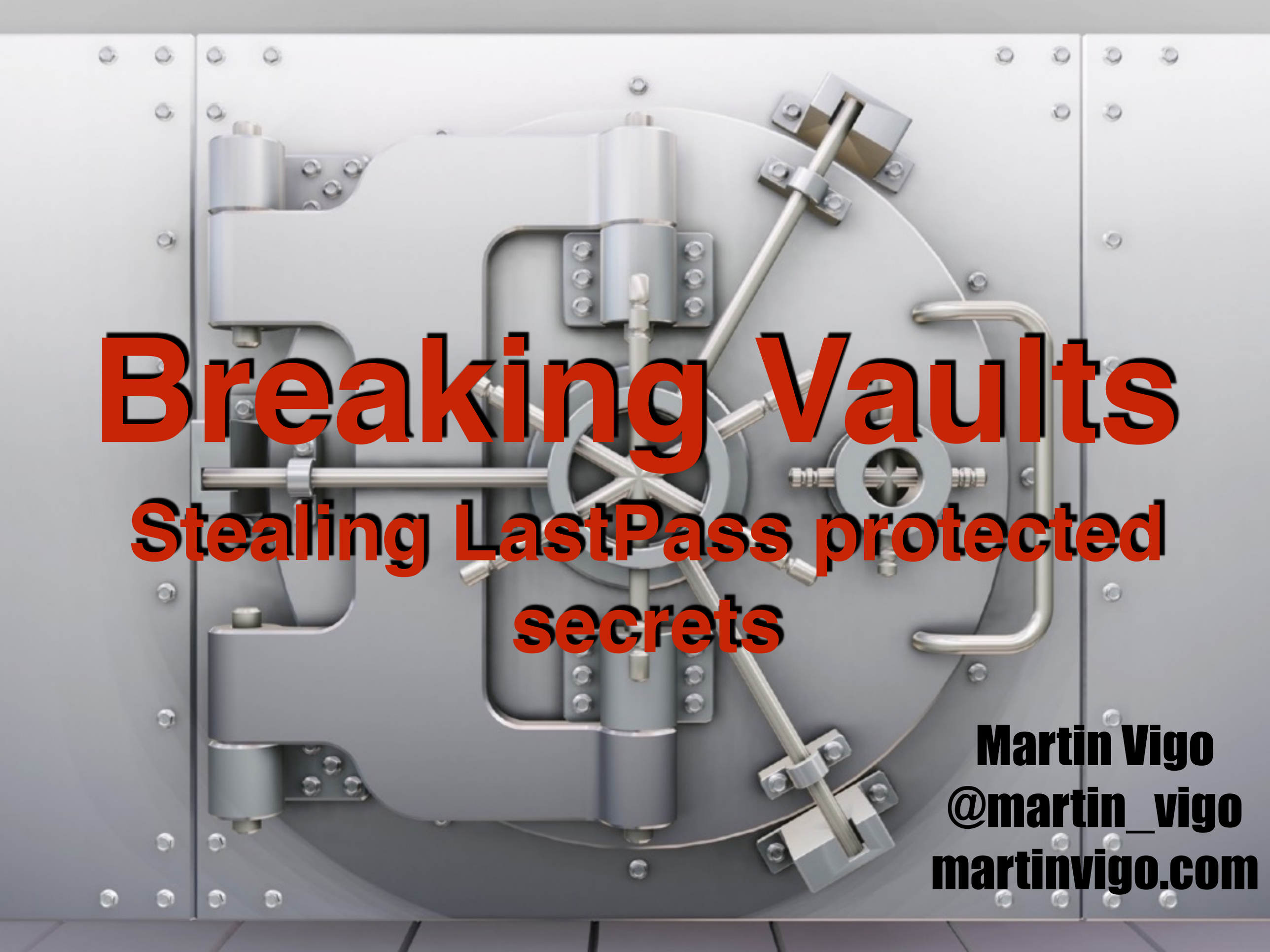


Breaking Vaults

Stealing LastPass protected secrets

Martin Vigo
@martin_vigo
martinvigo.com

Who am I

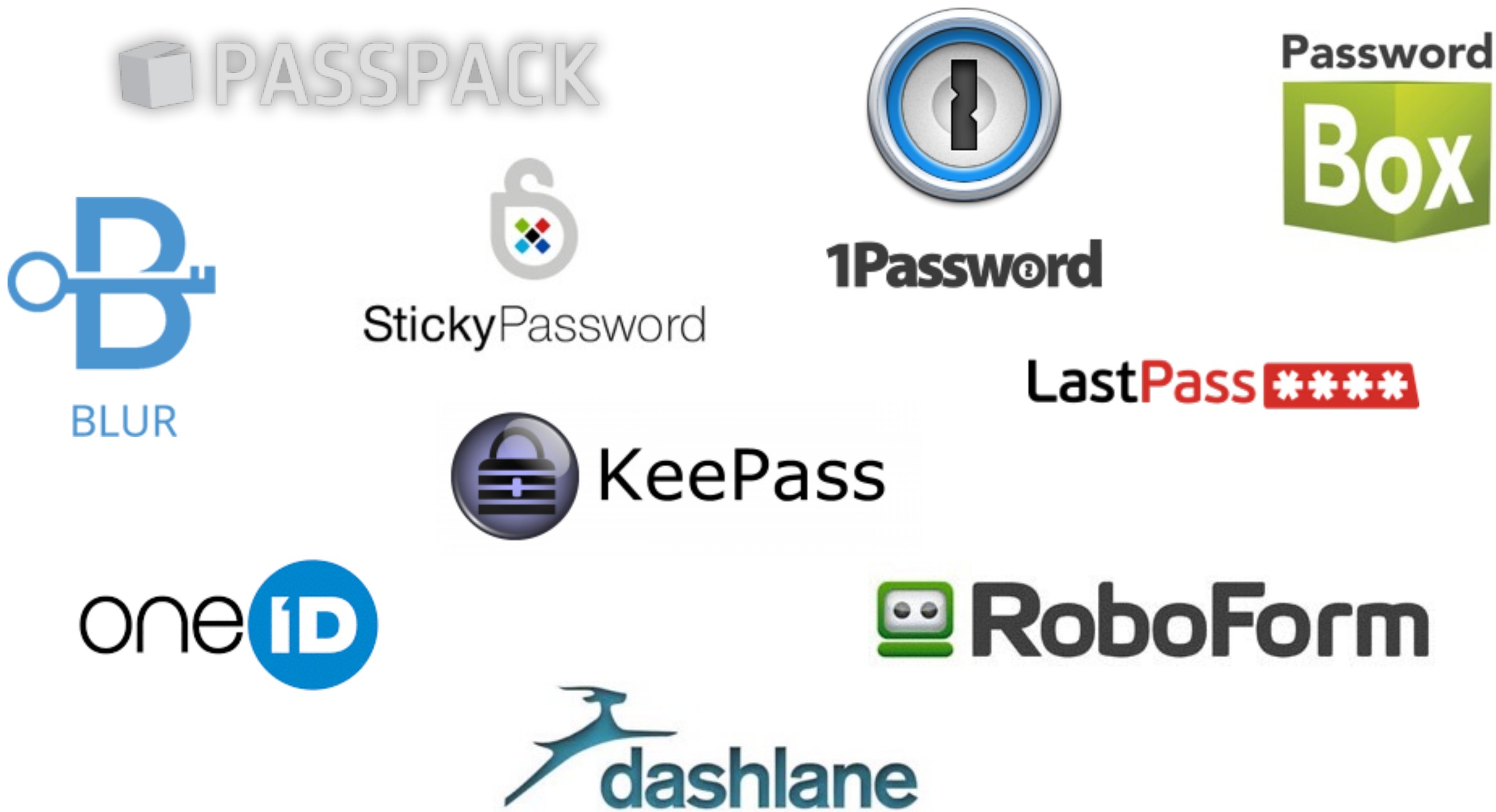
- Product Security Engineer
- Spaniard / Galician
  - Most beautiful beach in the world
  - Amazing seafood
  - Charlie Sheen's grandfather was Galician

- Diver
- Gin tonic consumer
- @martin_vigo / martinvigo.com

“LastPass is a password management service which seeks to resolve the password fatigue problem by centralizing user password management in the cloud”

Wikipedia

Password Managers

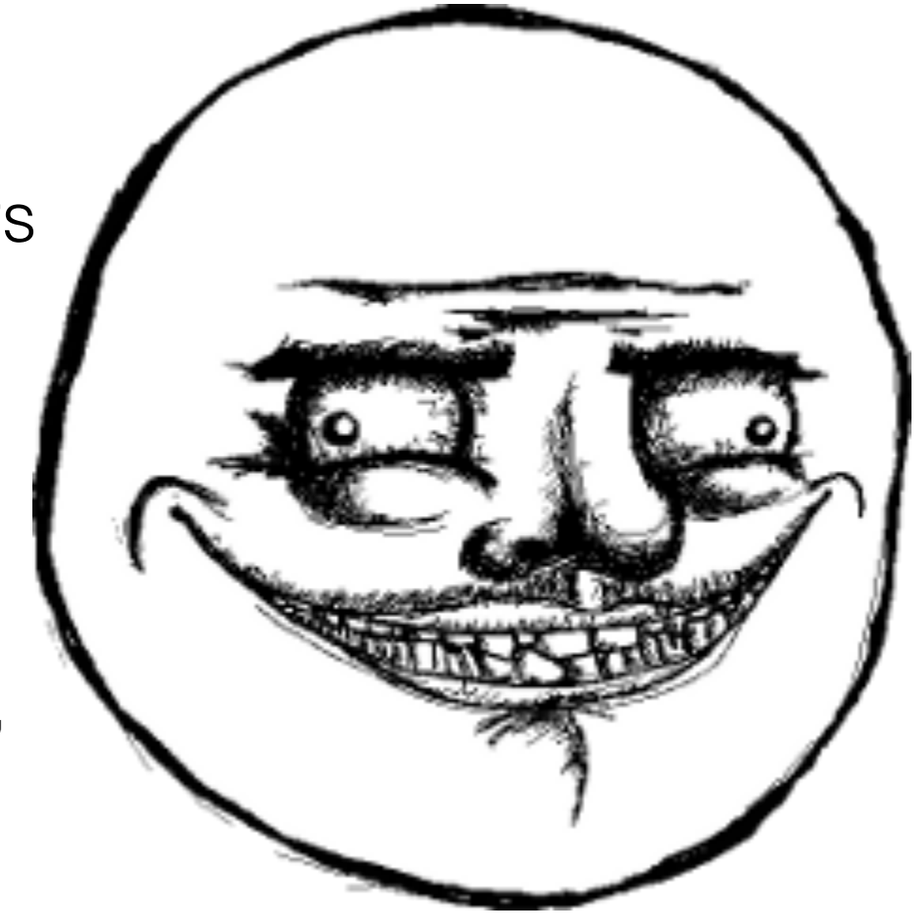


Why targeting Password Managers?

- All you want to hack is in one place
  - Social Networks
  - Banks
  - Email accounts
  - Corporate credentials

Why LastPass?

