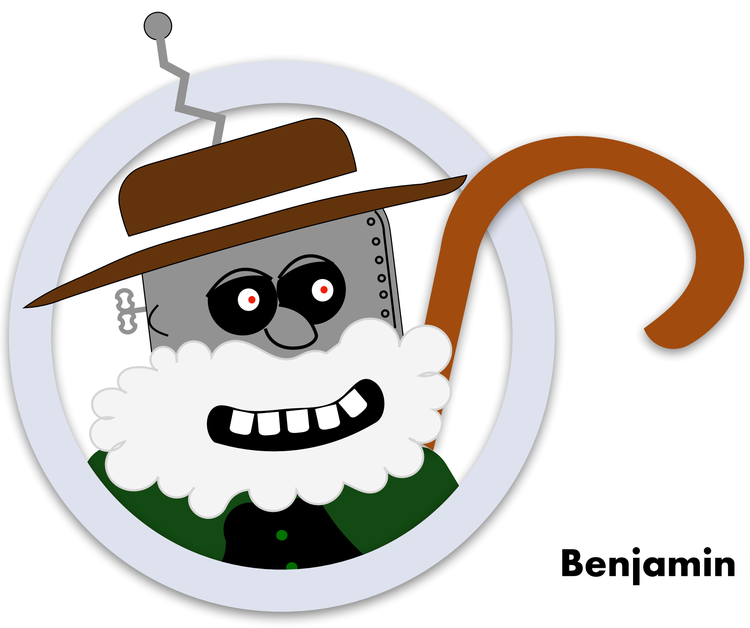


Shepherd

Enabling large-scale post login studies

Benjamin Krumnow, Hugo Jonker, Marc Sleegers, Alan Verresen, Jelmer Kalkmann

Contact: benjamin.krumnow@th-koeln.de and Hugo.Jonker@ou.nl

4 Steps: Automated end-to-end logging in framework

1. Login dataset

Sourcing BugMeNot for credentials[1].

50K Domains with multiple logins credentials.

[1] *Entries of this database are unreliable.*

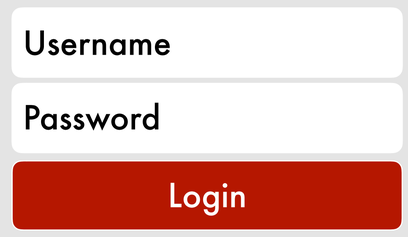
2. Finding login areas

1. Landing page
2. 1st level URLs
3. Clickable Elements
4. Standard URLs
5. Search engines
6. 2nd level URLs

38K login areas identified.
Success rate: 79%

3. Submitting credentials

One-step and two-step logins.



Detected failures:

- Invalid credentials	23K
- CAPTCHAs	1.5K
- Others:	2.7K
Submission succeeded:	11K

4. Verifying logins

1. Find usernames, emails, logout buttons.
2. Find missing login area and buttons.

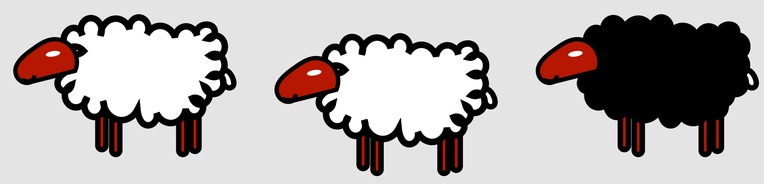
→ Repeat steps with and without cookies.

7,113 verified logins!

Success for 64% of sites with valid credentials.

Security evaluation

Every 3rd website is vulnerable!



Sites scanned	7.1K	100 %
Susceptible to hijacking	2.4K	34 %

Susceptible if:

- no *Secure* flag, and
- no *SameSite* flag, and
- no HSTS header

24th European Symposium on Research in Computer Security
23 - 27 September, Luxembourg

Technology
Arts Sciences
TH Köln