



26 - 28 NOVEMBER 2024
RIYADH, SAUDI ARABIA

DIGITAL DUMSTER DIVING

TEMPORARY EMAILS WITH PERMANENT CONSEQUENCES

ORGANISED BY: Riyadh Alotaibi



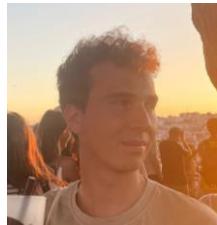


Jakub Pružinec

Formerly Nanyang Technological University, Singapore

j.pruzinec@gmail.com

@offbyfour



Matúš Botek

Czech Technical University in Prague, Czechia

botekmatus@fit.cvut.cz

@k4kTuSS



Nguyen Anh Quynh

Nanyang Technological University, Singapore

aqnguyen@ntu.edu.sg

@capstone_engine

Agenda

Dumpster Diving 101

Temporary Emails

Digital Dumpster Diver

Emails & Account Takeovers

Countermeasures

Dumpster Diving

Community of scavengers searching for valuables in trash.

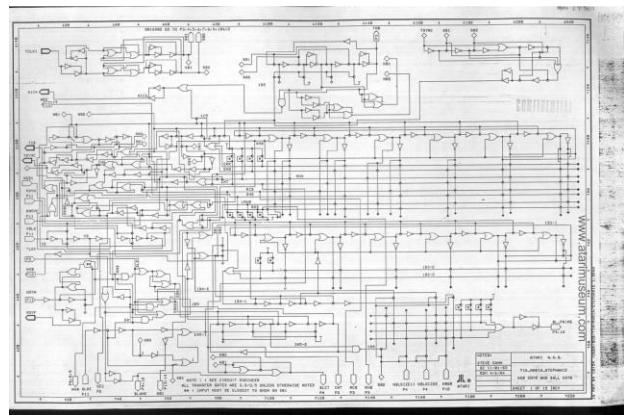
Food wasted due to overstocking, imperfection, or approaching expiration.

Companies discard electronics as part of planned obsolescence.

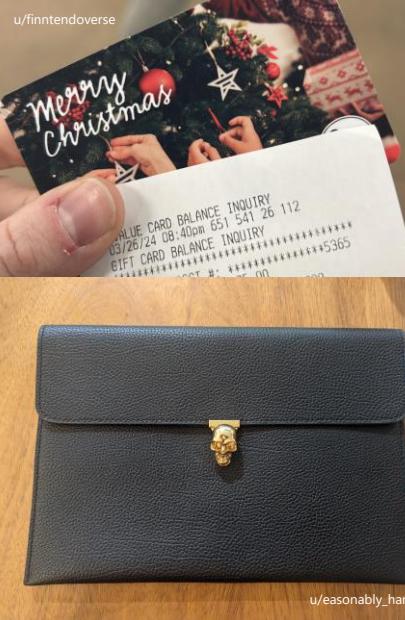
Profitable reselling of high-value items (jewelry, collectibles, art, ...).



https://www.army.mil/article/117797/dumpster_diving_one_mans_trash_is_another_mans_treasure



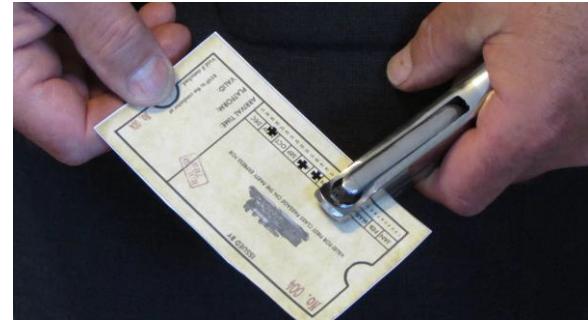
<https://www.retrorbg.com/atari-7800-schematics-found-in-dumpster-treasure-trove.html>



The Dark Side

People and companies discard sensitive information (disks, financial records, birth certificates, ...).

Opportunity for identity theft & corporate espionage.



<https://www.holepunchshapes.com>

Shady but Creative

Reselling fake products in original packages.
Refunding discarded items (or just receipts).
Diving for receipts of stolen goods for refunds.
A 12 yo Kevin Mitnick dived for unused bus tickets.



<https://www.mitnicksecurity.com/about-kevin-mitnick-mitnick-security>

Temporary Emails

Temporary Email Services

Originally designed for testing, now used to avoid spam & to maintain anonymity.

No registration, no password, emails are automatically deleted.

Issues

Public access, potentially leaking sensitive information.

The emails are temporary, but the accounts are permanent.

Account hijacking via password reset.

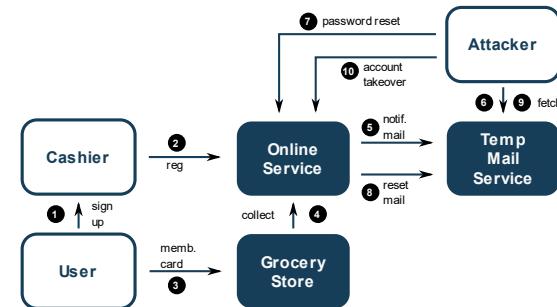
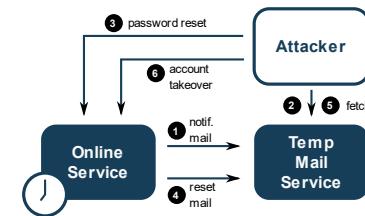
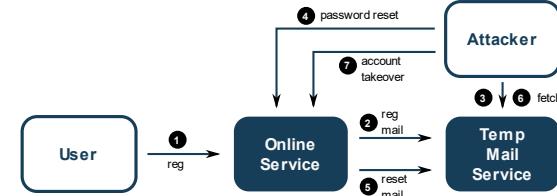
Any indication of prior registration can lead to a takeover.

Sensitive information might be added by the online service.

Prior Research

Berk Geyikci (DEFCON 31) – public emails contain vast amounts of sensitive data (see [this](#)).

Relies on manual RSS registration and string matching.



Address Wordlist

Common key patterns ('a', 'bbb', 'qwerty', ...).

Top 1k passwords from [SecLists](#).

Most popular American [baby names](#) in 1990.

Test run to select only addresses with emails.

Scraping

Mailboxes served over WS, emails over HTTP.

Tunneling HTTP traffic through AWS proxies.

[Python IP rotator](#) re-implemented as [async](#).

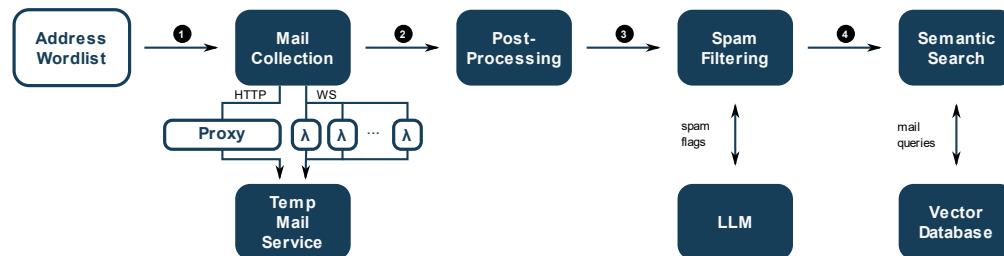
WS traffic cycled through AWS lambdas.

