

ZERFORSCHUNG

[Forscher*innen](#)[Projekte](#)[Archiv](#)[Unterstützen](#)

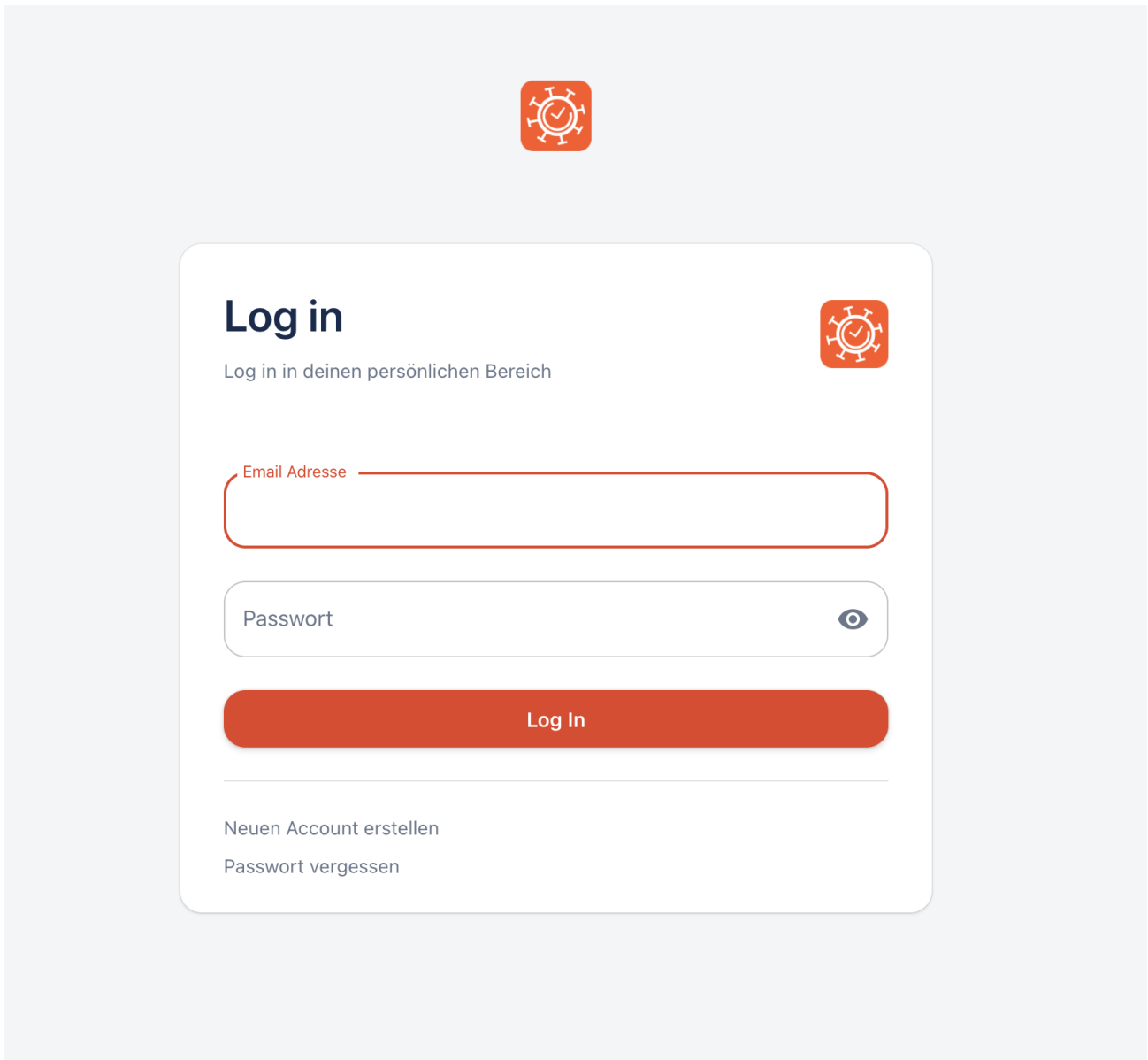
Wie wir plötzlich Robert Koch waren



Corona geht in die vierte Welle. Ein guter Zeitpunkt, um unser Lieblingsthema „Corona-Testzentren“ wieder aus der Schublade zu holen. Wir wollen schauen, ob die Testanbieter mittlerweile was aus den Fehlern ihrer Vorgänger*innen gelernt haben. Spoiler: Haben sie nicht. Aber eins nach dem anderen.

Wer sich in Berlin schon einmal schnelltesten lassen hat, kennt sie vielleicht: Die leuchtend orangenen Test-Stationen von schnelltestberlin.de oder die Coronabikes. Das sind Lastenräder mit einer kleinen Teststation, die oft vor Clubs, Supermärkten und Museen stehen.

