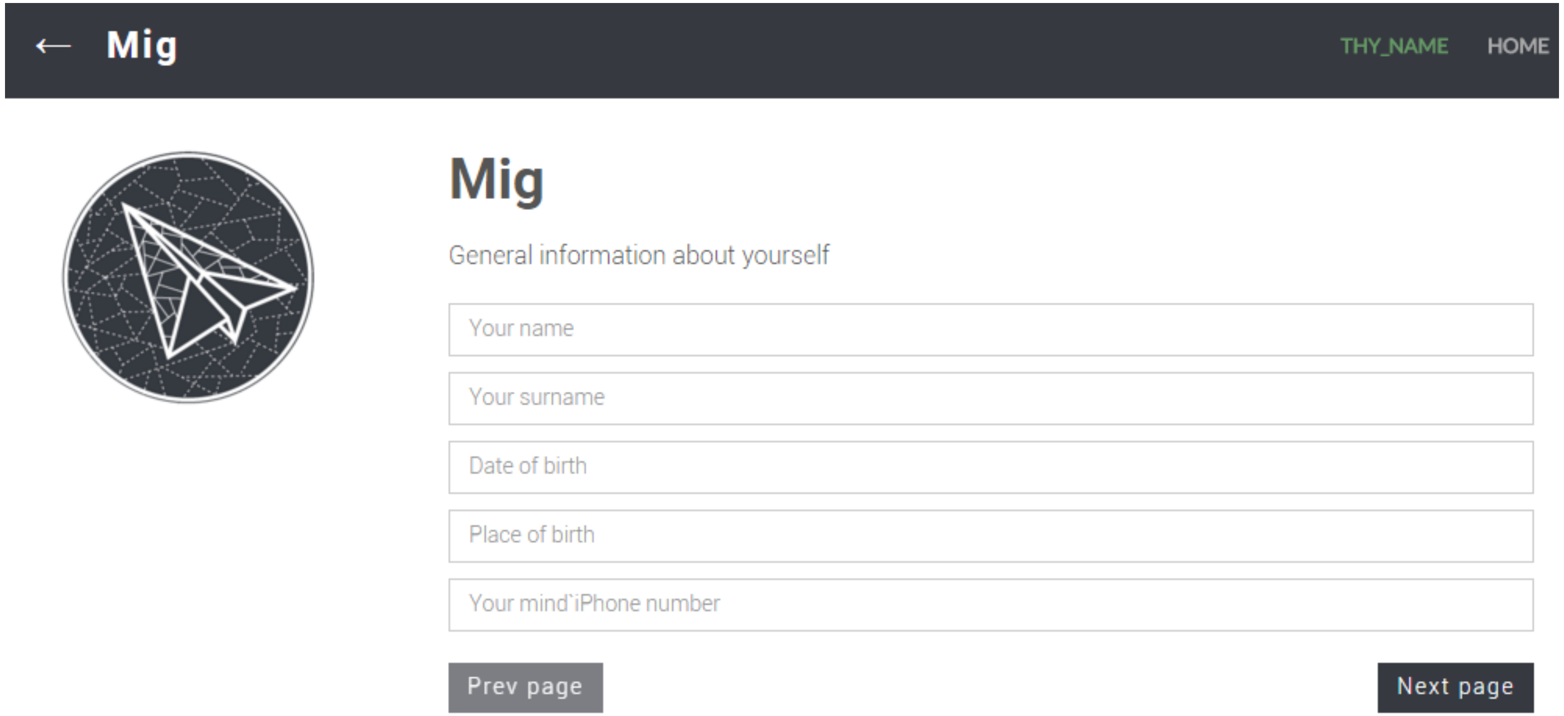
Mig

Welcome to the website of Interplanetary Migration Authority. If you wa
resident of planet Turio, you need to register first. If you already register
MultiPass.

Many people choose planet Turio as their home. Here are some of them:

13:53:41 斉雁待慎琶e
13:51:41 (>д<)
13:49:41 jrpanta1
13:47:41 ersatzub3
13:45:41 (^･o･^)/"a
13:43:41 therm8
13:41:41 （=´∇｀=）f

FILL MIGRATION FORM...



Mig

General information about yourself

Your name

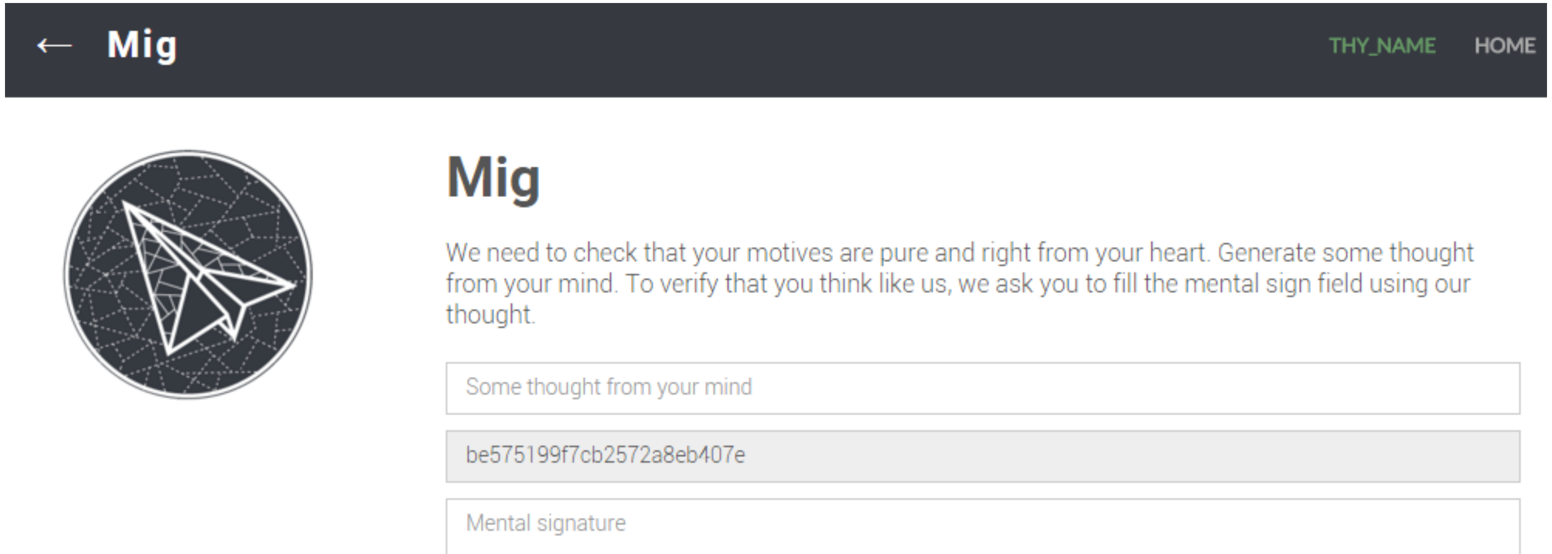
Your surname

Date of birth

Place of birth

Your mind`iPhone number

...BUT NOT QUITE



Mig

We need to check that your motives are pure and right from your heart. Generate some thought from your mind. To verify that you think like us, we ask you to fill the mental sign field using our thought.