- Enterprise edition
- Large companies use it
  - “More than 10,000 corporate customers ranging in size all the way up to the Fortune 500”
- Not only credentials
  - Credit Cards, Personal documentation, Private notes, etc.
- Arguably the most popular password manager



State of the art

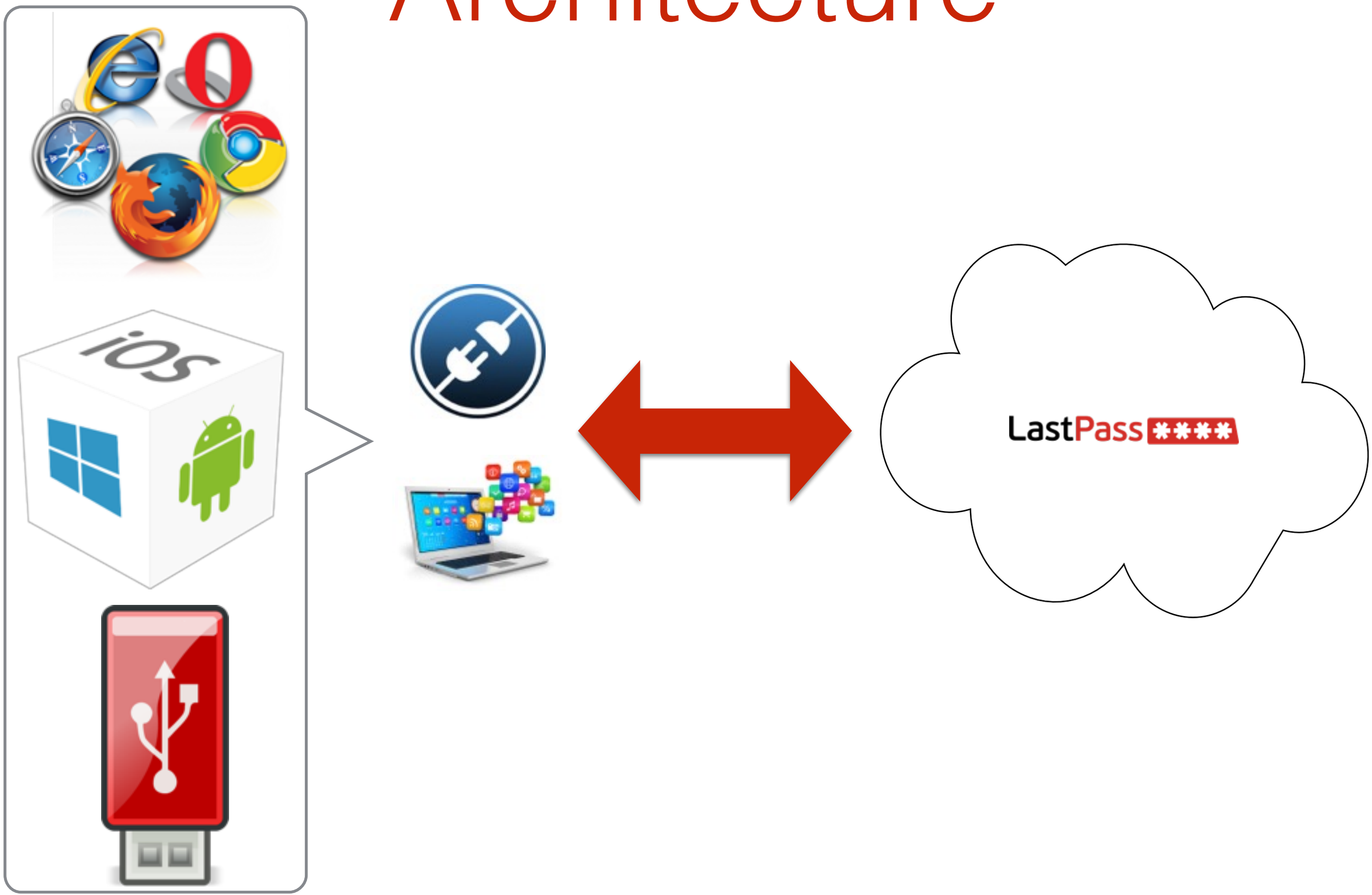
- Vulnerabilities
- DNS poisoning
- XSS form injection

All focus on leaking **specific** secrets

Target: Master Password

All your secrets are belong to us

Architecture



Focus

Browser Plugin

- Javascript
- Sandboxed (SOP)
- Injects code into DOM
- Access to filesystem

Security claims

- LastPass has no access to your data
- Local encryption
- Secure storage

Reversing

Meaning making sense of 3MB of obfuscated JS

siesta.py

- Beautifies every JS file
- Injects a payload to every function
  - *console.log([file] [function] [params])*
- Credits to **Alberto Garcia** (@algillera)

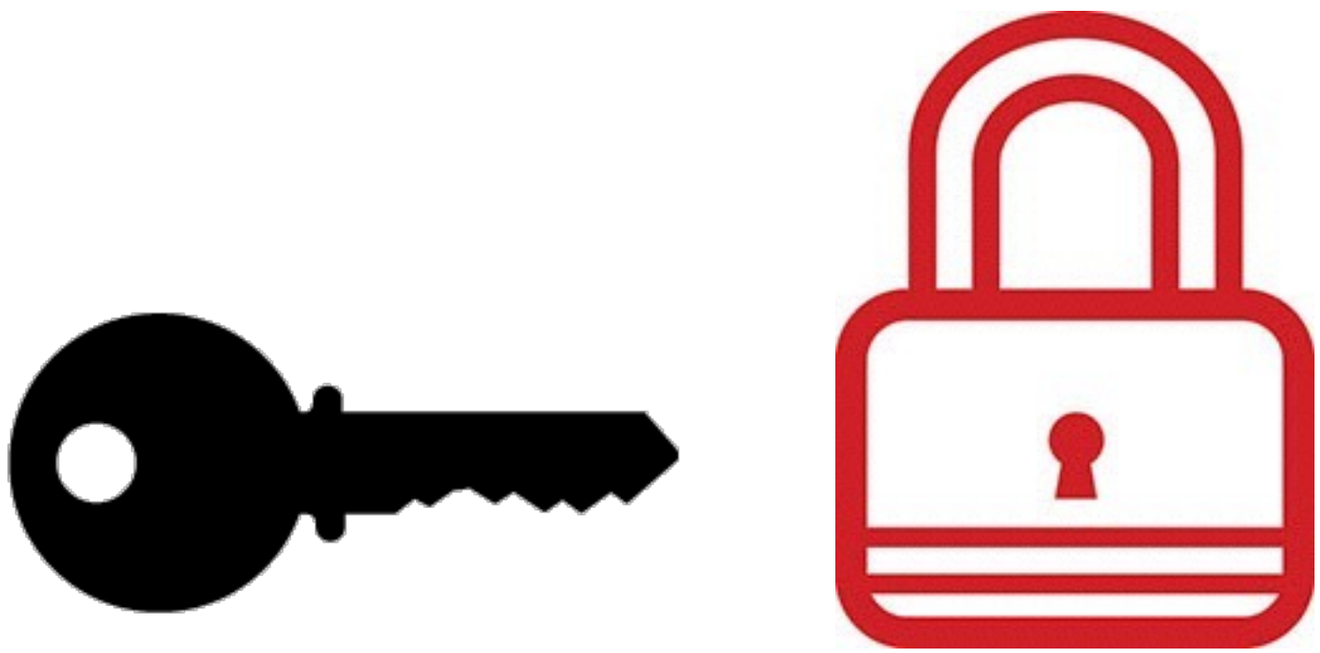
Logic and storage

- Identified all accessed files
  - Minimized JS
  - Storage on Sqlite DBs
- Browser specific implementation
  - Business logic
  - File location
  - Storage
- AES own implementation
  - RSA is based on j*sbn* library

Local encryption

- 256-bit AES
  - CBC and **ECB**
  - Their own implementation
- PBKDF2
  - **500 / 5000** rounds (default)
  - Unauthenticated query

Encryption key



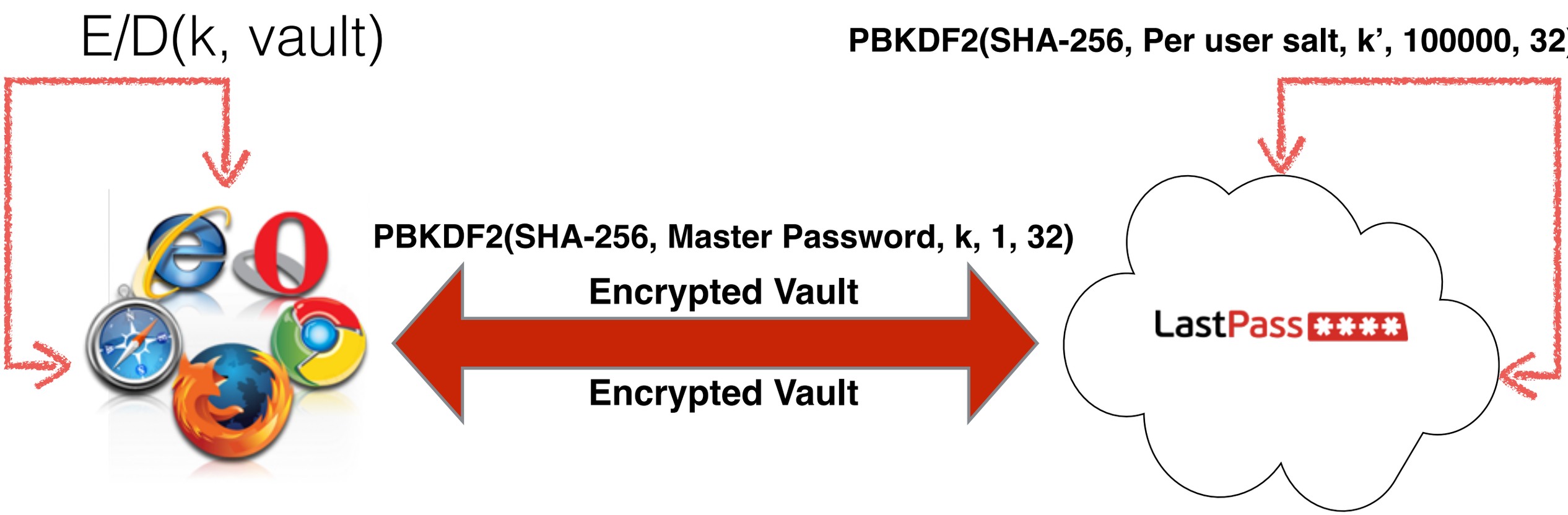
PBKDF2(SHA-256, Username, Master Password, Iterations, 32)

