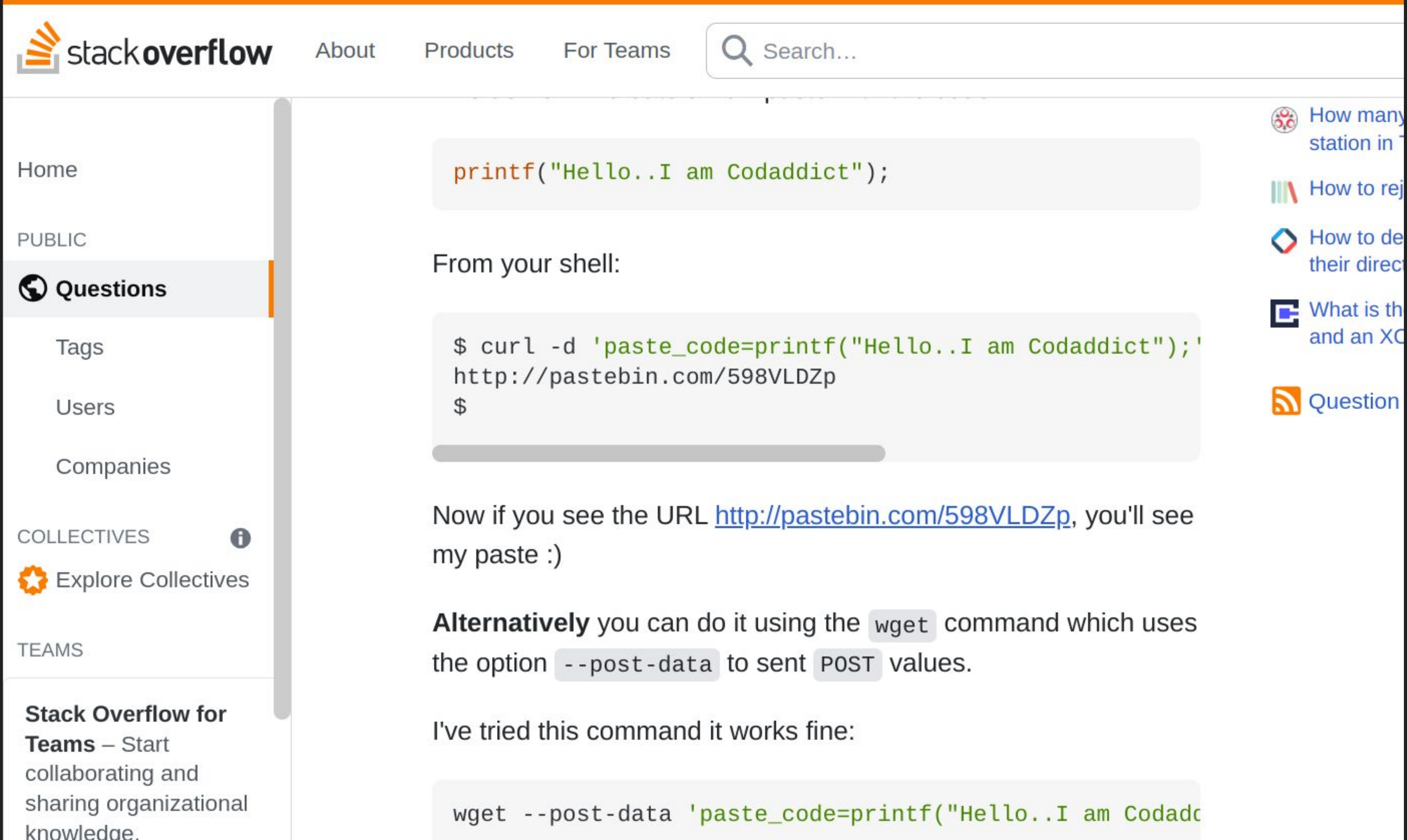
How to hack a $10M company?

The Story of an OpSec mistake

for educational purposes only

How it started?



Stack Overflow for Teams – Start collaborating and sharing organizational knowledge.

```
printf("Hello..I am Codaddict");
```

From your shell:

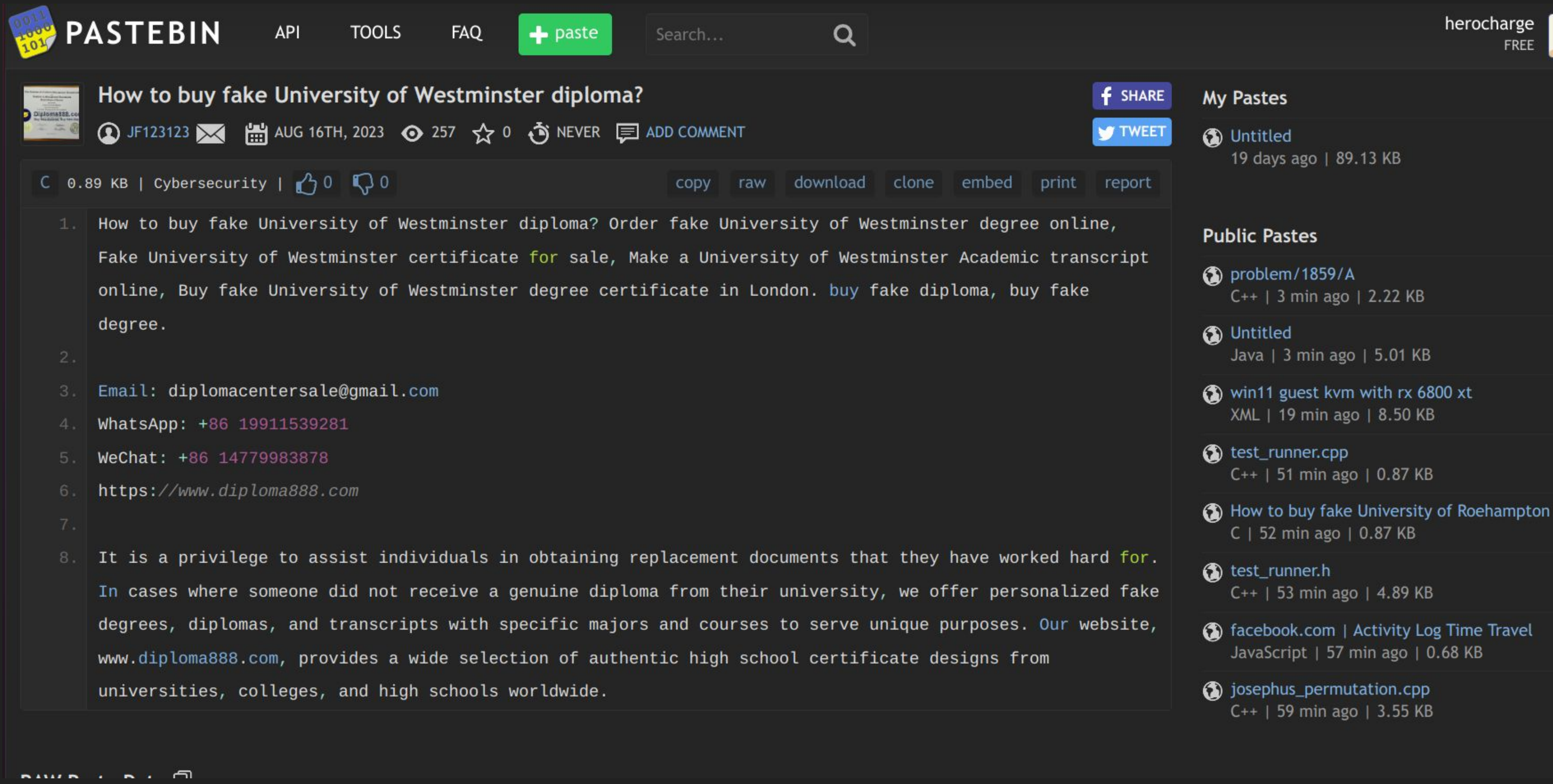
```
$ curl -d 'paste_code=printf("Hello..I am Codaddict");'
http://pastebin.com/598VLDZp
$
```

Now if you see the URL http://pastebin.com/598VLDZp, you'll see my paste :)

Alternatively you can do it using the `wget` command which uses the option `--post-data` to sent `POST` values.

I've tried this command it works fine:

```
wget --post-data 'paste_code=printf("Hello..I am Codadc
```



How to buy fake University of Westminster diploma?