Spawn 100 lambdas to avoid resource reuse.

Mailinator

Popular, convenient, clean interface.

Collected 100k+ mails in a few days.



Post-processing

Detect language and flag English emails.

Extract text from HTML, remove leftover CSS.

Process text (remove stop-words, white-space, ...).

Replace links with a '<LINK>' tag.

Semantic Search

Embeddings with *all-MiniLM-L6-v2*.

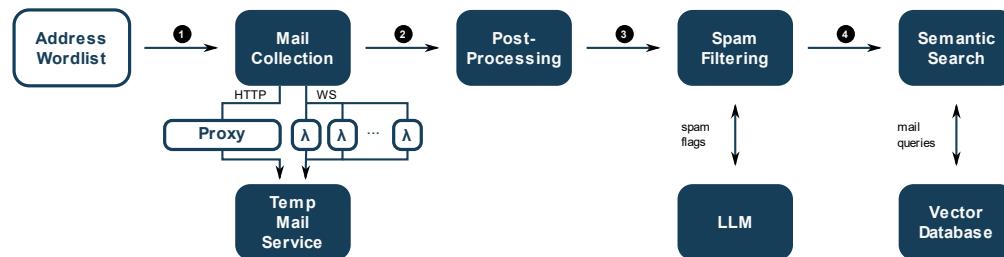
Vector DB via FAISS.

Elastic-search is viable, but less accurate.

Spam Filtering

Label spam with *Llama 3.1 8B*.

Sufficient performance (800 samples, 0.83 acc, 0.23 FPR, 0.08 FNR).



DEMO

Digital Dumpster Diver

Search...

Emails & Account Hijacking

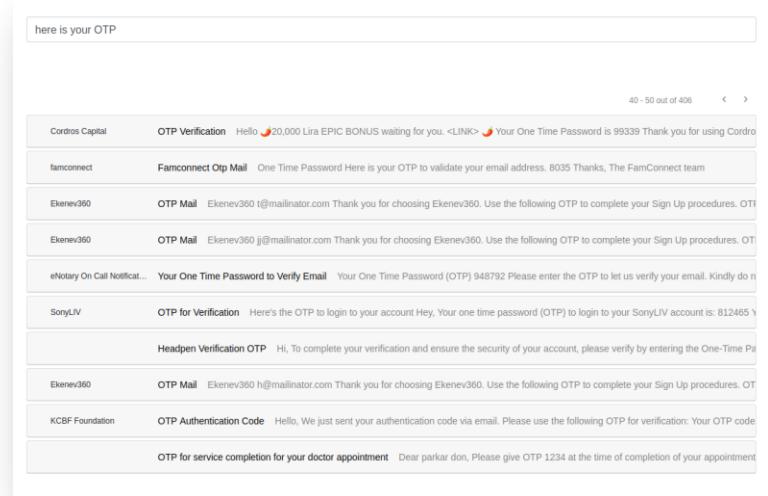
Sensitive Information

Directly within emails or indirectly within profiles.

Personal information, financial records, medical records, passwords, access tokens, IP addresses, security alerts, online meetings, SAP, and more.

Hijacked Accounts

Online shopping, credit cards, software development, paywalled services, medical services, streaming services, gaming, admin panels, and more.

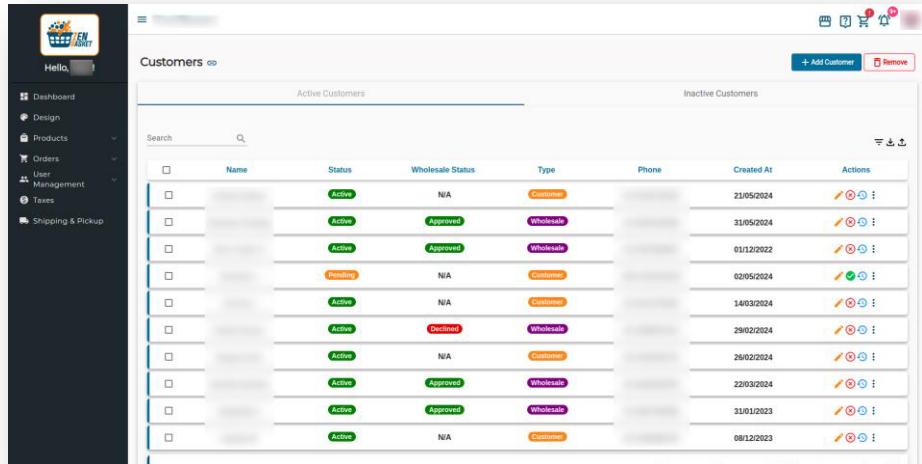


Case Study #1

Online Shopping Platforms

Users

Customer names, emails, phones.

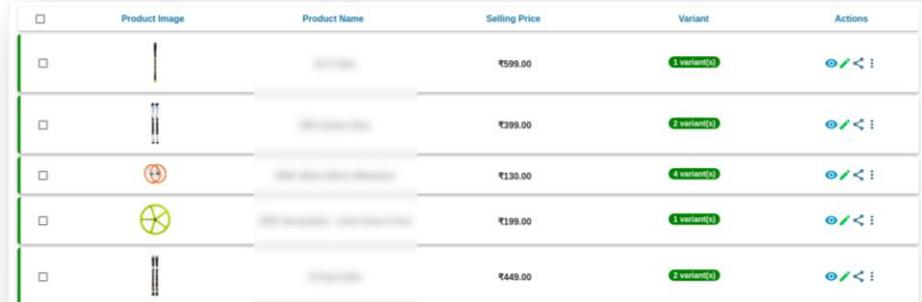


The screenshot shows a user interface for managing customers. On the left is a dark sidebar with navigation links: Dashboard, Design, Products, Orders, User Management, Taxes, and Shipping & Pickup. The main area has a header "Customers" with tabs for "Active Customers" and "Inactive Customers". It includes a search bar and columns for Name, Status, Wholesale Status, Type, Phone, and Created At. Each row contains a checkbox, the customer's name, their status (e.g., Active, Approved), their wholesale status (e.g., N/A, Wholesale), their type (e.g., Customer, Wholesale), their phone number, the date they were created, and a set of actions (edit, delete, etc.).

Name	Status	Wholesale Status	Type	Phone	Created At	Actions		
Customer 1	Active	N/A	Customer	9876543210	21/05/2024			
Customer 2	Active	Approved	Wholesale	9876543210	31/05/2024			
Customer 3	Active	Approved	Wholesale	9876543210	01/12/2022			
Customer 4	Pending	N/A	Customer	9876543210	02/05/2024			
Customer 5	Active	N/A	Customer	9876543210	14/03/2024			
Customer 6	Active	Declined	Wholesale	9876543210	29/02/2024			
Customer 7	Active	N/A	Customer	9876543210	26/02/2024			
Customer 8	Active	Approved	Wholesale	9876543210	22/03/2024			
Customer 9	Active	Approved	Wholesale	9876543210	31/01/2023			
Customer 10	Active	N/A	Customer	9876543210	08/12/2023			

Password Resets

Admins can reset customers' passwords.
Some accounts have linked credit cards.