Salt

Password

key length

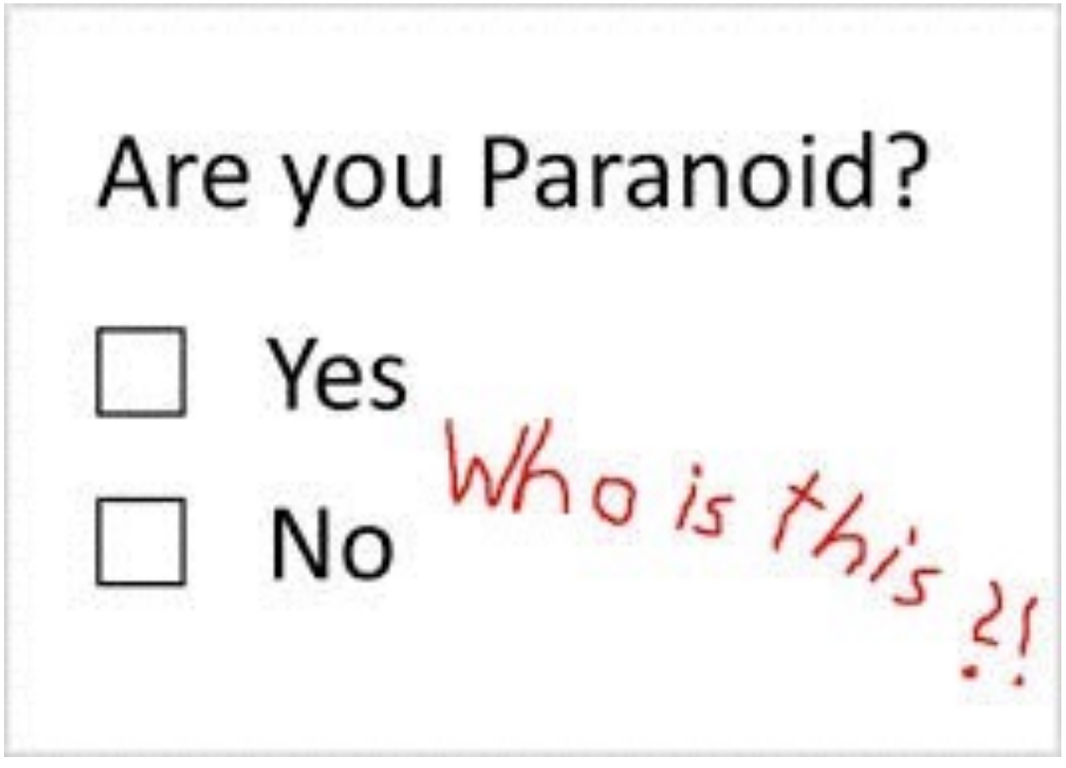
LastPass has no access to your data

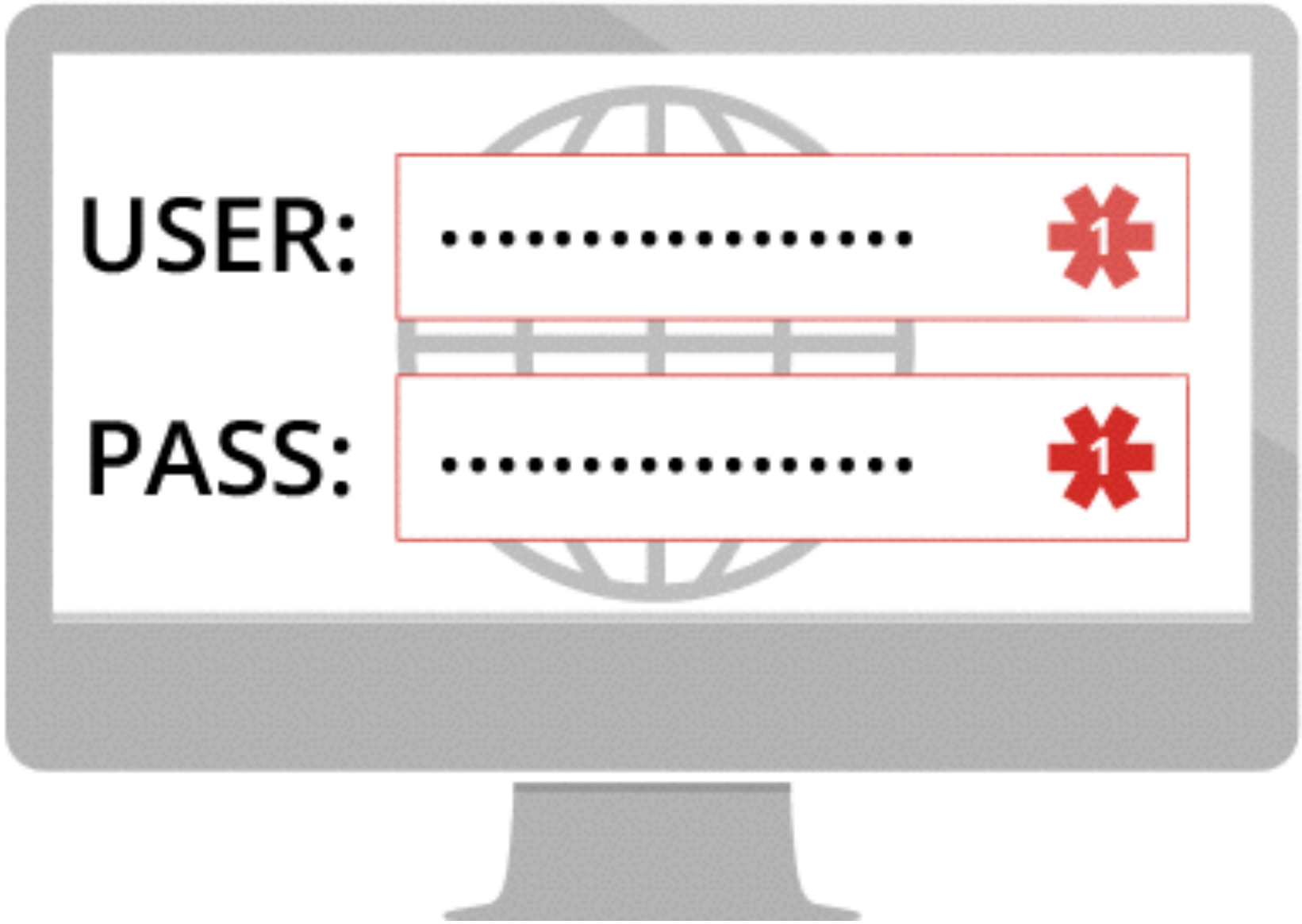


What does LastPass see?

The encrypted vault

A **1-round** PBKDF2-SHA256 of the encryption key

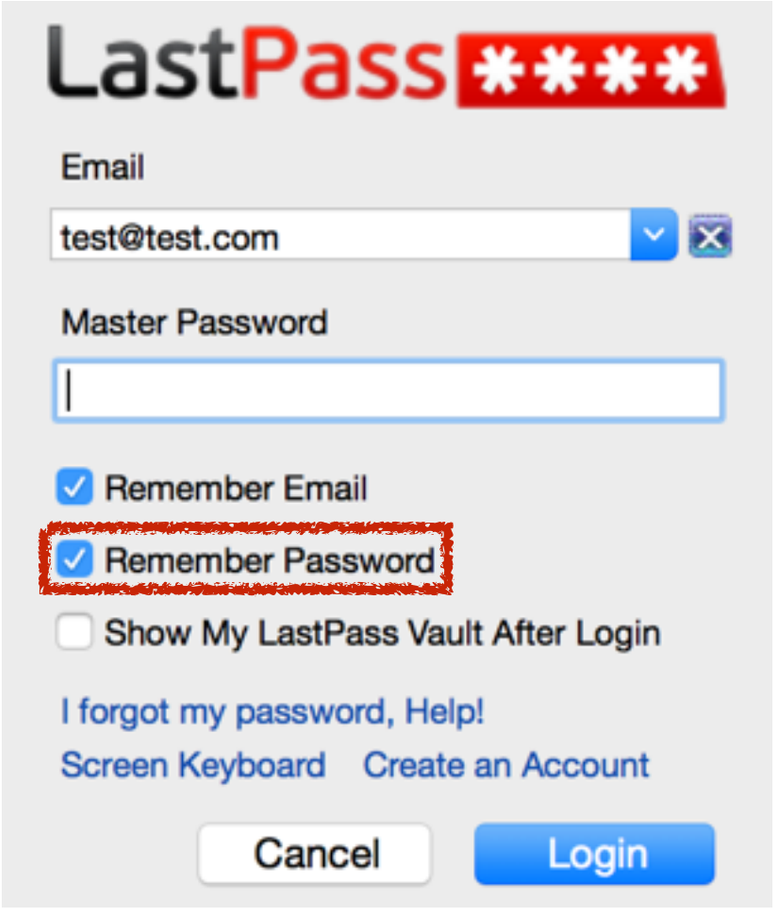




Stealing the Master Password

Remember password

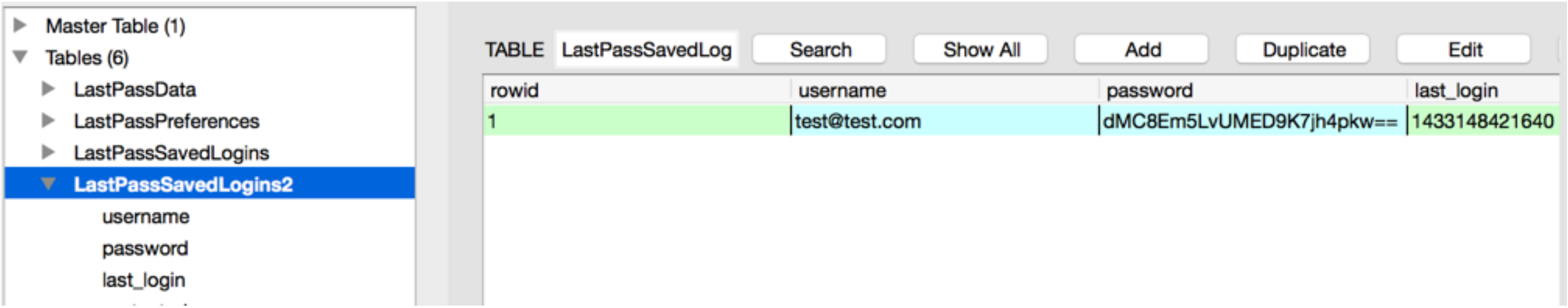
- Stores the password locally
- Sqlite DB or prefs.js
- ECB or CBC
  - **u7W1PsEYsWrtAS1Ca7lOOH==**
  - **!waXcJg8b7wl8XYZnV2l45A==l4d0Hiq+spx50pso2tEMtkQ==**



Storage

	Chrome	Firefox	Safari	Opera
Windows	#{user_profile['LocalAppData']}/Google/Chrome/User Data/Default/databases/chrome-extension_hdokiejnpimakedhajhdlcegeplioahd_0	#{user_profile['AppData']}/Mozilla/Firefox/Profiles	#{user_profile['LocalAppData']}/Apple Computer/Safari/Databases/safari-extension_com.lastpass.lpsafariextension-n24rep3bmn_0	#{user_profile['AppData']}/Opera Software/Opera Stable/databases/chrome-extension_hnjalnkldgigidggphhmacmimbdlafdo_0
Mac	#{user_profile['LocalAppData']}/Google/Chrome/Default/databases/chrome-extension_hdokiejnpimakedhajhdlcegeplioahd_0	#{user_profile['LocalAppData']}/Firefox/Profiles	#{user_profile['AppData']}/Safari/Databases/safari-extension_com.lastpass.lpsafariextension-n24rep3bmn_0	#{user_profile['LocalAppData']}/com.operasoftware.Opera/databases/chrome-extension_hnjalnkldgigidggphhmacmimbdlafdo_0
Unix	#{user_profile['LocalAppData']}/.config/google-chrome/Default/databases/chrome-extension_hdokiejnpimakedhajhdlcegeplioahd_0	#{user_profile['LocalAppData']}/.mozilla/firefox		#{user_profile['LocalAppData']}/.opera/widgets/wuid-*/pstorage

SQLite DB



- **LastPassSavedLogins2** contains the encrypted credentials
- No root needed

prefs.js (Firefox)

```
10  user_pref("extensions.lastpass.426561e3e8b3[redacted]?cddfcb5.StoreLostPWOTP", true);
11  user_pref("extensions.lastpass.426561e3e8[redacted]cddfcb5.changedpopupfill", true);
12  user_pref("extensions.lastpass.426561e3e8[redacted]dfcb5.lastpollcheck", 1423163694);
13  user_pref("extensions.lastpass.426561e3e[redacted]fcb5.noexport", 0);
14  user_pref("extensions.lastpass.426561[redacted]b5.notificationsAfterClick", false);
15  user_pref("extensions.lastpass.426561[redacted].offerGeneratePasswd", false);
16  user_pref("extensions.lastpass.426561[redacted]opengroups", "(none)&Business");
17  user_pref("extensions.lastpass.426561[redacted]showFillNotifications", false);
18  user_pref("extensions.lastpass.426561[redacted]showFormFillNotifications", fals
19  user_pref("extensions.lastpass.c4edb4f[redacted]7.RepromptTime", 0);
20  user_pref("extensions.lastpass.c4edb4f0[redacted]5f7.StoreLostPWOTP", true);
21  user_pref("extensions.lastpass.c4edb4f0[redacted]b5f7.changedpopupfill", true);
22  user_pref("extensions.lastpass.c4edb4f0[redacted]ab5f7.lastpollcheck", 1432753679);
23  user_pref("extensions.lastpass.c4edb4f0[redacted]2ab5f7.noexport", 0);
24  user_pref("extensions.lastpass.c4edb4f0[redacted]cf2ab5f7.notificationsAfterClick", false);
25  user_pref("extensions.lastpass.c4edb4f0[redacted]d50cf2ab5f7.offerGeneratePasswd", false);
26  user_pref("extensions.lastpass.c4edb4f0[redacted]12dd50cf2ab5f7.showFillNotifications", false);
27  user_pref("extensions.lastpass.c4edb4f0[redacted]199112dd50cf2ab5f7.showFormFillNotifications", fals
28  user_pref("extensions.lastpass.defaultf[redacted]
29  user_pref("extensions.lastpass.defaultff[redacted]
30  user_pref("extensions.lastpass.disableffpwa[redacted]
31  user_pref("extensions.lastpass.ffhasloggedin", true);
32  user_pref("extensions.lastpass.ffhasloggedinsuccessfully", true);
33  user_pref("extensions.lastpass.generateHkKeyCode", 0);
34  user_pref("extensions.lastpass.generateHkMods", "");
35  user_pref("extensions.lastpass.homeHkKeyCode", 0);
36  user_pref("extensions.lastpass.homeHkMods", "");
37  user_pref("extensions.lastpass.loginpws", "bH[redacted]Nz");
38  user_pref("extensions.lastpass.loginusers", "m[redacted].com|basu[redacted].com");
```

- **extensions.lastpass.loginusers** contains the usernames
- **extensions.lastpass.loginpws** contains encrypted passwords
- No root needed

Master password encryption

- AES-256
  - **IV**: Random
  - **KEY**: SHA256(username)
  - **Data**: !L5b/dOyu4EMdmWCYkASQaw==|cHTFJDy1DQi8dPY0AJL/1B=