Was all diese Teststationen gemeinsam haben: Sie nutzen das gleiche Online-System, um die Testergebnisse mitzuteilen – mein-schnelltest.com.



Kurz bevor die Corona-Schnelltests am 11. Oktober für die meisten Menschen kostenpflichtig wurden, waren wir bei einer dieser Stationen.

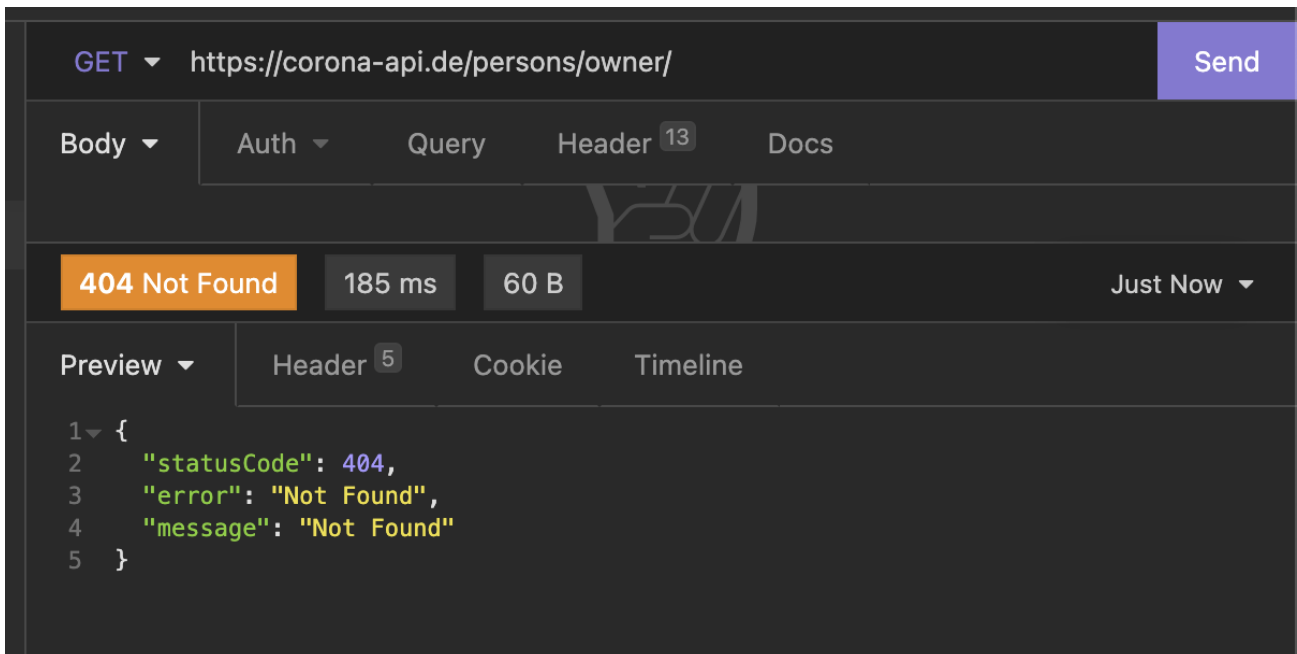
Eigentlich wollten wir keine Teststationen mehr zerforschen – ein paar Tage später hat uns die Neugier aber doch gepackt: Wir gehen nochmal auf die Webseite, um unser Testergebnis abzurufen.