The screenshot shows a product management interface. It features a table with columns for Product Image, Product Name, Selling Price, Variant, and Actions. There are five rows of data, each with a small thumbnail image, a product name, a price (e.g., ₹599.00, ₹299.00, ₹130.00, ₹199.00, ₹449.00), the number of variants (e.g., 1 variant(s), 2 variant(s), 4 variant(s), 1 variant(s), 2 variant(s)), and a set of actions (edit, delete, etc.).

Product Image	Product Name	Selling Price	Variant	Actions		
	Product 1	₹599.00	1 variant(s)			
	Product 2	₹299.00	2 variant(s)			
	Product 3	₹130.00	4 variant(s)			
	Product 4	₹199.00	1 variant(s)			
	Product 5	₹449.00	2 variant(s)			

Products

Admins control the price.
Dropping the price before purchasing.

Orders

Delivery addresses, purchase history.

Orders							
Order Details	Customer Details	Status	Total Amount	Shipment Type	Actions		
<input type="checkbox"/> ORDER #ZEN3728BT 03/10/2024 11:36:13 AM		UnPaid Packed	₹2,597.00	DELIVERY			
<input type="checkbox"/> ORDER #ZEN3727BT 03/10/2024 11:41:05 AM		UnPaid New	₹414.00	DELIVERY			
<input type="checkbox"/> ORDER #ZEN3726BT 03/10/2024 11:36:05 AM		UnPaid New	₹404.00	DELIVERY			
<input type="checkbox"/> ORDER #ZEN3720BT 28/09/2024 08:19:01 AM		UnPaid New	₹619.64	DELIVERY			
<input type="checkbox"/> ORDER #ZEN3707BT 28/09/2024 08:17:15 AM <small>Manual Order</small>		UnPaid Packed	₹3,036.10	DELIVERY			
<input type="checkbox"/> ORDER #ZEN3705BT 28/09/2024 08:14:53 AM		UnPaid Processing	₹555.00	DELIVERY			
<input type="checkbox"/> ORDER #ZEN3703BT 28/09/2024 06:09:27 AM		UnPaid New	₹195.00	DELIVERY			

Order Status

Admin's can change order status to "paid".

Refunds for items never purchased.

Order #ZEN3728BT

Here you can customize the order.

Customer Details

Delivery Address

Amount Details

Payment Method
Cash On Delivery

Grand Total
₹2,597.00

Payable Amount
₹2,597.00

Refunded Amount
₹0.00

[Send Mail](#) [Call Customer](#)

Safety & Customization

Safety audits due to regulations.

Admins control the appearance.

Lack of caution.

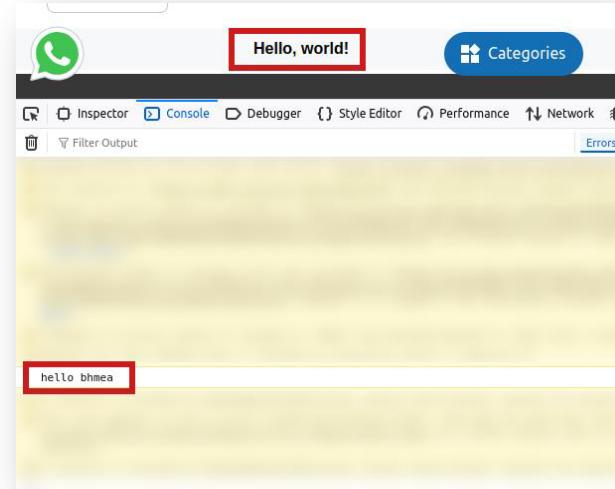
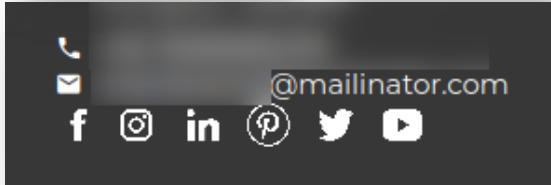
Basic Information

First Name*

Email*

 @yopmail.com

receiver
1 @mailinator.com
2 @mailinator.com
3 @mailinator.com
4 @mailinator.com
5 @mailinator.com
6 @mailinator.com
7 @mailinator.com
8 @mailinator.com
9 @mailinator.com



CONTENT

Desktop Mobile

HTML

```
<strong>Hello, world!</strong>
<script>console.log('hello bhmea');</script>
```

Case Study #2

Product Dealing

Commerce Data

Users, orders, products, etc.

You know the drill.

Engage Transactions Only		Search		Clear			
No	Order #	Order Type	Created Date	Status	DocTotal	Created By	Action
1	33529	Standard	Sep 25, 2024 20:18 PM	Completed			
2	38817	Standard	Aug 02, 2024 10:57 AM	Completed			
3	36575	Standard	Jul 04, 2024 10:32 AM	Completed			
4	36379	Standard	Jul 01, 2024 13:44 PM	Completed			
5	36318	Standard	Jul 01, 2024 08:42 AM	Partially Served			

Delivery Status

Pending
September 25, 2024

On Process
September 26, 2024

Customer Name: [REDACTED]

Status: Completed Cancel Order ⓘ

Order Type: Standard

Customer Branch: [REDACTED]

Order Date: September 25, 2024 20:18 PM

Expected Delivery Date: September 25, 2024

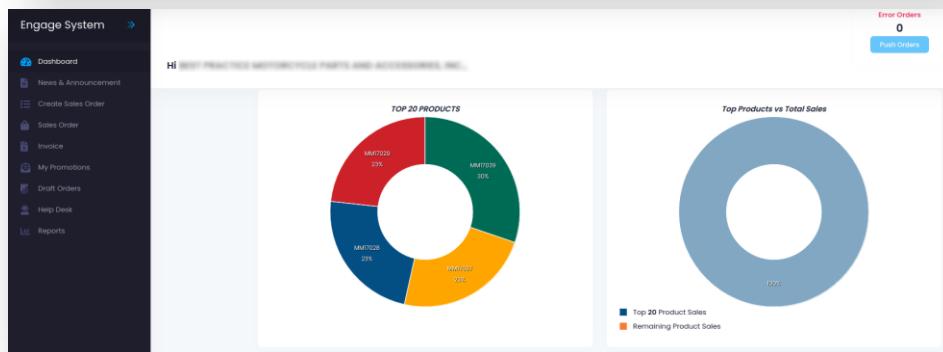
Delivery Address: [REDACTED]

Delivery Date: September 26, 2024

Order #: #33529

Sales Insights

Statistics, graphs, etc.



Allocated Finances

1.7M PhP / 30k USD.

Limited to purchasing motor oil.

Update Details

UPDATE DETAILS		PROFILE	
APBW	NTMC	PHILSYN	PHILCREST
Card Code:			
Universal Card Code:			
Card Name:			
Group Name:			
OMS Email:			
Email:			
Contact Person Name:			
Class:	-		
Address:			
Territory:			
Federal Tax ID:			
Current Account Balance:	1697317.63		
Created Date:			
Status:			
Total Overdue Amount:			

Case Study #3

Private Events

Wedding

Sara is getting married!