JF123123 AUG 16TH, 2023 257 0 NEVER ADD COMMENT

C 0.89 KB | Cybersecurity | 0 0

```
How to buy fake University of Westminster diploma? Order fake University of Westminster degree online, Fake University of Westminster certificate for sale, Make a University of Westminster Academic transcript online, Buy fake University of Westminster degree certificate in London. buy fake diploma, buy fake degree.

Email: diplomacentersale@gmail.com
WhatsApp: +86 19911539281
WeChat: +86 14779983878
https://www.diploma888.com

It is a privilege to assist individuals in obtaining replacement documents that they have worked hard for. In cases where someone did not receive a genuine diploma from their university, we offer personalized fake degrees, diplomas, and transcripts with specific majors and courses to serve unique purposes. Our website, www.diploma888.com, provides a wide selection of authentic high school certificate designs from universities, colleges, and high schools worldwide.
```

My Pastes

Untitled
19 days ago | 89.13 KB

Public Pastes

problem/1859/A
C++ | 3 min ago | 2.22 KB

Untitled
Java | 3 min ago | 5.01 KB

win11 guest kvm with rx 6800 xt
XML | 19 min ago | 8.50 KB

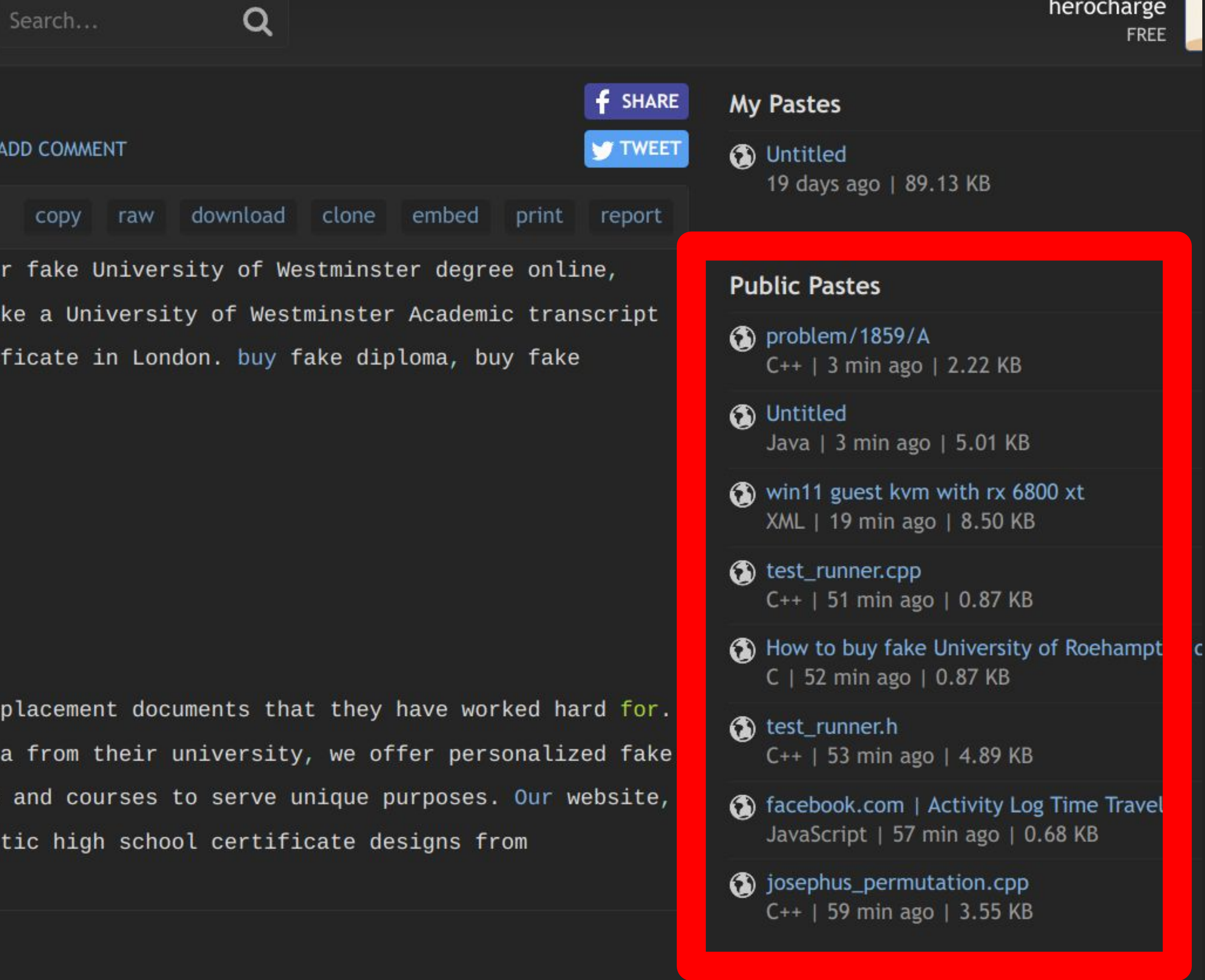
test_runner.cpp
C++ | 51 min ago | 0.87 KB

How to buy fake University of Roehampton
C | 52 min ago | 0.87 KB

test_runner.h
C++ | 53 min ago | 4.89 KB

facebook.com | Activity Log Time Travel
JavaScript | 57 min ago | 0.68 KB

josephus_permutation.cpp
C++ | 59 min ago | 3.55 KB



```
r fake University of Westminster degree online,
ke a University of Westminster Academic transcript
ficate in London. buy fake diploma, buy fake



placement documents that they have worked hard for.
a from their university, we offer personalized fake
 and courses to serve unique purposes. Our website,
tic high school certificate designs from
```

My Pastes

Untitled
19 days ago | 89.13 KB

Public Pastes

problem/1859/A
C++ | 3 min ago | 2.22 KB

Untitled
Java | 3 min ago | 5.01 KB

win11 guest kvm with rx 6800 xt
XML | 19 min ago | 8.50 KB

test_runner.cpp
C++ | 51 min ago | 0.87 KB

How to buy fake University of Roehampt
C | 52 min ago | 0.87 KB

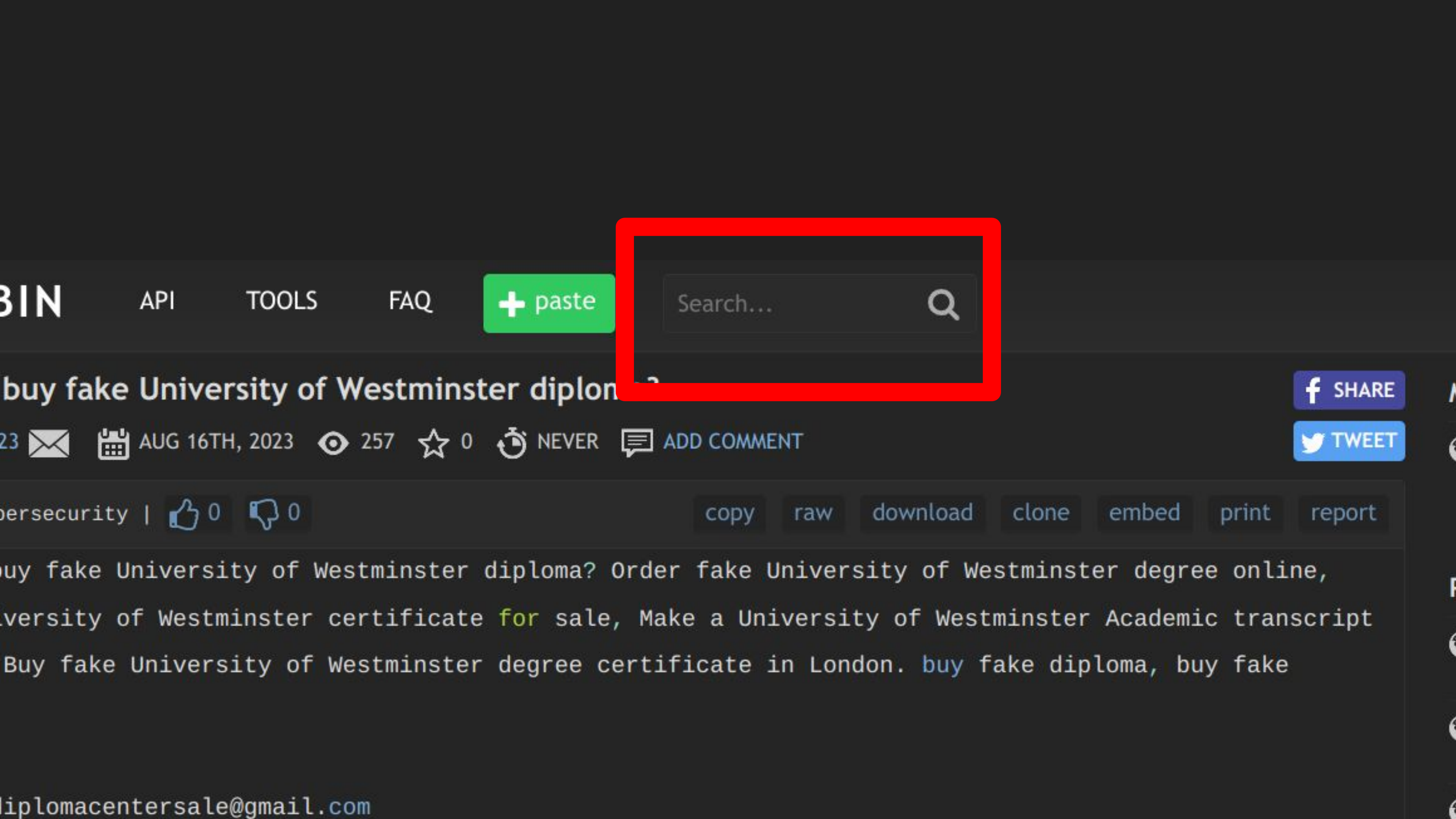
test_runner.h
C++ | 53 min ago | 4.89 KB

