

This is the export of a building block from the TMC Threat Library. This project aims to propose mitigations for relevant threats to reusable building blocks of modern tech systems. For more information about the project visit <https://threat-modeling.net/library/>

Public User Profiles

Gains

-  Have profile creators present themselves - by Hendrik
-  Have profile consumers find out who the others are - by Hendrik
-  Create a sense of community - by Hendrik

System Model

-  Profile Creator - by Hendrik
-  Profile Consumer - by Hendrik
-  Profile API - by Hendrik
-  Unique usernames - by Hendrik
-  Profile images - by Hendrik
-  Freetext about - by Hendrik
-  Structured answers (depending on service type) - by Hendrik
-  Real names - by Hendrik
-  Profile creator edits profile - by Hendrik
-  Profile creator uploads image - by Hendrik
-  Profile consumer views profile overviews - by Hendrik
-  Profile consumer views profile details - by Hendrik

More info

⚡ Threats and 🛡️ Mitigation Ideas

Confidentiality? Integrity? Availability? / Usability? Privacy? Safety? €\$? ...

→ Protect? Detect? Respond? → Follow-up threats?

⚡ Profile scraping: Rogue profile consumer collects massive amounts of profile data - by Hendrik

🛡️ Rate limiting on profile request API - by Hendrik

🛡️ Detection of suspicious request patterns + blocking - by Hendrik

🛡️ Hard to guess ID pattern - by TMC DACH

⚡ Fake profile: Made-up person, other person, ... - by TMC DACH

🛡️ Validation of identity - by TMC DACH

🛡️ validate faces with live camera validation - by TMC DACH

🛡️ Consider trade-offs, when users don't want to share their ID or faces - by TMC DACH

⚡ Scamming - by TMC DACH

⚡ Linking usernames and info to other platforms - by TMC DACH

⚡ Sensitive personal info, like phone numbers, etc - by TMC DACH

⚡ Background info / meta data in profile images - by TMC DACH

🛡️ Strip meta data from image uploads - by TMC DACH

⚡ Spamming on API - by TMC DACH

🛡️ Throtteling, rate limits - by TMC DACH

⚡ API allows guessing of user IDs + enumeration attacks - by TMC DACH

🛡️ UUID IDs - by TMC DACH

⚡ Inappropriate content in profile and images - by TMC DACH

⚡ Oversharing in API response - by TMC DACH

- ⚡ Unauthorized API requests - by TMC DACH
- ⚡ Upload of other mime types with image upload API - by TMC DACH
 - ☂ Check for mime types - by TMC DACH
- ⚡ Malicious content - by TMC DACH
 - ☂ Check for mime types - by TMC DACH
 - ☂ Validate contents at the server-side - by TMC DACH
- ⚡ Cross-site scripting in about or other profile info - by TMC DACH
 - ☂ Validate / escape - by TMC DACH
- ⚡ Impersonation attacks: Pretend to be someone else - by TMC DACH
 - ☂ Identity verification - by TMC DACH
 - ☂ Alert about (strange) modifications in profile - by TMC DACH
- ⚡ Saving of other people's profiles - by TMC DACH
 - ☂ Authenticate profile creators - by TMC DACH
 - ☂ Only let the creator themselves edit their profile - by TMC DACH
 - ☂ RBAC (Role-based access control) - by TMC DACH
- ⚡ Strange usernames - by TMC DACH
 - ☂ allowed characters - by TMC DACH
 - ☂ Be careful with error responses - by TMC DACH