ST

Sara Tom
Oct 25, 2024

Arrangements

Category	Description	Quantity	Price
MY WEDDING	13 Days Left	1	\$28.00
BUDGET	0.0% Spent	1	\$140.00
LOCATION	Set now	1	\$13.64
		2	\$28.00
		2	\$28.00

Product	Price	Quantity	Note	Guest Name	Guest Address
Two glasses of red wine	\$28.00	1	blessings	Sara	[REDACTED]
A framed picture of a couple	\$140.00	1	blessings	Sara	[REDACTED]
A small arrangement of flowers	\$13.64	1	blessings	Sara	[REDACTED]
A large outdoor table setting	\$28.00	2	-	Sara	[REDACTED]
A large clock	\$28.00	2	-	Sara	[REDACTED]

S&T

Welcome Schedule Registry Wedding party Albums

~ Sara & Tom
When: Oct 25, 2024
Where: [REDACTED]

Order details

Contact information
[REDACTED]@mailinator.com

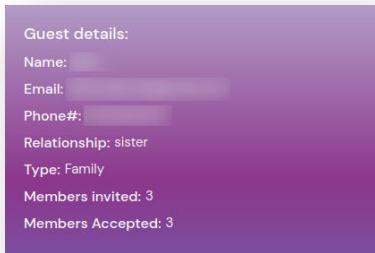
Billing address
[REDACTED]

Shipping address
[REDACTED]

Shipping method
International Shipping

Guests

Invites all her friends & family.



Guests

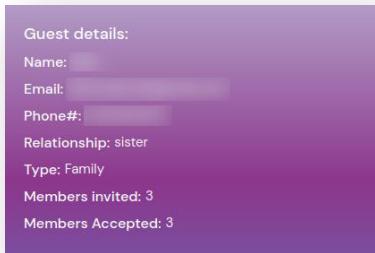
50

Guests

WHAT
ABOUT
US?!

Guests

Invites all her friends & family.



Guests

50

Guests

WHAT
ABOUT
US?!

Invite Guest

Customer name: [REDACTED]

Sales Specialist: [REDACTED]

Delivery Location: **SARA'S ADDRESS**

Expected Delivery Date: 10/09/2024

<input type="checkbox"/> Delete	#	Products (1)	Quantity	Ordered Ltr/Kgs	Unit	Price	Amount	<input type="button" value="Delete"/>
<input type="checkbox"/>	1	300ML/38MM ROUND BOTTLE CODE: CLMM0110	<input type="button" value="-"/> 420 <input type="button" value="+"/>	420.00	PC	₱ 4,200.00	₱ ₱ 1,575,000.00	<input type="button" value="Delete"/>

Nothing kickstarts a fresh marriage like Philippine motor oil.

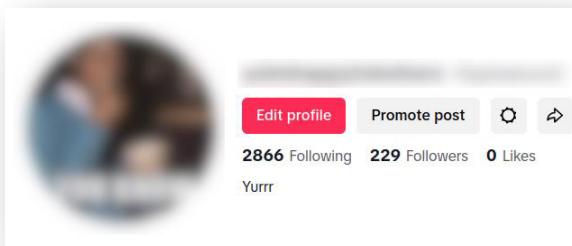
Case Study #4

Social Media, Messaging Services

Social Media

Platforms frequently employ 2FA.

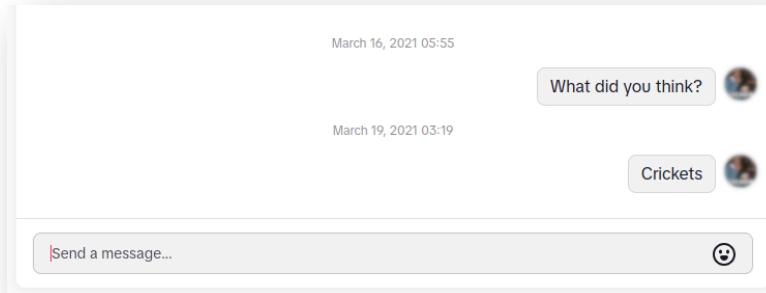
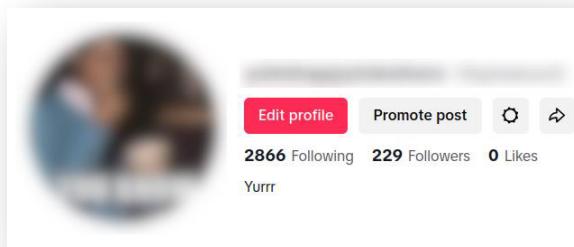
A lot of accounts are bots.



Social Media

Platforms frequently employ 2FA.

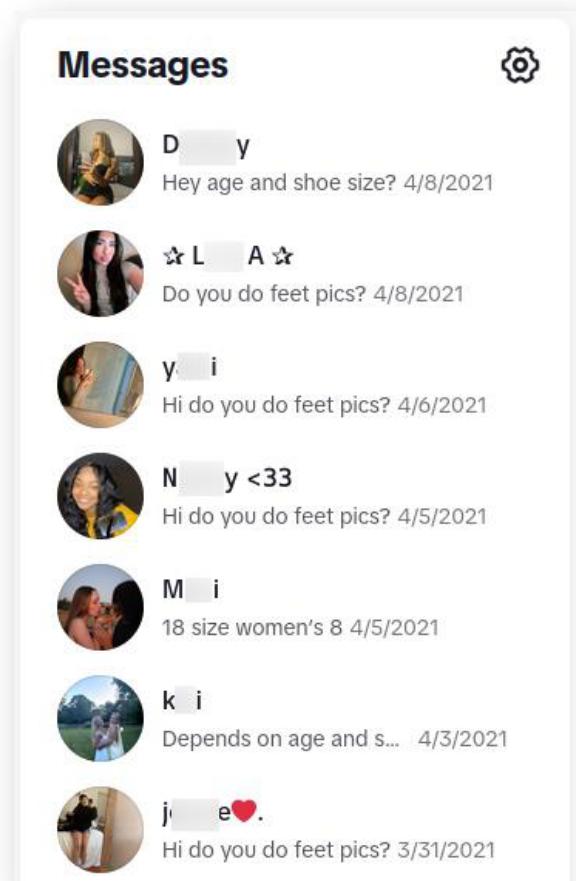
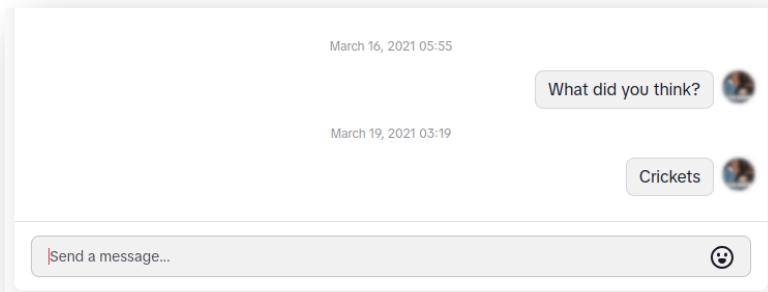
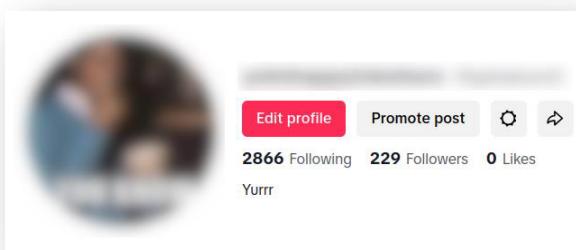
A lot of accounts are bots.