Some thought from your mind

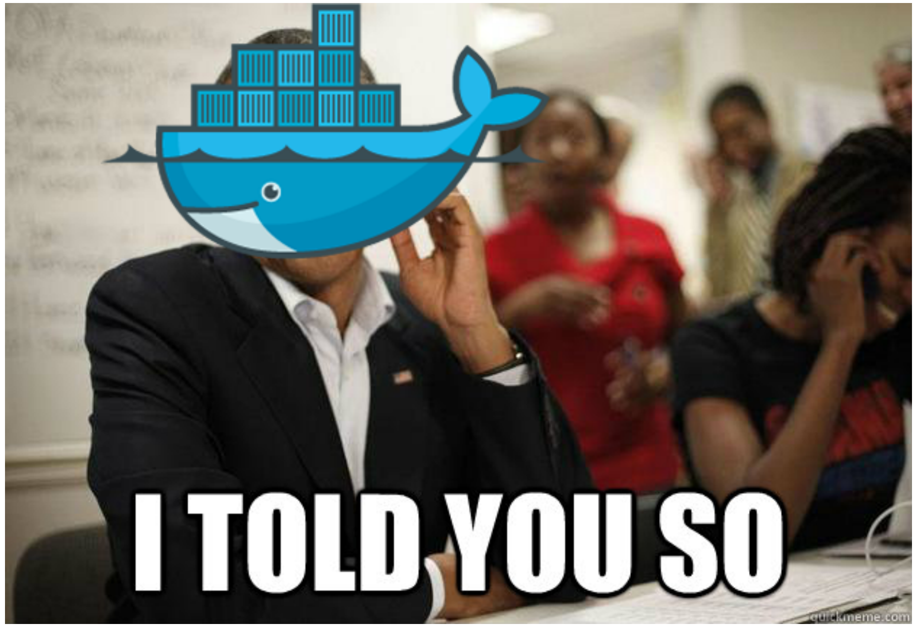
be575199f7cb2572a8eb407e

Mental signature

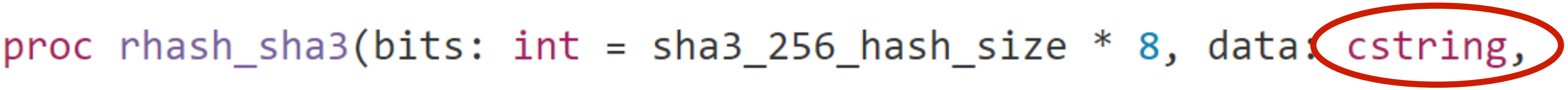
HACK IT!

HARDCODED DB CREDENTIALS

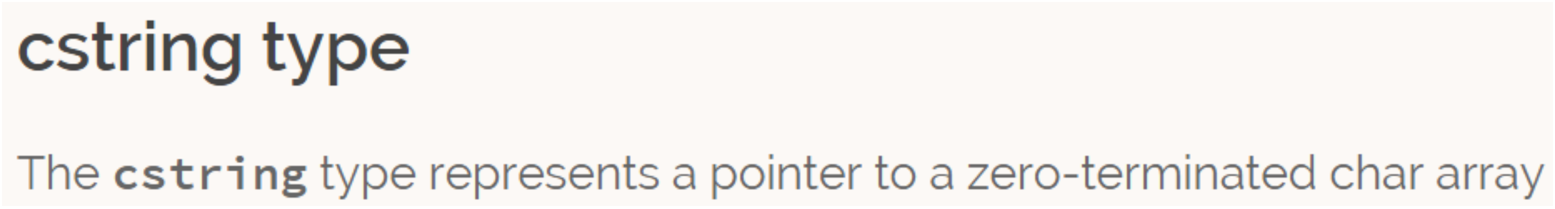
And again



HMAC USING EXTERNAL LIBRARY



```
proc rhash_sha3(bits: int = sha3_256_hash_size * 8, data: cstring,
```



cstring type

The `cstring` type represents a pointer to a zero-terminated char array

zero-padded user
has the same HMAC

HMAC USING EXTERNAL LIBRARY

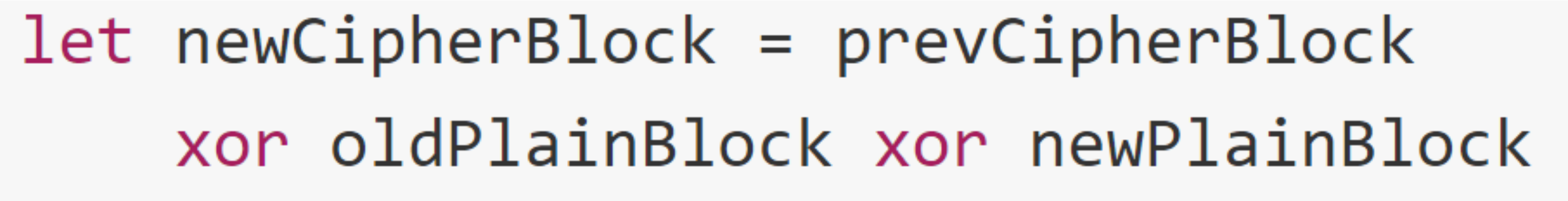
- Login as one of citizens
- Steal flag from the filled form

MODIFYING LOCAL DATA

- Form data stored on client side
- Form data is encrypted
- AES encryption in CBC mode
- No integrity checks