facebook.com | Activity Log Time Travel
JavaScript | 57 min ago | 0.68 KB

josephus_permutation.cpp
C++ | 59 min ago | 3.55 KB

pastebin social media?

whatever lets move on



buy fake University of Westminster diploma?

uy fake University of Westminster diploma? Order fake University of Westminster degree online,
versity of Westminster certificate for sale, Make a University of Westminster Academic transcript
 Buy fake University of Westminster degree certificate in London. buy fake diploma, buy fake

iplomacentersale@gmail.com

Wait!?
How many people share code on pastebin?

19 MILLION MONTHLY USERS
WITH 95 MILLION TOTAL ACTIVE PASTES !!!!

That's a lot of room to mess things up

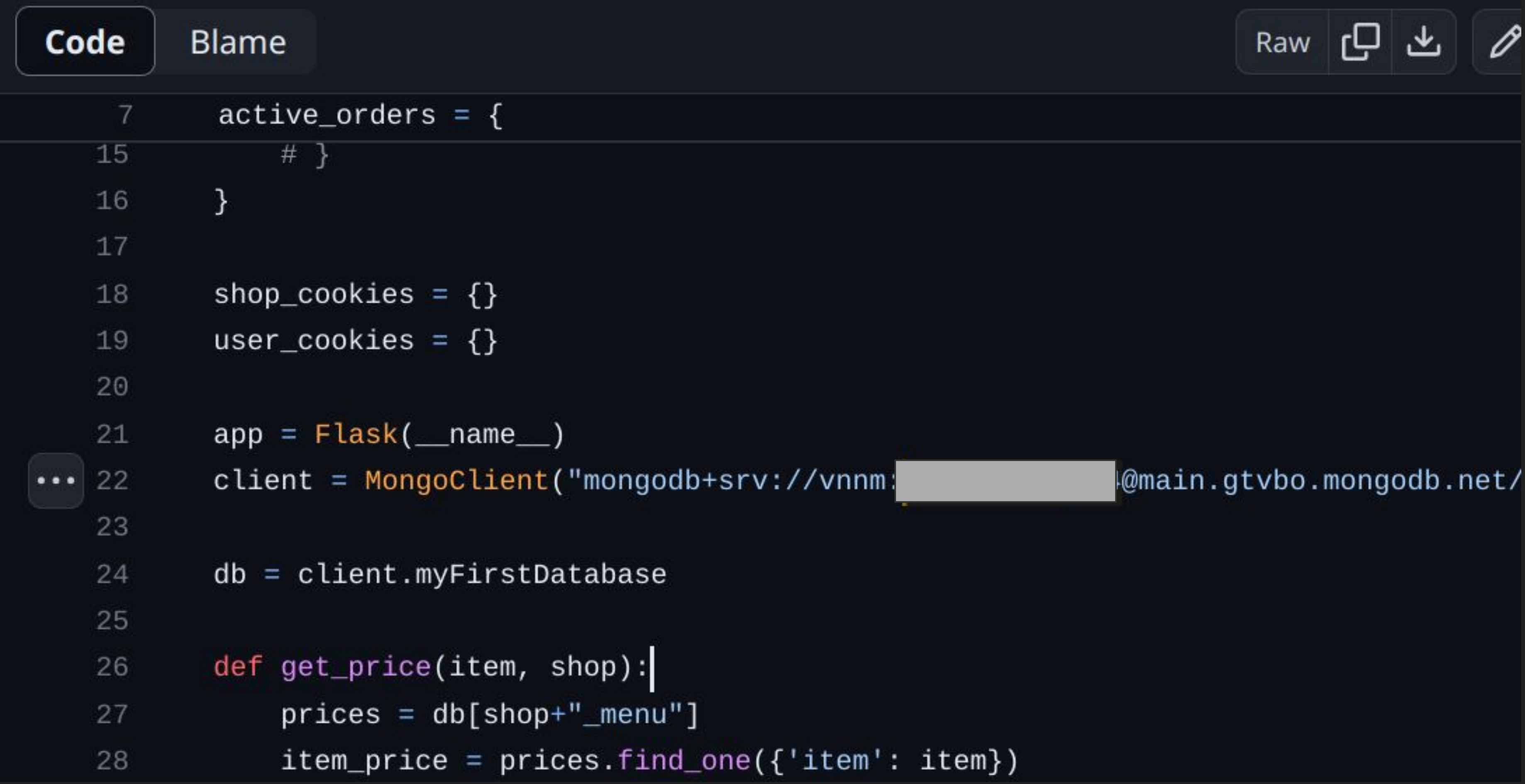
My Thoughts

- Mistakes happen

- People accidentally push confidential info to git all the time

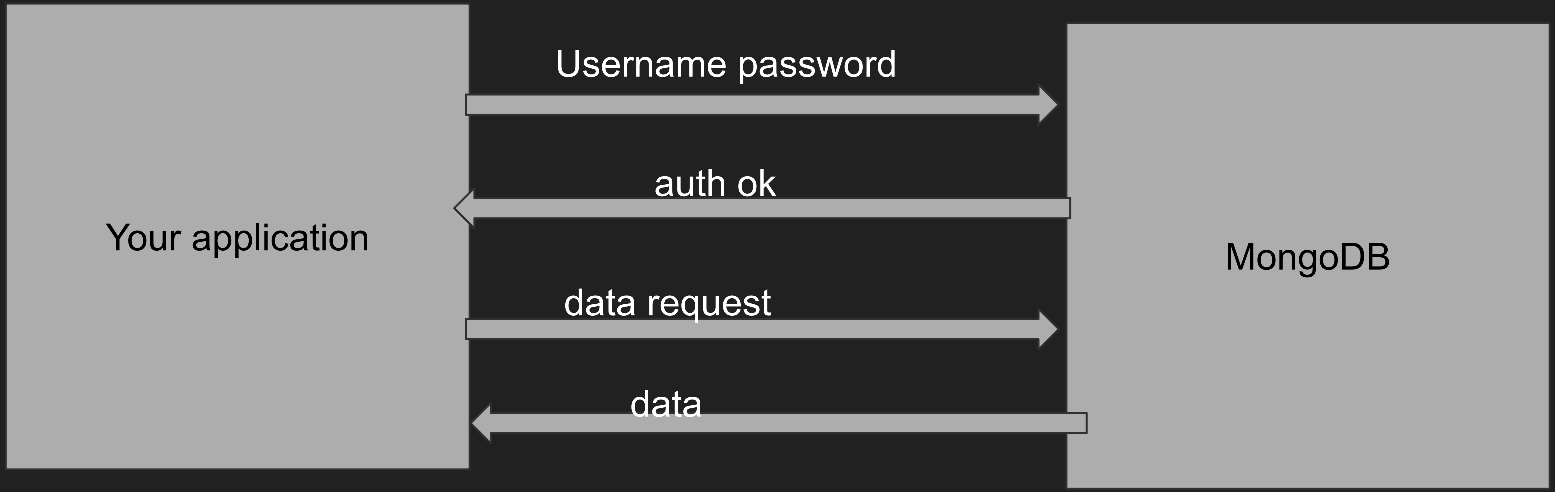
- Surely some one accidentally made a paste with confidential info

What do I search for tho?



```
active_orders = {
    # }
}

shop_cookies = {}
user_cookies = {}

app = Flask(__name__)
client = MongoClient("mongodb+srv://vnnm:[redacted]@main.gtvbo.mongodb.net/

db = client.myFirstDatabase

def get_price(item, shop):
    prices = db[shop+"_menu"]
    item_price = prices.find_one({'item': item})
```