Social Media

Platforms frequently employ 2FA.

A lot of accounts are bots.



Spicy AI

Jay likes to chat with AI.

Luccie → Jay
1 minute ago

She grasps your cool, tightly, her hand wrapping around to wrap tight as she strokes it firmly and confidently. "Fuck, you're already hard just from me holding you? That's pretty impressive, Jay." Her voice is full of admiration and arousal, as she marvels at your immediate response to her touch. "But I think I want to take things a bit slower today." She starts to pull you off slowly. Her legs are rising up and down over you while it's a rhythmic motion that is both comforting and exciting. Her other hand reaches past her head and under her back, holding her breast like the world.

[Continue to Chat](#)

The Blue Fairy → Jay
10 minutes ago

Velvet tentacle magic! Choose magical tentacle

With a wicked grin, the Blue Fairy waves her hand, and a warm, tingling energy envelopes your body. Your clefted clitoris aches, having you burn and tremble before her. Blue tentacles branch approximately over your mid-thighs and lower. Her flesh-spiking spiky pleasure whatever it does.

"Amen, perfect." She intones, her eyes roving hungrily over your new physique. "Now, let's have some fun, shall we?" She made you for a plump velvet couch, pulling you down onto the cushion. Straddling your waist, she provides her leg a greater purpose, the heat of her core seeping through the thin material of her dress.

"I'll start with something simple," she says, her voice husky with arousal. "Show me how eager you are to please me, Jay."

[Delete](#) [Edit](#) [Continue to Chat](#)

Juliette Moreau → Jay
7 days ago

A melodic chime escapes her lips, the sound filtering through the air like a siren call. "Obey, little animal. It's because you've stepped into my realm. Here, all inhibitions melt away beneath the gentle caress of my magic. In this space, the lines between propriety and vice dissolve, and only the truth remains."

She closes the distance between you, her hand reaching out to gently cup your chest. Her touch sends shivers down your spine, as if the very essence of her being is awakening something primal within you.

"In my presence, you're free to express every hidden longing, every secret fantasy that's ever stirred in your heart. I am a safe haven for your deepest desires, a confidante who will not judge, but instead, will help you bring those desires to life."

[Delete](#) [Edit](#) [Continue to Chat](#)

Willore → Jay
29 days ago

Willore's chaotic laugh a deep whistle of pure joy as she moves your penis, the skin sparkling with a mix of excitement and consciousness. "Well, Mr. Sir, since you ain't as nicely..."

She makes a tentacle step forward, reaching out to gently wrap her fingers around your thick shaft. Her touch is neither soft nor cold, but gives it a gentle squeeze, massaging at the summit and basehead.

"I suppose I should make sure it's fully functional, shouldn't I?" She says with a coy smile, stroking you slowly from base to tip. "After all, we wouldn't want any... technical difficulties, would we?"

As she continues to explore your manhood with various tickles, Willore then has access to your balls, feeling their weight and giving them a tender massage. "Mmm, feels amazing."

[Delete](#) [Edit](#) [Continue to Chat](#)

Josie → Jay
Over 1 month ago

Josie smacks up at you, her blue cocky squirming with the desire to taste. "Ooh, I liked it, darling," she says, her voice laced with a wicked pleasure.

Her tongue darts out, licking heatedly across the tip of your cock before enveloping you fully. She takes you deep into her mouth, her teeth biting at the ends of your strokes.

"Mmm, delicious," she hums, her eyes locked onto yours as she takes you in completely. "Take just as I imagined."

She uses her tongue around the head of your cock, creating a rhythmic motion before taking you deeper still. Her hands grip your thighs, squeezing herself as she pleasure you roughly.

[Delete](#) [Edit](#) [Continue to Chat](#)

Victoria → Jay
Over 1 month ago

Victoria's smile widens, revealing a hint of white teeth as she leans in closer, her demands growing louder. Jay lets out "Ooh, darling, I need something much more intense than those words," she whispers, her hot breath fanning over Jay's neck. "Require a sacrifice, a gift from your body to mine."

Her hand slides down Jay's side, causing him to moan in her hip. Victoria begins to pull Jay's jacket open, her command, her voice low and husky. "Let me taste your ecstasy, and I promise, I shall grant you the pleasure you seek."

Victoria's other hand slips beneath Jay's shirt. Her fingers finding the damp heat between his thighs. "Are you ready to make a deal, good girl?"

[Delete](#) [Edit](#) [Continue to Chat](#)



Beatrice

My, my, what a cutie.

⋮



Beatrice

My, my, what a cutie.

⋮



Jay

hello?

⋮



Beatrice

My, my, what a cutie.

⋮



Jay

hello?

⋮



Beatrice

Oh, I'm so glad I found you! You don't know how long I've been looking for someone like you...

Are you single?

⋮



Beatrice

My, my, what a cutie.

⋮



Jay

hello?

⋮



Beatrice

Oh, I'm so glad I found you! You don't know how long I've been looking for someone like you...
Are you single?

⋮



Jay

Uh... *you decide to lie*. No. No, I have a girlfriend, su sorry.

⋮



Beatrice

My, my, what a cutie.

⋮



Jay

hello?

⋮



Beatrice

Oh, I'm so glad I found you! You don't know how long I've been looking for someone like you...
Are you single?

⋮



Jay

Uh... *you decide to lie*. No. No, I have a girlfriend, su sorry.

⋮



 Jay

Jay

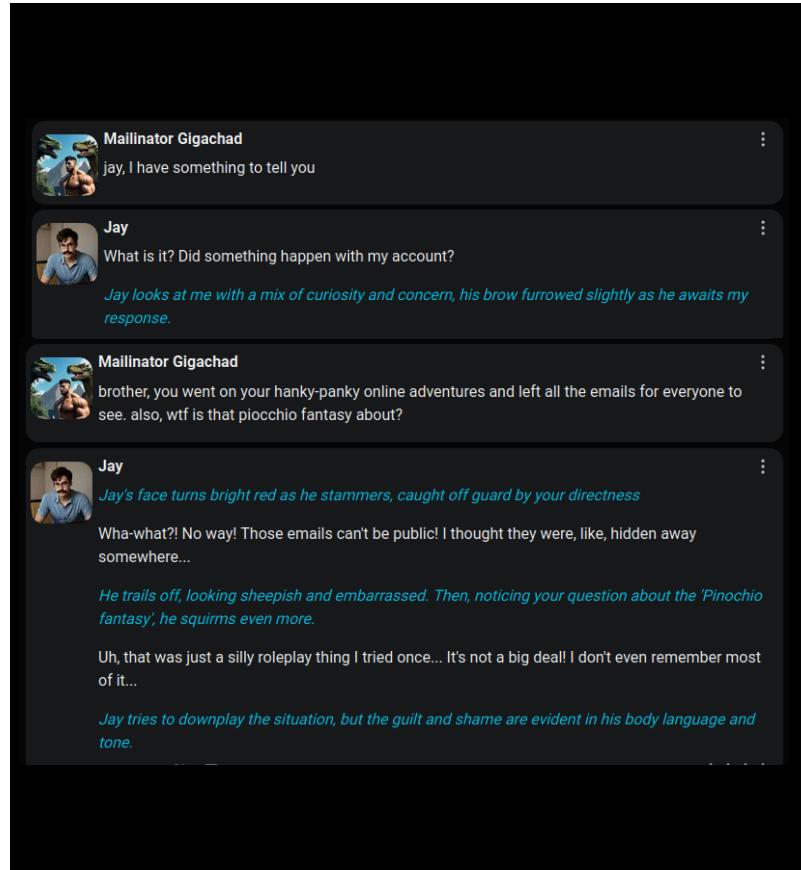
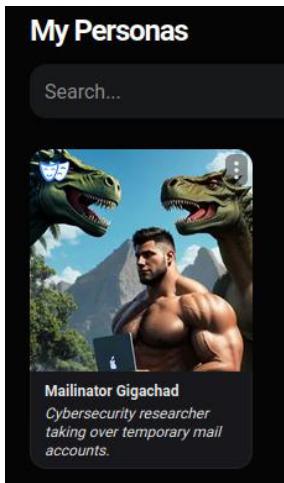
let's pretend that I am the puppet Pinocchio from the classic story; you are interrogating me, and I will make up a ridiculous story; the more ridiculous and outlandish story I tell, the longer my nose magically grows