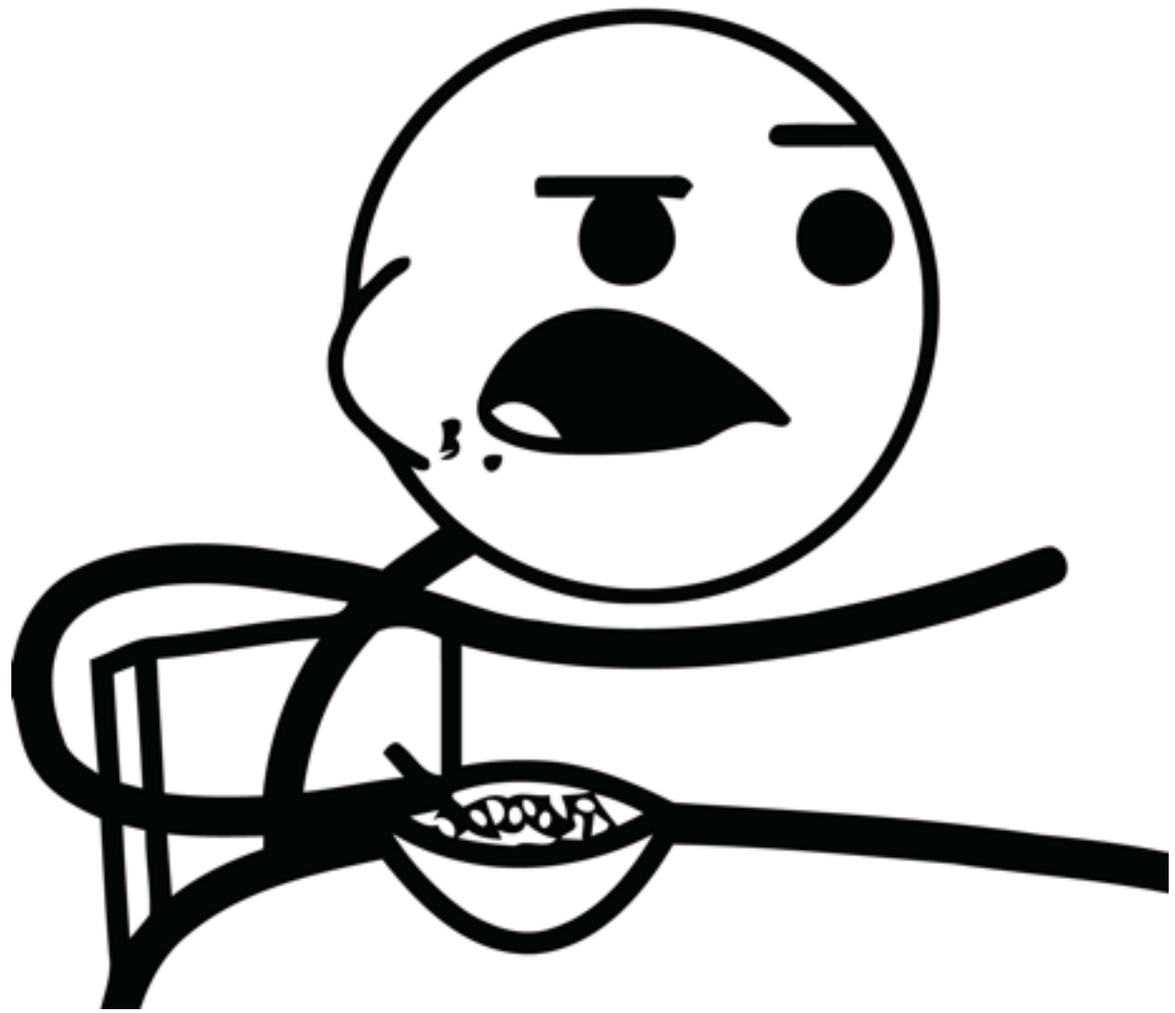
IV
24 chars (ignoring !)

Separator
26th char

Data
Starting 27th char

Profit!

- We located the files
- We know the encryption system
- We have the IV
- We have the key
- We have the data

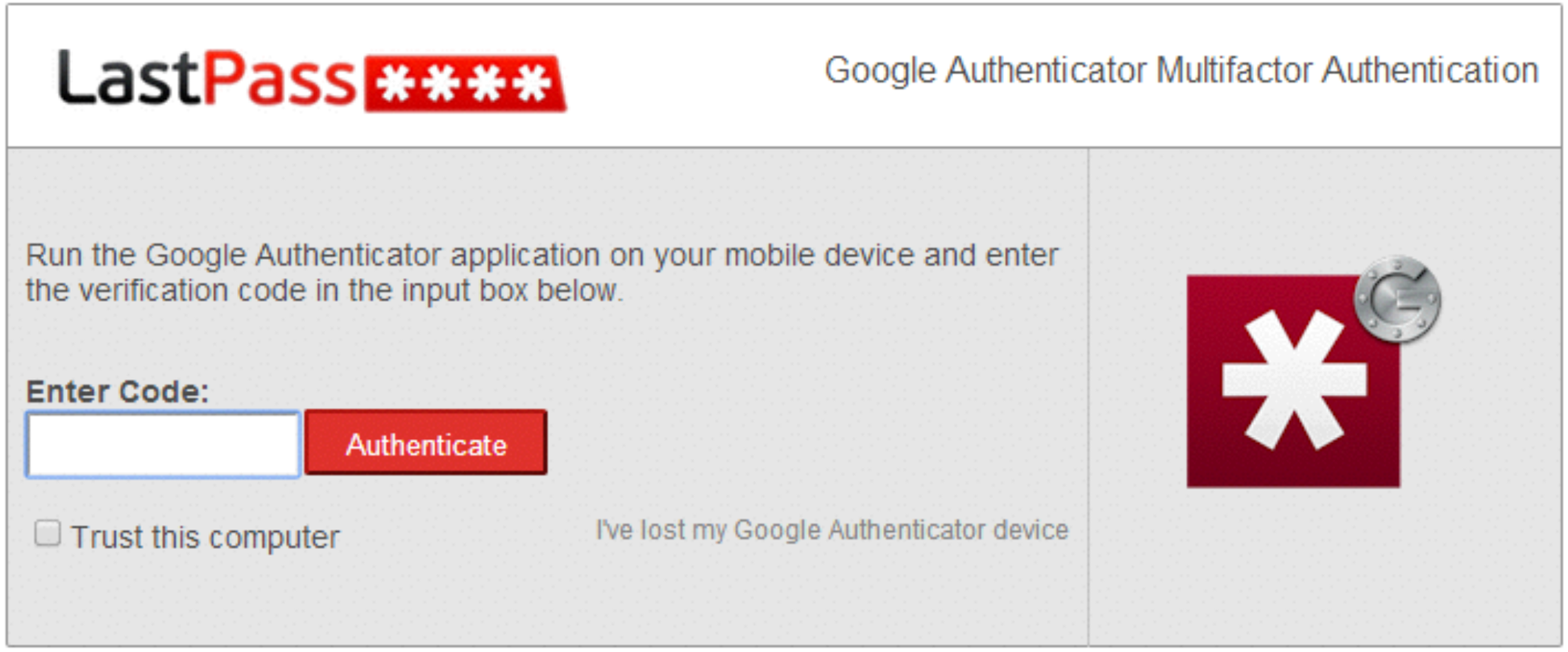


What about 2 factor auth?

Google Authenticator
LastPass + Multifactor

Bypassing 2-factor Auth

2-factor auth



- Supports multiple platforms
  - Google Auth, Yubikey, Toopher, etc.

UUID is the “trust token”

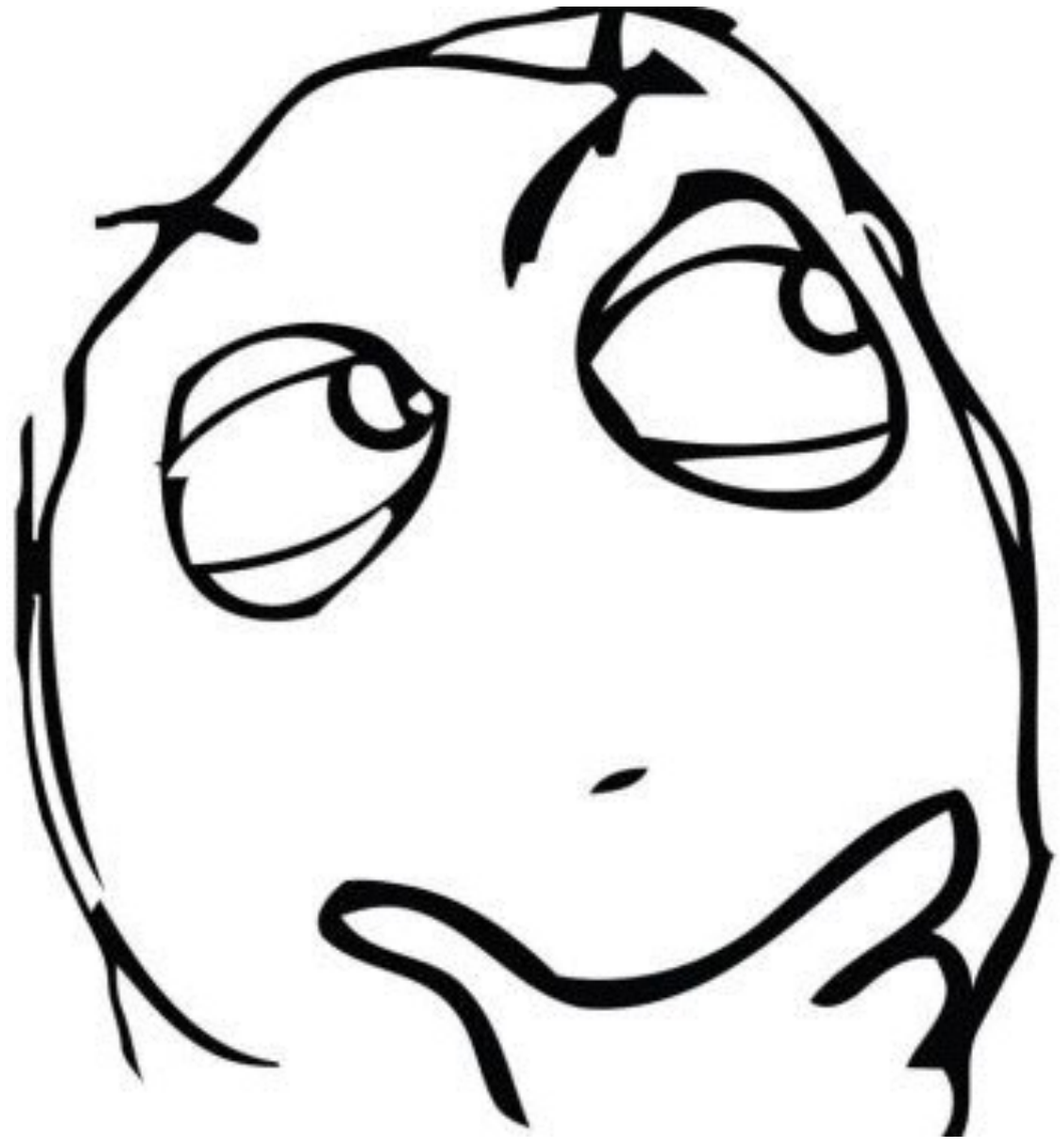
```
POST /login.php HTTP/1.1
Host: lastpass.com
Connection: keep-alive
Content-Length: 669
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/40.0.2214.94 Safari/537.36
Origin: chrome-extension://hdokiejnpimakedhajhdl
Content-Type: application/x-www-form-urlencoded
Accept: */*
DNT: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8,es;q=0.6
Cookie: lang=es_ES; sessonly=0

sentms=1423206028711&xml=2&username=martinvigo%4                                    0af
0dd218f9ced100912c39edccb2&version=3.1.89&encryp                                    3D&
uuid=NdAm!%2                          x!bmv7&lang=e                                 esp
onse=&outofbandsupported=1&lostpwotphash=3740af1                                    en=
MTQyMzIwNTk0MC4xNjQ2LcxiD8Ke6VFmxwA1MikJpK2TPhN1                                    h2G
Z07a6SYyU3z%2Bqw%3D&requestsrc=cr&encuser=CV8%2E
```

