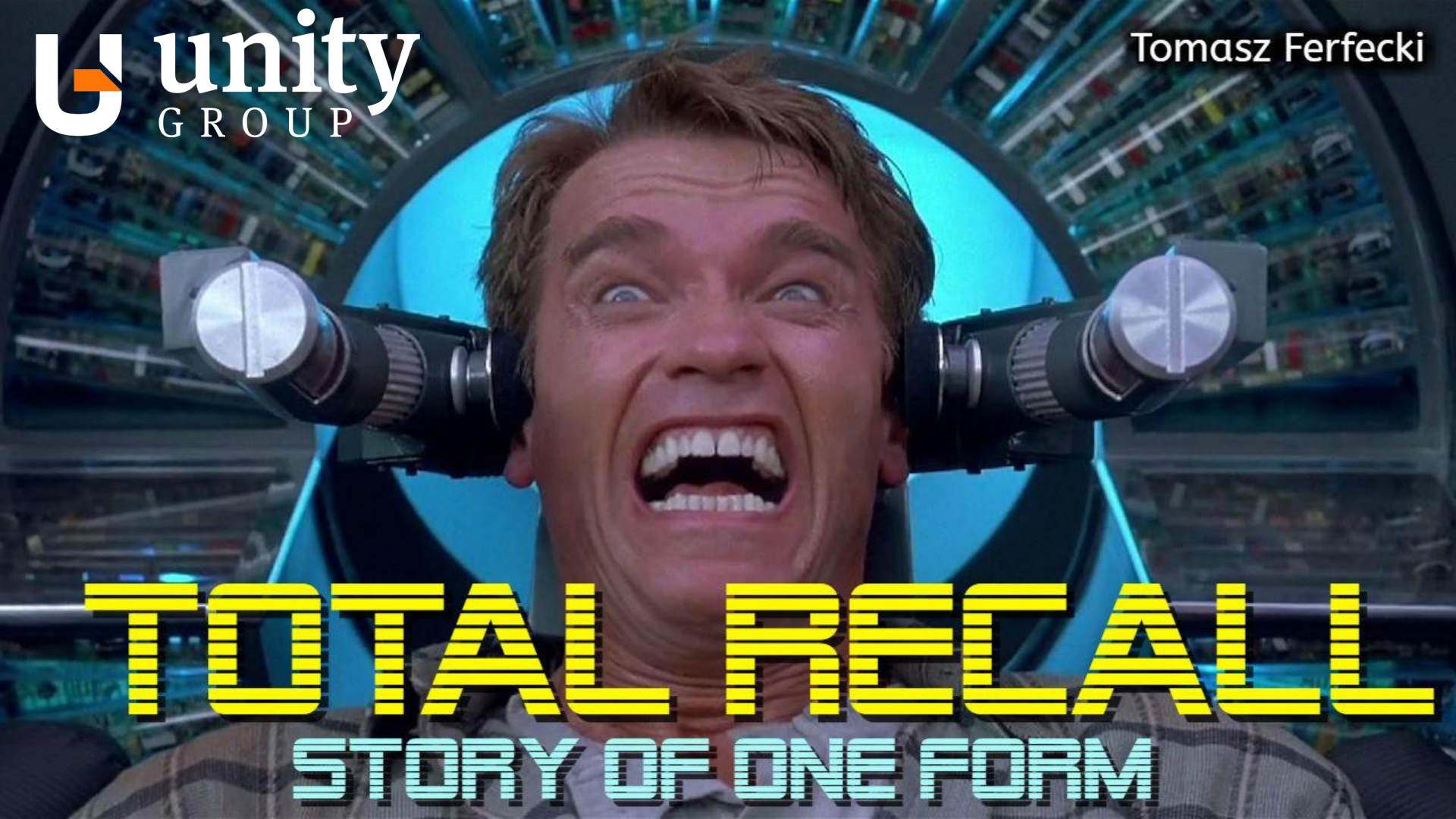

unity
GROUP
Tomasz Ferfecki
TOTAL RECALL
STORY OF ONE FORM

# WHOAMI

PHP developer at Unity Group

6+ years of coding

Organizer of corporate knowledge sharing initiative - Coders

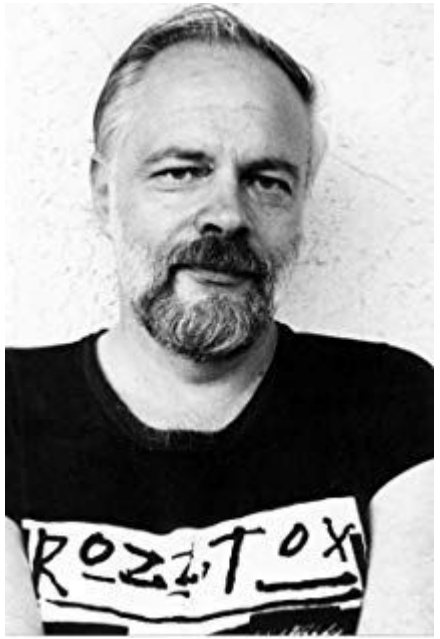
# Shout-out

American science fiction writer

"*Total recall*" based at story from "*We Can Remember It for You Wholesale*"(1966)

Worth reading:

- *Do Androids Dream of Electric Sheep?*
- *The Man in the High Castle*




Philip K. Dick

# Story setup

- Who?
  - Students at University of Technology
- What?
  - Startup with investor
- Where?
  - City in eastern Poland
- When?
  - Around 6-7 years ago
- How?
  - PHP 5.5 with CakePHP 2.x

PIEROGI /pɛˈroːgi/

# How we can code

“*Forgot your password*”

