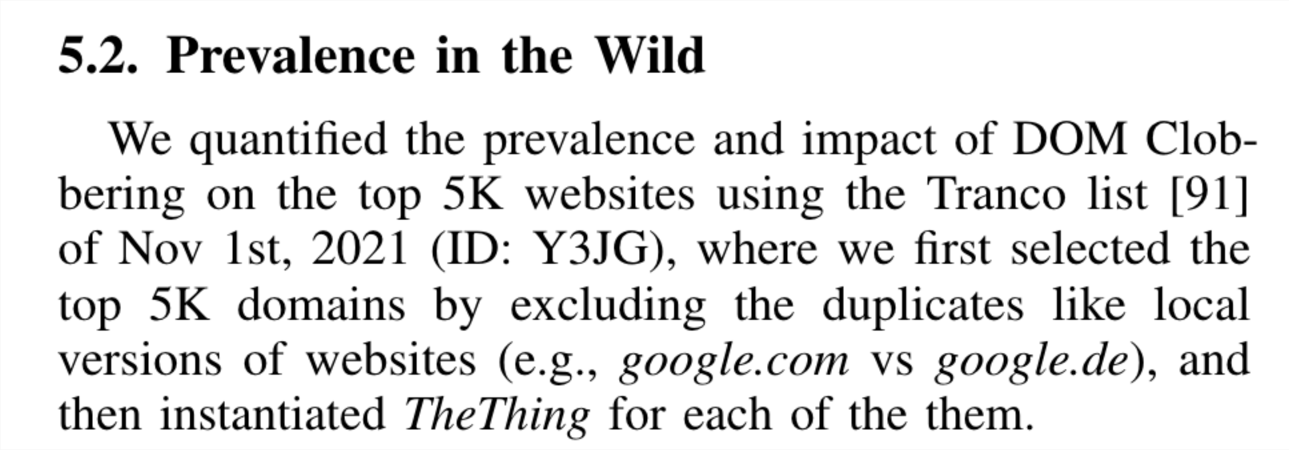
To Auth or Not To Auth? A Comparative Analysis of the Pre- and Post-Login Security Landscape

Jannis Rautenstrauch, *Metodi Mitkov, Thomas Helbrecht, Lorenz Hetterich, Ben Stock*
CISPA Helmholtz Center for Information Security
jannis.rautenstrauch@cispa.de, *@jannis_r*

45th IEEE Symposium on Security and Privacy 2024

Web Security Research Crawls Top-Sites

Web Security Research Crawls Top-Sites

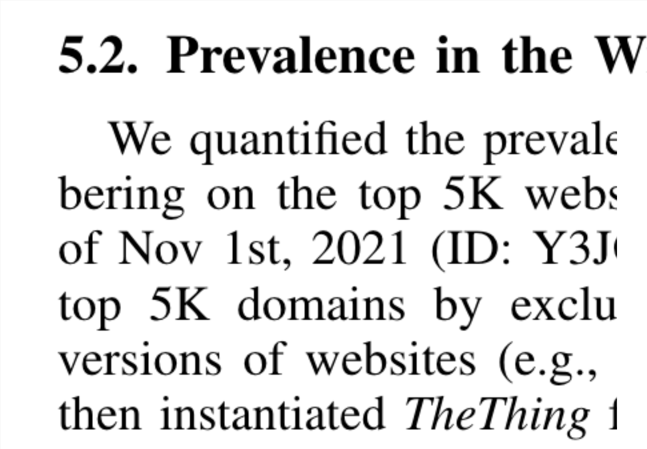


5.2. Prevalence in the Wild

We quantified the prevalence and impact of DOM Clobbering on the top 5K websites using the Tranco list [91] of Nov 1st, 2021 (ID: Y3JG), where we first selected the top 5K domains by excluding the duplicates like local versions of websites (e.g., *google.com* vs *google.de*), and then instantiated *TheThing* for each of the them.

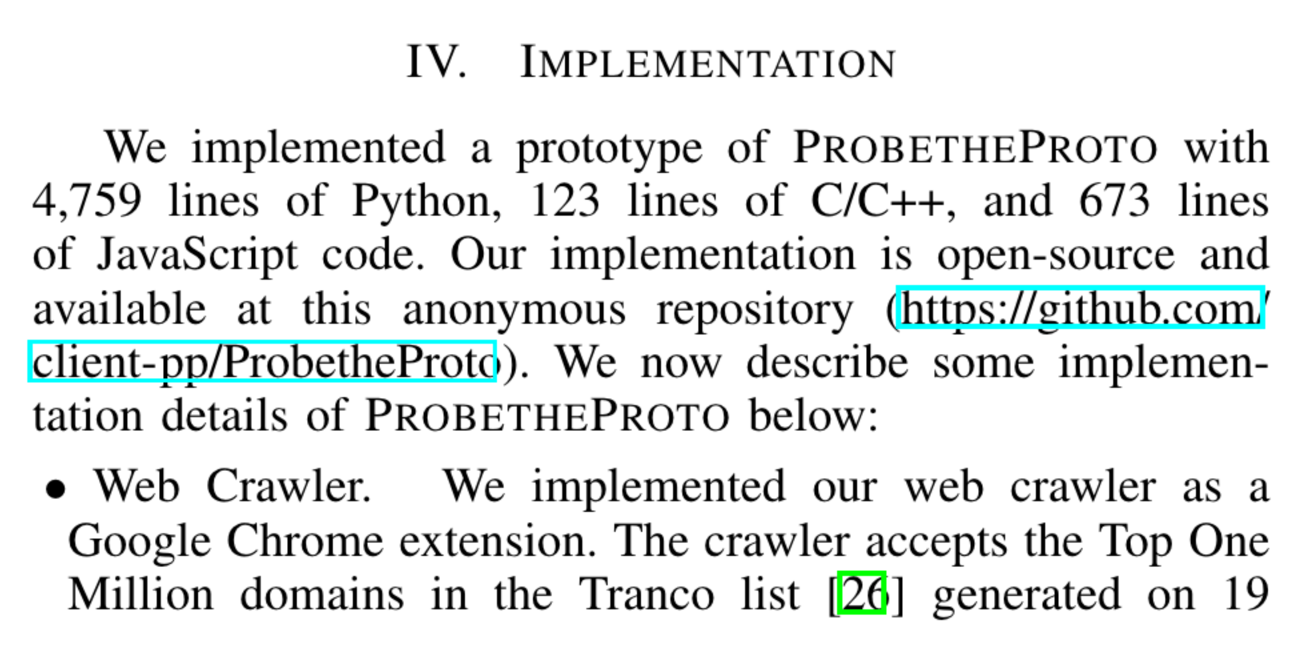
Khodayari, Soheil, and Giancarlo Pellegrino. "It's (DOM) Clobbering Time: Attack Techniques, Prevalence, and Defenses." IEEE S&P 2023