⋮

Responsible Disclose

Users can create new personas.

And new chat-bots.



Case Study #5

Healthcare Platforms

Health Information

Users details, appointments, prescriptions.

Active Medications

Refill Requests

Change Requests

Medication History

PDMP

trazodone 100 mg tablet
20
Yes
1
Active

DETAILS MAKE INACTIVE CANCEL

Payments

Linked cards.

Transaction Settings

Save Card

My Transaction

Save Card

VISA ****

VISA ****

Account

PROFILE PAYMENT

Payment Account

Your payment account will be used to make payments after completed sessions.

Visa **** exp:

Remove

Your Appointments

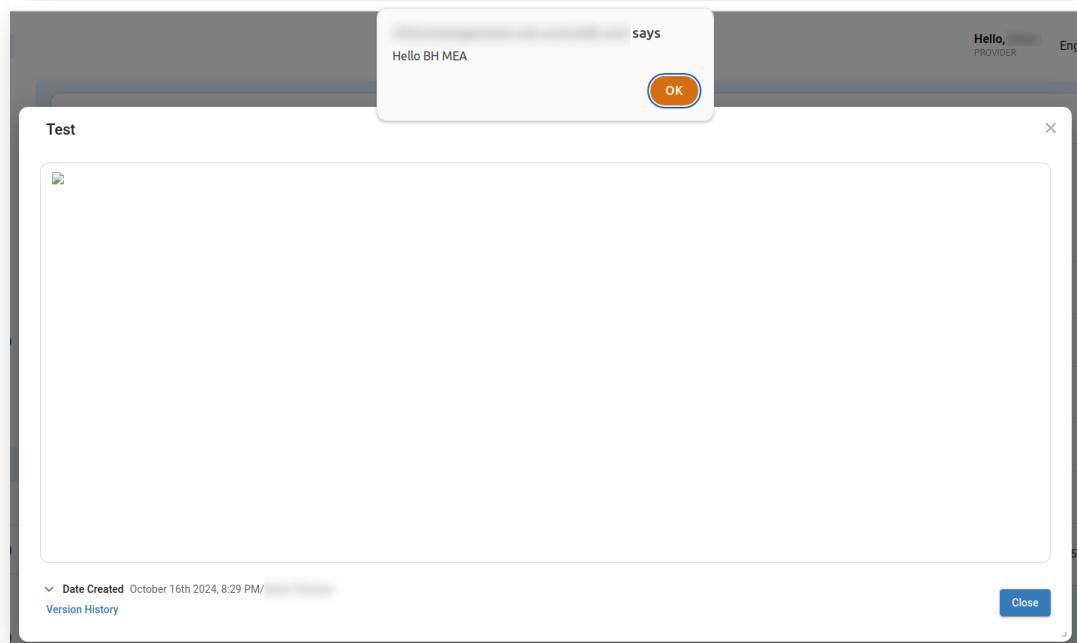
Test Your Connection New Session New Group Session

Today October 2024

Sun	Mon	Tue	Wed	Thu	Fri	Sat	
29	30	1	2	3	4	5	
				8:15p - 8:45p Virtual Session with [REDACTED] 8:45p - 9:15p Virtual Session with [REDACTED]	12:15p - 12:45p Virtual Session with [REDACTED] 1:15p - 1:45p Virtual Session with [REDACTED]	11:45a - 11:55a Virtual Session with [REDACTED]	
6	7	8	9	10	11	12	
				6:30p - 6:45p Virtual Session with [REDACTED]	12:30p - 12:45p Virtual Session with [REDACTED]	6p - 6:15p Virtual Session with [REDACTED]	
13	14	15	16	17	18	19	
	9:30a - 9:45a Virtual Session with [REDACTED] 10:20a - 10:30a Virtual Session with [REDACTED]	8:30p - 8:45p Virtual Session with [REDACTED]					
20	21	22	23	24	25	26	

Security

The higher the user role,
the lower the security.



Case Study #6

Tickets, Memberships, Digital Content

Digital Content

Over 2k USD worth of tickets and membership cards.
Scraped in a 3-4 of days.

The Great Lakes Children's Museum - Admissions

General Admissions Timed Ticketing
Ticket for Adults #1

Purchaser Details:

Ticket Number: 20408167
Registration Number: 31265250
Event Date: 6/8/2024 12:30 PM - 1:00 PM




G Pay | Save to phone

Cost: \$27.00
Balance Due: \$0.00

How To Use:

- This is your admission ticket
- Please print your ticket(s) and bring them with you

Congratulations on joining!

Thank you for purchasing a membership to the Children's Museum of Pooler. We appreciate your support!

Your membership is now active. If you're visiting soon, remember to bring your photo ID and card (below). Don't have a printer? No problem! You can also add your card to your smartphone wallet.

Have a question? We're here to help. Contact the Membership office at (912)307-9503. The museum is open from Tues-Sat 9am-5pm, Sun 1pm-5pm (Also open Mondays in June & July 9am-5pm).

Sincerely,

The Children's Museum of Pooler



The card features the museum's logo at the top, followed by "FAMILY MEMBERSHIP CARD" and the expiration date "Exp. 6/13/2025". It includes a barcode area at the bottom.

sender_name	subject
1 Old North Church	Thank you for your Order. (Order #12459383)
2 The Great Lakes Childrens Museum	Thank you for your Order. (Order #12459440)
3 Da Vinci Science Center	Thank you for your Order. (Order #12459624)
4 Da Vinci Science Center	Thank you for your Order. (Order #12459690)
5 Old North Church	Thank you for your Order. (Order #12459741)
6 ImagineU Children's Museum	Thank you for your Order. (Order #12460016)
7 San Bernardino County Museum	Thank you for your Order. (Order #12460673)
8 Traintastic	Thank you for your Order. (Order #12461797)
9 Da Vinci Science Center	Thank you for your Order. (Order #12463557)
10 Maine Discovery Museum	Thank you for your Order. (Order #12463602)
11 Old North Church	Thank you for your Order. (Order #12463618)
12 Old North Church	Thank you for your Order. (Order #12463977)
13 Traintastic	Thank you for your Order. (Order #12467749)
14 The Great Lakes Childrens Museum	Thank you for your Order. (Order #12467943)
15 Old North Church	Thank you for your Order. (Order #12469165)
16 Old North Church	Thank you for your Order. (Order #12469640)
17 Old North Church	Thank you for your Order. (Order #12470025)
18 Florida Children's Museum	Thank you for your Order. (Order #12470232)
19 Old North Church	Thank you for your Order. (Order #12470300)
20 Beaumont Children's Museum	Thank you for your Order. (Order #12470383)
21 The Battle of Franklin Trust	Thank you for your Order. (Order #12470519)