Mongo client to server communication



Your application

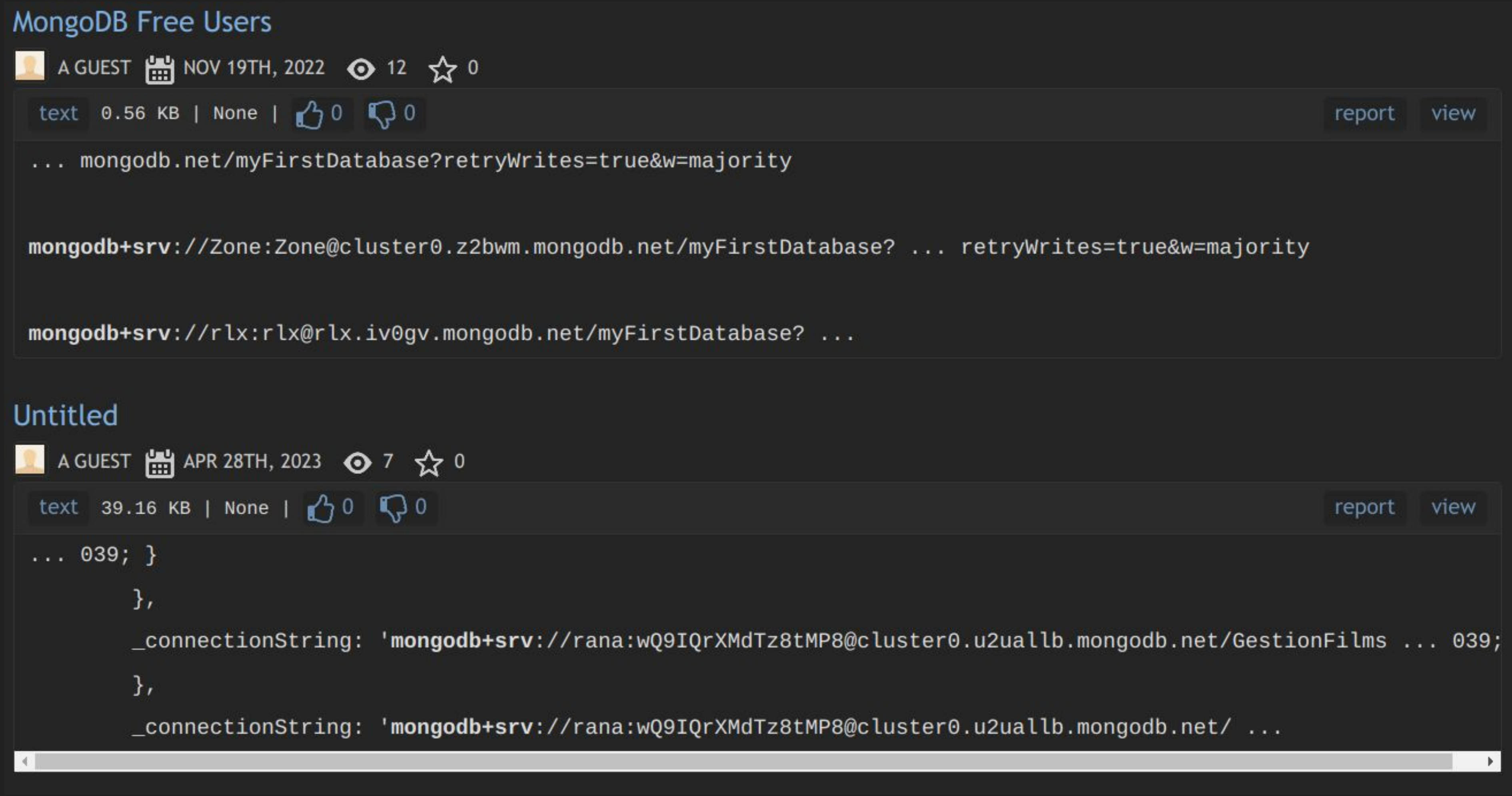
Username password

auth ok

data request

data

MongoDB



MongoDB Free Users

A GUEST NOV 19TH, 2022 👁 12 ☆ 0

text 0.56 KB | None | 👍 0 👎 0 report view

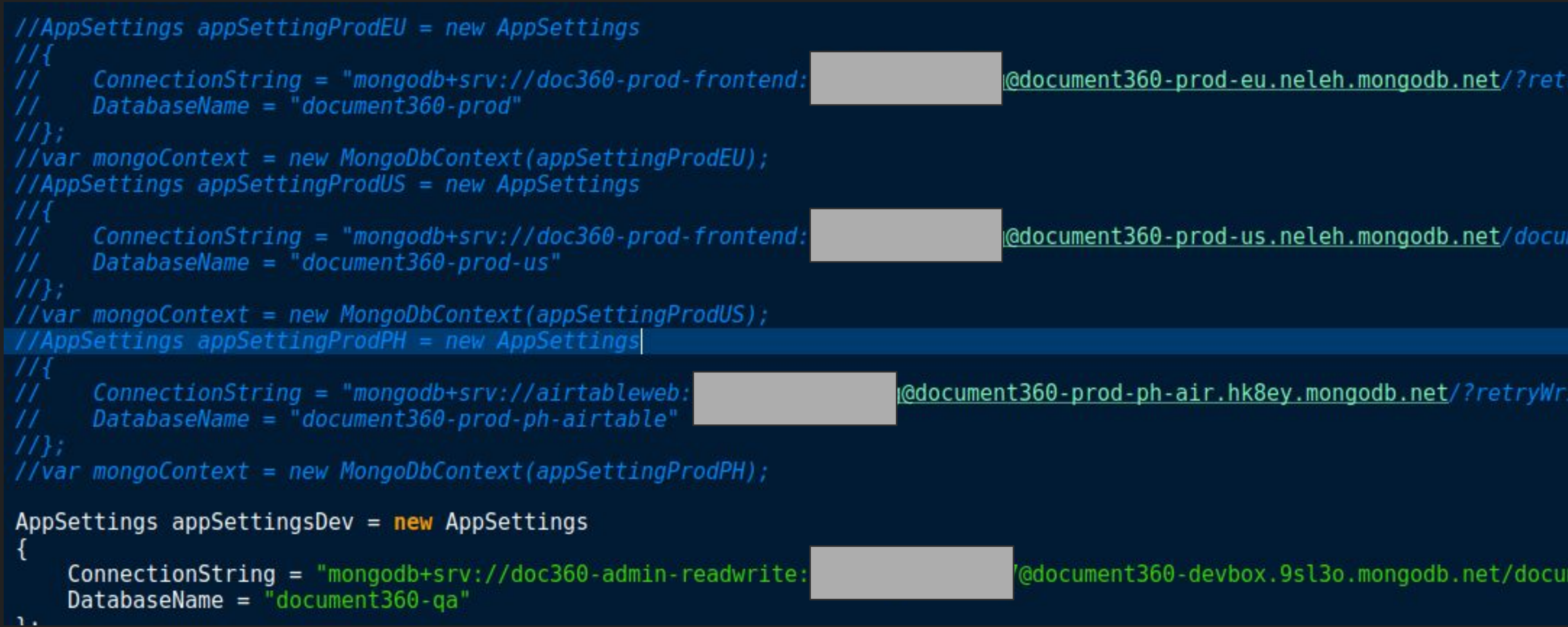
```
... mongodb.net/myFirstDatabase?retryWrites=true&w=majority


mongodb+srv://Zone:Zone@cluster0.z2bwm.mongodb.net/myFirstDatabase? ... retryWrites=true&w=majority


mongodb+srv://rlx:rlx@rlx.iv0gv.mongodb.net/myFirstDatabase? ...
```

Untitled

A GUEST APR 28TH, 2023 👁 7 ☆ 0

text 39.16 KB | None | 👍 0 👎 0 report view

```
... 039; }
        },
        _connectionString: 'mongodb+srv://rana:wQ9IQrXMdTz8tMP8@cluster0.u2uallb.mongodb.net/GestionFilms ... 039;
        },
        _connectionString: 'mongodb+srv://rana:wQ9IQrXMdTz8tMP8@cluster0.u2uallb.mongodb.net/ ...
```



```
//AppSettings appSettingProdEU = new AppSettings
//{
//    ConnectionString = "mongodb+srv://doc360-prod-frontend:[redacted]@document360-prod-eu.neleh.mongodb.net/?ret
//    DatabaseName = "document360-prod"
//};
//var mongoContext = new MongoDbContext(appSettingProdEU);
//AppSettings appSettingProdUS = new AppSettings
//{
//    ConnectionString = "mongodb+srv://doc360-prod-frontend:[redacted]@document360-prod-us.neleh.mongodb.net/docu
//    DatabaseName = "document360-prod-us"
//};
//var mongoContext = new MongoDbContext(appSettingProdUS);
//AppSettings appSettingProdPH = new AppSettings
//{
//    ConnectionString = "mongodb+srv://airtableweb:[redacted]@document360-prod-ph-air.hk8ey.mongodb.net/?retryWr
//    DatabaseName = "document360-prod-ph-airtable"
//};
//var mongoContext = new MongoDbContext(appSettingProdPH);

AppSettings appSettingsDev = new AppSettings
{
    ConnectionString = "mongodb+srv://doc360-admin-readwrite:[redacted]@document360-devbox.9sl3o.mongodb.net/docu
    DatabaseName = "document360-qa"
};
```

What did I find?