# How we can code “Forgot your password”

- Send old password via email

# How we can code “Forgot your password”

- Send new password via email

# How we can code “Forgot your password”

- Answering security questions on website

# How we can code “Forgot your password”

- Send reset password code via text message

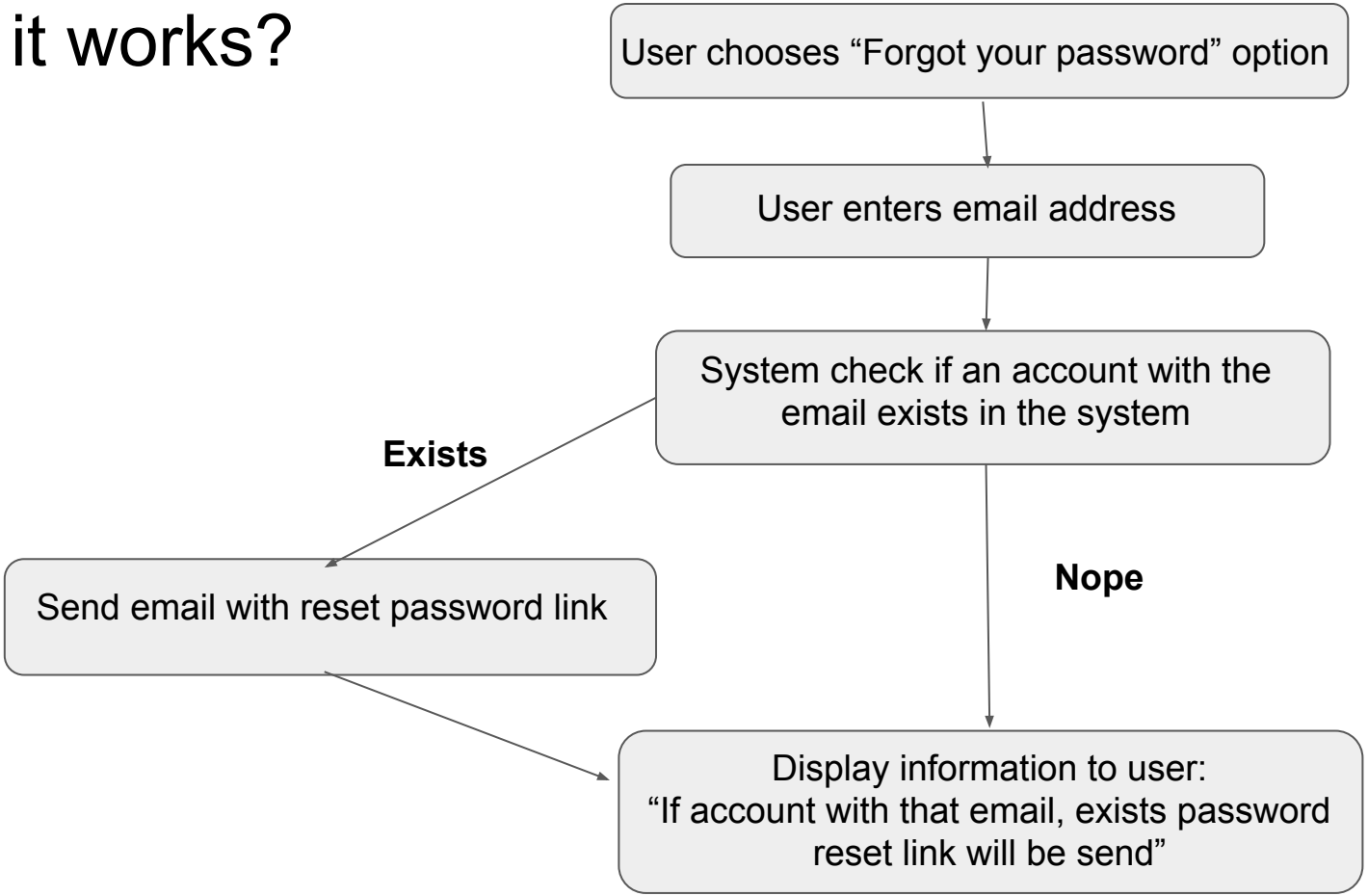
# How we can code “Forgot your password”

- Send reset password link via email

# How we can code “Forgot your password”

- *Send old password via email*
- *Send new password via email*
- *Answering security questions on website*
- *Send reset password code via text message*
- **Send reset password link via email**

# How it works?


User chooses “Forgot your password” option
User enters email address