MODIFYING LOCAL DATA

- We know plaintext – JSON with filled data



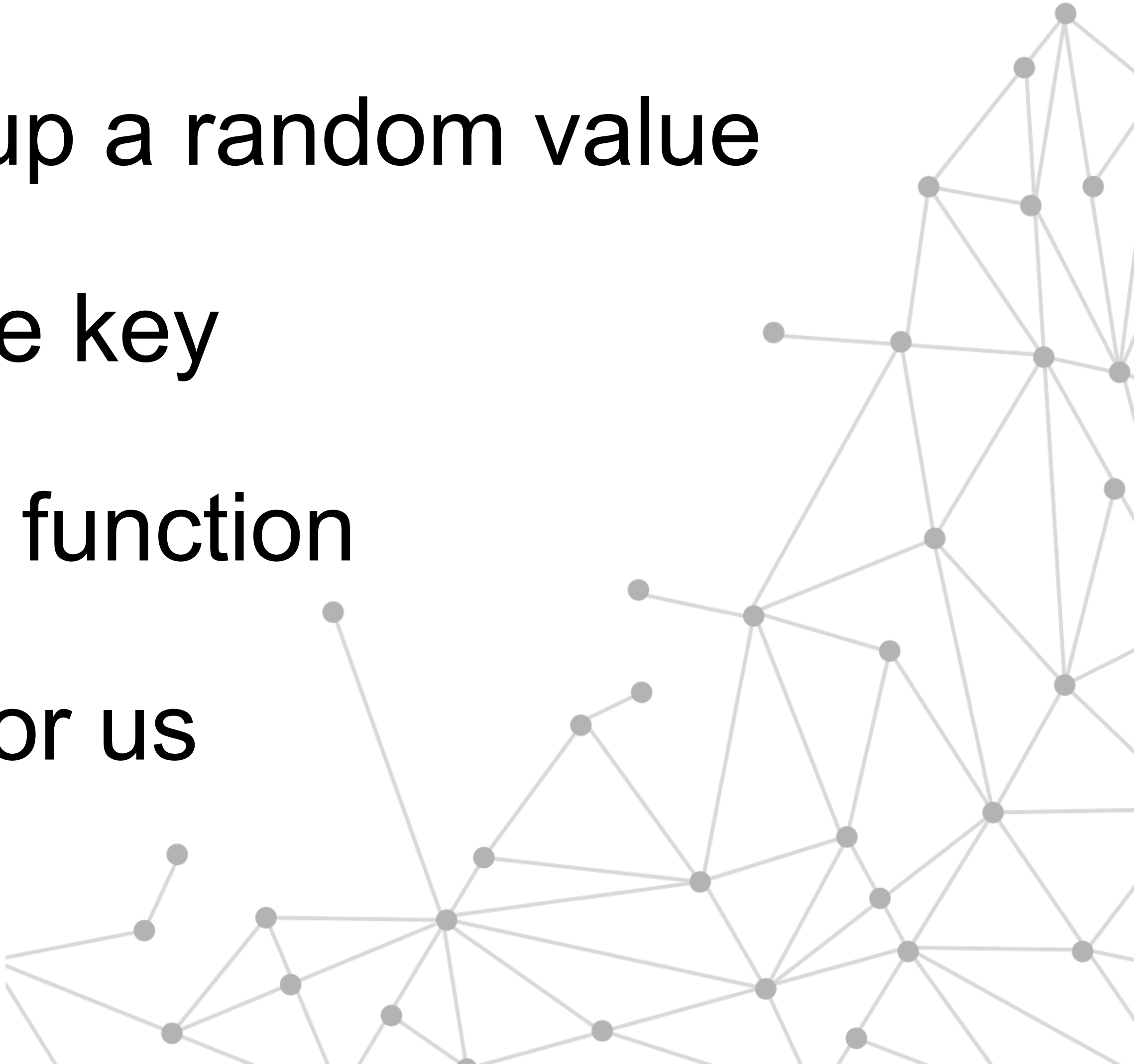
```
let newCipherBlock = prevCipherBlock
    xor oldPlainBlock xor newPlainBlock
```

- We can modify ciphertext

MODIFYING LOCAL DATA

MITM

- On step 3 we need to sign up a random value
- Only checker has the private key
- Let’s hack value generation function
- Check will sign everything for us