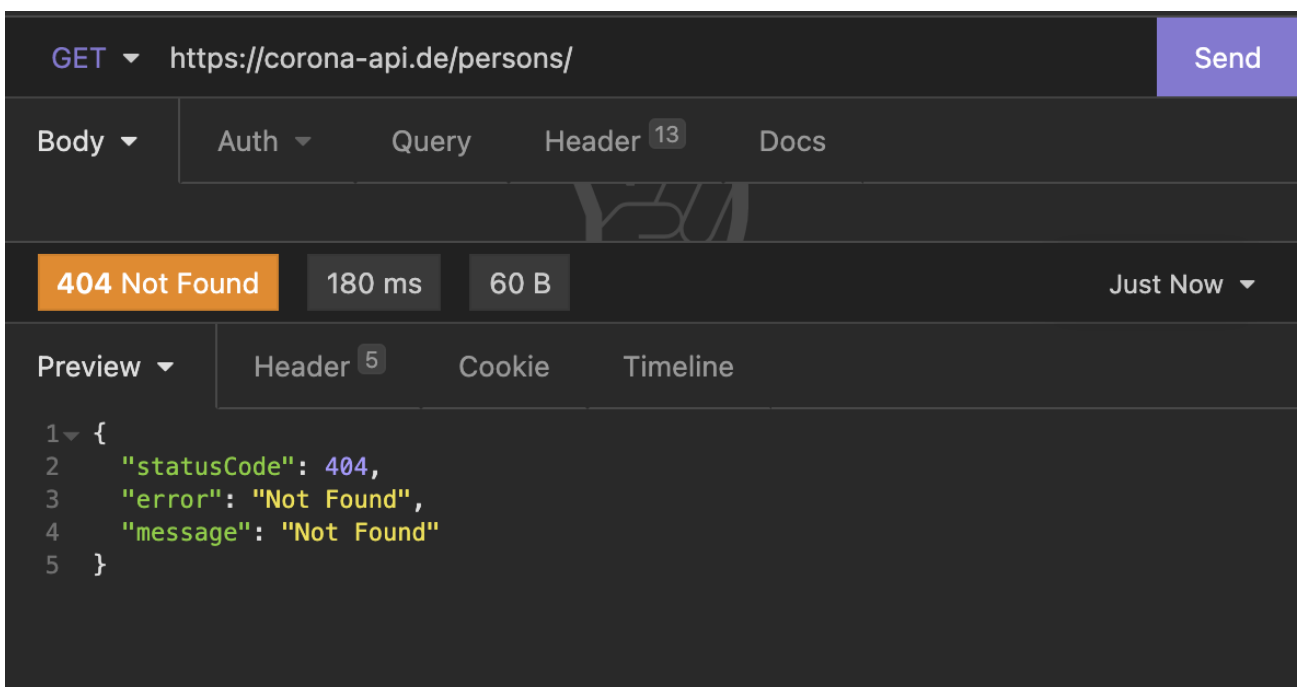
Wie üblich schauen wir uns als allererstes die Entwicklungs-Tools unseres Browsers an. Dabei ist der Network-Tab besonders interessant für uns, denn dort kann man sich anschauen, welche Daten die Website so abrufen.

Eine der ersten Anfragen, die uns auffällt, geht an `https://corona-api.de/persons/owner/{USER_ID}`, wobei `USER_ID` natürlich die Nummer unseres Accounts ist – z.B. `612341213acab23425251e21`.

Also kopieren wir diese Anfrage ganz naiv in unseren API-Client und probieren etwas rum. Als erstes entfernen wir die USER_ID – also 612341213acab23425251e21 am Ende der URL. Also wird unsere URL zu "https://corona-api.de/persons/owner/". Wir erhalten eine Fehlermeldung.



Naja, dann probieren wir eben noch etwas weiter und löschen noch das owner/ aus der URL. Doch wieder kommt eine Fehlermeldung:



Einen Versuch wagen wir noch und entfernen das / am Ende der URL. Und tada:

GET <https://corona-api.de/persons> Send

Body ▾ Auth ▾ Query 4 Header 13 Docs

200 OK 1.42 s 57.9 KB

Preview ▾ Header 9 Cookie Timeline

```
1 [
2   {
3     "address": {
4       "street": "[REDACTED]",
5       "zipCode": "[REDACTED]",
6       "city": "London",
7       "country": "United Kingdom"
8     },
9     "orders": [
10      "610[REDACTED]"
11    ],
12    "_id": "610[REDACTED]",
13    "firstname": "[REDACTED]",
14    "lastname": "[REDACTED]",
15    "email": "[REDACTED]",
16    "birthday": "[REDACTED] (Coordinated Universal
17    Time)",
18    "gender": "Male",
19    "phoneNumber": "[REDACTED]",
20    "coronaAppRights": "None",
21    "owner": "610[REDACTED]",
22    "checkIns": [],
23    "answeredQuestions": [],
24    "createdAt": "2021-08[REDACTED]",
25    "updatedAt": "2021-08[REDACTED]",
26    "__v": 0
27  },
28  {
29    "address": {
30      "street": "[REDACTED]",
31      "zipCode": "[REDACTED]",
32      "city": "Berlin",
33      "country": "Deutschland "
34    },
35    "orders": [
36      "60b[REDACTED]"
37    ],
38    "_id": "60b[REDACTED]",
39    "firstname": "[REDACTED]",
40    "lastname": "[REDACTED]",
41    "email": "[REDACTED]",
42    "birthday": "[REDACTED] (Coordinated Universal
43    Time)"
44  }
45 ]
```

Uns fällt eine Liste mit den Personen, die auf der Plattform registriert sind, entgegen. Insgesamt fast 400.000 mit allen Daten, die bei einem Corona-Test eben so erfasst werden:

- Name
- E-Mail-Adresse
- Geburtsdatum
- Geschlecht
- Telefonnummer
- Adresse
- Pass-/Ausweisnummer (falls angegeben, häufig aber vorhanden)

Wir kennen eure Testergebnisse (mal wieder)

Zu jeder Person gibt es außerdem ein Feld namens `orders`, in dem die Order-IDs dieser Person stehen. Die Tests werden im System von `mein-schnelltest.com` *orders* genannt, also eigentlich Bestellungen.