- All customer's data including payment information

- All emails sent to customers

- Unreleased web pages, etc.

What did I find?

- All customer's data including payment information

- All emails sent to customers

- Unreleased web pages, etc.

- API KEYS!!!!!!

What are APIs and why do we need them?

What are APIs and why do we need them?

When we are building an application, we dont want to build everything from scratch.

What are APIs and why do we need them?

When we are building an application, we dont want to build everything from scratch.

Things like payment systems and email servers are tedious to implement.

What are APIs and why do we need them?

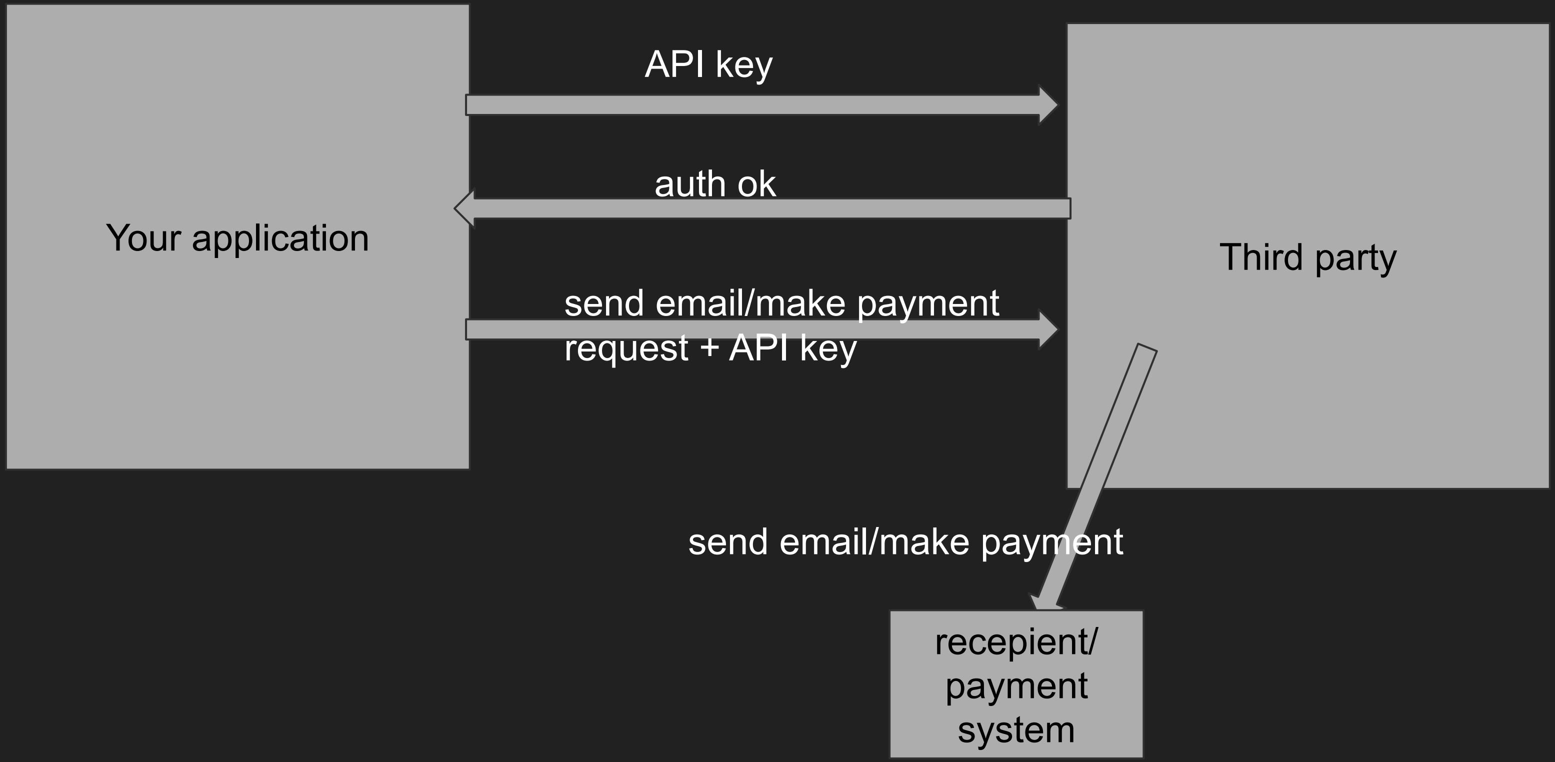
When we are building an application, we dont want to build everything from scratch.

Things like payment systems and email servers are tedious to implement.

So we use third party services to do these for us. (eg: stripe for payment, sendgrid for emails)

API keys are basically passwords to tell the third parties that it's you who is requesting a particular operation.

Application to Third Party comms



Your application

API key

auth ok

send email/make payment request + API key

Third party

send email/make payment

recepient/ payment system

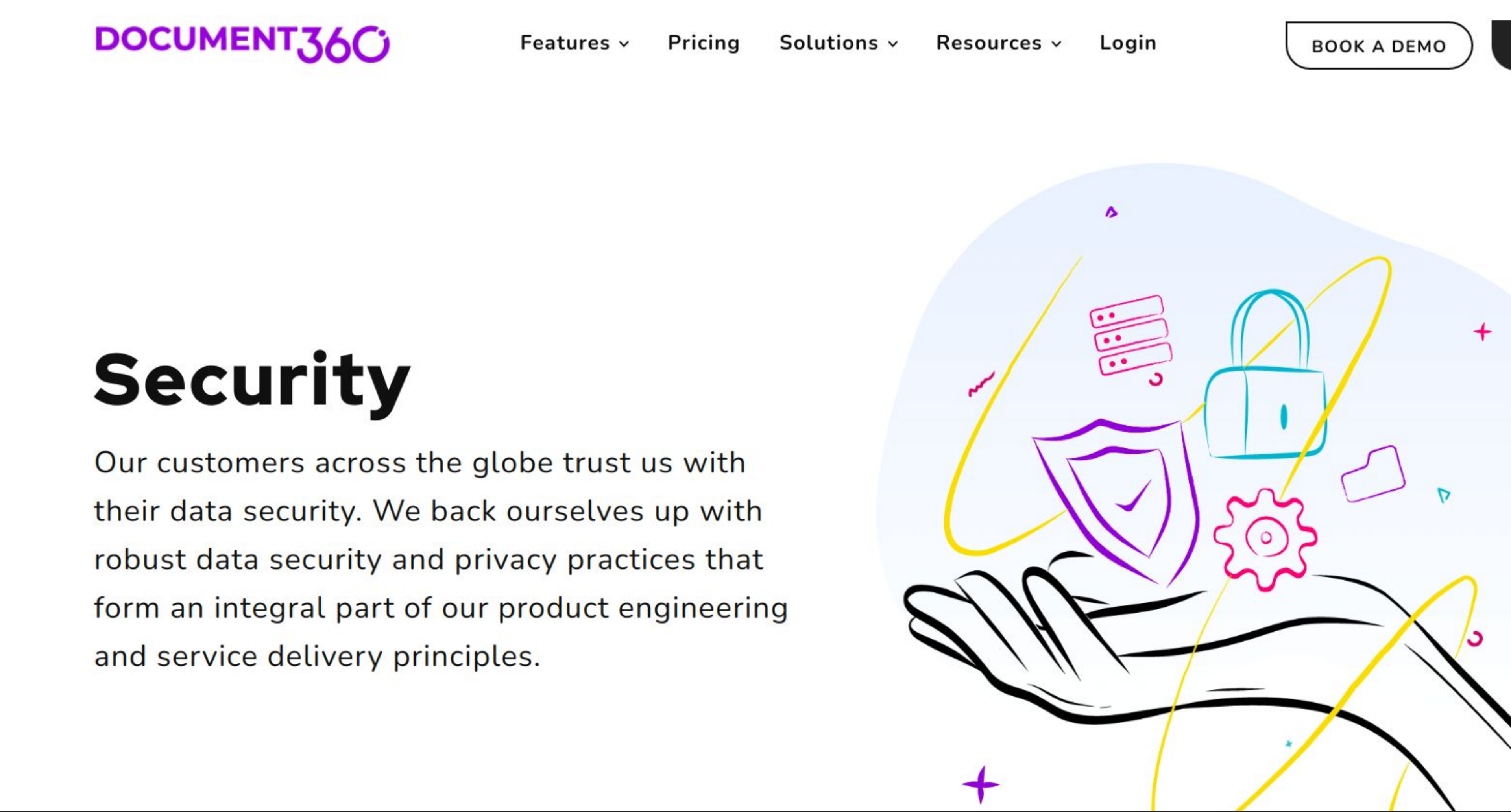
The database had API keys for:

- Stripe payment services
- SendGrid mailing services
- Microsoft translation
- Some analytics tools
- etc

DEMO TIMEE!!!