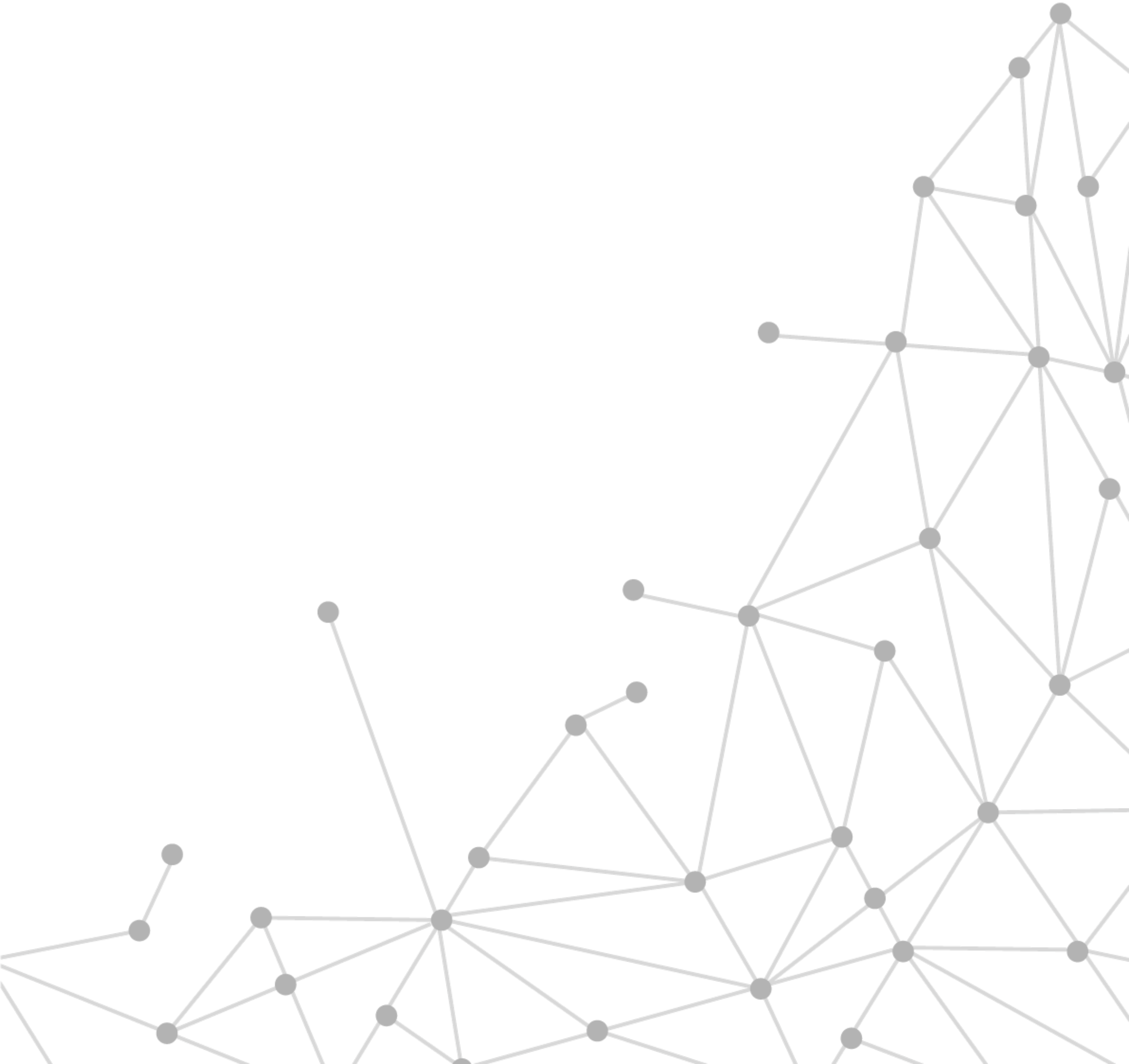
bit.ly/ructfe_mig_sploit

THE BANK

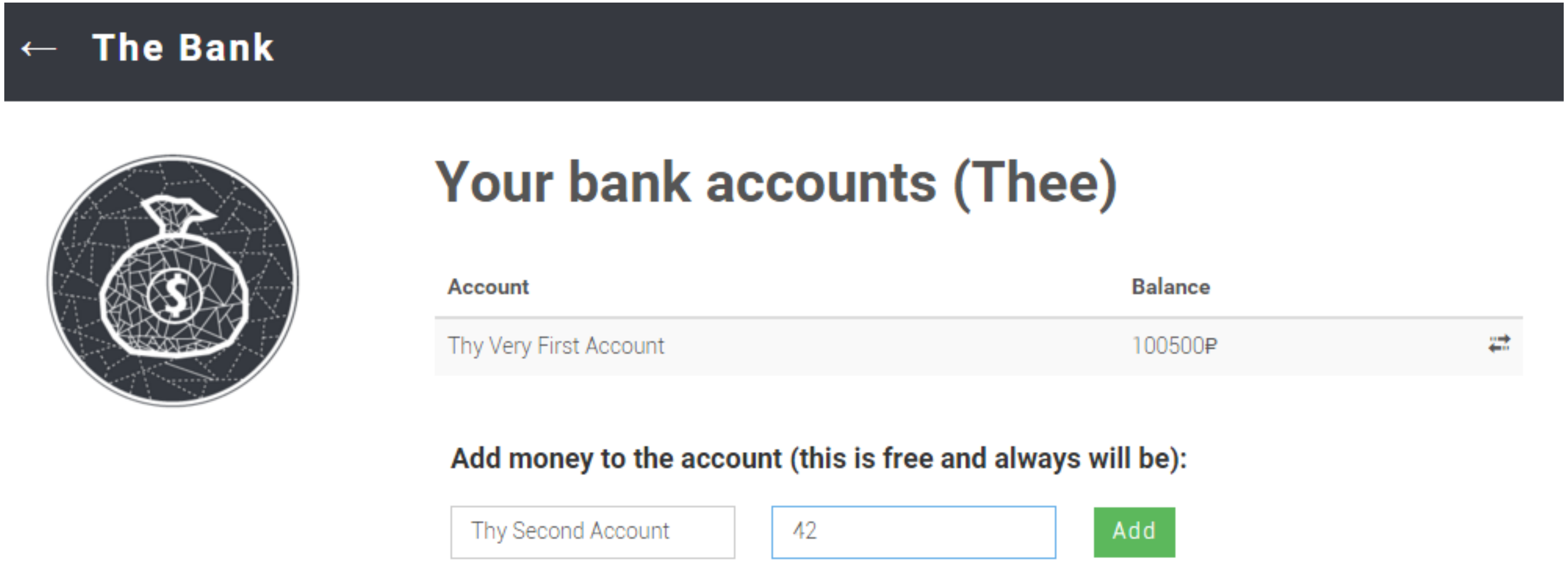
Alexander Bersenev aka bay

ABOUT SERVICE

- C
- Mongoose
- Custom dictionary



CREATE ACCOUNTS



← The Bank

Your bank accounts (Thee)