Web Security Research Crawls Top-Sites



5.2. Prevalence in the Wild

We quantified the prevale
bering on the top 5K webs
of Nov 1st, 2021 (ID: Y3J
top 5K domains by exclu
versions of websites (e.g.,
then instantiated *TheThing* f



IV. Implementation

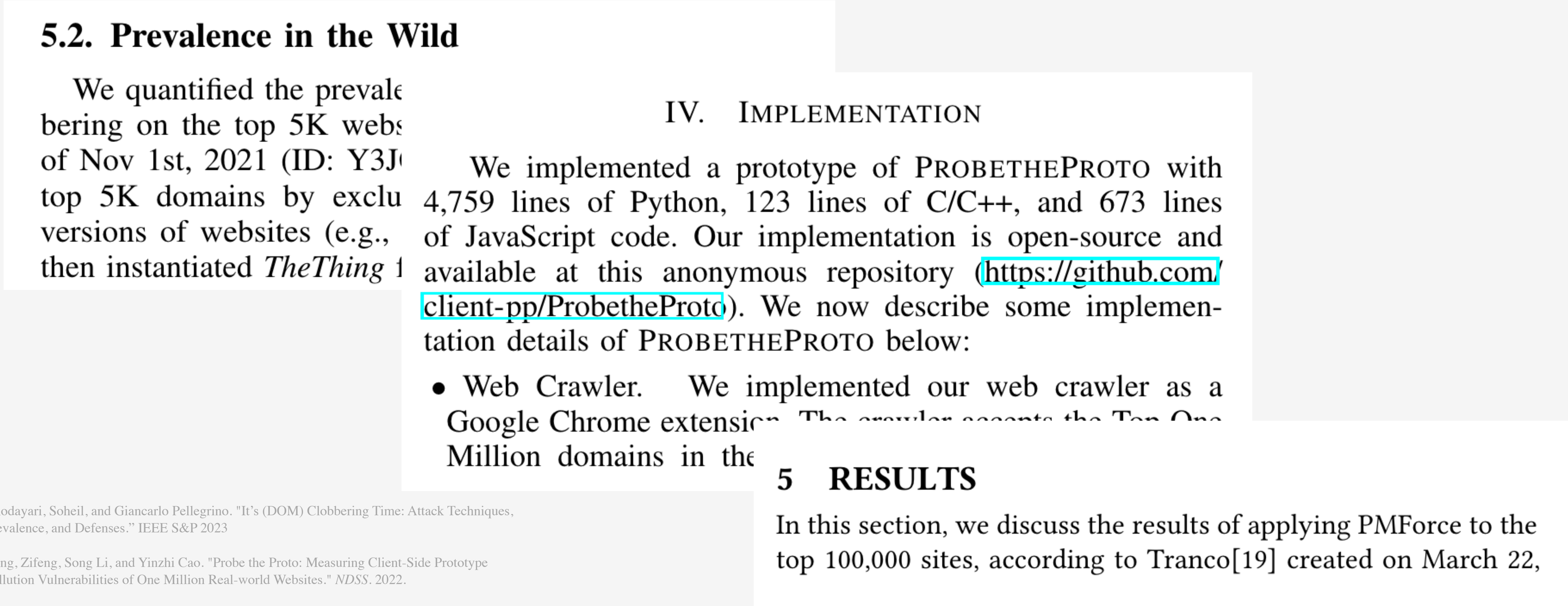
We implemented a prototype of ProbeTheProto with 4,759 lines of Python, 123 lines of C/C++, and 673 lines of JavaScript code. Our implementation is open-source and available at this anonymous repository (https://github.com/client-pp/ProbetheProto). We now describe some implementation details of ProbeTheProto below:

- Web Crawler. We implemented our web crawler as a Google Chrome extension. The crawler accepts the Top One Million domains in the Tranco list [26] generated on 19

Khodayari, Soheil, and Giancarlo Pellegrino. "It's (DOM) Clobbering Time: Attack Techniques, Prevalence, and Defenses." IEEE S&P 2023

Kang, Zifeng, Song Li, and Yinzhi Cao. "Probe the Proto: Measuring Client-Side Prototype Pollution Vulnerabilities of One Million Real-world Websites." *NDSS*. 2022.

Web Security Research Crawls Top-Sites



5.2. Prevalence in the Wild

We quantified the prevale
bering on the top 5K webs
of Nov 1st, 2021 (ID: Y3J(
top 5K domains by exclu
versions of websites (e.g.,
then instantiated *TheThing* f

IV. Implementation

We implemented a prototype of ProbeTheProto with 4,759 lines of Python, 123 lines of C/C++, and 673 lines of JavaScript code. Our implementation is open-source and available at this anonymous repository (https://github.com/client-pp/ProbetheProto). We now describe some implementation details of ProbeTheProto below:

- Web Crawler. We implemented our web crawler as a Google Chrome extension. The crawler accepts the Top One Million domains in the

5 RESULTS

In this section, we discuss the results of applying PMForce to the top 100,000 sites, according to Tranco[19] created on March 22,

Khodayari, Soheil, and Giancarlo Pellegrino. "It's (DOM) Clobbering Time: Attack Techniques, Prevalence, and Defenses." IEEE S&P 2023

Kang, Zifeng, Song Li, and Yinzhi Cao. "Probe the Proto: Measuring Client-Side Prototype Pollution Vulnerabilities of One Million Real-world Websites." *NDSS*. 2022.