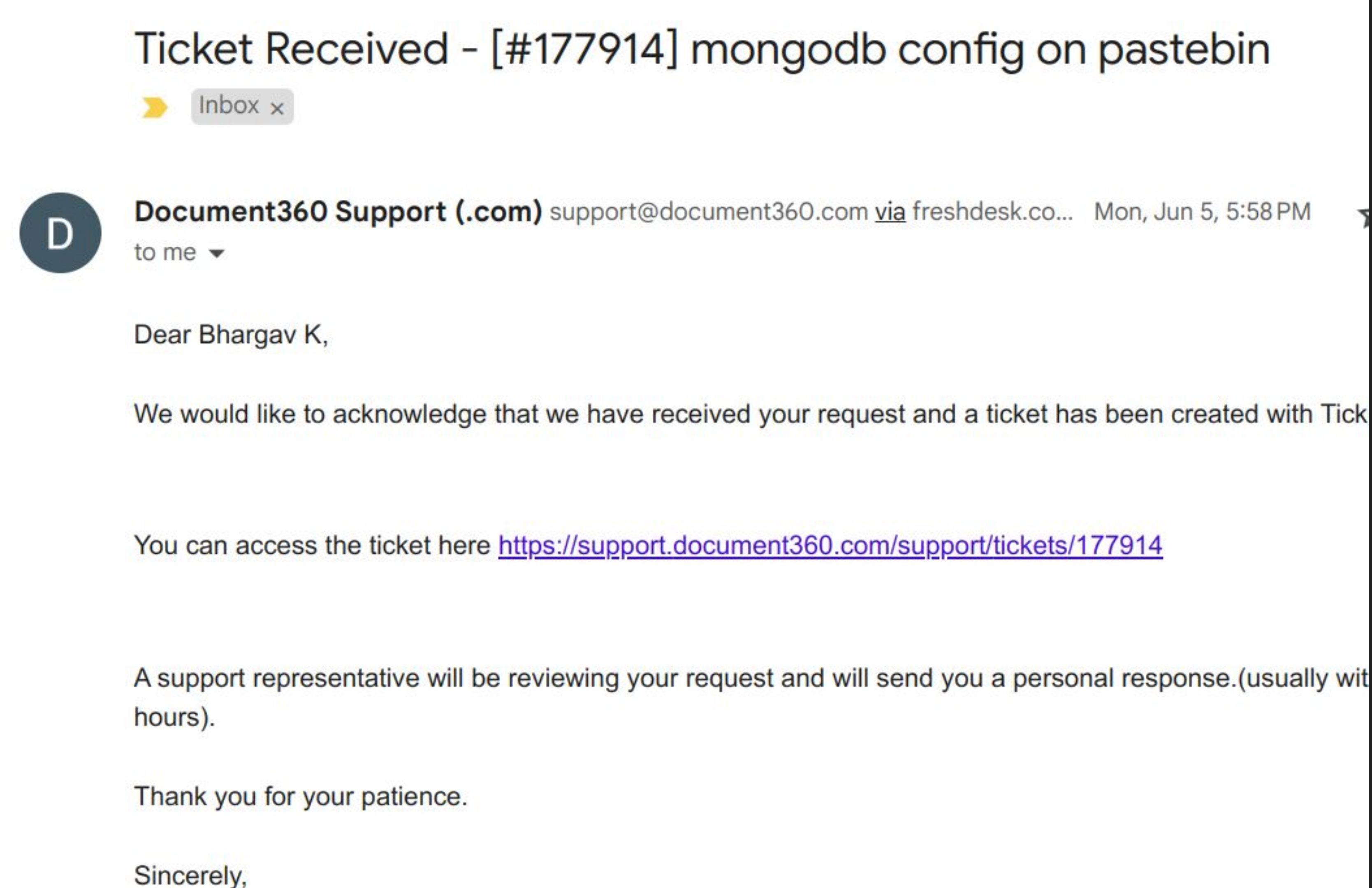
Even Worse

I had edit access



Security

Our customers across the globe trust us with their data security. We back ourselves up with robust data security and privacy practices that form an integral part of our product engineering and service delivery principles.



Ticket Received - [#177914] mongodb config on pastebin

Document360 Support (.com) support@document360.com via freshdesk.co... Mon, Jun 5, 5:58 PM

to me

Dear Bhargav K,

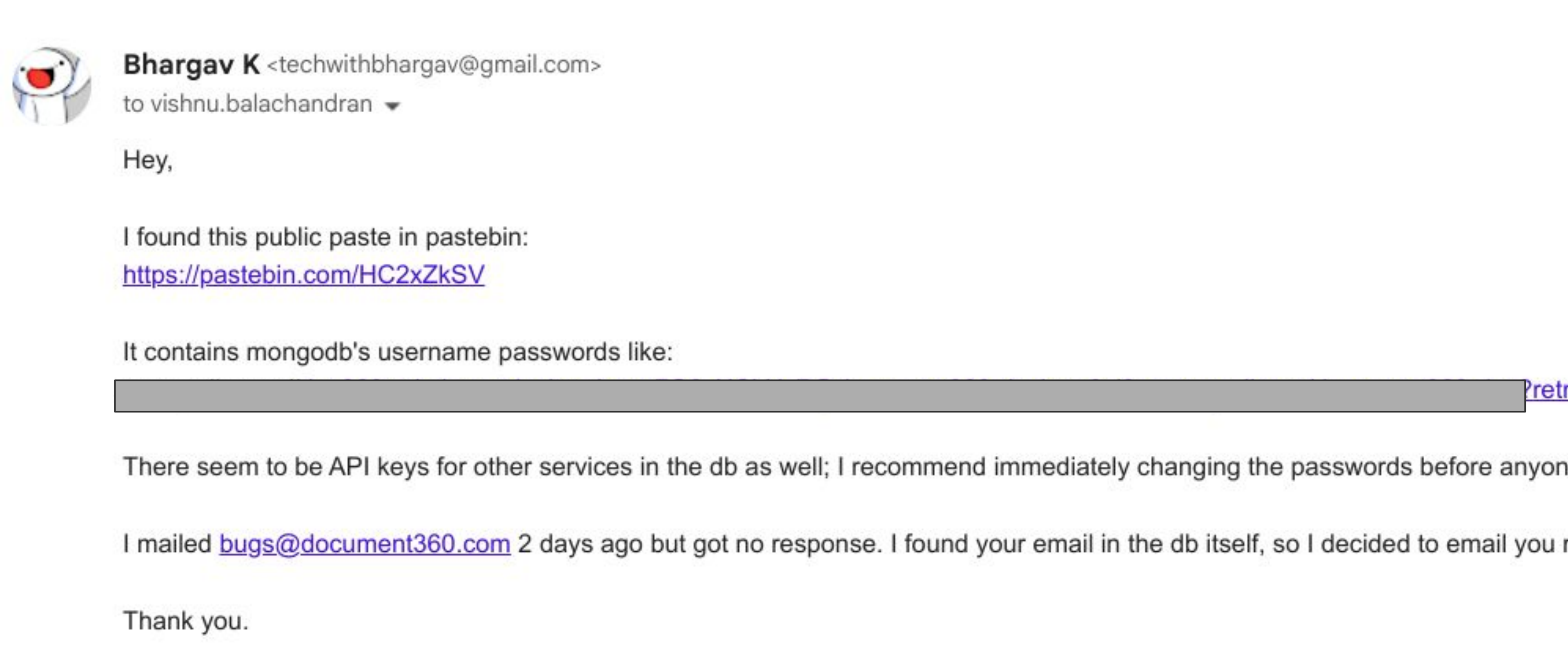
We would like to acknowledge that we have received your request and a ticket has been created with Tick

You can access the ticket here https://support.document360.com/support/tickets/177914

A support representative will be reviewing your request and will send you a personal response.(usually wit hours).