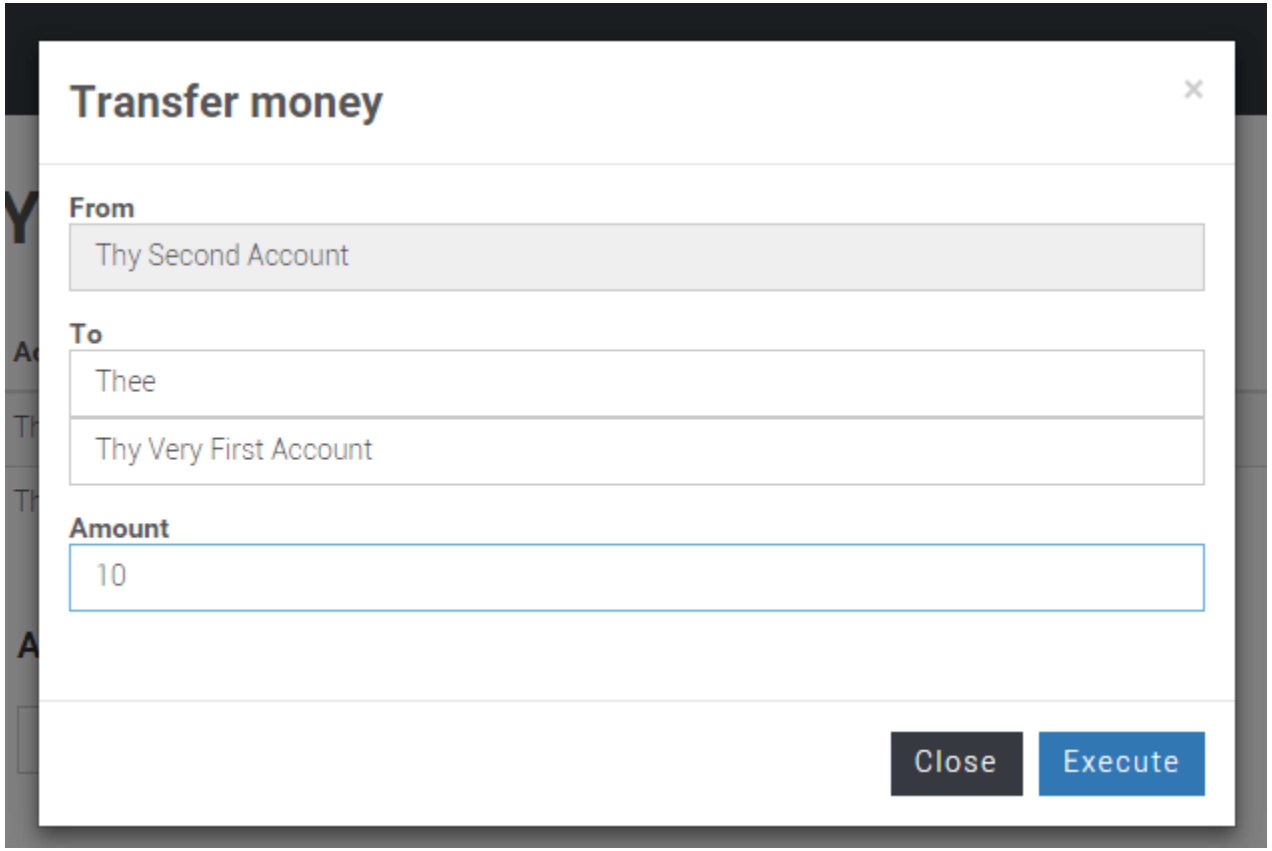
Account	Balance	
Thy Very First Account	100500₽	⇄

Add money to the account (this is free and always will be):

Thy Second Account

42

TRANSFER MONEY



Transfer money

From

Thy Second Account

To

Thee

Thy Very First Account

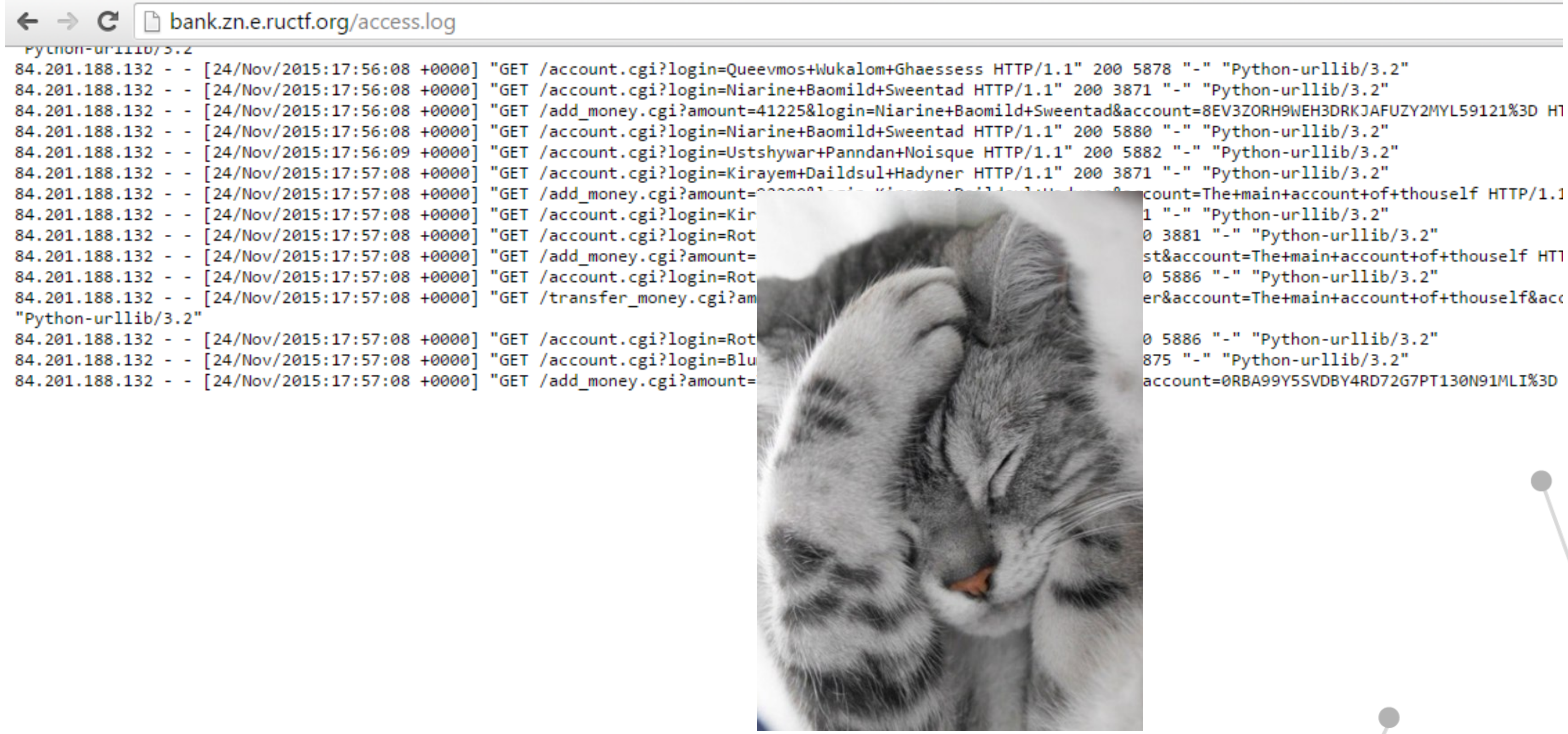
Amount

10

HACK IT!