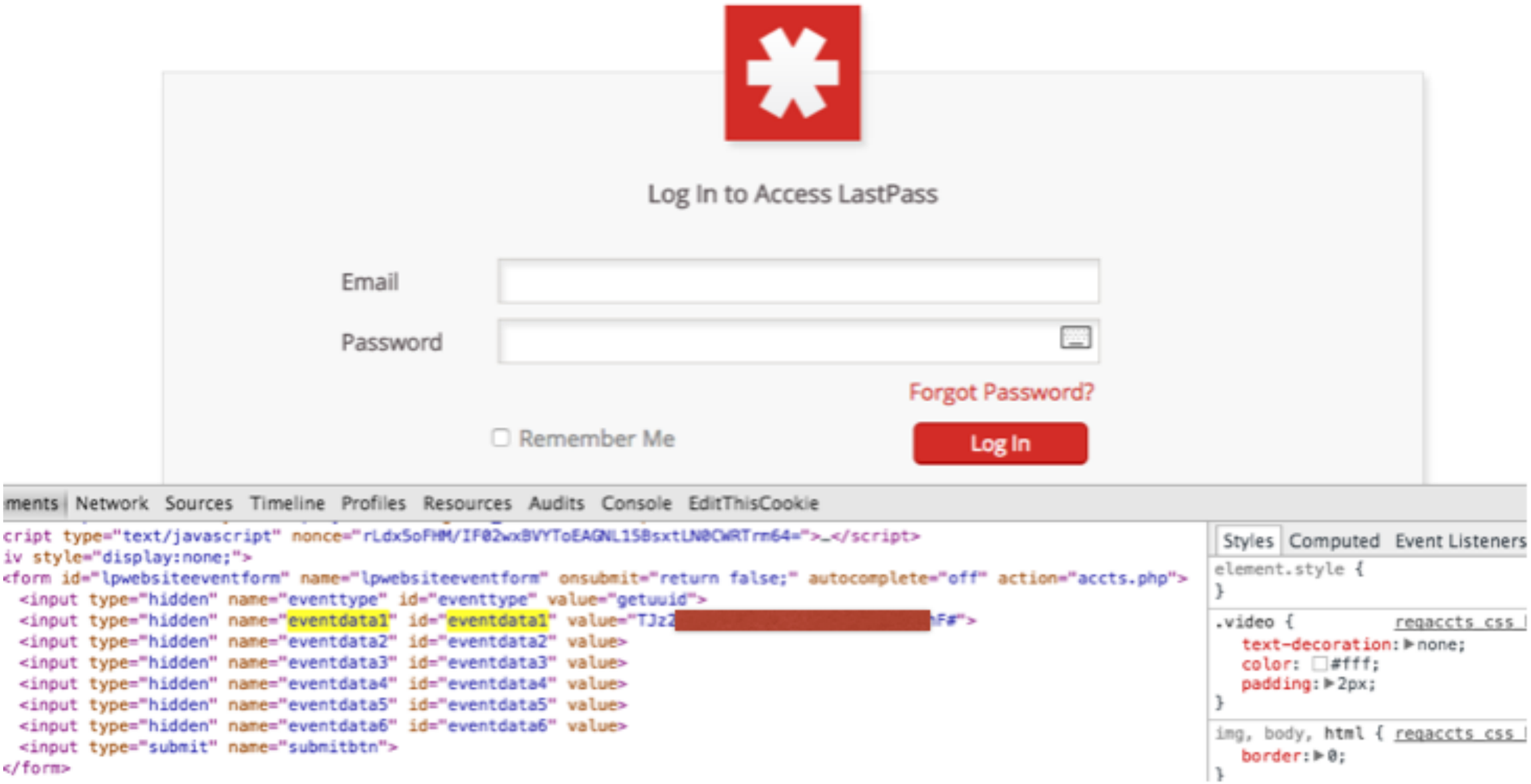

COOL STORY BRO
NOW, GIVE ME COOKIE.

What’s going on?

- How is the request forged?
- How is the token generated?
- How is it stored?
- Where is it stored?



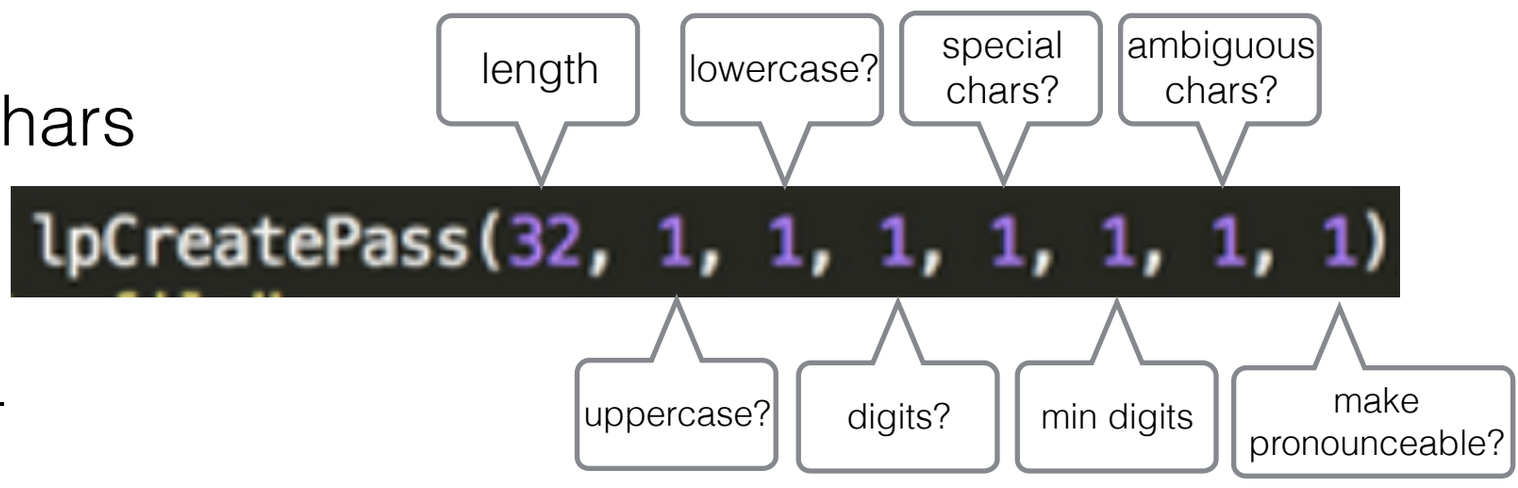
How is the request forged?



The token is injected into the DOM

How is the token generated?

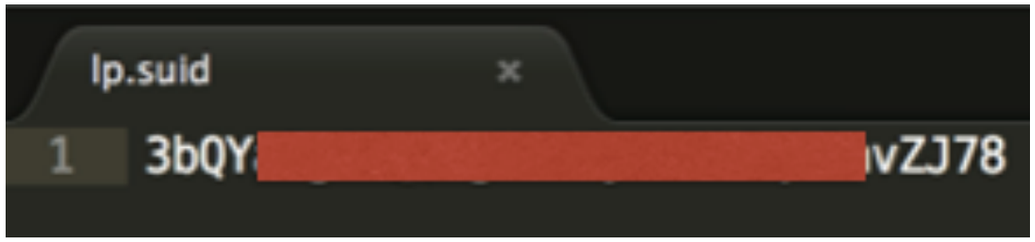
- At plugin installation 32 chars length
- 0-9 A-Z a-z !@#$%^&*()_



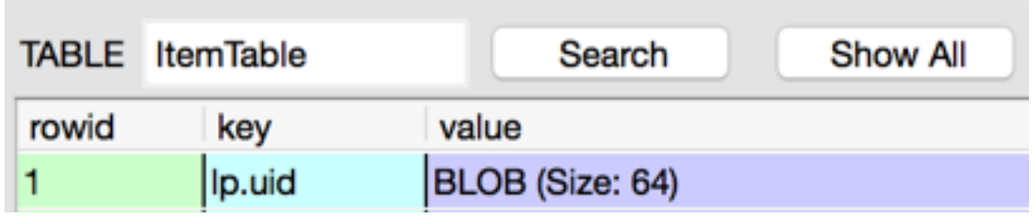
How/Where is it stored?

- In plaintext

- Firefox
  - In the file "*lp.suid*"

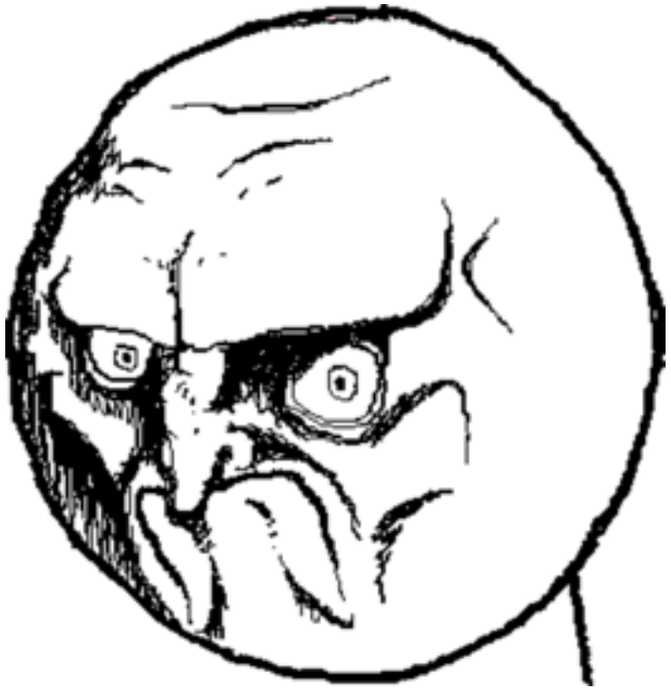


- Chrome/Safari/Opera
  - Local-storage SQLite DB



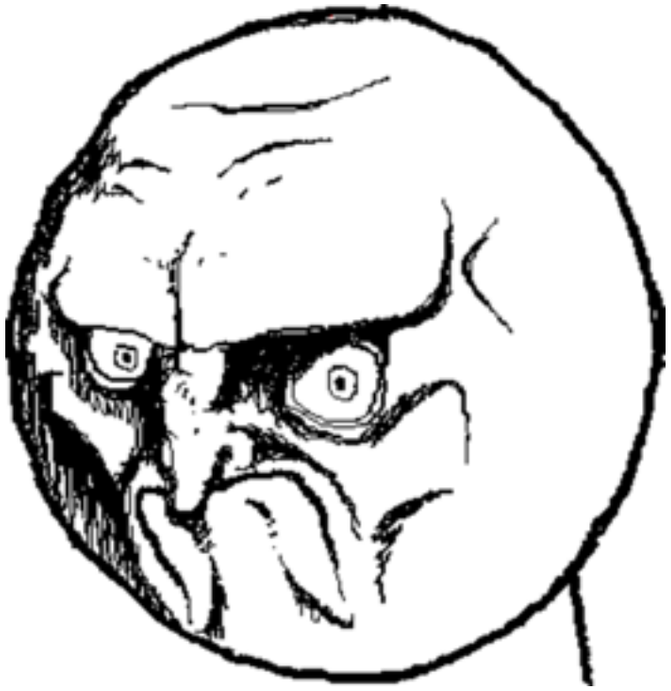
Design Problems?

- Browsers don’t encrypt local storage
- LocalStorage DB and *lp.suid* are accessible and unencrypted
- The token is stored in plaintext
- Token is injected in DOM
  - XSS means game over



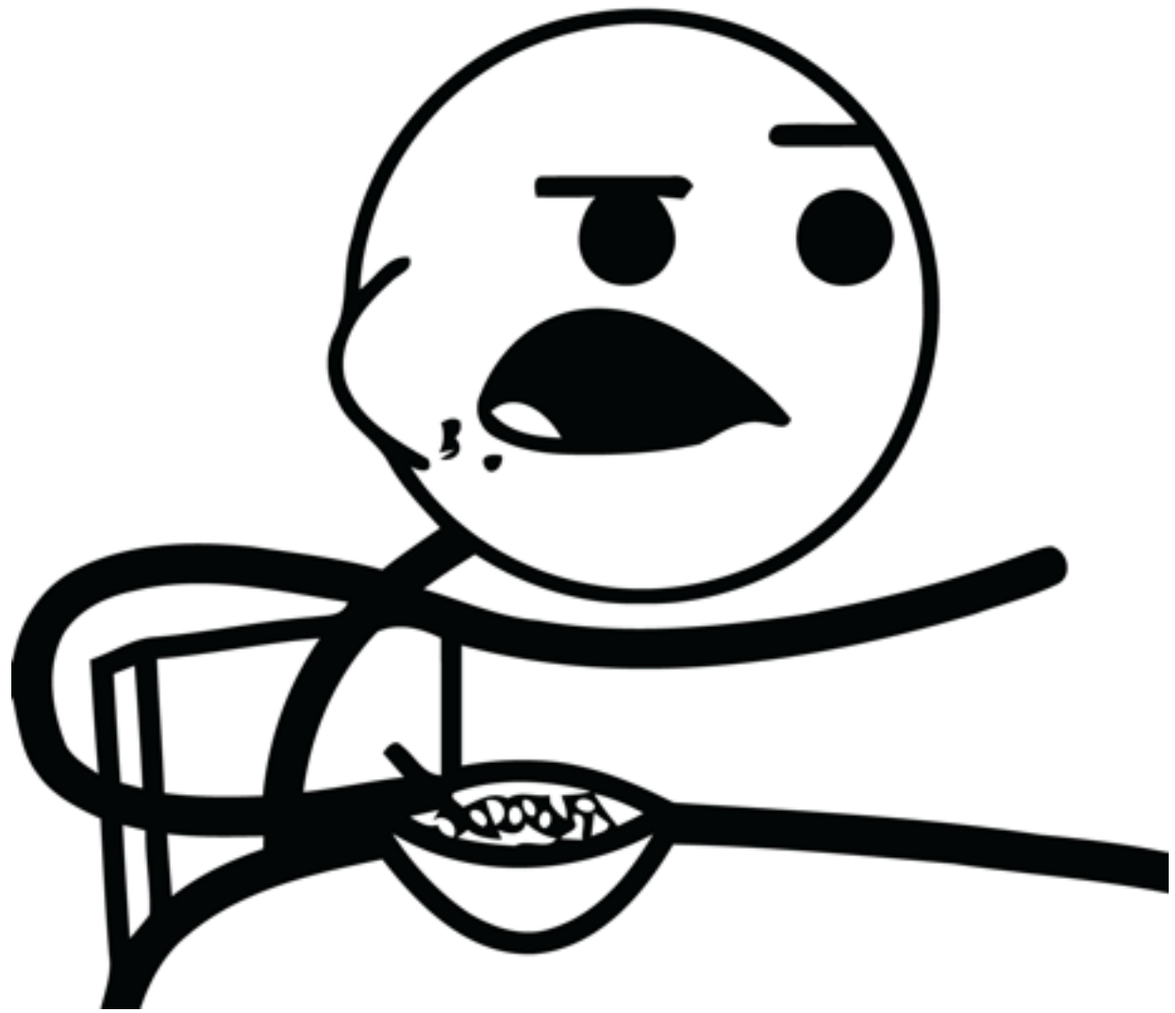
More problems

- Same token for all browser users
- Fixed token till plugin is reinstalled
  - Untrusting the browser has no real effect
  - Same token when changing QR Code
- Token fixation
  - Attacker can set a token on the client
- Proactive token stealing
  - Steal token today, use it tomorrow



Profit!

