

How to make password managers play ball with your login form

HIDDE DE VRIES

23.09.2018

#HackOnMDN, London



moz://a

moderator.mozilla.org

Log In with email or third-party

ENTER

 Log in with GitHub

 Log in with Google

The IAM Project

identity



The IAM Project



access

identity

— proving/verifying who you are

access

- allowing you to see things when you have been identified

The IAM Project facilitates group curation: if you're in a group, you can see the things that group has access to.

Our users

- Mozilla IAM is used by staff as well as by contributors
- people sometimes have various identities with differences in access rights
- some people want to use specific identities on specific sites

The “Lock” / NLX

moz://a

moderator.mozilla.org

Log in with email or third-party

Email address



ENTER



Log in with GitHub



Log in with Google

[Legal](#)

[Privacy](#)

[Need help?](#)

moz://a

moderator.mozilla.org

Log in with email or third-party



ENTER



Log in with GitHub



Log in with Google

[Legal](#)

[Privacy](#)

[Need help?](#)

Login with

- Mozilla LDAP
- Passwordless
- GitHub
- Google

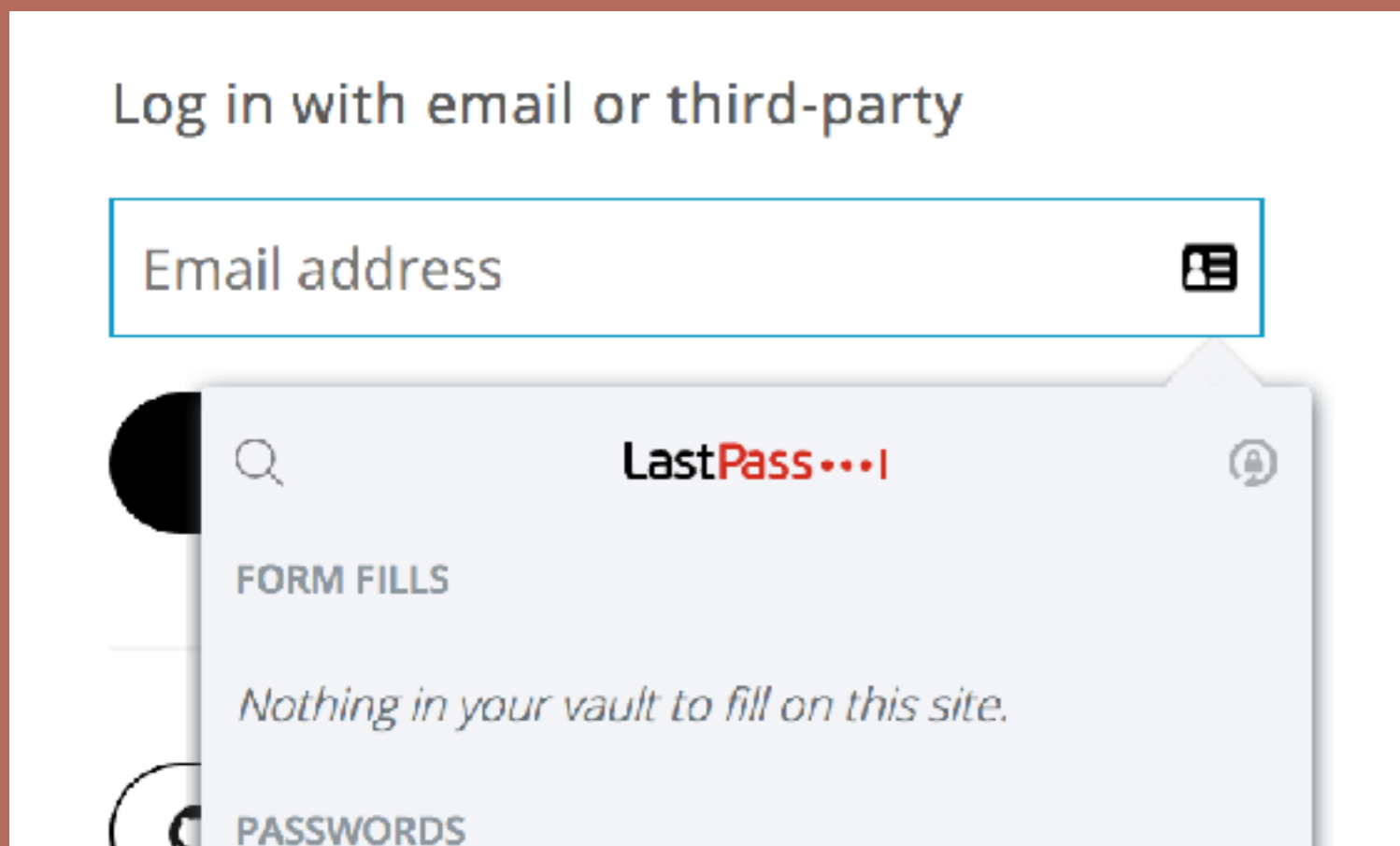
A screenshot of the Mozilla login page. At the top left is the 'moz://a' logo. Below it is the URL 'moderator.mozilla.org'. The text 'Log in with email or third-party' is followed by an input field labeled 'Email address' with a search icon on the right. Below the input field is a black button with the text 'ENTER'. Further down are two buttons: 'Log in with GitHub' with the GitHub logo and 'Log in with Google' with the Google logo. At the bottom of the page are links for 'Legal', 'Privacy', and 'Need help?'.