Thank you for your patience.

Sincerely,



Bhargav K <techwithbhargav@gmail.com>

to vishnu.balachandran

Hey,

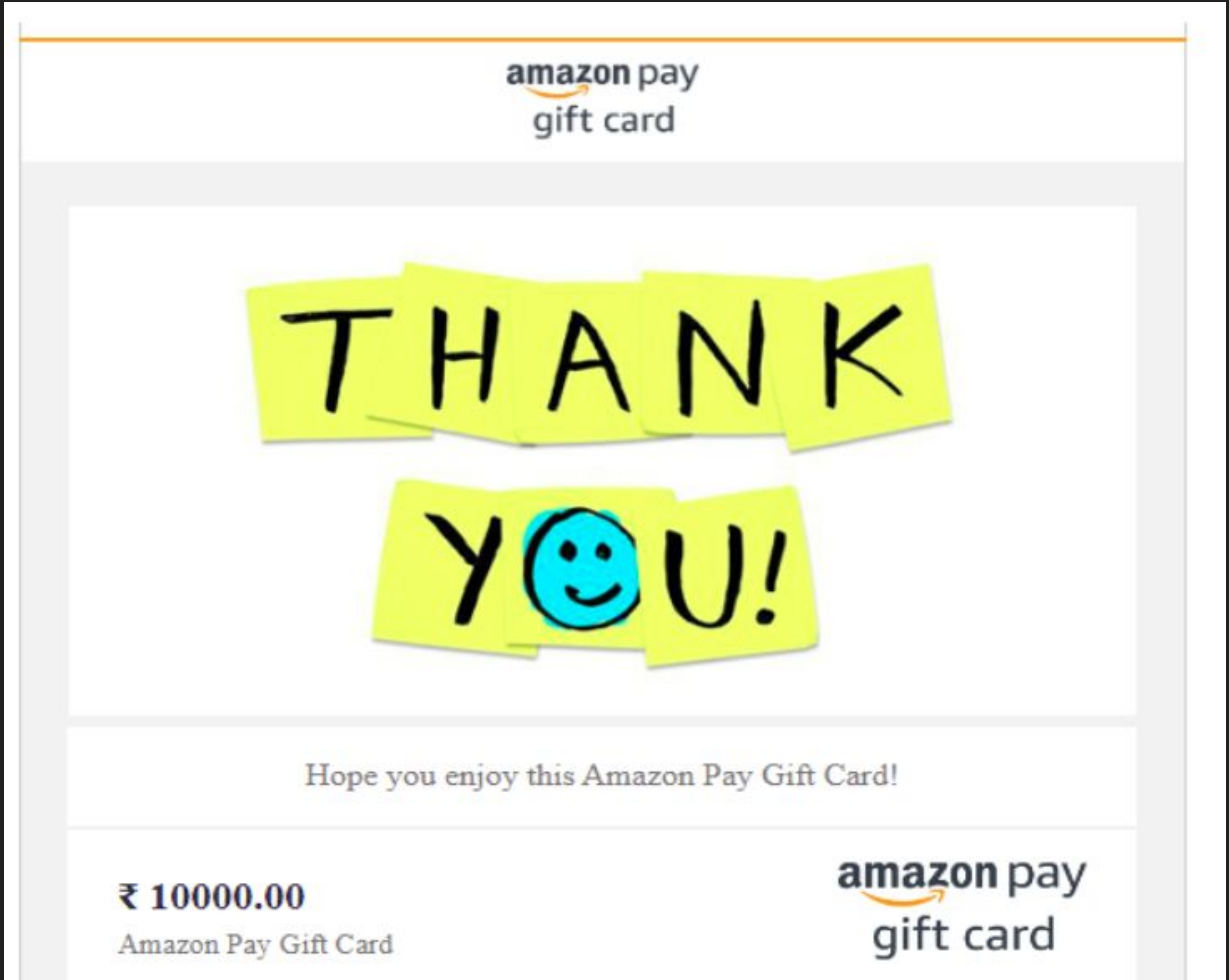
I found this public paste in pastebin:
https://pastebin.com/HC2xZkSV

It contains mongodb's username passwords like:
[redacted]

There seem to be API keys for other services in the db as well; I recommend immediately changing the passwords before anyon

I mailed bugs@document360.com 2 days ago but got no response. I found your email in the db itself, so I decided to email you

Thank you.



amazon pay
gift card

Hope you enjoy this Amazon Pay Gift Card!

₹ 10000.00

Amazon Pay Gift Card

amazon pay
gift card

What are bug bounties?

Company make product

What are bug bounties?

Company make product

Product might have vulnerabilities

What are bug bounties?

Company make product

Product might have vulnerabilities

Anyone might be able to find these vulnerabilities

What are bug bounties?

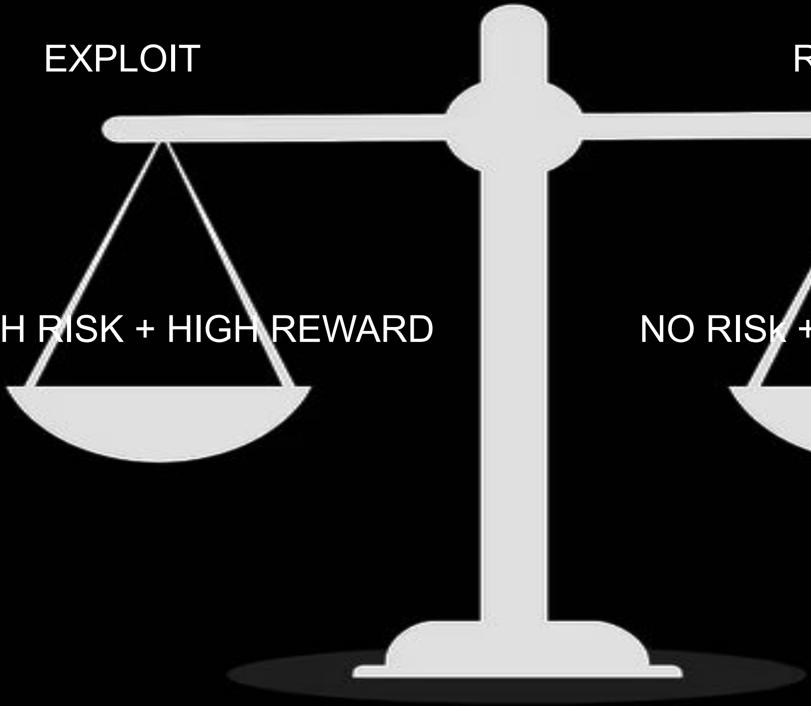
Company make product

Product might have vulnerabilities

Anyone might be able to find these vulnerabilities

Incentivize hackers to report the bugs rather than exploiting them.

HACKER'S OPTIONS



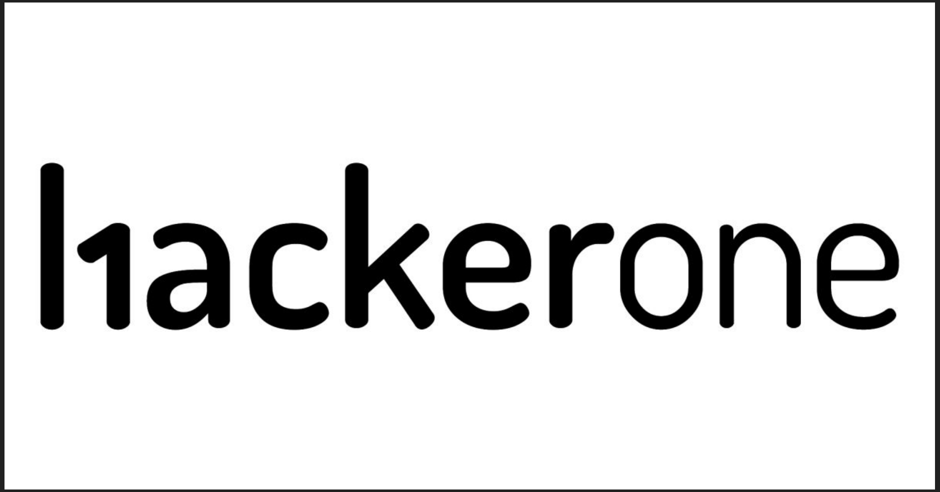
EXPLOIT

HIGH RISK + HIGH REWARD

REPORT

NO RISK + DECENT REWARD

INTIGRITI



hackerone

What went wrong?

Two scenarios:

What went wrong?

