



Best Student Paper awarded @ S&P'21!

# They Would do Better if They Worked Together

## The Case of Interaction Problems Between Password Managers and Websites



Nicolas Huaman, Sabrina Amft, Marten Oltrogge, Yasemin Acar, and Sascha Fahl

CISPA Helmholtz Center for Information Security, Leibniz University Hannover

{nicolas.huaman-groschopf, sabrina.amft, marten.oltrogge}@cispa.de | acar@sec.uni-hannover.de | fahl@cispa.de



### Have you tried using a Password Manager on the Web before?

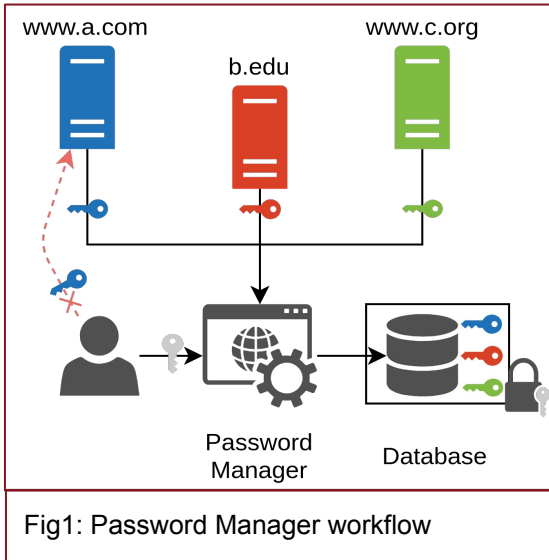


Fig1: Password Manager workflow

### Password Managers (PWMs)....

- Store passwords in database
- Generate secure passwords
- Automatically provide passwords

### But they...

- Do not work with all websites
- May cause problematic interactions when failing  
(Example: PWM phishing)

### We investigated PWM Interactions:

1. Analyzed 2,947 user reviews & issues
2. Created 39 minimal working examples
3. Tested 15 popular PWMs

#### Usecase D-05: Redirects after login

Delete existing credentials. Basic Login (user: password, pw: manager) then test whether autosave still works. "Not Applicable" for any pwm without autosave.

**Username**

**Password**



Fig2: One of our minimal working examples

### PWMs failed with many Interactions:

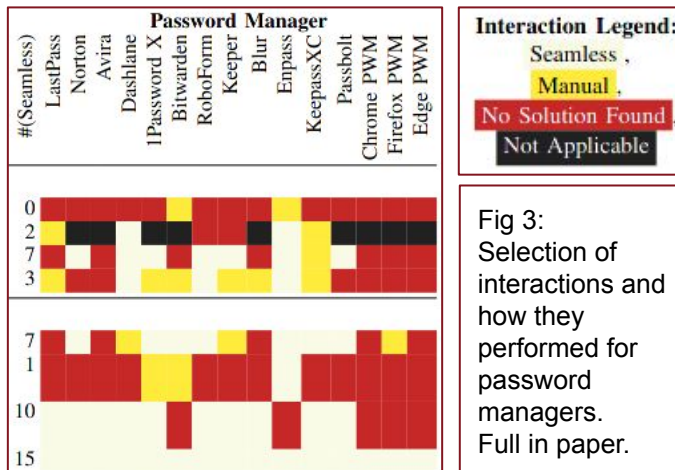


Fig 3: Selection of interactions and how they performed for password managers. Full in paper.

### Problematic Interaction Examples:

- Providing accounts across domains: <https://www.example.com> vs <https://auth.example.com>
- Support for input field arguments: `<input name="unm" autocomplete="username" maxlength="20" />`
- Problematic Javascript interactions: Client-side "encryption", dynamic fields
- Additional elements to address: Pin inputs, firstname & lastname
- Web standard support: HTTP Basic Authentication, Interaction with non-standard forms

### Replication Package:

<https://publications.teamusec.de/passwordManagers/>

- More details and all interactions
- Coding process
- Source code
- Minimal working examples