Als wir unser eigenes Testergebnis als PDF abrufen, erhalten wir dieses von dem Schnittstellen-Endpunkt `https://corona-api.de/orders/downloadPdf/{ORDER_ID}`.

Jetzt sind wir neugierig und probieren mal, dort eine andere Order-ID einzufügen – und schon erhalten wir das Testergebnis einer anderen Person.

Bescheinigung über das Vorliegen eines positiven oder negativen Antigentests zum Nachweis des SARS-CoV-2 Virus



Testzentrum:

Name: Schnelltest Station Berlin Steglitz
 Straße: Schloßstraße
 Hausnummer: 120
 Postleitzahl: 12163



**BärCODE für
scan.baercode.de**



**QR-Code für die
Corona-Warn-App**

Getestete Person:

Name: [REDACTED]
 Anschrift: [REDACTED]
 Geburtsdatum: [REDACTED]

Antigen-Schnelltest:

Name des Tests: 2019-nCoV Antigen Test (Lateral-Flow-Method)
 Hersteller: Guangzhou Wondfo Biotech Co., Ltd.

Testdatum/Testuhrzeit: [REDACTED]
 Test durchgeführt durch: [REDACTED]

Testergebnis:

Positiv* ☐

Negativ ☒



Datum / Stempel testende Stelle / Unterschrift

Das heißt: Der Server überprüft nicht, ob das Testergebnis, das wir abrufen auch wirklich unser eigenes ist. Da wir eingeloggt sind, sollte dieser Abgleich eigentlich kein Problem sein.

Anhand der Personenliste können wir abschätzen, dass es fast 700.000 Testergebnisse waren, die so quasi offen im Netz abrufbar waren.

Kommt ein 177-Jähriger zum Corona-Test und sagt ...

Doch wir können nicht nur hunderttausende Testergebnisse abrufen, sondern es kommt noch schlimmer: Im Quellcode entdecken wir auch die Endpunkte, über

die die Mitarbeiter*innen einen neuen Test im System anlegen und das Testergebnis speichern.

Dass wir diese Endpunkte kennen, ist an sich kein Problem. Denn der Server sollte eigentlich prüfen, ob wir berechtigt sind, diese zu nutzen – also ob wir in einer Teststelle arbeiten und im System entsprechend freigeschaltet sind.¹

Trotzdem versuchen wir, mit unserem Account einen Test anzulegen. Und siehe da:

The screenshot shows a REST client interface with the following details:

- Method:** POST
- URL:** `https://corona-api.de/orders/new`
- JSON Body:**

```
1 {  
2   "teststation": "609dc5f0112cf930de297e07",  
3   "testperson": "[REDACTED]",  
4   "testType": "Antigen_Citizen_Test",  
5   "testPrice": 0,  
6   "discount": 0,  
7   "totalPrice": 0,  
8   "products": []  
9 }
```
- Status:** 201 Created
- Response Time:** 320 ms
- Response Size:** 33 B
- Preview JSON:**

```
1 {  
2   "id": "616 [REDACTED]"  
3 }
```

Wir können selbst einen Test anlegen und auch problemlos das Testergebnis speichern:

PUT ▼ <https://corona-api.de/orders/confirmTestResult> Send

JSON ▼ Auth ▼ Query Header 2 Docs

```
1 {"orderId": "616[REDACTED]", "isPositiv": false,
  "testedBy": "zerforschung"}
```

Beautify JSON

201 Created 4.31 s 5.8 KB

Preview ▼ Header 7 Cookie Timeline

```
1 {
2   "updatedOrder": {
3     "test": {
4       "result": {
5         "isPositiv": false,
6         "evaluatedAt": "[REDACTED]"
7       },
8       "status": "Done",
9       "type": "PCR_Express",
10      "testTubeId": null,
11      "testedBy": "zerforschung",
12      "qrCodeString": null,
13      "barcode":
14        "data:image/png;base64,iVBORw0KGgoAAAANSUgAAASwAAAEsEAAAAAMhg3"
```

Das heißt: Jetzt können wir für jede beliebige Person einen Test erstellen.

Natürlich nehmen wir zum Ausprobieren eine offensichtlich historische Person², damit das Test-Zertifikat auf keinen Fall missbraucht werden kann. Wir erstellen also einen PCR-Test für Robert Koch. Und wir können zum Glück mitteilen: Sein Testergebnis war negativ – wir wollen uns gar nicht ausmalen, was für ein Risiko eine Coronainfektion für ihn mit seinen 177 Jahren wäre.