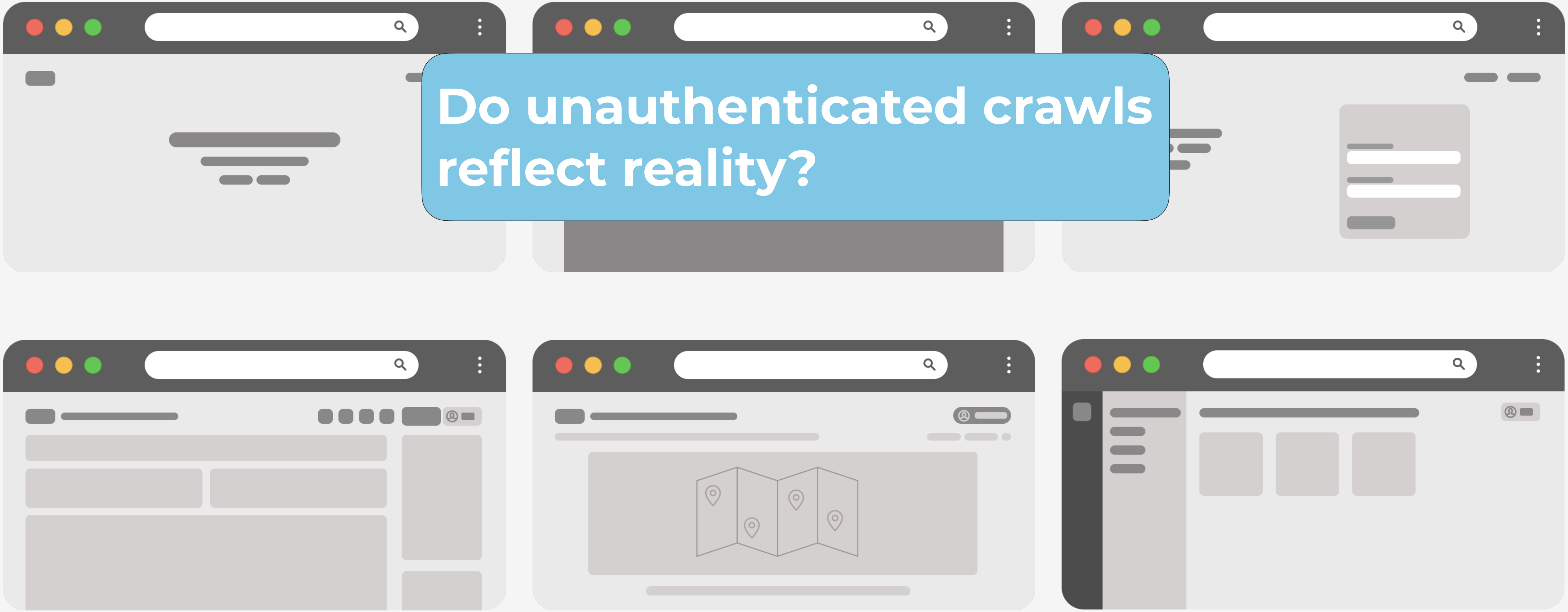
Steffens, Marius, and Ben Stock. "PMForce: Systematically Analyzing postMessage Handlers at Scale." *CCS* 2020.

Do Crawlers Experience The Same Web?

Do Crawlers Experience The Same Web?

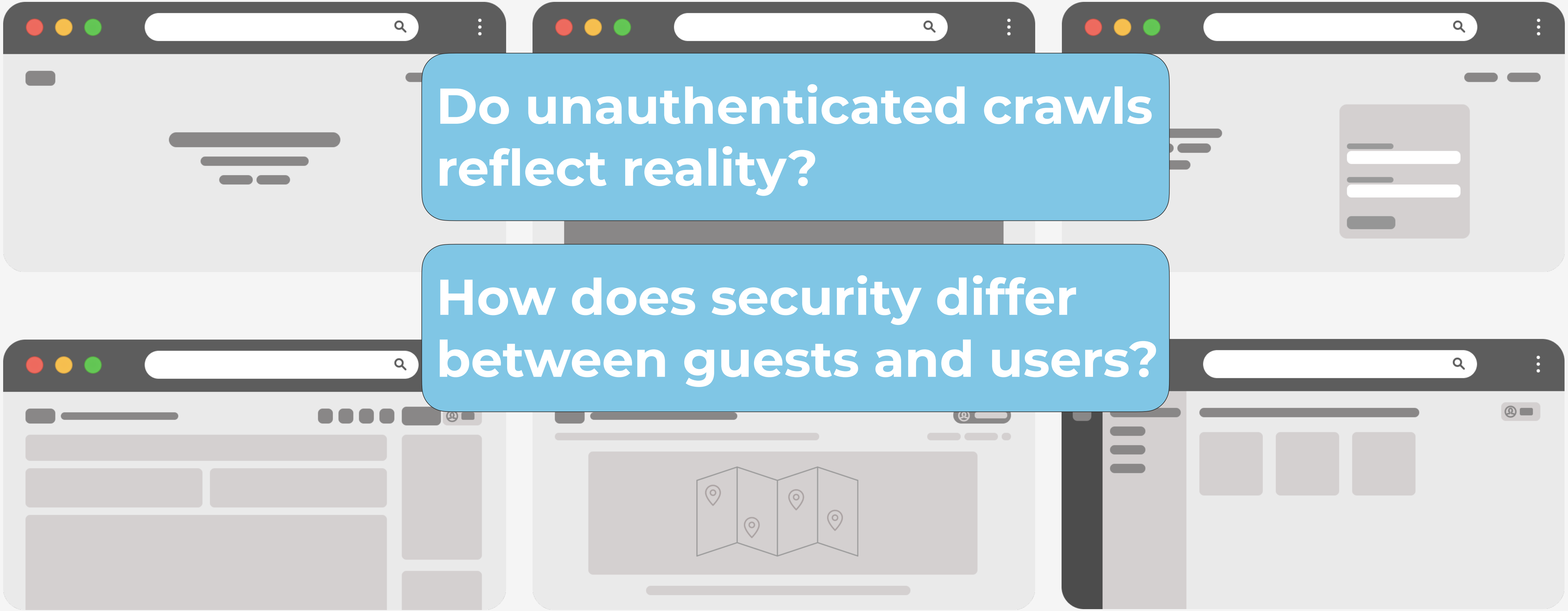
Do Crawlers Experience The Same Web?