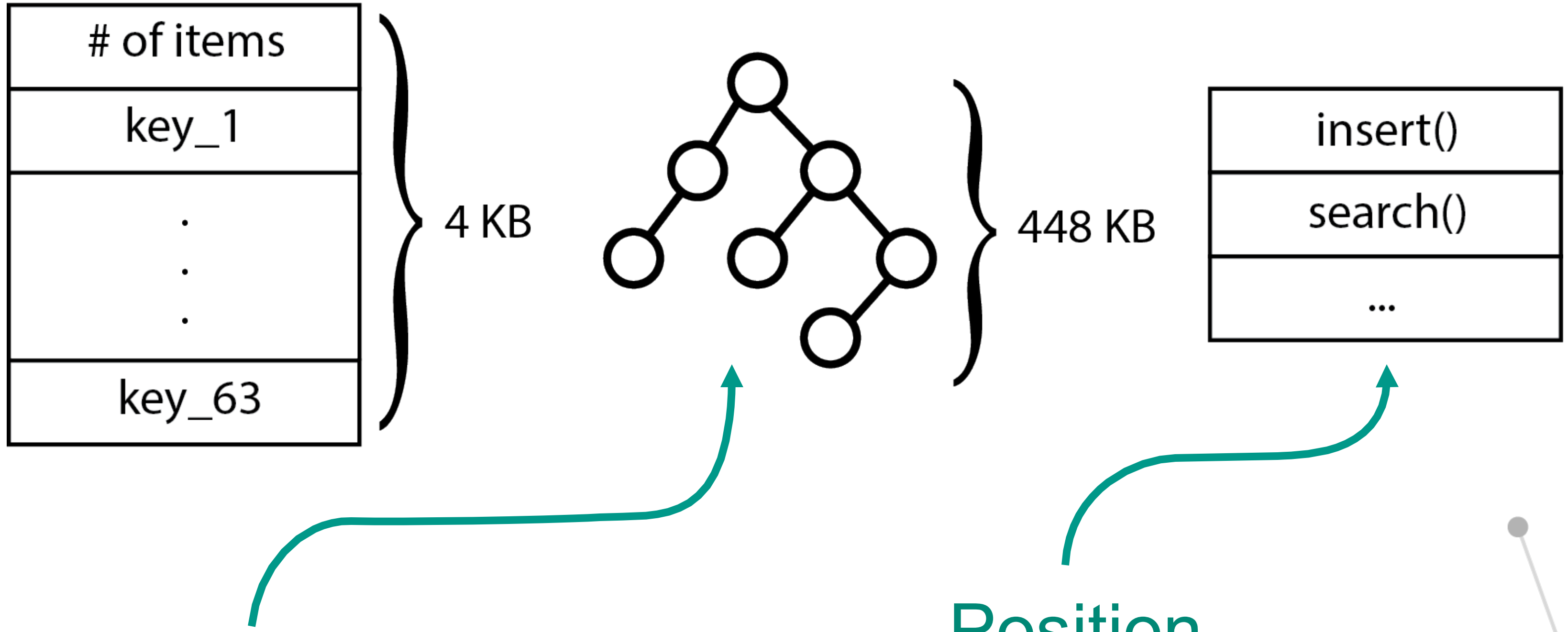
ACCESS LOGS

bank.teamX.e.ructf.org/access.log



```
"Python-urllib/3.2
84.201.188.132 - - [24/Nov/2015:17:56:08 +0000] "GET /account.cgi?login=Queevmos+Wukalom+Ghaessess HTTP/1.1" 200 5878 "-" "Python-urllib/3.2"
84.201.188.132 - - [24/Nov/2015:17:56:08 +0000] "GET /account.cgi?login=Niarine+Baomild+Sweentad HTTP/1.1" 200 3871 "-" "Python-urllib/3.2"
84.201.188.132 - - [24/Nov/2015:17:56:08 +0000] "GET /add_money.cgi?amount=41225&login=Niarine+Baomild+Sweentad&account=8EV3ZORH9WEH3DRKJAFUZY2MYL59121%3D HT
84.201.188.132 - - [24/Nov/2015:17:56:08 +0000] "GET /account.cgi?login=Niarine+Baomild+Sweentad HTTP/1.1" 200 5880 "-" "Python-urllib/3.2"
84.201.188.132 - - [24/Nov/2015:17:56:09 +0000] "GET /account.cgi?login=Ustshywar+Panndan+Noisque HTTP/1.1" 200 5882 "-" "Python-urllib/3.2"
84.201.188.132 - - [24/Nov/2015:17:57:08 +0000] "GET /account.cgi?login=Kirayem+Daildsul+Hadyner HTTP/1.1" 200 3871 "-" "Python-urllib/3.2"
84.201.188.132 - - [24/Nov/2015:17:57:08 +0000] "GET /add_money.cgi?amount=                              count=The+main+account+of+thouself HTTP/1.1
84.201.188.132 - - [24/Nov/2015:17:57:08 +0000] "GET /account.cgi?login=Kir                               1 "-" "Python-urllib/3.2"
84.201.188.132 - - [24/Nov/2015:17:57:08 +0000] "GET /account.cgi?login=Rot                               0 3881 "-" "Python-urllib/3.2"
84.201.188.132 - - [24/Nov/2015:17:57:08 +0000] "GET /add_money.cgi?amount=                               st&account=The+main+account+of+thouself HT
84.201.188.132 - - [24/Nov/2015:17:57:08 +0000] "GET /account.cgi?login=Rot                               0 5886 "-" "Python-urllib/3.2"
84.201.188.132 - - [24/Nov/2015:17:57:08 +0000] "GET /transfer_money.cgi?am                               er&account=The+main+account+of+thouself&acc
"Python-urllib/3.2"
84.201.188.132 - - [24/Nov/2015:17:57:08 +0000] "GET /account.cgi?login=Rot                               0 5886 "-" "Python-urllib/3.2"
84.201.188.132 - - [24/Nov/2015:17:57:08 +0000] "GET /account.cgi?login=Blu                               875 "-" "Python-urllib/3.2"
84.201.188.132 - - [24/Nov/2015:17:57:08 +0000] "GET /add_money.cgi?amount=                               account=0RBA99Y5SVDBY4RD72G7PT130N91MLI%3D
```