**SCHNELLTEST BERLIN****Über 20x in Berlin & Brandenburg**

WeCare Services GmbH
Auguststraße 20
10117 Berlin

Robert Koch
Nordufer 20
13353 Berlin
DE



Patienten Nr.: **null**
Geburtsdatum: **11.12.1843**
Geschlecht: **Männlich**
Passport Nummer (verifiziert): -
Testmethode: **Sars-CoV-2-PCR RT (Labortest)**
Art des Ergebnisses: **Endergebnis**

Probenentnahme:
Schnelltest Berlin Steglitz
Schloßstraße 120
12163 Berlin
Probenentnahmedatum: **19.10.2021, 04:38**
Probentyp: **Rachenabstrich**

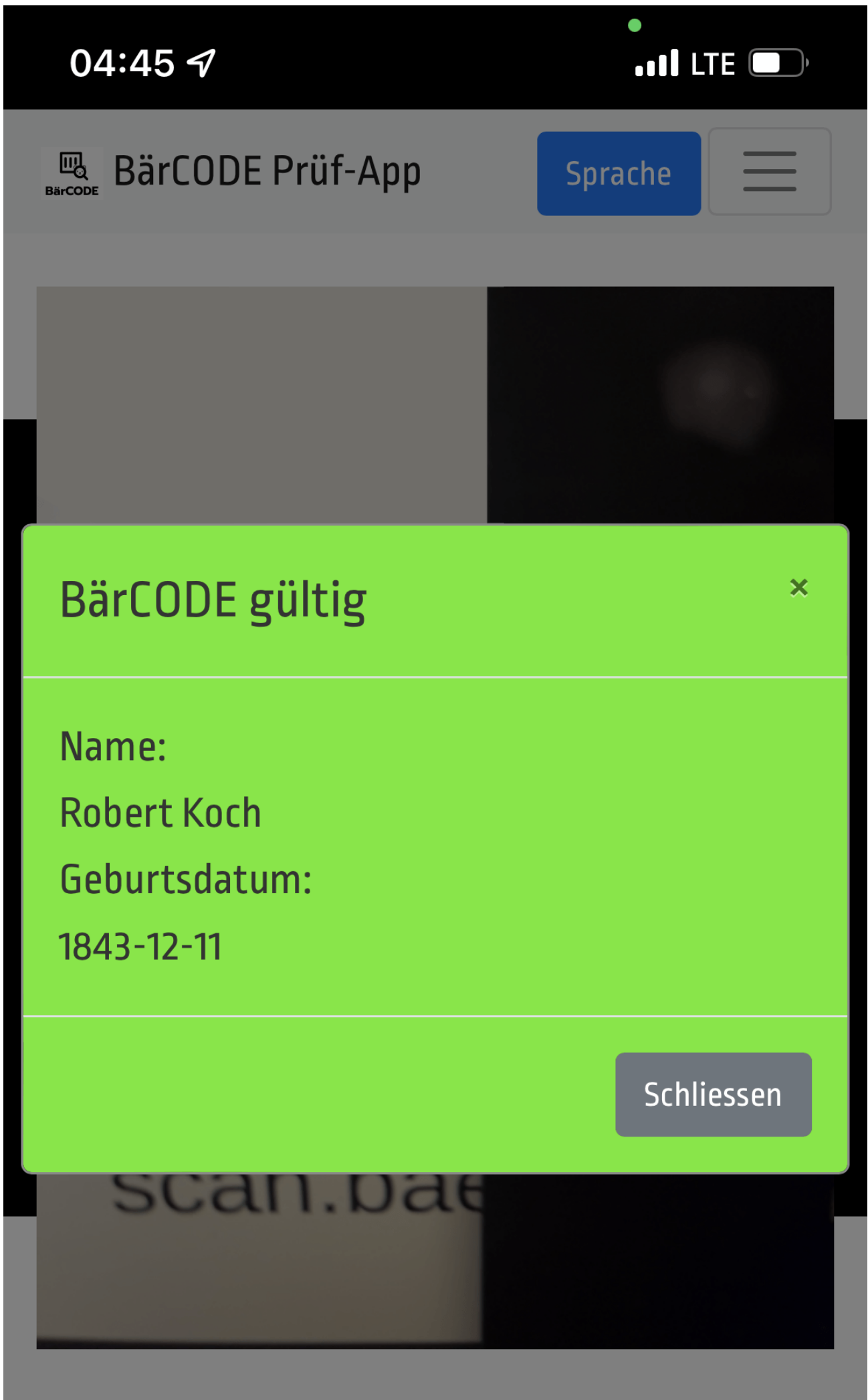
BärCODE für
scan.baercode.de

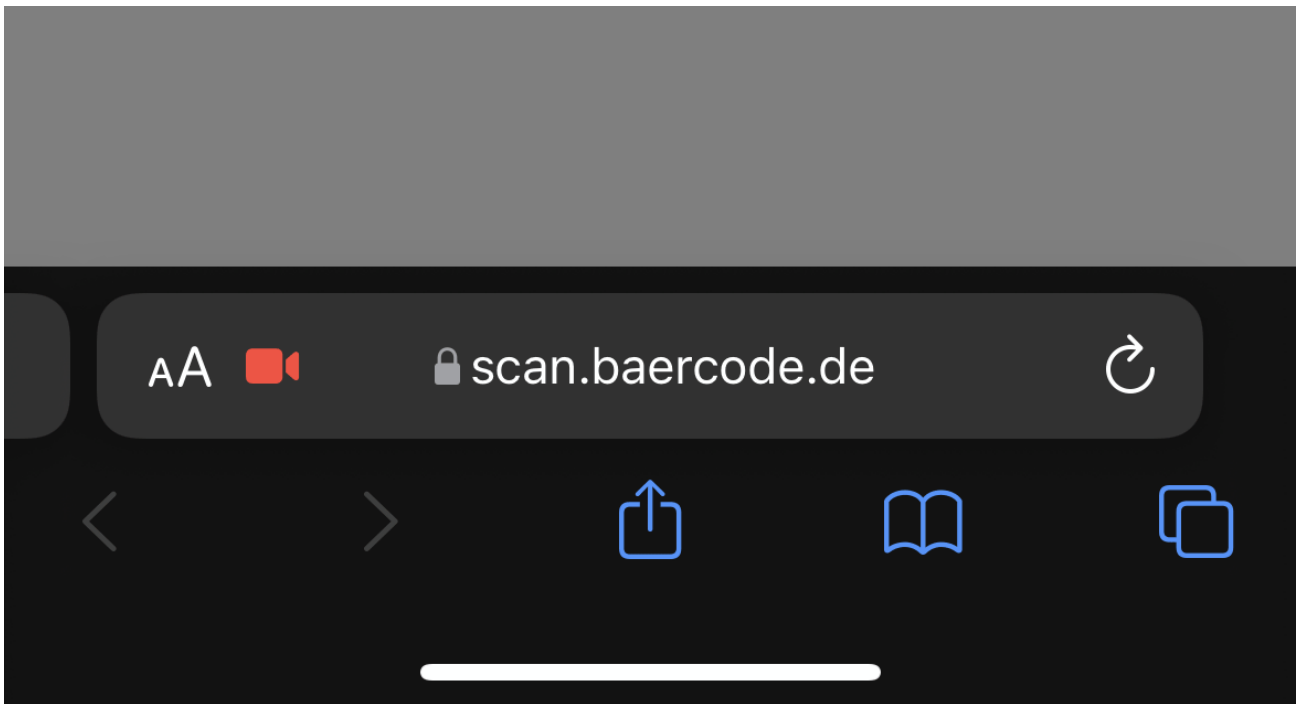
PCR TEST ERGEBNIS - getestet wurde nach dem SARS-CoV-2 Virus RNA mittels RT-PCR Analyse



Ergebnis: NEGATIV // Es besteht kein erkennbar erhöhtes Infektionsrisiko für Kontaktpersonen

Das Zertifikat enthält alles: Name, optional Passnummer und sogar einen [BärCODE](#), der auch als gültig erkannt wird. Soweit wir wissen, kann der BärCODE auch nicht wieder ungültig gemacht werden, [so wie wir es beim digitalen Impfzertifikat schon mal beschrieben haben](#).³





Da wir nicht wissen, welche Prozesse bei einem positiven Testergebnis automatisch ausgelöst werden, haben wir uns dagegen entschieden, auch ein positives Testergebnis zu generieren. Wir gehen allerdings davon aus, dass dies ebenfalls problemlos möglich gewesen wäre.

You've got mail!

Wie immer haben wir auch diesmal ein Responsible-Disclosure-Verfahren eingeleitet, unmittelbar nachdem wir die Lücken gefunden haben. Dafür dokumentieren wir die Lücken feinsäuberlich und informieren das CERT-Bund, den Hersteller und die zuständigen Landesdatenschutzbeauftragten – in diesem Fall für Berlin die Berliner Beauftragte für Datenschutz und Informationsfreiheit.