System check if an account with the email exists in the system
Exists
Nope
Send email with reset password link
Display information to user:
“If account with that email, exists password reset link will be send”

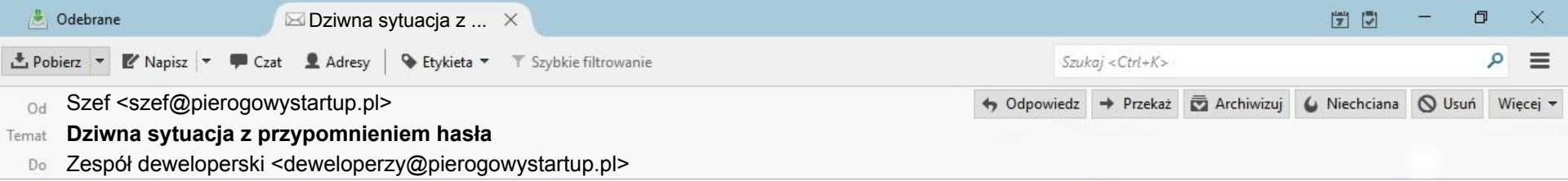
What is important for that flow?

- Client has to receive email (sic!)
- Sending reminder should not block access to application
- Url to password reset should not be weak to manipulation

# Did I mention it all?

Nah, but we will get to the point soon


SMALL CITY IN EASTERN POLAND
MORNING




Dear team,

Something disturbing happen lately.
Just a minute ago I received a few mails for password reset in our application.
Is it some kind of a joke from some of you?

Odebrane | ODP: Dziwna syt ...