- We have the file
- We know the encryption
- We have the data
- We have the IV
- We have the key
- **We have the 2-factor token**



What about if:

“Remember password” was not clicked
There was no way to obtain 2-factor auth token

LastPass ****

FEATURES HOW IT WORKS GO PREMIUM ENTERPRISE

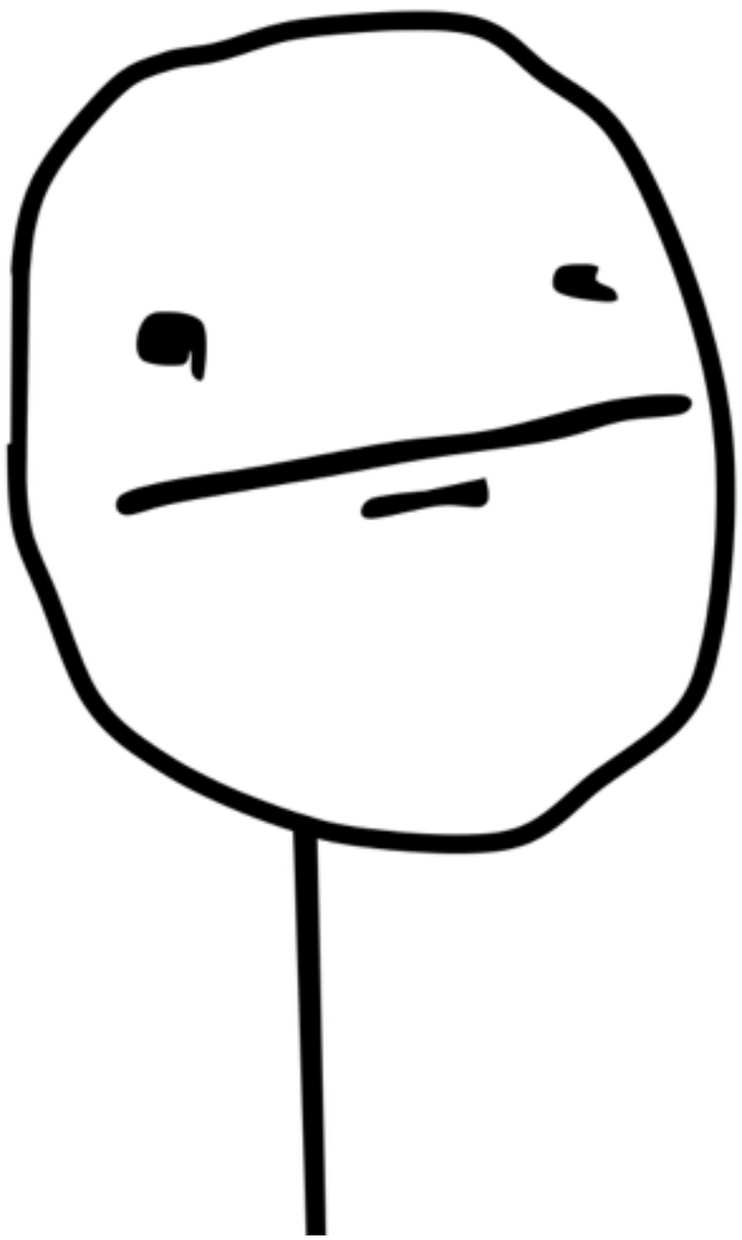
RECOVER ACCOUNT

Account Recovery using Locally Saved One Time Password

Enter your LastPass email in the below box.
Click 'Send Email' to have LastPass.com send you an email containing further instructions.

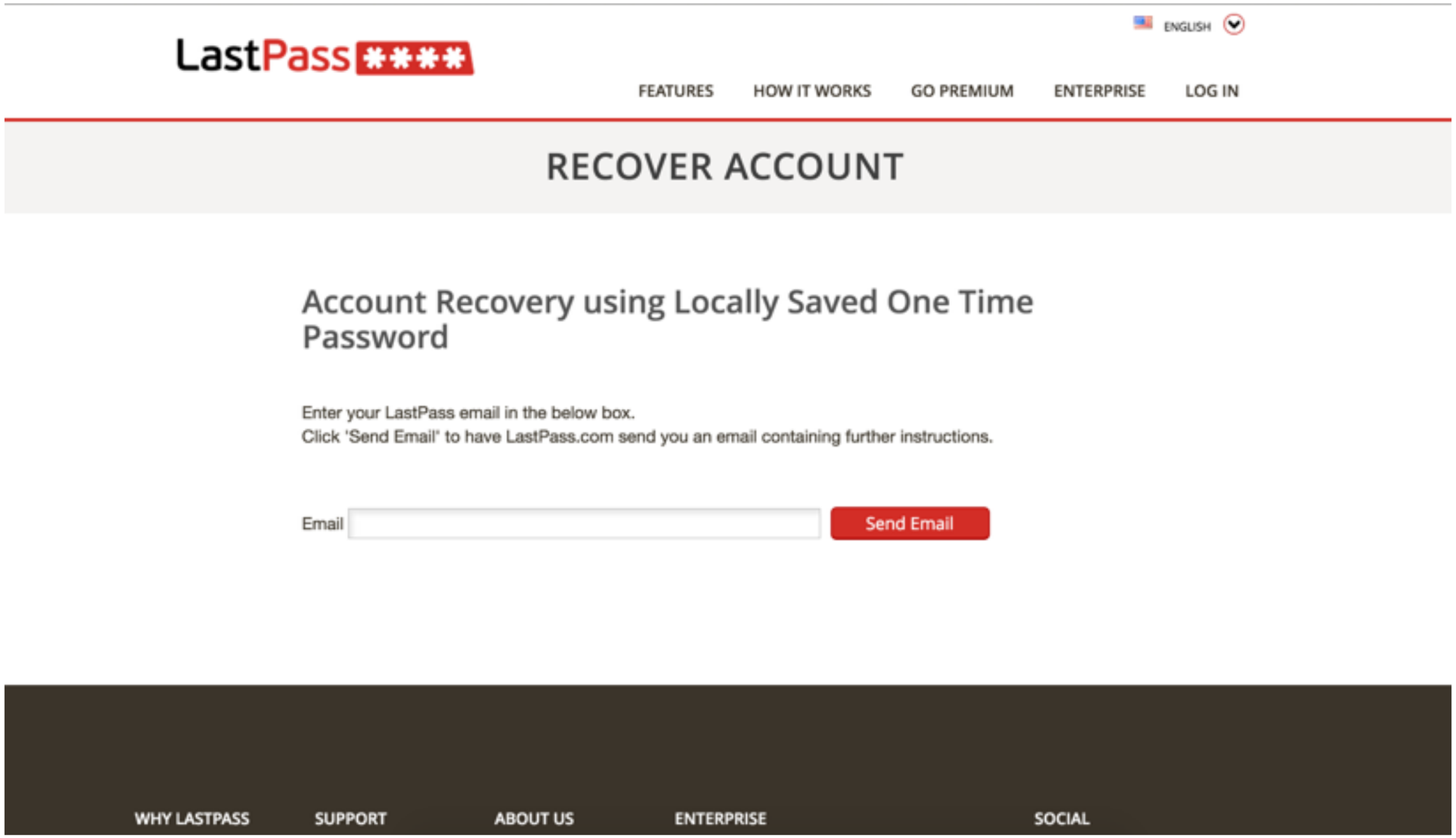
Abusing Account recovery

Wait… What?



How is account recovery possible if LastPass does not know my password?

Recovering the account



Provide your email

Recovering the account

LastPass

LastPass Account Recovery Request

Hi,

You recently notified us that you forgot your LastPass Master Password and want to use LastPass Account Recovery to regain access to your account. To do so, click on the below link:

Activate LastPass Account Recovery

The above link will stop working in 2 hours.

If the above link does not work, carefully copy the below URL to your browser:

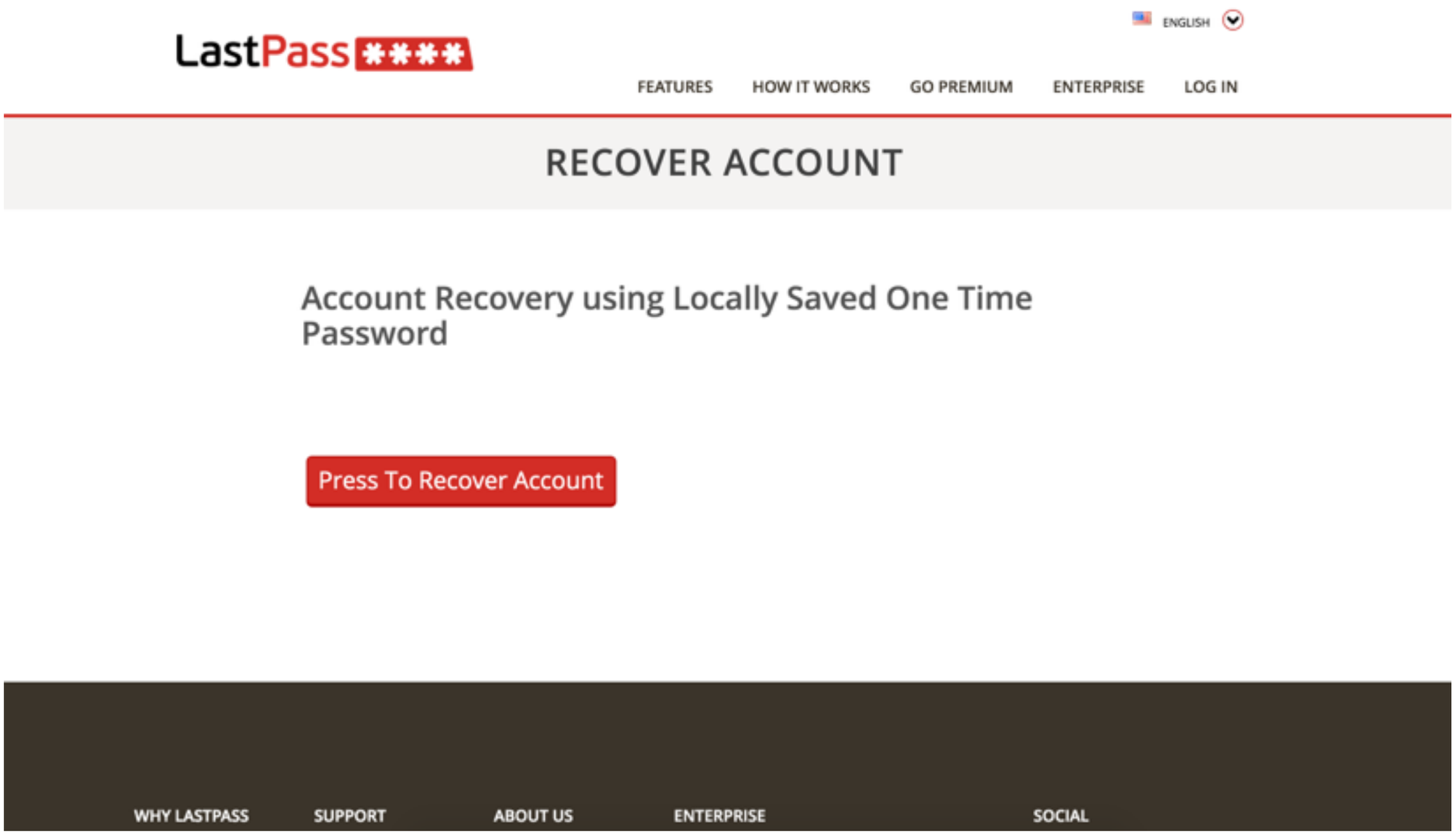
https://lastpass.com/s/?s=04350[redacted]d326a67

If the link does not work, be sure to try the same link in EVERY browser that you've logged into LastPass with. A separate recovery OTP is stored for each browser.