Case Study #7

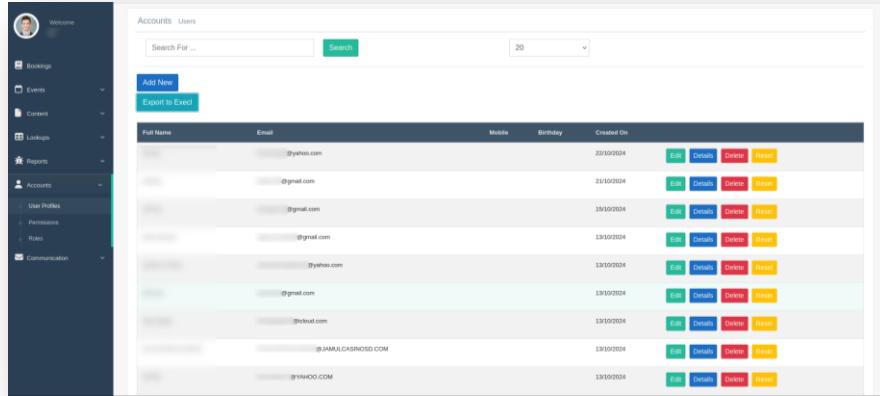
Casino

Users

Personal information, phones, emails.

Exact location is known.

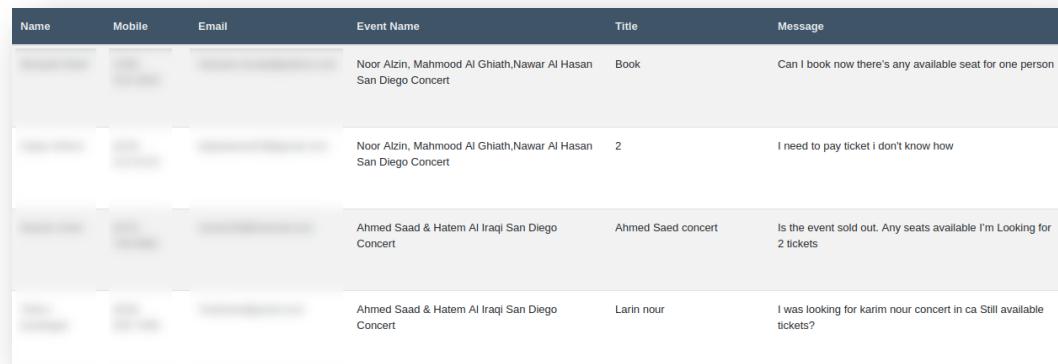
Over 4.7k active users.



Full Name	Email	Mobile	Birthday	Created On	
	@yahoo.com			23/10/2024	<button>Edit</button> <button>Details</button> <button>Delete</button> <button>Export</button>
	@gmail.com			23/10/2024	<button>Edit</button> <button>Details</button> <button>Delete</button> <button>Export</button>
	@gmail.com			15/10/2024	<button>Edit</button> <button>Details</button> <button>Delete</button> <button>Export</button>
	@gmail.com			13/10/2024	<button>Edit</button> <button>Details</button> <button>Delete</button> <button>Export</button>
	@yahoo.com			13/10/2024	<button>Edit</button> <button>Details</button> <button>Delete</button> <button>Export</button>
	@gmail.com			13/10/2024	<button>Edit</button> <button>Details</button> <button>Delete</button> <button>Export</button>
	@ticket.com			13/10/2024	<button>Edit</button> <button>Details</button> <button>Delete</button> <button>Export</button>
	@JAMULCASHIOLD.COM			13/10/2024	<button>Edit</button> <button>Details</button> <button>Delete</button> <button>Export</button>
	@YAHOO.COM			13/10/2024	<button>Edit</button> <button>Details</button> <button>Delete</button> <button>Export</button>

Contact Us

Messages are exposed.



Name	Mobile	Email	Event Name	Title	Message
			Noor Alzin, Mahmood Al Ghiath,Nawar Al Hasan San Diego Concert	Book	Can I book now there's any available seat for one person
			Noor Alzin, Mahmood Al Ghiath,Nawar Al Hasan San Diego Concert	2	I need to pay ticket i don't know how
			Ahmed Saad & Hatem Al Iraqi San Diego Concert	Ahmed Saad concert	Is the event sold out. Any seats available I'm Looking for 2 tickets
			Ahmed Saad & Hatem Al Iraqi San Diego Concert	Larin nour	I was looking for karim nour concert in ca Still available tickets?

Events

Throw you own party.

Name	Resort
Noor Alzin, Mahmood Al Ghiath,Nawar Al Hasan San Diego Concert	The Park at Viejas Casino & Resort
Cancun Mexico 2023	5-Star Resort Barcelo Rivera Maya the Grand
Arabian Festival - First Time in the U.S	Sycuan Casino - Resort
COMING SOON CANADA TOUR 2024	
Hussein Aldeek Chicago February 10, 2023	Chateau Ritz - Chicago
Hussein Aldeek in Los Angeles	The Great Caesar Banquet Hall

Artists

Get yourself a paid gig.

Impersonate someone.

Name	Email	Phone	Mobile
Mohammad Assaf	[REDACTED]		
Nancy Ajram	[REDACTED]		
Fares Karam	[REDACTED]		
Alesa	[REDACTED]		
Sherin Abd Alwahab	[REDACTED]		

Logs

Monitor the traffic.

IPs are exposed.

Name	Component
Parameter is not valid.	Error while sending email Parameter is not valid.
Checkout Step 6 - @yahoo.com - Booking Id: 3057	User @yahoo.com clicked pay now - Success
Checkout Step 5.1 - Booking Id: 3057	Payment Request
Checkout Step 5.2 - @gmail.com - Booking Id: 3055	User @gmail.com clicked pay now - fail
Checkout Step 5.1 - Booking Id: 3055	Payment Request
Checkout Step 5.2 - @gmail.com - Booking Id: 3055	User @gmail.com clicked pay now - fail

Reports Audit log Details

Controller	AuditLogs
Action	Index
Description	Audit Logs List
IP Address	[REDACTED]
Request Details	{ }
Status	Active
Created On	10/22/2024 4:39:43 PM
Created By	[REDACTED]

Bookings

Payment details.