Pobierz | Napisz | Czat | Adresy | Etykieta | Szybkie filtrowanie | Szukaj <Ctrl+K>

Od Tomek <tomek@pierogowystartup.pl>

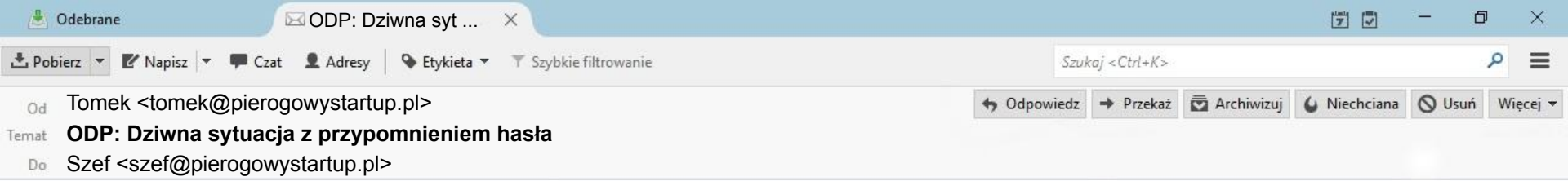
Temat **ODP: Dziwna sytuacja z przypomnieniem hasła**

Do Szef <szef@pierogowystartup.pl>

Odpowiedz | Przekaż | Archiwizuj | Niechciana | Usuń | Więcej

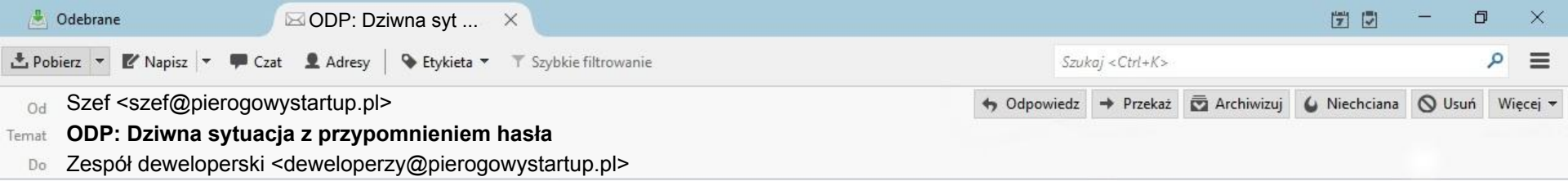
I don’t think it is connected with any of our tasks in current sprint.

Also I’m completely sure that nobody would be so immature, to make such silly and childish joke.



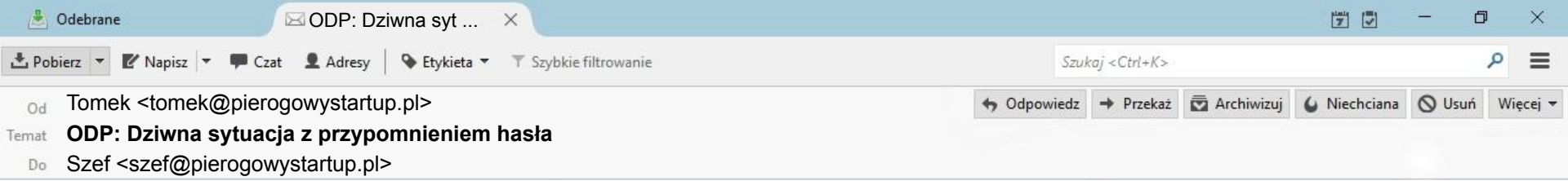

# WE ARE PROFESSIONALS!


2 HOURS LATER




I would like to inform you, that I keep receiving this emails!

It’s become annoying like hell!




Yes, I can only imagine that.
Furthermore, I would like to suggest cause of all this commotion:
It is possibly one of our beta testers.
However, if you try to ask one of them about this emails, problem with emails might escalate even more.

Odebrane | ODP: Dziwna syt ...