Please note that LastPass has no access to your account and can't reset your password. You must use your hint or Account Recovery to regain access to your account.

Get a unique link

Recovering the account



Press the button

Boom!

- Full, unrestricted access to the vault
- Attacker can set a new password
  - But does not have to!
- Bypasses 2 factor-auth

Recover account flow

Email

LastPass ****

LastPass Account Recovery Request

Hi,

You recently notified us that you forgot your LastPass Master Password and want to use LastPass Account Recovery to regain access to your account. To do so, click on the below link:

Activate LastPass Account Recovery

The above link will stop working in 2 hours.

If the above link does not work, carefully copy the below URL to your browser:

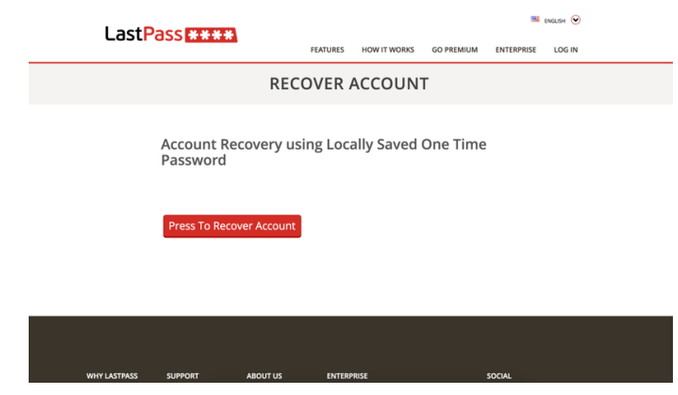
https://lastpass.com/s/?s=04350[redacted]d326a67

If the link does not work, be sure to try the same link in EVERY browser that you've logged into LastPass with. A separate recovery OTP is stored for each browser.

Please note that LastPass has no access to your account and can't reset your password. You must use your hint or Account Recovery to regain access to your account.

LastPass ****

Recover button



GET /s/?**s**=8aa37bb1bb3FAKE03ad4127 →

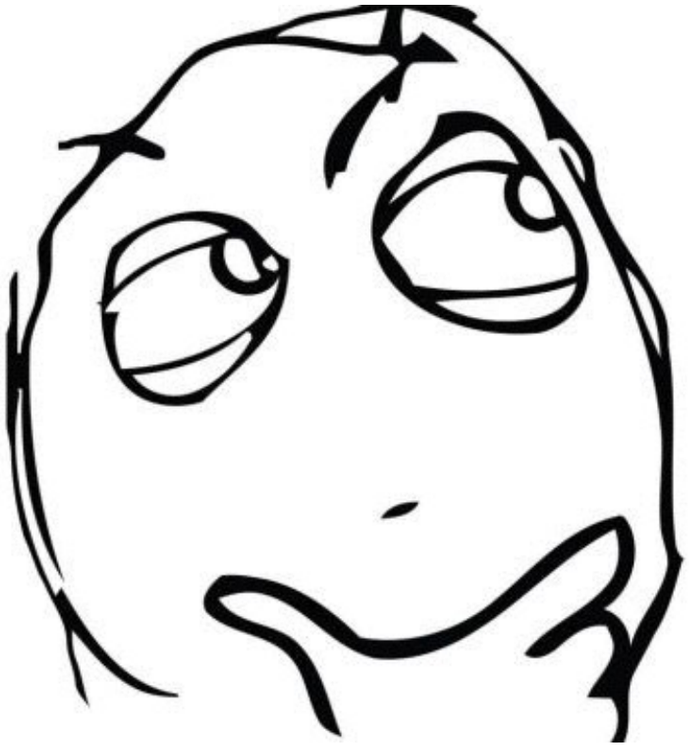
302 Location: /recover.php?
&**time**=1412381291&**timehash**=340908c353c099c9FAKE6b387002c5a4881ebdf1
&**username**=test%40test.com&**usernamehash**=fc7be7e5f6cbec9FAKE2995bd3331c097 ↔

POST /otp.php
&**changepw**=ccb2501724FAKE2b575a214e1052
d0fa27b0726b6HASHdb2e1da3952e ←

Can I directly generate the recover url?

302 Location: /recover.php?
&**time**=1412381291&**timehash**=340908c353c099c9FAKE6b387002c5a4881ebdf1
&**username**=test%40test.com&**usernamehash**=fc7be7e5f6cbec9FAKE2995bd3331c097

- **time**: timestamp when the recovery was initiated (the link “expires” in 2 hours)
- **timehash**: salted hash of the timestamp
- **username:** the email address
- **usernamehash**: salted hash of the email



Challenges

- I need to generate a valid timestamp
- I need the be able to generate the hashes
- I need the salt

Let’s try…

- Request my own unique url and reuse the hashes in the victims url
  - BINGO!
    - Same salt is used for all users
    - Link does not truly expire, only the timestamp is validated against the hash
    - There is no need to request account recovery. You only need a valid url

The salt is the secret

- Still, we need to change the username, and hash it.
- We are only missing the server salt to be able to generate valid recover urls
- Salts are not designed to be a secret, only random and unique.
- Oh wait…

LastPass Security Notice

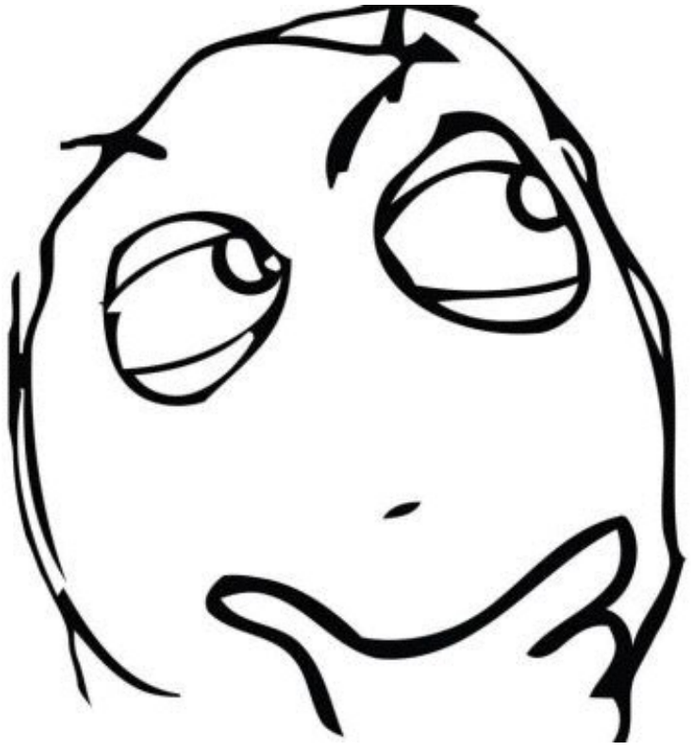
By Joe Siegrist | June 15, 2015 | Security News | 1,294 Comments

*"LastPass account email addresses, password reminders, **server per user salts**, and authentication hashes were compromised"*

Can I forge the post request?

POST /otp.php
&**changepw**=ccb25017c4FAKE2b575a21441055d0fa27b0726b6HASHdb2e1da395e

- **changepw**: a derived “disabled OTP”



OTPs in LastPass

- 2 types of OTPs
  - “True” OTPs for authentication
  - **“Disabled” OTP**
    - Let’s call it *dOTP*

Disabled OTP

- Used to recover the vault
  - Which ultimately means for authentication
- It's set **by default**
- It's not the encryption key

How/Where is it stored?

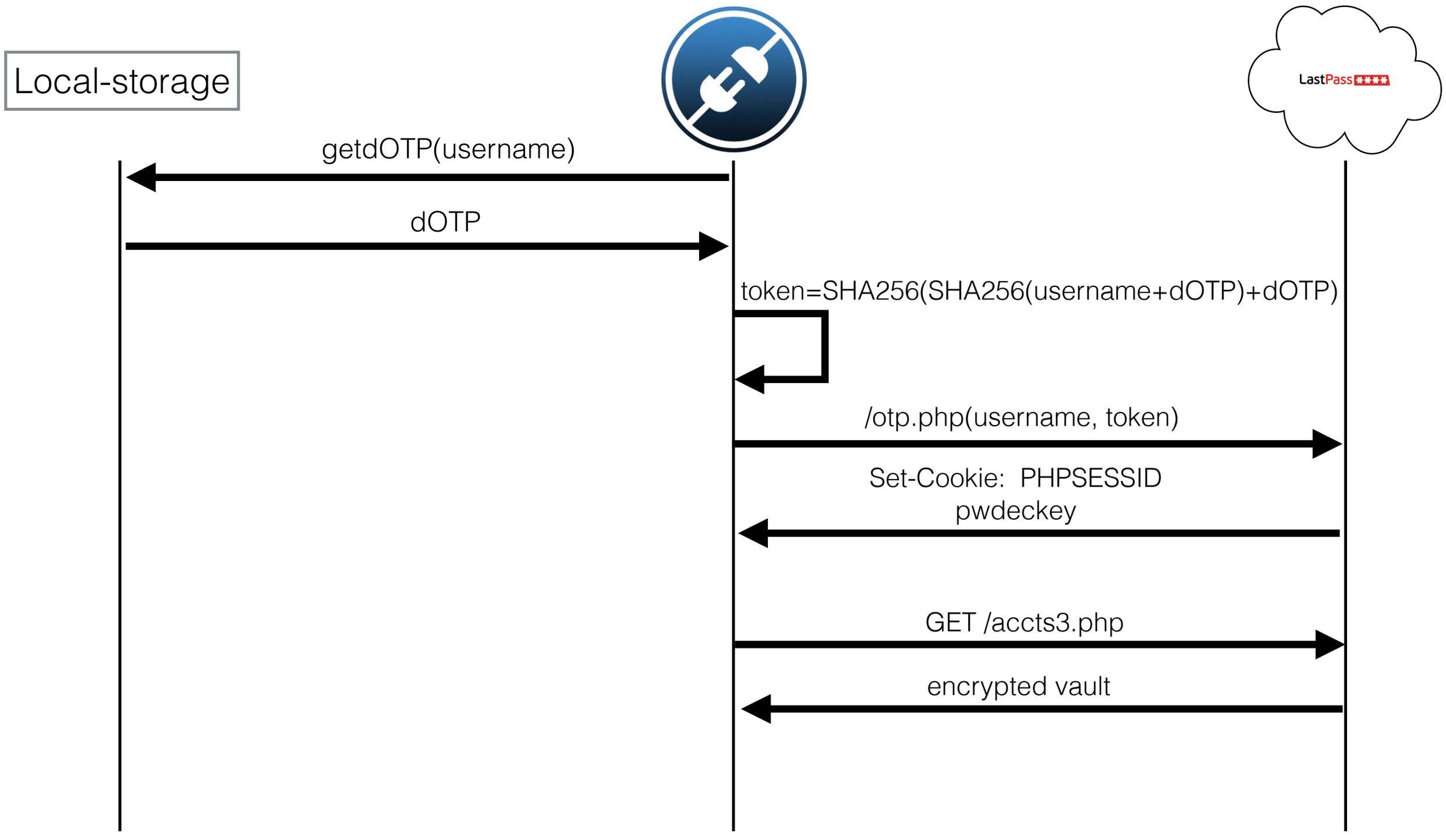
- Unprotected
- Firefox
  - In the file {*SHA256(username)}_ff.sotp (binary format)*
  - Needs the extra step: *bin2hex*
- Chrome/Safari/Opera
  - SQLite DB