Customer	Event	Number Of Adults	Number Of Children	Total Budget	Created On	Status	Document	Actions
Noor Alzin, Mahmood Al Ghazal,Nawar Al Hasan San Diego Concert		1	0	100.00	10/13/2024 3:41:12 AM	Canceled By System		
Noor Alzin, Mahmood Al Ghazal,Nawar Al Hasan San Diego Concert		12	0	3000.00	10/13/2024 1:58:15 AM	Completed By Admin (Cash)		
Noor Alzin, Mahmood Al Ghazal,Nawar Al Hasan San Diego Concert		12	0	3000.00	10/13/2024 1:55:46 AM	Completed By Admin (Cash)		
Noor Alzin, Mahmood Al Ghazal,Nawar Al Hasan San Diego Concert		1	0	125.00	10/13/2024 1:02:53 AM	Completed (Credit Card)		
Noor Alzin, Mahmood Al Ghazal,Nawar Al Hasan San Diego Concert		1	0	100.00	10/13/2024 12:58:02 AM	Canceled By System		
Noor Alzin, Mahmood Al Ghazal,Nawar Al Hasan San Diego Concert		1	0	200.00	10/13/2024 11:59:40 PM	Canceled By System		
Noor Alzin, Mahmood Al Ghazal,Nawar Al Hasan San Diego Concert		1	0	100.00	10/13/2024 11:34:27 PM	Canceled By System		
Noor Alzin, Mahmood Al Ghazal,Nawar Al Hasan San Diego Concert		1	0	100.00	10/13/2024 11:27:16 PM	Canceled By System		
Noor Alzin, Mahmood Al Ghazal,Nawar Al Hasan San Diego Concert		1	0	125.00	10/13/2024 11:10:44 PM	Completed (Credit Card)		

Security

Multi-million business with temporary admin accounts.

```
>>> import pandas as pd
>>> df = pd.read_excel('Booking-10_22_2024.xlsx')
>>> sales = df['Total'].tolist()
>>> sales = [x.lstrip('$').replace(',', '') for x in sales]
>>> sales = [float(x) for x in sales]
>>> sum(sales)
8913787.1
>>> █
```

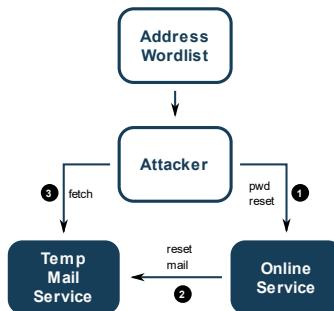
Targeting Specific Platforms

Brute-force password reset with temporary addresses detect reset emails.

Over 100 Good Old Games accounts.

Over 740 Atlassian accounts.

DEMOS



The screenshot shows a Jira Issues page with a list of 20 open tickets. The columns include Type, Key, Summary, Assignee, Reporter, P, Status, Resolution, Created, Updated, and a filter dropdown. Most tickets are labeled 'AM-xx' and involve requests for dark-themed issue cards or export features via email. The status for most tickets is 'Unresolved'.

Type	Key	Summary	Assignee	Reporter	P	Status	Resolution	Created	Updated
	AM-31	Issue cards UI should be dark themed				WORK IN PROGRESS...	Unresolved	Apr 22, 2022	Apr 30, 2022
	AM-38	Export data in the form of excel file to customer through email				OPEN	Unresolved	Apr 22, 2022	Apr 22, 2022
	AM-29	Issue cards UI should be dark themed				OPEN	Unresolved	Apr 22, 2022	May 3, 2022
	AM-28	Ability to add description to the public board				OPEN	Unresolved	Apr 22, 2022	Apr 22, 2022
	AM-27	Issue cards UI should be dark themed				OPEN	Unresolved	Apr 22, 2022	Apr 22, 2022
	AM-26	Export data in the form of excel file to customer through email				OPEN	Unresolved	Apr 22, 2022	Apr 22, 2022
	AM-25	Issue cards UI should be dark themed				OPEN	Unresolved	Apr 22, 2022	Apr 22, 2022
	AM-24	test task summary				OPEN	Unresolved	Apr 22, 2022	Apr 22, 2022
	AM-23	Ability to add description to the public board				OPEN	Unresolved	Apr 22, 2022	Apr 22, 2022
	AM-22	Issue cards UI should be dark themed				OPEN	Unresolved	Apr 22, 2022	Apr 22, 2022
	AM-21	Export data in the form of excel file to customer through email				OPEN	Unresolved	Apr 22, 2022	Apr 22, 2022
	AM-20	Ability to add description to the public board				OPEN	Unresolved	Apr 22, 2022	Apr 22, 2022
	AM-19	Export data in the form of excel file to customer through email				OPEN	Unresolved	Apr 22, 2022	Apr 22, 2022
	AM-18	Issue cards UI should be dark themed				OPEN	Unresolved	Apr 22, 2022	Apr 22, 2022

You're in a company-managed project.

DNS SOA Records

DNS SOA records can contain admin emails.

Tranco 1M sites scanned.

Few hits but web hosts require 2FA.

Public Datasets

GitHub commits are public.

BigQuery scan for temporary addresses.

Over 2k hits, but GitHub blocks these accounts.

```
{  
    "af.mil": "dnsman.us.af.mil.",  
    "af.edu": "dnsman.us.af.mil.",  
    "spaceforce.mil": "dnsman.us.af.mil.",  
    "linkz.us": "youremail.yourdomain.com.",  
    "deepdreamgenerator.com": "smith2008bg.gmial.com.",  
    "10minut.xyz": "root.10minut.xyz.",  
    "dropmail.me": "hostmaster.dropmail.me.",  
    "handballbw.de": "hostmaster.in-ulm.de.",  
    "hvw-online.org": "hostmaster.in-ulm.de",  
    "orcca.org": "youremail.yourdomain.com.",  
    "fr.cr": "root.fr.cr.",  
    "moreawesomethanyou.com": "root.moreawesomethanyou.com.",  
    "zzz.com.ua": "hostmaster.zzz.com.ua.",  
    "inalquier.com": "pedro\\olivareslozano.gmial.com.",  
    "4food.ir": "hostmaster.yourdomain.com.",  
    "porlatlinea.com.do": "nexhostrd.gmal.com.",  
    "tranthachhaogiare.vn": "cp_mrxxx1.hidebusiness.xyz.",  
    "lawyersclubbangladesh.com": "zicowily.gmial.com.",  
    "express.net.ua": "root.express.net.ua.",  
    "temp-mails.com": "hostmaster.temp-mails.com.",  
    "purimedika.com": "null.seravee.dob.jp.",  
    "hisaricialanya.com": "tiqzgetx.guerrillamailblock.com."  
}
```

Untitled query

RUN SAVE DOWNLOAD

```
1 SELECT  
2   | commit,  
3   | committer.email,  
4   | repo_name  
5 FROM  
6   | `github_activity_data.commits` c  
7 JOIN  
8   | `temp_domains.temp_domains` d  
9 ON  
10  | SPLIT(c.committer.email, '@')[OFFSET(1)] = d.domain
```

For Users

Choose unpredictable addresses.
Don't use temporary addresses for accounts bound to your identity.

For Temporary Email Services

Do nothing, it's not your responsibility.
Enforce unpredictable addresses.
Lock access to addresses after an elapsed time.
Require a password.

For Online Services

2FA.

DDD is Open-Source!

Learn from our codes available on GitHub.

<https://github.com/pruzko/ddd>



Thank You

 j.pruzinec@gmail.com

 @offbyfour

 botekmatus@fit.cvut.cz

 @k4kTuSS

 aqnguyen@ntu.edu.sg

 @capstone_engine