Pobierz | Napisz | Czat | Adresy | Etykieta | Szybkie filtrowanie | Szukaj <Ctrl+K>

Od Tomek <tomek@pierogowystartup.pl>

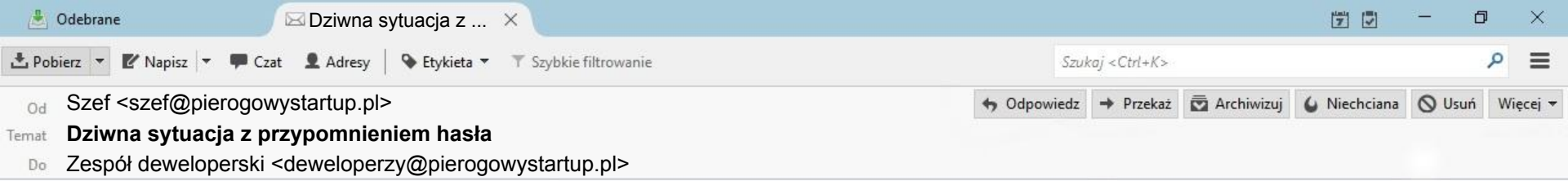
Temat **ODP: Dziwna sytuacja z przypomnieniem hasła**

Do Szef <szef@pierogowystartup.pl>

Odpowiedz | Przekaż | Archiwizuj | Niechciana | Usuń | Więcej

Maybe you could just create a task in JIRA and we will take care of it in free time.

Hopefully, before we've taken care of it, these jokers will get bored.




Ok Thomas,
I will create those tasks,
but I still need something to limit new email notifications.
They are really getting out off hand!
Could any of you come up with any solution?

Odebrane | ODP: Dziwna syt ...

Pobierz | Napisz | Czat | Adresy | Etykieta | Szybkie filtrowanie | Szukaj <Ctrl+K>

Od Tomek <tomek@pierogowystartup.pl>

Temat **ODP: Dziwna sytuacja z przypomnieniem hasła**

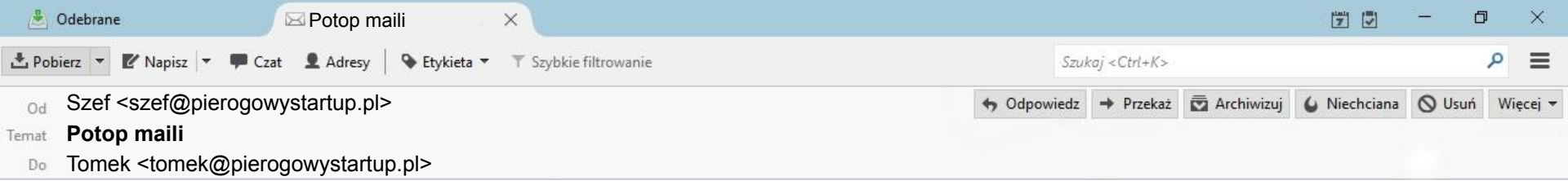
Do Szef <szef@pierogowystartup.pl>

Odpowiedz | Przekaż | Archiwizuj | Niechciana | Usuń | Więcej

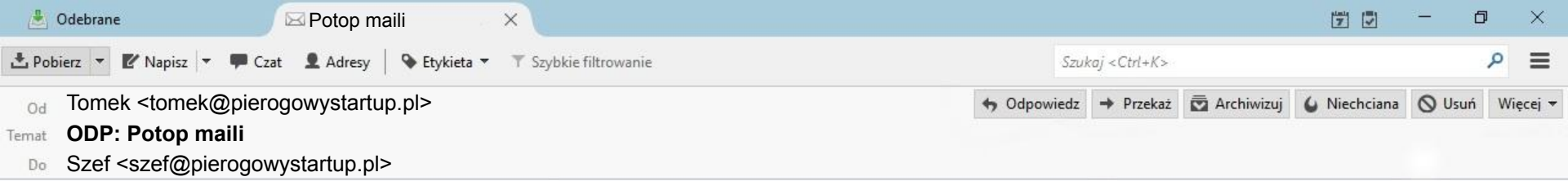
Sure thing boss,

I suggest  add filter on email application, that will help you ignore all new emails.
It will be as easy for you as it can be, because Michael will do it.
Furthermore, we can probably take care of that bug soon, maybe tomorrow.


