Zagweb Security Concerns

Max Chehab & Max Dulin

**Problem**:

* Able to view any Who’s Who profile pictures without session.
* Insecure session cookie
  + Only 22 characters long.
  + First half of the cookie is a six digit base36 number.
  + Half of the cookie is a unique, incremental, id that can be scraped from the Who’s Who public facing profile picture.
  + The incremental id is viewable from each Who’s Who profile picture, which is public.
* Who’s Who’s is 100% scrapable using the same, incremental, userID in a GET query.

**Solution:**

* How to improve the GU Who’s Who profile pictures:
  + At most, be protected behind a cookie, this is a very simple middleware router technique.
  + At the very least, use UUID-V4 identification instead of an incremental identification.
* How to improve the SESSID cookie:
  + The cookie should be much larger than 22 characters. Using another UUID-V4 can solve this issue.
* How to make web scraping difficult and fix the issue:
  + Replacing the Who’s Who query with a UUID-V4 will prevent web scraping.

**Examples:**

* Who’s Who profile picture.

The following is Sydney Chehab’s Who’s Who profile photo:

* <https://zagweb.gonzaga.edu/pls/gonz/docs/idphoto/682122/gozags.jpg>

Max Chehab’s is:

* <https://zagweb.gonzaga.edu/pls/gonz/docs/idphoto/682121/gozags.jpg>

Note that Sydney’s identification, 682122, is one less than Max’s, 682121.

* Session Cookie

The formula for generating session cookies is:

* base64(base36(32 bit int) + incremental\_ID)

The initial base64 encoded string is 22 characters making the base36 number only 6 digits long. To represent the amount of permutations required to crack this session is 36^6 or 2,176,782,336. This is **not** a very large number and a determined hacker can crack this in under 30 minutes.