80+ sites

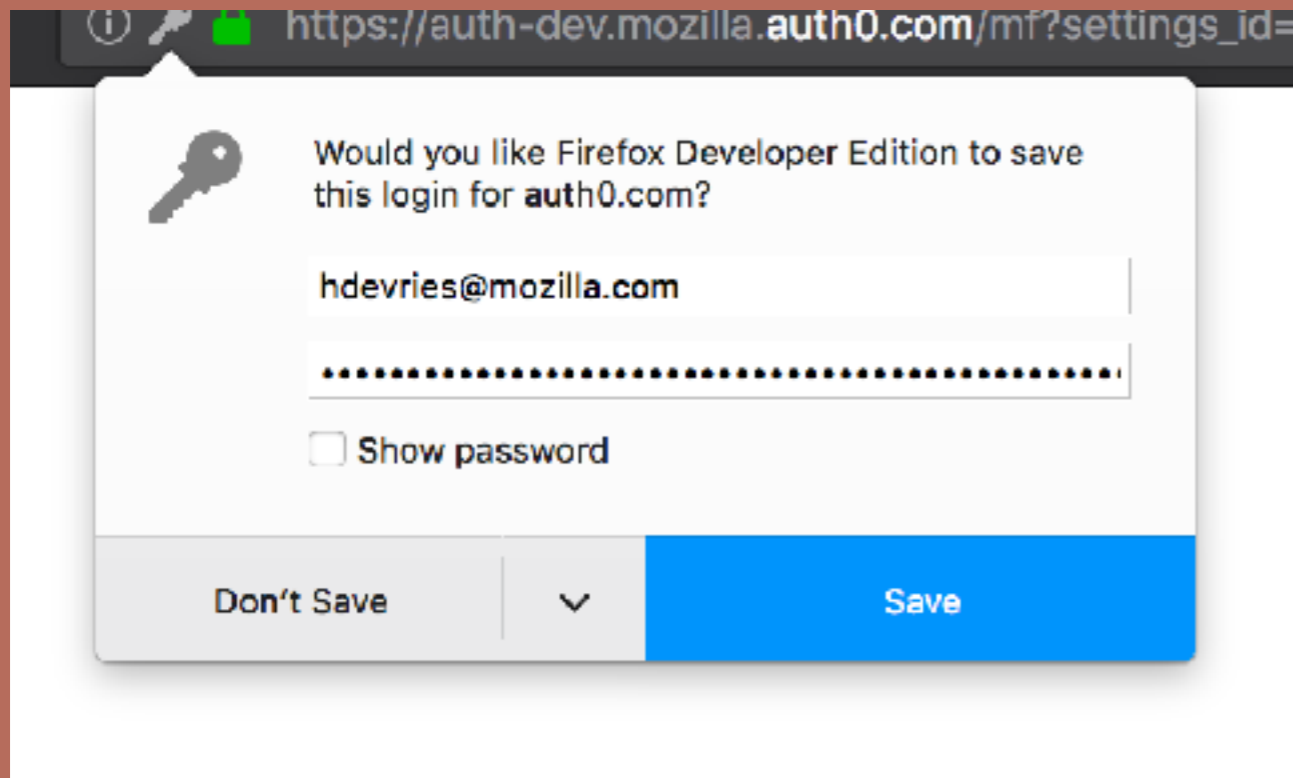
Password managers

The most secure passwords
are long and unique. And
therefore hard to remember

*making it work (1):
recognise the login screen*



*making it work (2): trigger
the 'Would you like to save
this password' prompt*



*making it work (3): have
the password manager fill
in the fields*

Lessons learned

Multi-page is hard

(because hiding is hard)

Use web standards

A form with
action and
method

The right
input
types

Labels
associated
with inputs

1.3.5 Identify input purpose

Autocomplete

`autocomplete="off"` often ignored

`autocomplete="username"`

`autocomplete="password"`

Updating Credentials

er Mediation

lection

Privacy Considerations

n credential access

ackage

s

ision

S

ackage

d Data

ion Considerations

ors

ints

nsions

e

nventions

Algorithms

d by this specification

d by reference

ferences

ferences

Credential Management Level 1

Editor's Draft, 19 June 2018



This version:

<https://w3c.github.io/webappsec-credential-management/>

Latest published version:

<http://www.w3.org/TR/credential-management-1/>

Previous Versions:

<http://www.w3.org/TR/2016/WD-credential-management-1-20160425/>

Version History:

<https://github.com/w3c/webappsec-credential-management/commits/master/index.src.html>

Feedback:

public-webappsec@w3.org with subject line "[credential-management] ... message topic ..." ([archives](#))

Editor:

[Mike West](#) (Google Inc.)

The autocomplete attribute offers a declarative mechanism by which websites can work with user agents to improve the latter's ability to detect and fill sign-in forms by marking specific fields as "username" or "password"

als from a user

This is a public copy of the editors' draft. It is provided for discussion only and may change at any moment. Its publication here does not imply endorsement of its contents by W3C. Don't cite this document other than as w
in progress

Multipage is hard

Web standards

autocomplete attr