1 HOUR 12 MINUTES LATER




Haven’t you forgotten about topic with emails?
I’ve just checked that folder created by Michael,
and it’s full of that notifications
right now it’s around 900 emails!
There is like twentish emails per minute!



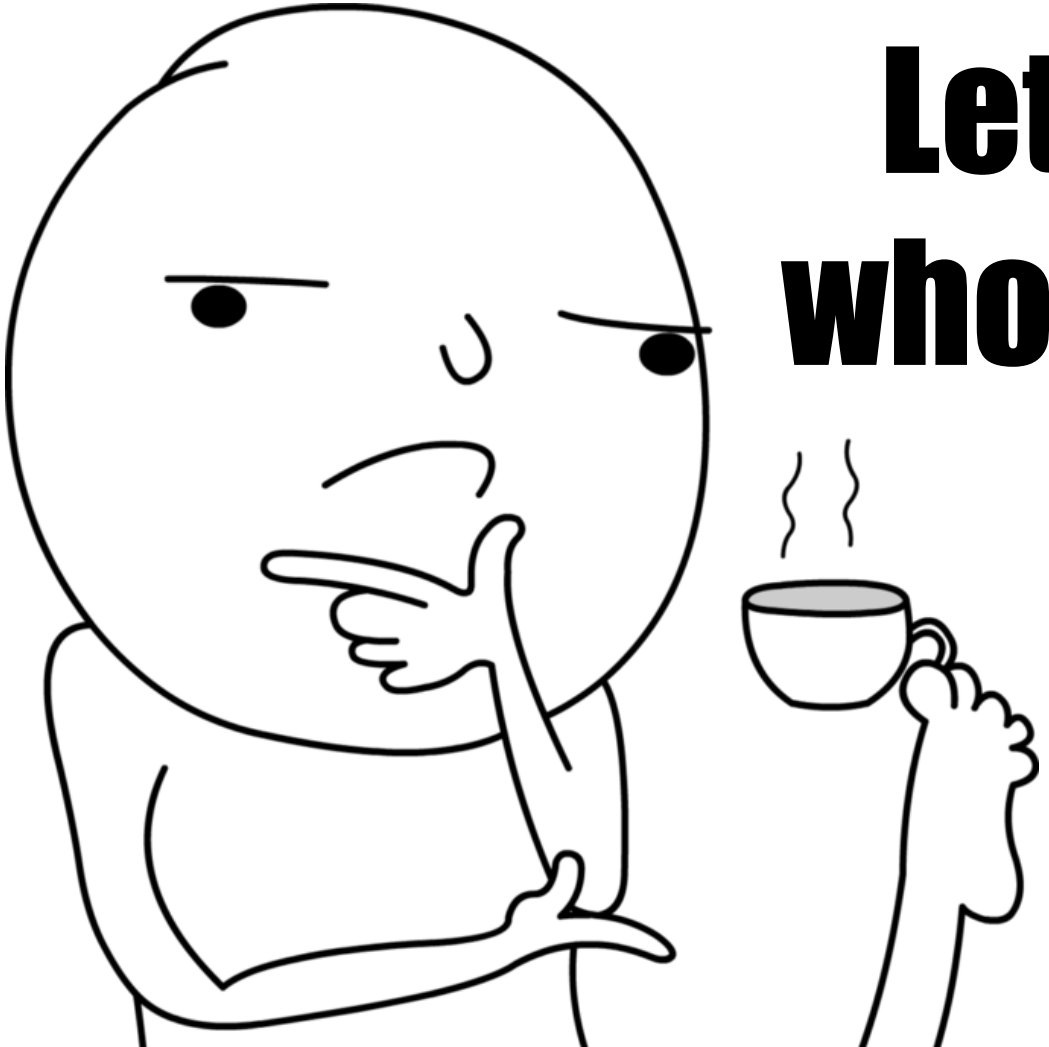

Uh oh,

In this case the problem is more important that we thought.