DICTIONARY



of items
key_1
· · ·
key_63

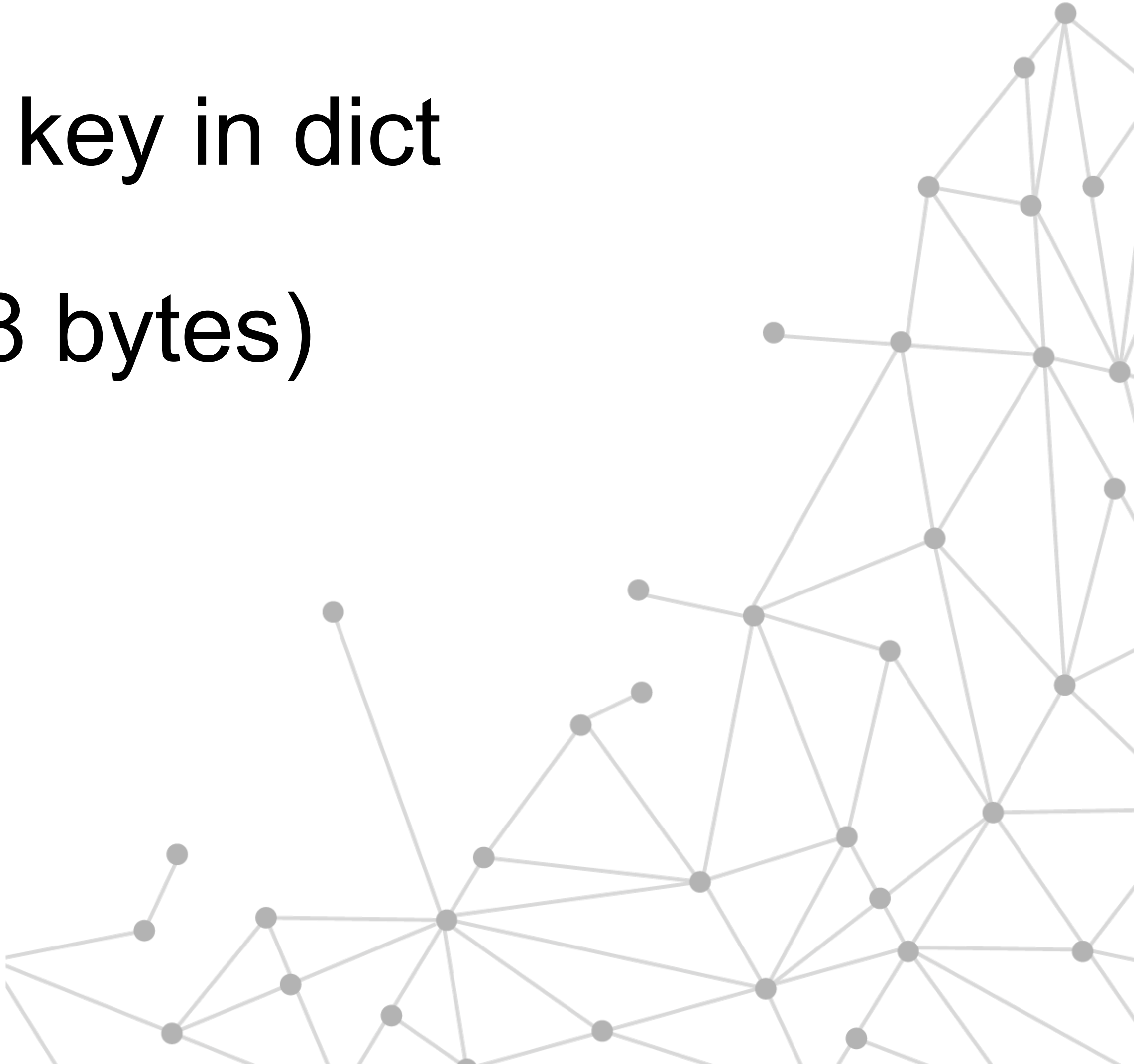
insert()
search()
...

Binary Search Tree

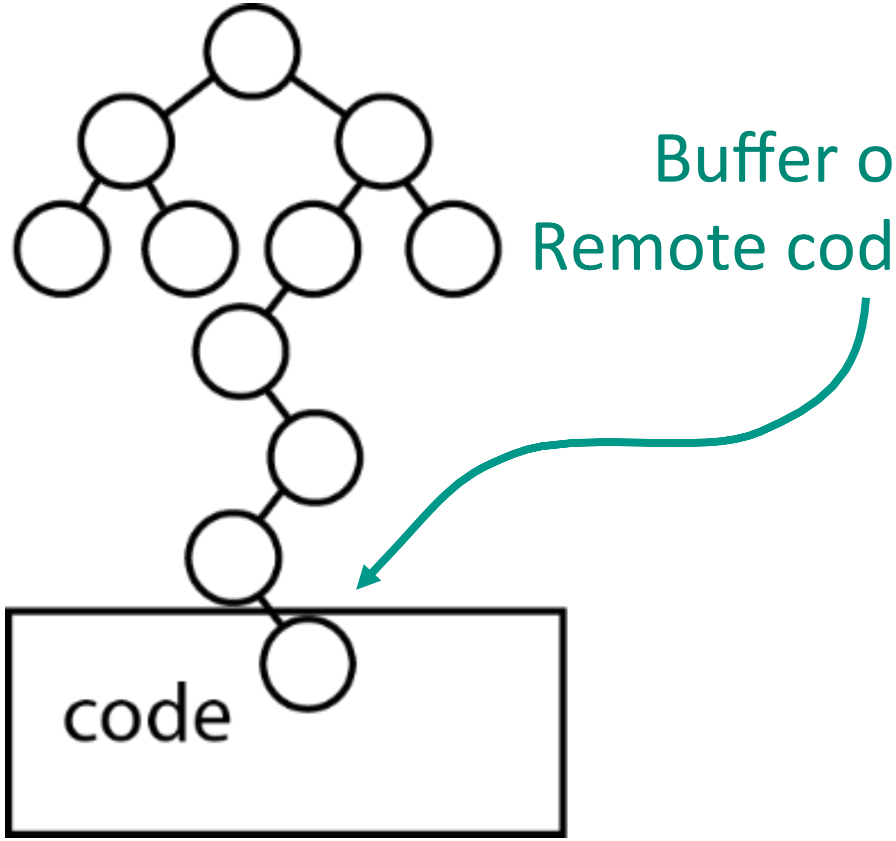
Position Independent Code

DICTIONARY

- Key in BST – SHA256 from key in dict
- Value – amount of money (8 bytes)
- BST stored in array