Do Crawlers Experience The Same Web?



Do unauthenticated crawls reflect reality?

Do Crawlers Experience The Same Web?



Do unauthenticated crawls reflect reality?

How does security differ between guests and users?

Comparative Security Measurement

Comparative Security Measurement

1. Repeat measurements from prior work

Comparative Security Measurement

1. Repeat measurements from prior work
2. **Client-Side XSS:**
   - Uses Foxhound and exploit generator from [Steffens et al. NDSS 2019]
   - How many flows from user controllable sources to XSS sinks exist?

Comparative Security Measurement

1. Repeat measurements from prior work
2. **Client-Side XSS:**
   - Uses Foxhound and exploit generator from [Steffens et al. NDSS 2019]
   - How many flows from user controllable sources to XSS sinks exist?
3. **Security Headers:**
   - Are there differences in usage, security, and consistency?

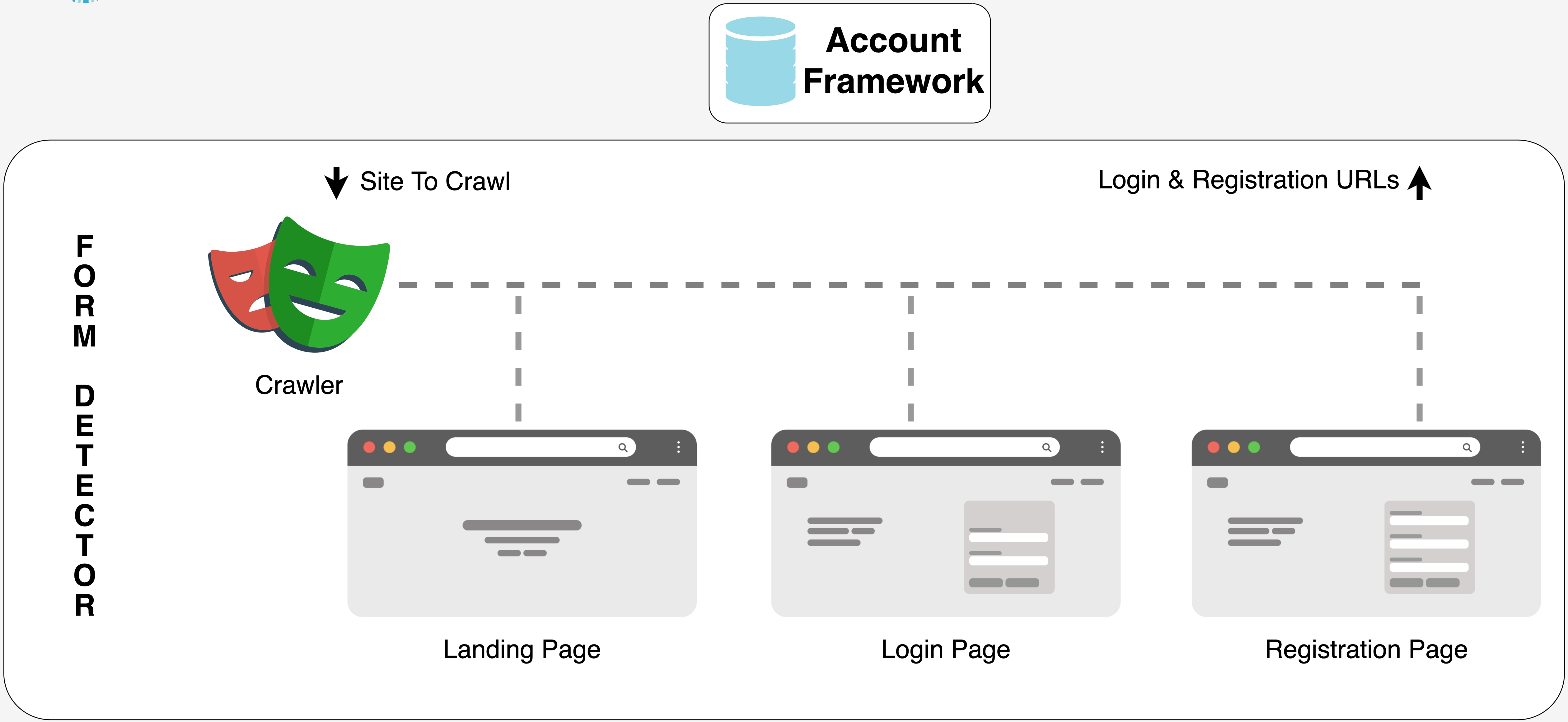
Comparative Security Measurement

1. Repeat measurements from prior work
2. **Client-Side XSS:**
   - Uses Foxhound and exploit generator from [Steffens et al. NDSS 2019]
   - How many flows from user controllable sources to XSS sinks exist?
3. **Security Headers:**
   - Are there differences in usage, security, and consistency?
4. **Javascript Inclusions:**
   - How do inclusions differ w.r.t script types, number of third-parties, trackers, known vulnerable libraries, and more?

Comparative Security Measurement

1. Repeat measurements from prior work
2. **Client-Side XSS:**
   - Uses Foxhound and exploit generator from [Steffens et al. NDSS 2019]
   - How many flows from user controllable sources to XSS sinks exist?
3. **Security Headers:**
   - Are there differences in usage, security, and consistency?
4. **Javascript Inclusions:**
   - How do inclusions differ w.r.t script types, number of third-parties, trackers, known vulnerable libraries, and more?
5. **PostMessages:**
   - Uses PMForce [Steffens and Stock CCS 2020]
   - How many (vulnerable) handlers exist?