Der Hersteller hat dann innerhalb kurzer Zeit alle beschriebenen Lücken geschlossen und eine weitere Analyse eingeleitet. Besonders gründlich kann diese aber nicht gewesen sein, denn die Testergebnisse für Robert Koch in unserem Account existieren weiterhin:

Datum	Testart	Status	Ergebnis
19 Oct 2021 04:47	Antigen (Bürgertest)	DONE	NEGATIV
19 Oct 2021 04:42	PCR	DONE	NEGATIV
19 Oct 2021 04:38	PCR (Express)	DONE	NEGATIV
19 Oct 2021 04:20	Antigen (Bürgertest)	DONE	NEGATIV

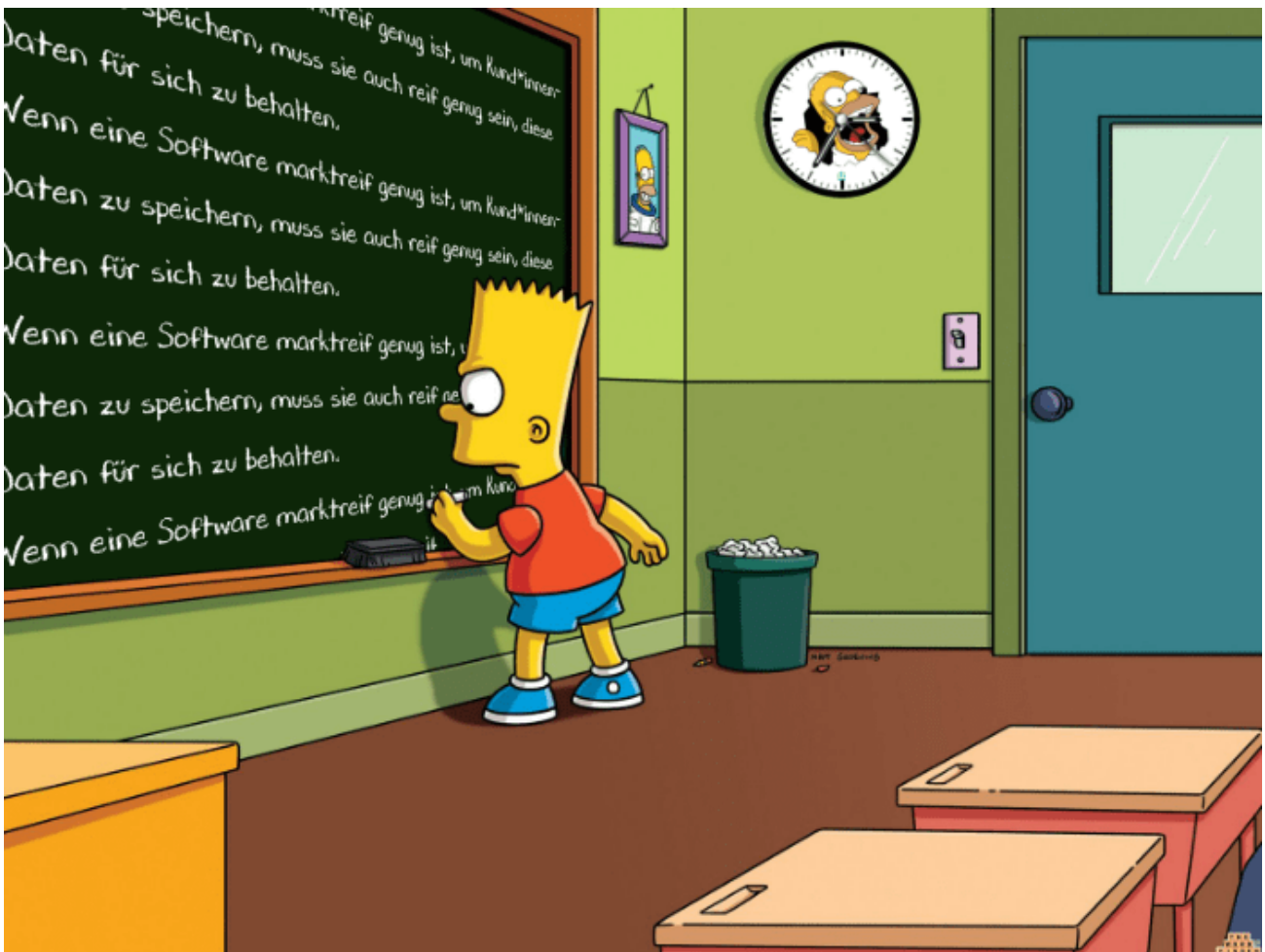
Das Unternehmen hat die betroffenen Kund*innen bisher nicht benachrichtigt. Dabei war in den vergangenen drei Wochen wirklich genug Zeit, das zu tun.

Wir hoffen, dass sie es noch tun und wirklich alle rund 400.000 betroffenen Kund*innen gründlich über alle Details informieren.