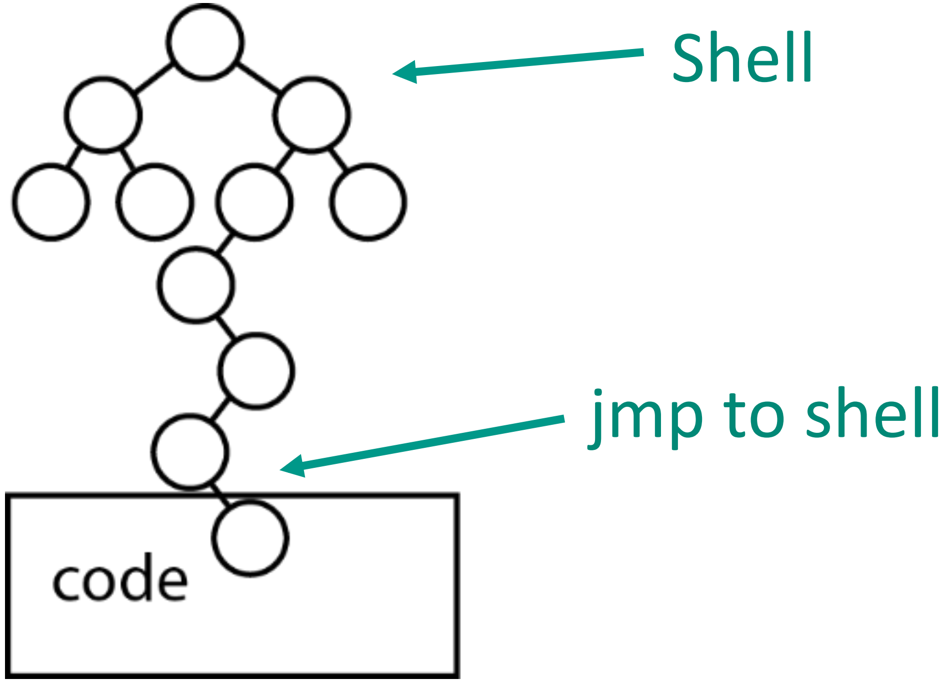
DICTIONARY



Buffer overflow

Remote code execution

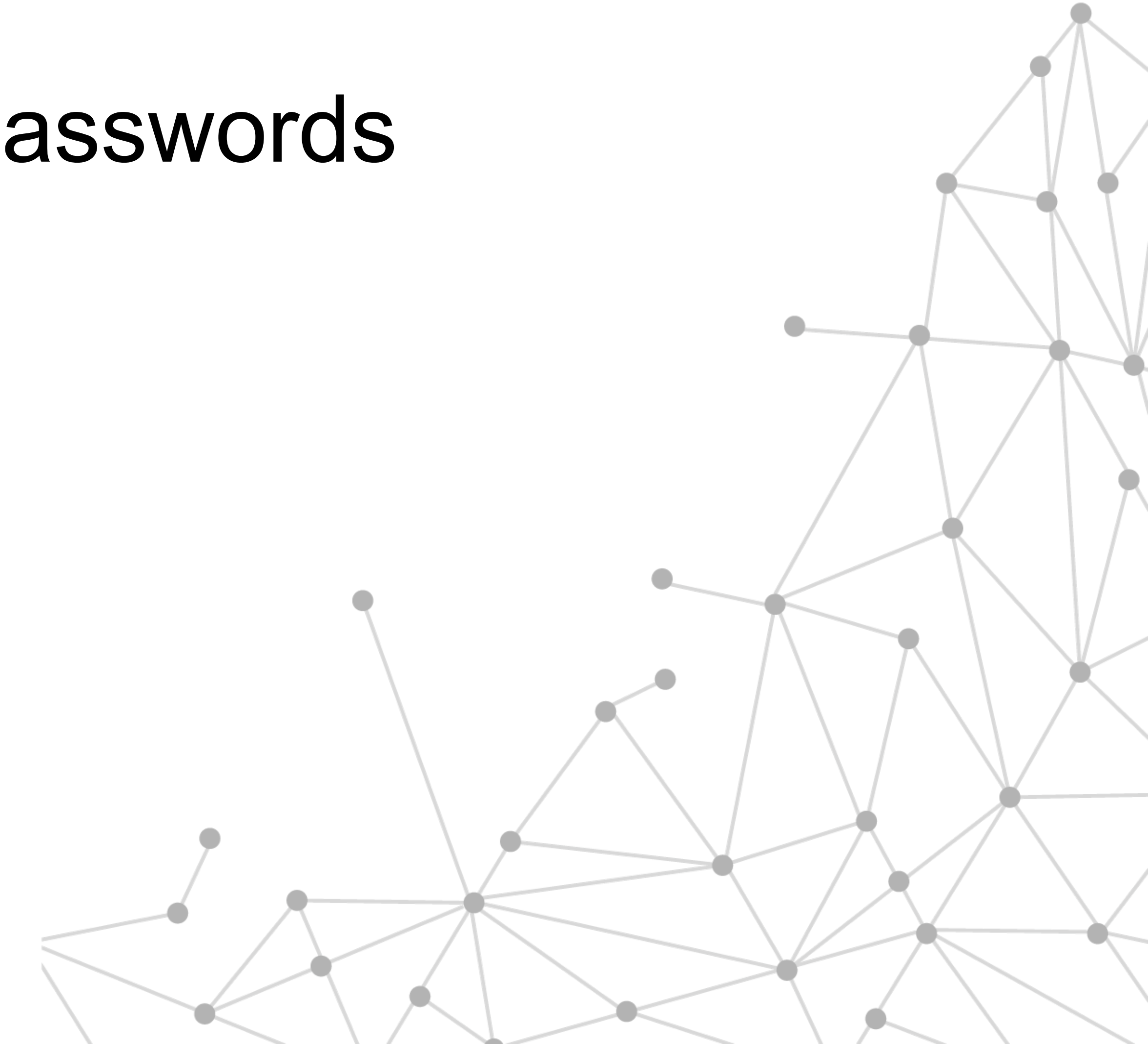
DICTIONARY



bit.ly/ructfe_bank_sploit

RECOMMENDATIONS

- Always change keys and passwords
- Learn Linux administration
- Stay positive & have fun!



Questions?

Thanks!

Сервисы

Ministry of Love

Interplanetary Migration Authority

Nasa Rasa

Сервисы

Health Monitor

Electro

Tax

Bank