We will take actions immediately, blocking access to form and fixing the bug.

# What happen next?

- Quick blocking form and action,
- Fixing functionality
  - added check of last password reminder
- Added CSRF field verification to the form

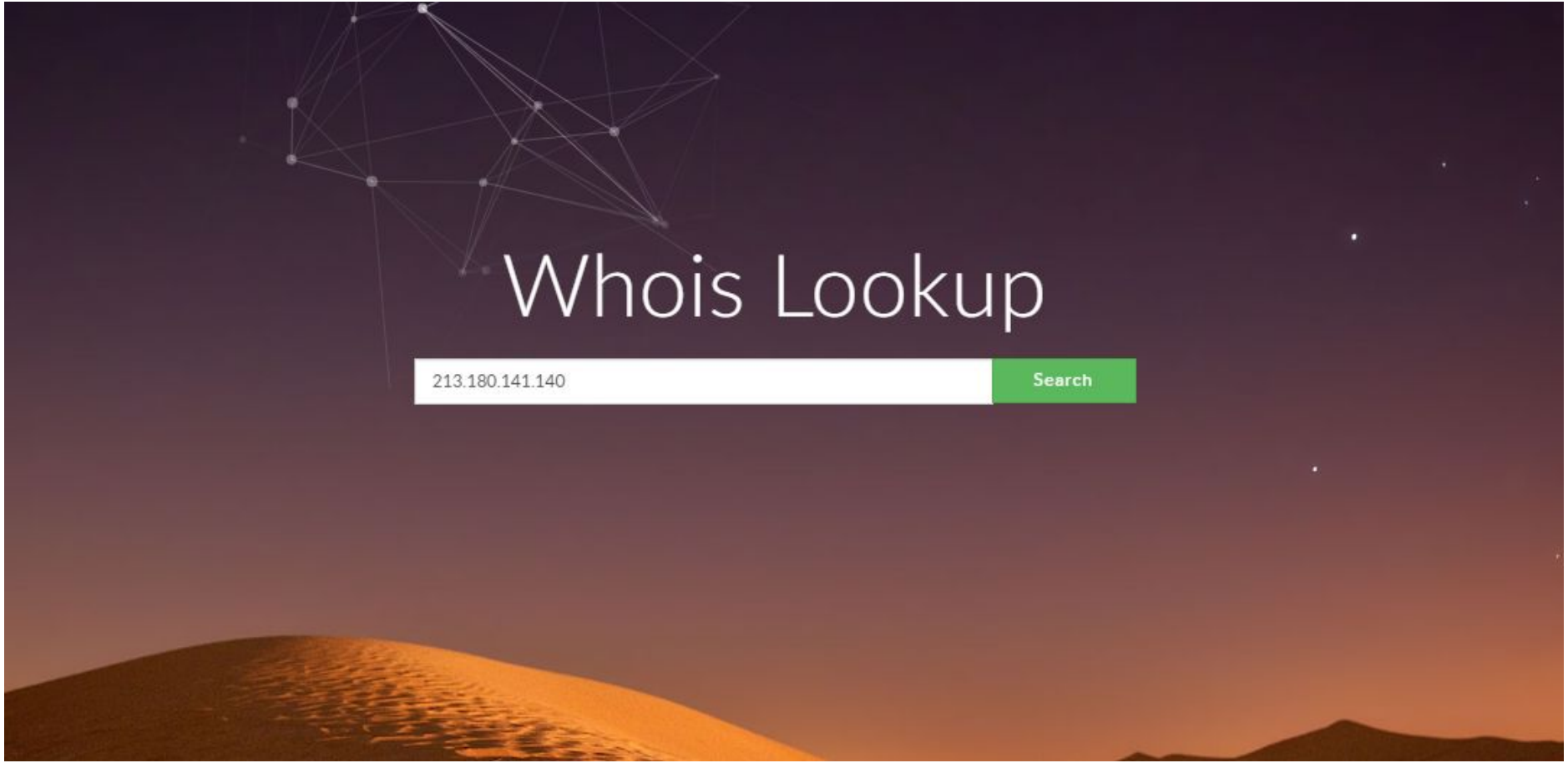


# Let’s analyze whole situation

What is origin source of all those request?

# Common part?

```
123.45.67.89 - - [06/Nov/2014:14:10:20 +0200] [..]
123.45.67.89 - - [06/Nov/2014:14:10:20 +0200] [..]
123.45.67.89 - - [06/Nov/2014:14:10:21 +0200] [..]
123.45.67.89 - - [06/Nov/2014:14:10:21 +0200] [..]
123.45.67.89 - - [06/Nov/2014:14:10:22 +0200] [..]
123.45.67.89 - - [06/Nov/2014:14:10:22 +0200] [..]
123.45.67.89 - - [06/Nov/2014:14:10:23 +0200] [..]
123.45.67.89 - - [06/Nov/2014:14:10:23 +0200] [..]
123.45.67.89 - - [06/Nov/2014:14:10:24 +0200] [..]
123.45.67.89 - - [06/Nov/2014:14:10:24 +0200] [..]
123.45.67.89 - - [06/Nov/2014:14:10:25 +0200] [..]
```


Whois Lookup
213.180.141.140
Search

Home > Whois Lookup > 213.180.141.140

# IP Information for 213.180.141.140

## Quick Stats

| | |
|---|---|
| IP Location | Poland Krakow Ringier Axel Springer Polska Sp. Z O.o. |
| ASN | AS12990 ONET-PL-AS1 Onet.pl portal network, PL (registered Feb 11, 2000) |
| Resolve Host | sg1.any.onet.pl |
| Whois Server | whois.ripe.net |
| IP Address | 213.180.141.140 |
| Reverse IP | 4 websites use this address. |

```
% Abuse contact for '213.180.141.0 - 213.180.141.255' is ' abuse@onet.pl '