Crawling Pipeline



Account Framework

Site To Crawl

Login & Registration URLs

FORM DETECTOR

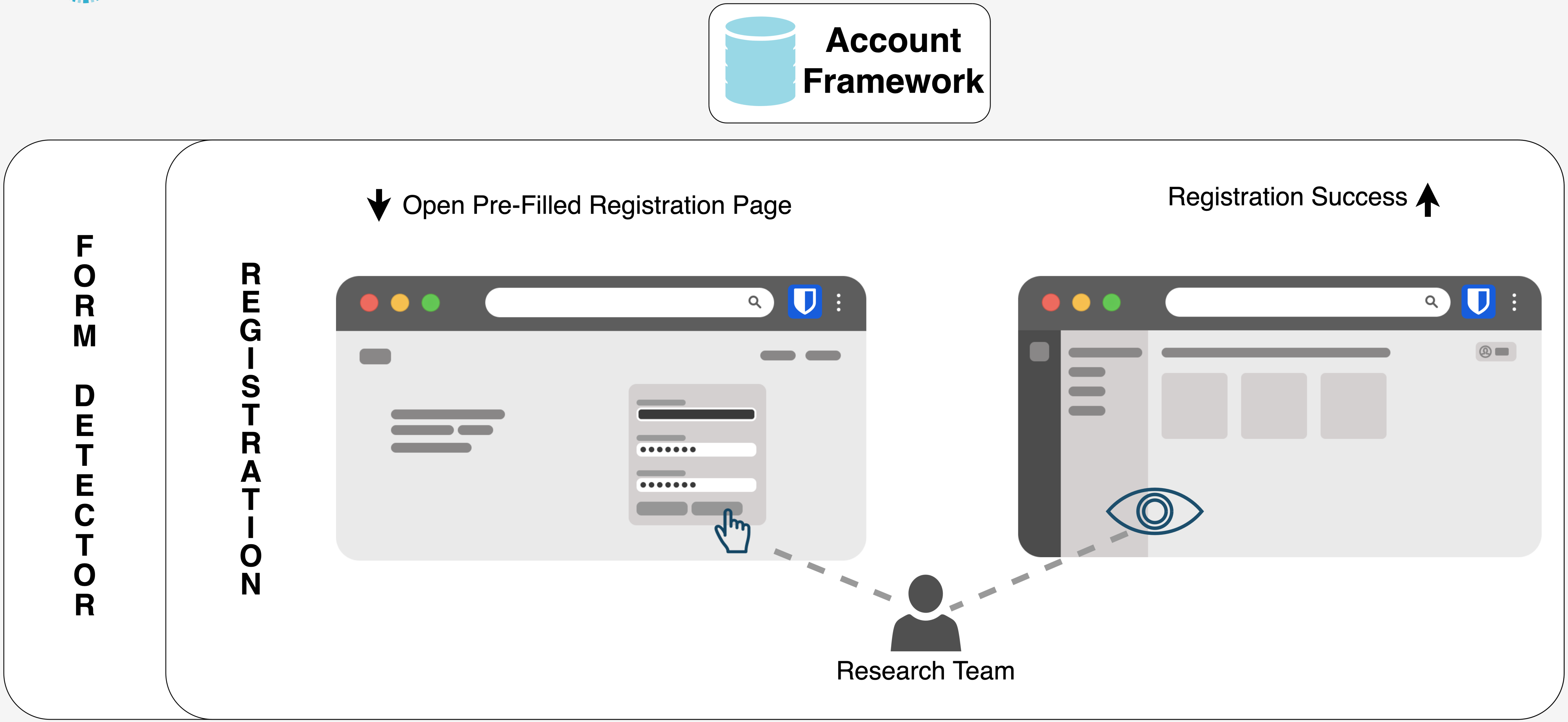
Crawler

Landing Page

Login Page

Registration Page

Crawling Pipeline



Account Framework

FORM DETECTOR

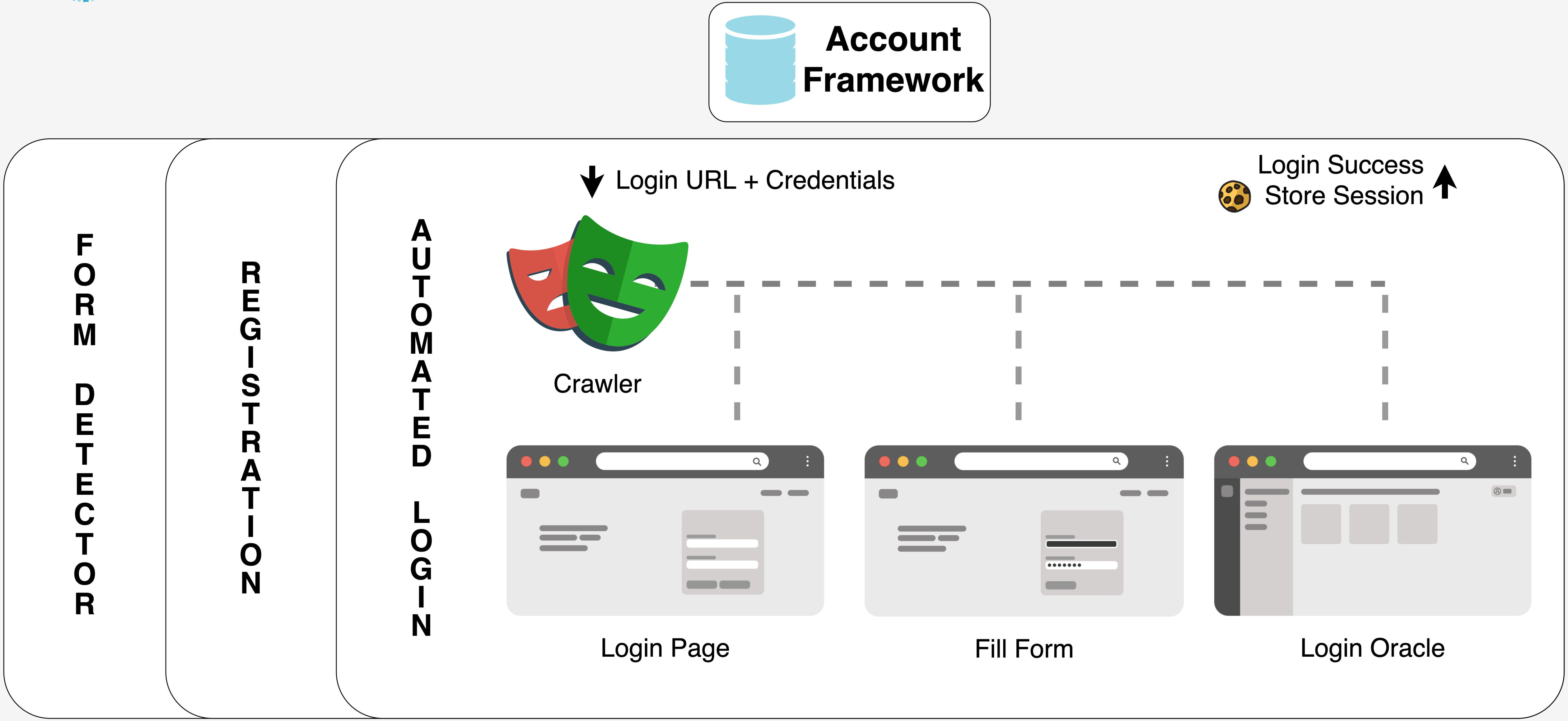
REGISTRATION

Open Pre-Filled Registration Page

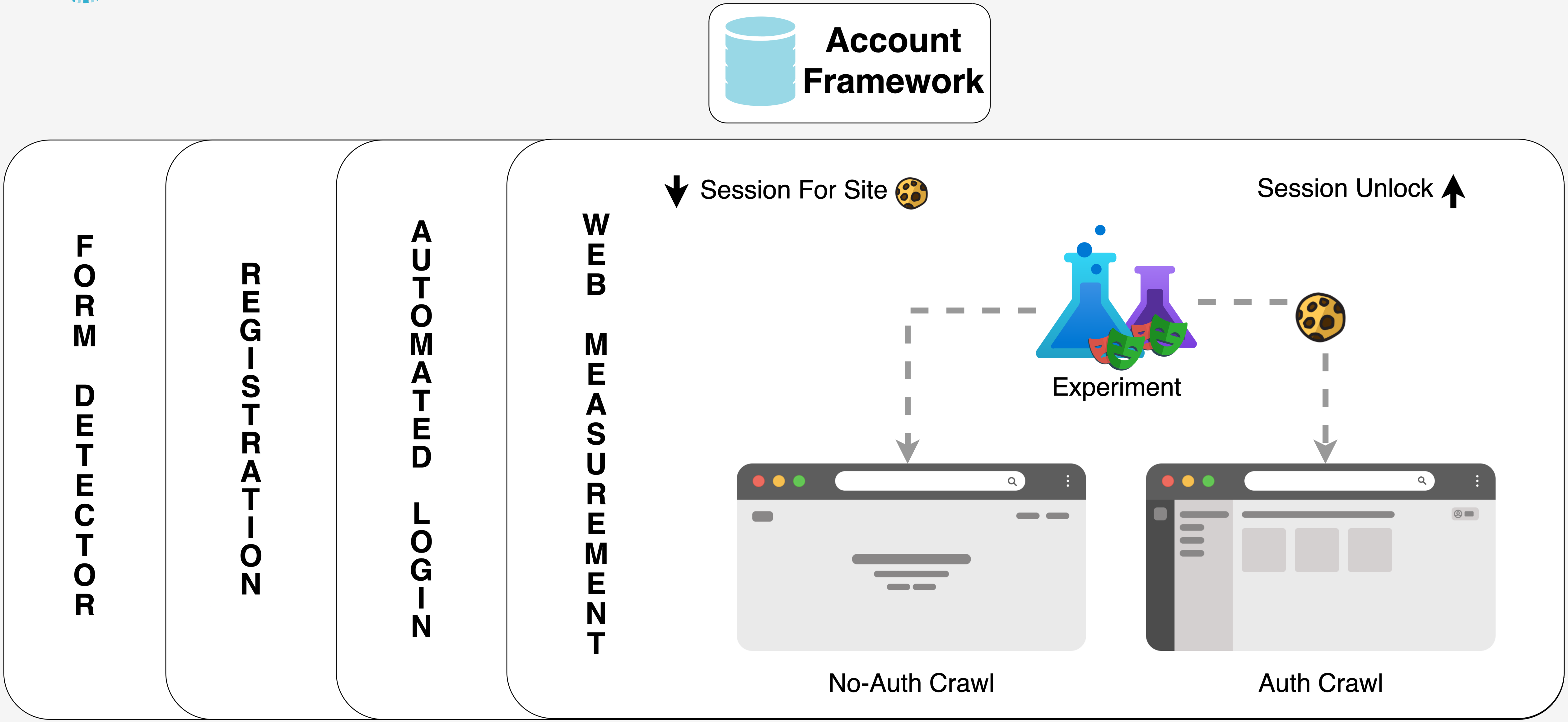
Registration Success

Research Team

Crawling Pipeline



Crawling Pipeline



Account Framework

FORM DETECTOR

REGISTRATION

AUTOMATED LOGIN

WEB MEASUREMENT

Session For Site

Session Unlock

Experiment

No-Auth Crawl

Auth Crawl

Experimental Settings and General Results

Experimental Settings and General Results

- Manually assisted registration on 200+ popular sites

Experimental Settings and General Results

- Manually assisted registration on 200+ popular sites
- Crawl up to 1000 same-site subpages and up to 24h

Experimental Settings and General Results

- Manually assisted registration on 200+ popular sites
- Crawl up to 1000 same-site subpages and up to 24h
- Playwright v1.33
  - CXSS: Foxhound (Firefox 109)
  - All Others: Chromium version 113

Experimental Settings and General Results

- Manually assisted registration on 200+ popular sites
- Crawl up to 1000 same-site subpages and up to 24h
- Playwright v1.33
  - CXSS: Foxhound (Firefox 109)
  - All Others: Chromium version 113

- Number of collected URLs differ:
  - Non-authenticated: average of 840 URLs
  - Authenticated: average of 820 URLs

Experimental Settings and General Results

- Manually assisted registration on 200+ popular sites
- Crawl up to 1000 same-site subpages and up to 24h
- Playwright v1.33
  - CXSS: Foxhound (Firefox 109)
  - All Others: Chromium version 113

- Number of collected URLs differ:
  - Non-authenticated: average of 840 URLs
  - Authenticated: average of 820 URLs
- Reasons: Authenticated users redirected to user portals with few links and many buttons