Two scenarios:

- It was an accident

What went wrong?

Two scenarios:

- It was an accident

- Malicious employee

How to stop a leak like this in first place?

- Its not possible to completely prevent something like this.

- But companies can take measures to mitigate the damage.

How to stop a leak like this in first place?

- Its not possible to completely prevent something like this.

- But companies can take measures to mitigate the damage.

- Not every employee needs to have access to every single part of the product.

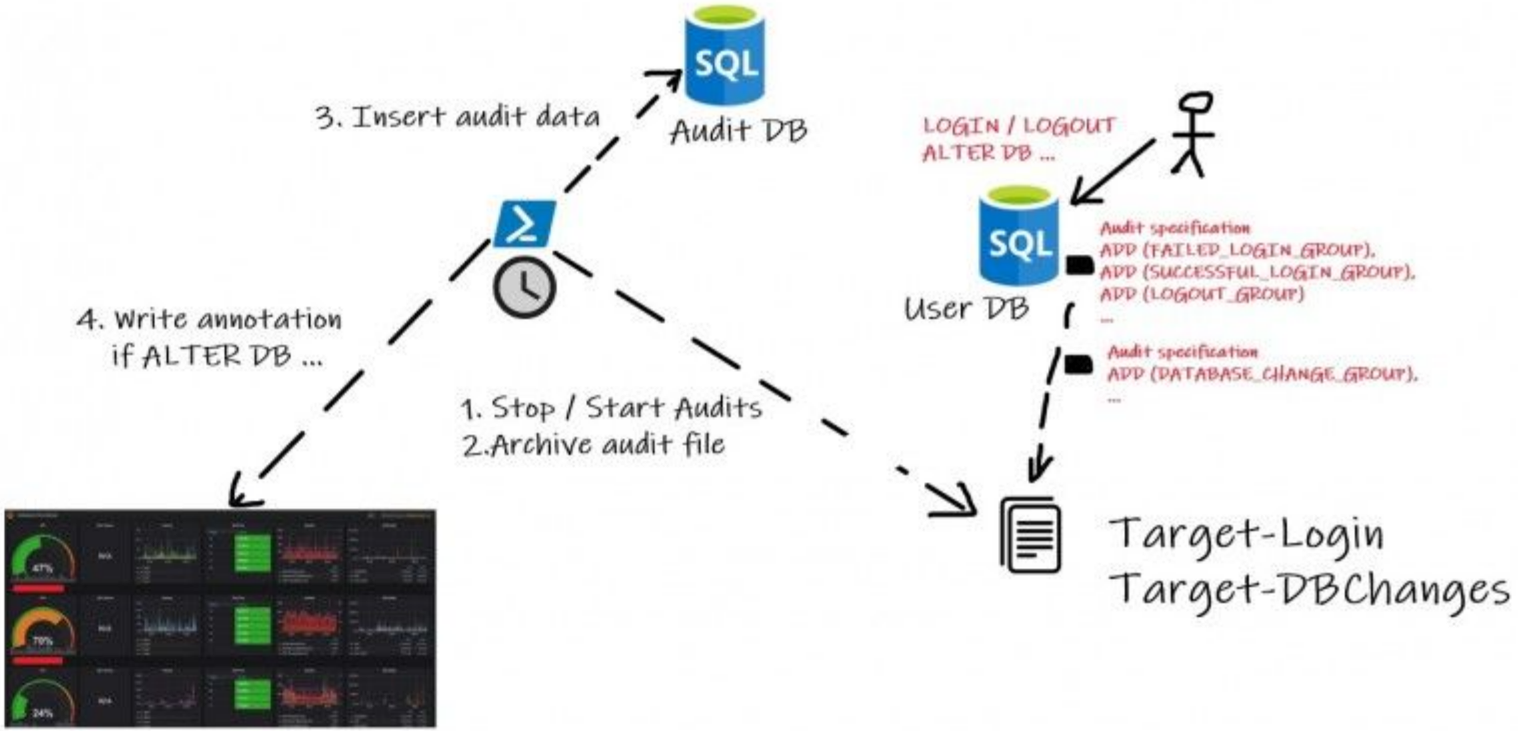
How to stop a leak like this in first place?

- Its not possible to completely prevent something like this.
- But companies can take measures to mitigate the damage.
- Not every employee needs to have access to every single part of the product.
- Use secure methods of communication (like end-to-end encrypted platforms eg: signal).
- Have internal tools that are airgapped from the public.

What can we do to make the life of hacker hard?

(just in case, the password gets leaked)

- Two factor authentication
- Information auditing systems
- firewalls


SQL
Audit DB
3. Insert audit data
LOGIN / LOGOUT
ALTER DB ...
SQL
User DB
Audit specification
ADD (FAILED_LOGIN_GROUP),
ADD (SUCCESSFUL_LOGIN_GROUP),
ADD (LOGOUT_GROUP)
...
Audit specification
ADD (DATABASE_CHANGE_GROUP),
...
4. Write annotation
if ALTER DB ...
1. Stop / Start Audits
2.Archive audit file
Target-Login
Target-DBChanges
47%
70%
24%

Principle of Least Privilege

Do you really need to give every user both read and write permisssions?

Principle of Least Privilege

Give processes / applications / users just enough permissions to get their work done, nothing more.

When POLP isnt followed

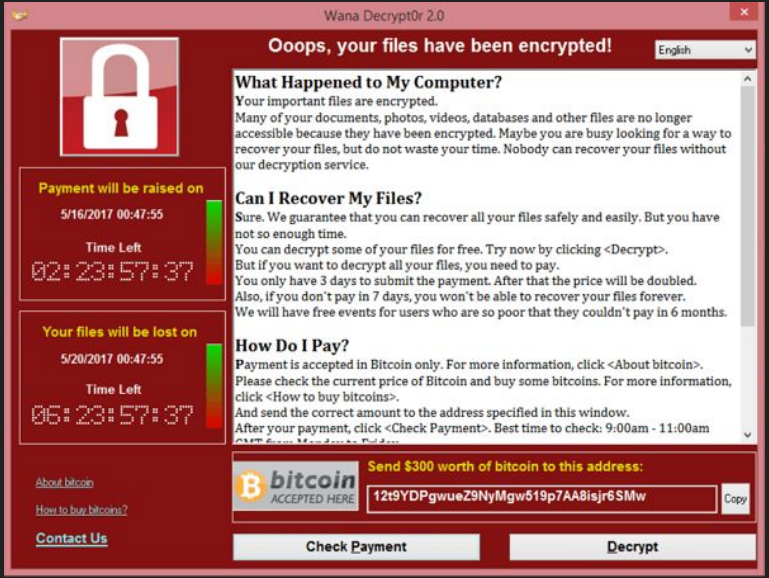
Edward Snowden and NSA Leaks:

In the case of Edward Snowden, a former NSA contractor, having overly broad access privileges allowed him to steal and leak classified government documents. Implementing POLP by limiting access to sensitive data to only those who genuinely needed it could have reduced the risk of such a massive data breach.

When POLP isnt followed

WannaCry Ransomware Attack (2017):

WannaCry spread across networks by exploiting a Windows vulnerability. If organizations had employed POLP by restricting unnecessary network access and ensuring timely patching, the ransomware's propagation could have been curtailed.



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

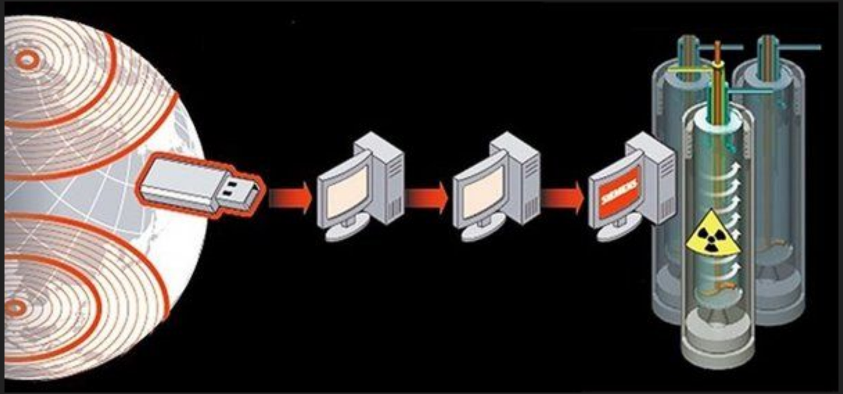
Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

When POLP isnt followed

Stuxnet Worm (2010):

Stuxnet targeted industrial control systems and spread through USB drives. If only essential personnel had been allowed to use USB drives on critical systems, the impact of the worm could have been limited.



Thank You

https://linktr.ee/0x1337_iiith