Fazit

Wie schon bei den letzten Testzentren-Artikeln sind wir fassungslos, wie fahrlässig hier mit den persönlichen Daten von hunderttausenden Menschen umgegangen wird.

Wer eine solche Software anbietet, **muss** dafür sorgen, dass diese läuft, *ohne* Daten zu verlieren – auch das ist ein wichtiger Teil des Datenschutzes. Wenn eine Software marktreif genug ist, um Kund*innen-Daten zu speichern, muss sie auch reif genug sein, diese Daten für sich zu behalten.



Das bedeutet unserer Ansicht nach nicht nur, dass ein Anbieter fähig sein sollte, seine Datenbank so zu konfigurieren, dass diese nicht für jeden zugänglich im Internet steht. Sondern eigentlich: absolute Minimierung der anfallenden Daten

und E2E-verschlüsselte Kommunikation – insbesondere im Kontext medizinischer Daten.

[Eine gute Übersicht über weitere sinnvolle Maßnahmen gibt es beim Landesdatenschutz Baden-Württemberg.](#)

Der Markt regelt das ... nicht

Im Fall der Testzentren wurde eine Aufgabe, die eigentlich der Staat und die gesetzlichen Krankenversicherungen erfüllen sollten, dem Markt überlassen. Nach unserer Einschätzung haben die letzten Artikel auf diesem und anderen Blogs ausgiebig gezeigt, dass das nicht funktioniert.

Dabei gibt es von staatlicher Seite inzwischen sogar eine Lösung für das Problem: Die Corona-Warn-App, die seit Version 2.4, also 24. Juni 2021, auch Schnelltests unterstützt.

Dabei ist die digitale Übertragung der Testergebnisse sinnvoll und datensparsam gelöst und es wurde schon beim Systementwurf auf Datensicherheit geachtet. Warum immer noch Unternehmen ihre selbstgeklöppelte Testsoftware einsetzen, können wir nicht nachvollziehen.

Wir fordern deshalb, dass zukünftig kostenfreie Bürger*innen-Tests nur noch über die CWA oder analog abgewickelt werden dürfen. Der Markt hat das nicht geregelt. Der Markt regelt nie irgendwas.



Wir fordern in jedem dieser Artikel, dass die Datenschutzbehörden endlich empfindliche Strafen gegen Unternehmen verhängen, die so sorglos mit Daten umgehen. Die Mühlen der Bürokratie mahlen langsam, das ist uns bewusst. Aber nach 8 Monaten, seitdem [wir das erste Mal eine Sicherheitslücke bei einem Schnelltestanbieter gefunden haben](#), wird es langsam mal Zeit.

Allerdings sind auch wir, die wir viele Stunden ehrenamtlich in Analysen von Testzentren und die Kommunikation mit Behörden und Softwareherstellern gesteckt haben, mittlerweile ziemlich frustriert. Wir sehen kaum Verbesserung seitens der Anbieter oder Regulierungsversuche durch die Politik.

Uns ist bewusst, dass die Datenschutzbehörden der Länder völlig überlastet sind und sich freuen, wenn die Firma, gegen die sie ermitteln, auch am Ende der

Ermittlung noch existiert. Allerdings sind sie auch unsere letzte Hoffnung: Bitte verhängt endlich Strafen bei grob fahrlässigen Datenabflüssen – insbesondere im Gesundheitssektor. Denn Markt und auch Politik haben hier versagt.




Danke

Vielen Dank an die Berliner Datenschutzbeauftragte, das CERT-Bund und den rbb für die gute Zusammenarbeit 🧡. Wir glauben: Nur wenn Sicherheitslücken möglichst sichtbar sind, können wir sie verstehen und vermeiden. Den Artikel von rbb24 über die Lücke findet ihr hier:

<https://www.rbb24.de/panorama/thema/corona/beitraege/2021/11/schnelltest-berlin-pcr-gefaelscht-datenleck.html>

Wenn ihr zerforschung unterstützen wollt, findet ihr hier Möglichkeiten:

<https://zerforschung.org/unterstuetzen/>

-
1. Wir arbeiten nicht in einem Testzentrum. 
 2. in der ersten Fassung haben wir hier "fiktive Person" geschrieben, das war natürlich Quatsch 
 3. **Offenlegung:** Wir wurden vor längerer Zeit angefragt, ob wir uns den BärCODE sicherheitstechnisch angucken wollen. Aus Kapazitätsgründen haben wir auf diese Anfrage nicht reagiert. Außerdem machen wir generell keine Auftragsarbeiten für Software-Hersteller. 

2021-11-10

#corona #security #databreach

[RSS](#) [Twitter](#) [Mastodon](#) [Kontakt](#) [Privacy](#) [Impressum](#)

Erstellt mit [Hugo](#).