Most Flows are Harmless

Most Flows are Harmless

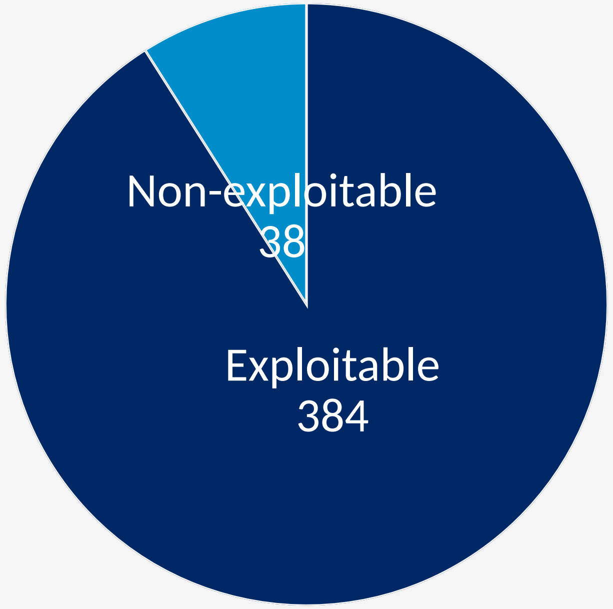
- CXSS exploits are rare:
  - 38,105,442 sink invocations → 2,905 exploits
  - Vulnerable sites: 4 (no-auth), 6 (auth), 7 (total)

Most Flows are Harmless

- CXSS exploits are rare:
  - 38,105,442 sink invocations → 2,905 exploits
  - Vulnerable sites: 4 (no-auth), 6 (auth), 7 (total)
- Are differences due to not exploitable or to not found?

Most Flows are Harmless

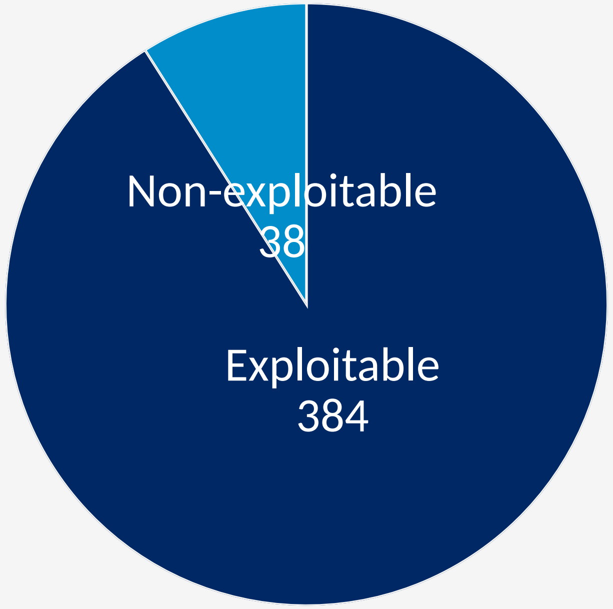
- CXSS exploits are rare:
  - 38,105,442 sink invocations → 2,905 exploits
  - Vulnerable sites: 4 (no-auth), 6 (auth), 7 (total)
- Are differences due to not exploitable or to not found?



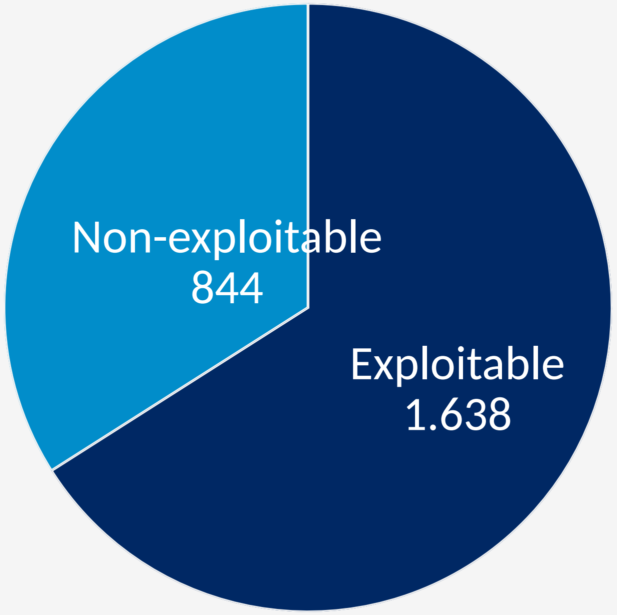
No-Auth Exploits in Auth

Most Flows are Harmless

- CXSS exploits are rare:
  - 38,105,442 sink invocations → 2,905 exploits
  - Vulnerable sites: 4 (no-auth), 6 (auth), 7 (total)
- Are differences due to not exploitable or to not found?



No-Auth Exploits in Auth



Auth Exploits in No-Auth

No Significant Changes in Security Headers

Header	No-Auth	Auth	Combined

No Significant Changes in Security Headers

Header	No-Auth	Auth	Combined
X-Frame-Options	165	162	167

No Significant Changes in Security Headers

Header	No-Auth	Auth	Combined
X-Frame-Options	165	162	167
Strict-Transport-Security	149	142	149

No Significant Changes in Security Headers

Header	No-Auth	Auth	Combined
X-Frame-Options	165	162	167
Strict-Transport-Security	149	142	149
CSP (XSS)	55	53	57

Major Differences in JavaScript Inclusions

Metric	No-Auth	Auth	Combined

Major Differences in JavaScript Inclusions

Metric	No-Auth	Auth	Combined
Unique Scripts	934,545	980,569	1,719,724

Major Differences in JavaScript Inclusions

Metric	No-Auth	Auth	Combined
Unique Scripts	934,545	980,569	1,719,724
Unique Third-Party Scripts	216,952	322,525	507,948