```

Odebrane | DDOS attempt

Pobierz | Napisz | Czat | Adresy | Etykieta | Szybkie filtrowanie | Szukaj <Ctrl+K>

Od Tomek <tomek@pierogowystartup.pl>

Temat **RE: DDOS attempt**

Do Carl <abuse@hosting.pl>

Odpowiedz | Przekaż | Archiwizuj | Niechciana | Usuń | Więcej

Good morning,

Lately we got problem with somebody trying to take down our application.
Attack came out from IP address in your domain.
From following IP address was send series of attacks, that disrupted correct work of our platform.
In attachments I enclose logs from the application.

Odebrane | RE: DDOS attempt

Pobierz | Napisz | Czat | Adresy | Etykieta | Szybkie filtrowanie | Szukaj <Ctrl+K>

Od abuse@hosting.pl

Temat **DDOS attempt**

Do Tomek <tomek@pierogowystartup.pl>

Odpowiedz | Przekaż | Archiwizuj | Niechciana | Usuń | Więcej

Good morning,

Thank you for letting us know, we'll take care of everything asap.
We always take such reports very seriously.

Carl


SOME TIME LATER

Congratulations for you on the quick resolution of the email issue

It only took 2 days, and around 1200 messages in my inbox

Also congratulations from software house ABC

What about ABC?

Apparently abuse emails to ISP are taken very seriously

How MUCH, seriously?

Well.. It took them like 3 hours to connect second internet link

# WHAT HAPPEN NEXT?


DON’T LAUNCH FUNNY SCRIPTS
FROM COMPANY NETWORK

# Questions?

# Thank you for your attention