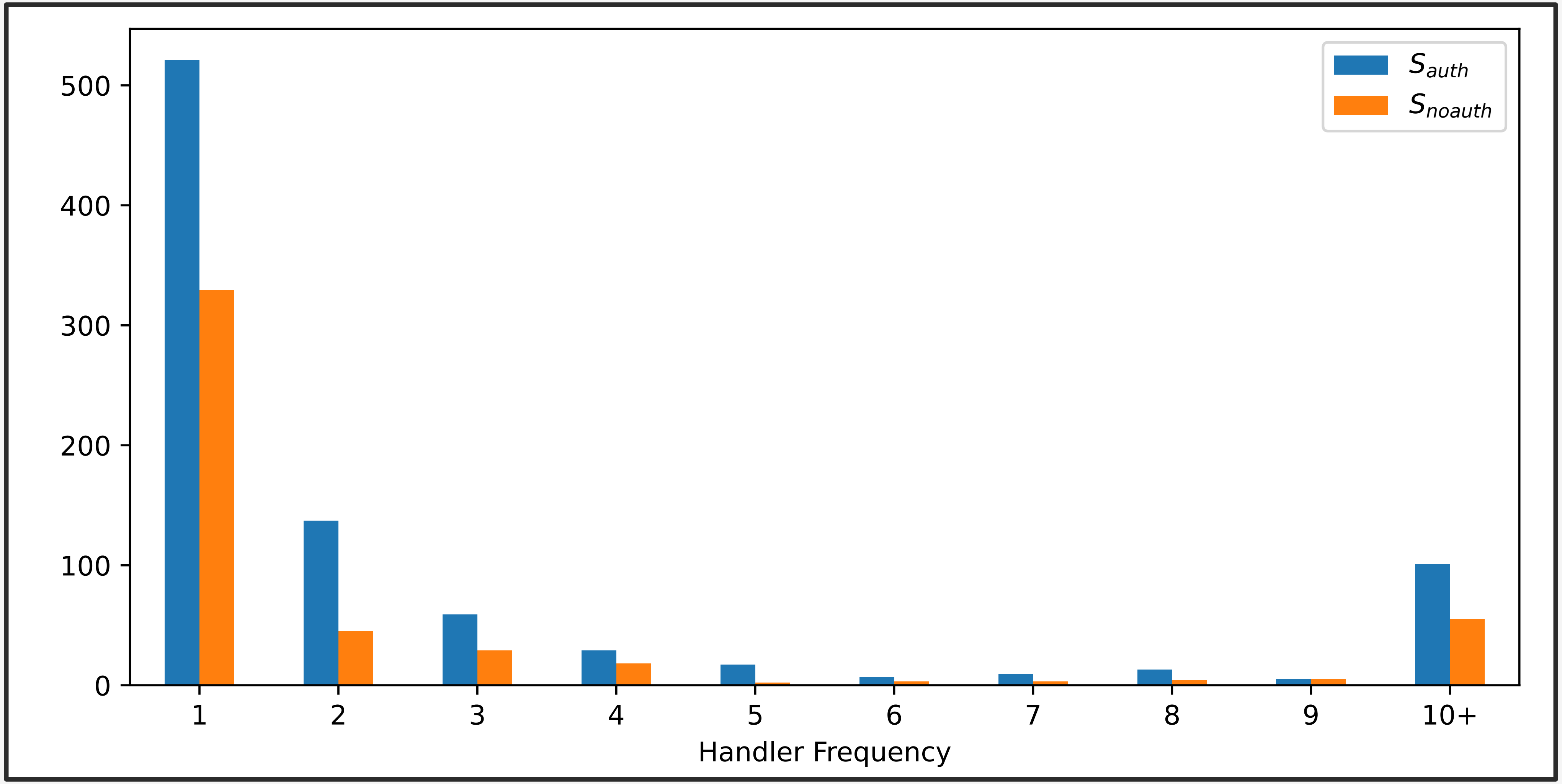
Major Differences in JavaScript Inclusions

Metric	No-Auth	Auth	Combined
Unique Scripts	934,545	980,569	1,719,724
Unique Third-Party Scripts	216,952	322,525	507,948
Unique Third Parties	1,053	1,146	1,231

Major Differences in JavaScript Inclusions

Metric	No-Auth	Auth	Combined
Unique Scripts	934,545	980,569	1,719,724
Unique Third-Party Scripts	216,952	322,525	507,948
Unique Third Parties	1,053	1,146	1,231
Unique Trackers	181	209	219

Authenticated Crawlers Detect More Handlers



Main Insights

Main Insights

- Impact of login depends on the research questions!
  - No substantial differences for security headers
  - Much more Javascript and PostMessages for authenticated state

Main Insights

- Impact of login depends on the research questions!
  - No substantial differences for security headers
  - Much more Javascript and PostMessages for authenticated state
- Authenticated state is not strictly better or worse
  - Some code only reachable by authenticated or non-authenticated state
  - In general the attack surface is larger for authenticated users

Limitations and Ethics

Limitations and Ethics

- Limitations:
  - Small-scale (only 200 sites)
  - Manual labor involved
  - Many websites could not be tested:
    - Require payment, phone number, or similar
    - Bot detection triggered

Limitations and Ethics

- Limitations:
  - Small-scale (only 200 sites)
  - Manual labor involved
  - Many websites could not be tested:
    - Require payment, phone number, or similar
    - Bot detection triggered
- Ethical consideration:
  - Only test own accounts
  - Only client-side security issues
  - Reasonable load
  - Responsible disclosure

Login Matters For Security Measurements

Login Matters For Security Measurements

- Web measurements depend on many factors

Login Matters For Security Measurements

- Web measurements depend on many factors
- We investigated implications of login:
    - 3/4 experiments had major differences

Login Matters For Security Measurements

- Web measurements depend on many factors
- We investigated implications of login:
  - 3/4 experiments had major differences
- Suggestion for future research:
  - Perform small-scale comparative crawl and large-scale non-authenticated crawl

Login Matters For Security Measurements

- Web measurements depend on many factors
- We investigated implications of login:
  - 3/4 experiments had major differences
- Suggestion for future research:
  - Perform small-scale comparative crawl and large-scale non-authenticated crawl
  - Tools open-sourced to help!

Login Matters For Security Measurements

- Web measurements depend on many factors
- We investigated implications of login:
  - 3/4 experiments had major differences
- Suggestion for future research:
  - Perform small-scale comparative crawl and large-scale non-authenticated crawl
  - Tools open-sourced to help!

Thanks for your attention!

https://github.com/cispa/login-security-landscape

jannis.rautenstrauch@cispa.de