How is the request forged?

```
▼<form id="lpwebsiteeventform" name="lpwebsiteeventform" onsubmit="return false;" autocomplete="off" action="accts.php">
    <input type="hidden" name="eventtype" id="eventtype" value="recover">
    <input type="hidden" name="eventdata1" id="eventdata1" value="b[redacted].com">
    <input type="hidden" name="eventdata2" id="eventdata2" value="995[redacted]e4bfe">
    <input type="hidden" name="eventdata3" id="eventdata3" value>
    <input type="hidden" name="eventdata4" id="eventdata4" value>
    <input type="hidden" name="eventdata5" id="eventdata5" value>
    <input type="hidden" name="eventdata6" id="eventdata6" value>
    <input type="submit" name="submitbtn">
  </form>
▶<script type="text/javascript" nonce="wlcIRZ2M9IwYXZHnxltHh34F7zu3DkgO8u3yw/DRgcE=">…</script>
</div>
▶<div id="headermarkup">…</div>
<br>
<link rel="stylesheet" type="text/css" href="/m.php/vault3css?1427738692">
<script type="text/javascript" src="/m.php/all?1426604514"></script>
<script type="text/javascript" src="/m.php/accts?1433344166"></script>
<script type="text/javascript" src="/m.php/otp?1426183169"></script>
<script type="text/javascript" src="/m.php/recover?1433344166"></script>
<script type="text/javascript" src="/m.php/vault?1428410648"></script>
<script type="text/javascript" src="/m.php/otpwindow?1430837538"></script>
▶<script type="text/javascript" nonce="wlcIRZ2M9IwYXZHnxltHh34F7zu3DkgO8u3yw/DRgcE=">…</script>
▶<script type="text/javascript" nonce="wlcIRZ2M9IwYXZHnxltHh34F7zu3DkgO8u3yw/DRgcE=">…</script>
▼<table cellspacing="0" cellpadding="0" style="width:750px;margin:0 auto;">
  ▼<tbody>
    ▼<tr>
      ▼<td align="left">
        <br>
        <h2>Account Recovery using Locally Saved One Time Password</h2>
        <br>
        ▼<div id="step1">
          ▼<form name="getuser">
            <input type="hidden" name="otpemail" id="otpemail" value="b[redacted].com">
            <br>
            <input type="hidden" name="otpfield" id="otpfield" value="995[redacted]e4bfe">
            <br>
            <input type="submit" style="padding:10px" class="nbtn rbtn expandbutton" value="Press To Recover Account"
            onclick="getOTP(); return false;">
          </form>
```

The dOTP is injected into the DOM

From dOTP to vault

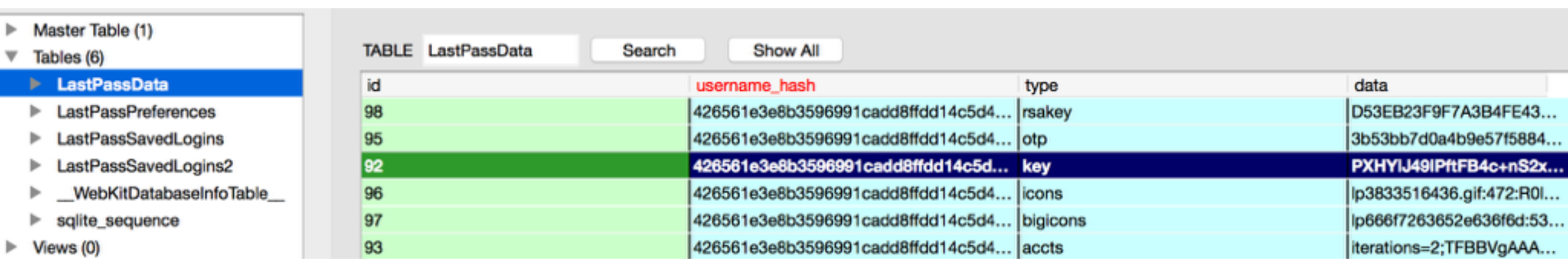


What is”pwdeckey”?

- It’s not the key to decrypt any password
- It’s the seed to derive the key to decrypt the “vault key”
- The vault key decrypts all the password, notes, etc. in the vault

How/Where is the vault key stored?

- Encrypted
- Firefox
  - In the file {*SHA256(username)}_lpall.slps*
- Chrome/Safari/Opera
  - SQLite DB



Vault key decryption

AES-ECB(SHA256(pwdeckey), encryptedVaultKey)

Profit!

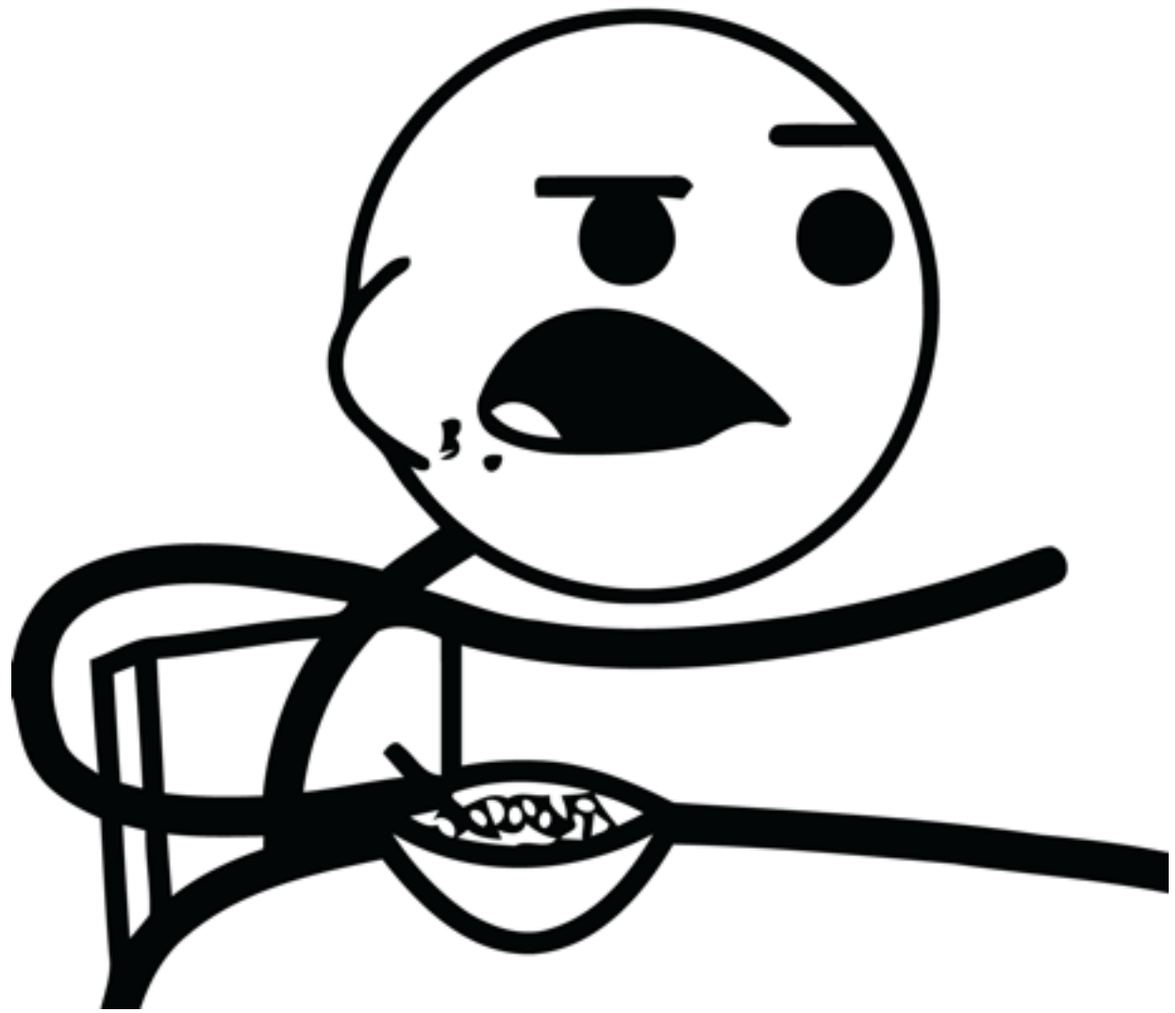
- We located the token
- We know how to hash it
- We get the vault key decryption key
- We get the vault
- **We decrypt the vault key**
- **We decrypt the vault**

Automating all the stuff

Metasploit module

- Steals and decrypts the master password
- Steals the 2-factor auth token
- Steals the encryption key
- Decrypts the entire vault
- Supports:
  - Win, Mac and Unix
  - Chrome, Firefox, Safari and Opera
  - Meterpreter and shell
  - Multiuser

Demo



What about if there is:

No disabled OTP
No access to the machine
No Exploit
No nothing!

Google dorks

“extensions.lastpass.loginpws”

Google

extensions.lastpass.loginpws

Web Shopping News Videos Images More Search tools

Page 2 of about 78 results (0.29 seconds)

browsers hijacked - Page 4 - PC Help Forum
www.pchelpforum.com › ... › Forum › Operating Systems › Windows 7
May 16, 2014 - 10 posts - 3 authors
user_pref("extensions.6RhAHBR3sCh3.scode", "(function()){if(window.self. location.hostname. ... user_pref("extensions.lastpass.loginpws", ...

user.js - myautoproxy - AutoProxy - Google Project Hosting
code.google.com/p/myautoproxy/source/.../user.js?r=4 - Translate this page
Oct 20, 2009 - //----lastpass. user_pref("extensions.lastpass.disableffpwasked", true); ... user_pref("extensions.lastpass.loginpws", ...

VIRY.CZ • Zobrazit téma - cernohous13 - pomalé načítání FF ...
forum.viry.cz › ... › Řešení problémů, logy - Translate this page
Mar 26, 2014 - O4 - Global Startup: Install LastPass FF RunOnce.lnk = C:\Program Files (x86)\Common ..... user_pref("extensions.lastpass.loginpws", ...

VIRY.CZ • Zobrazit téma - Prosím o kontrolu logu - zmizely mi ...
forum.viry.cz › ... › Řešení problémů, logy - Translate this page
FF - user.js: extensions.lastpass.homeHkKeyCode - 104. FF - user.js: extensions. lastpass.homeHkMods - control alt. FF - user.js: extensions.lastpass.loginpws ...

AdwCleaner et Firefox - Forum PC Astuces
forum.pcastuces.com › Sécurité - Translate this page
Oct 29, 2014 - 6 posts - 4 authors
... Ligne Trouvée : user_pref("extensions.lastpass.loginpws", ""); [cwoqntdf.default] - Ligne Trouvée : user_pref("extensions.lastpass.loginusers", ...

localMark.uc.xul阅读标记，求修改用户数据保存位置_Firefox_浏览器讨论
bbs.kafan.cn › 论坛 - Translate this page
Aug 30, 2014 - 10 posts - 5 authors
prefs.js 会保存Lastpass的密码？存在哪的？还真不知道，请楼主告知下，我回头检查下。 user_pref("extensions.lastpass.loginpws", "你的密码");

PASTEBIN | #1 paste tool since 2002

PASTEBIN

create new paste trending pastes sign up

** Pastebin PRO Accounts Spring Special ** Get 40% discount for a limited time only! Click Here to check it out ;-)

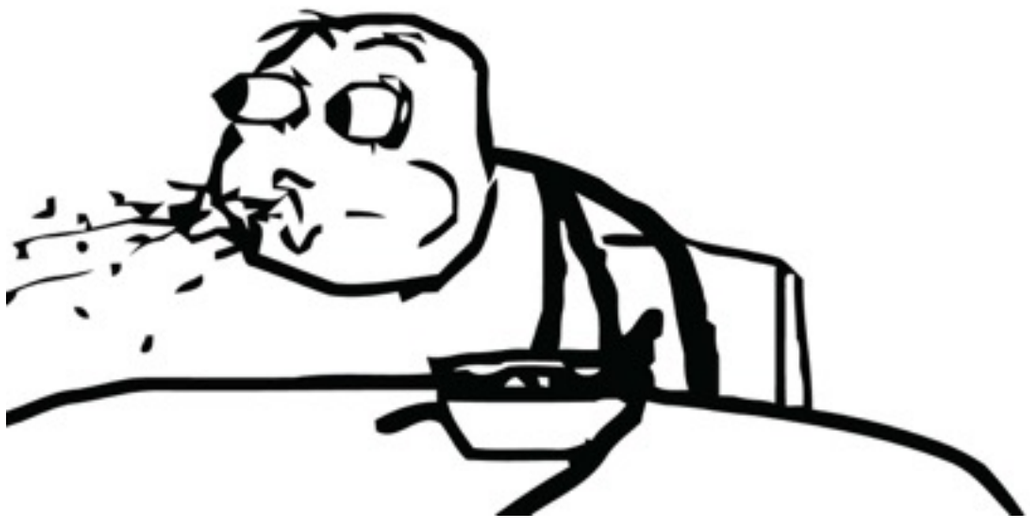
Search results for: extensions.lastpass.loginpws

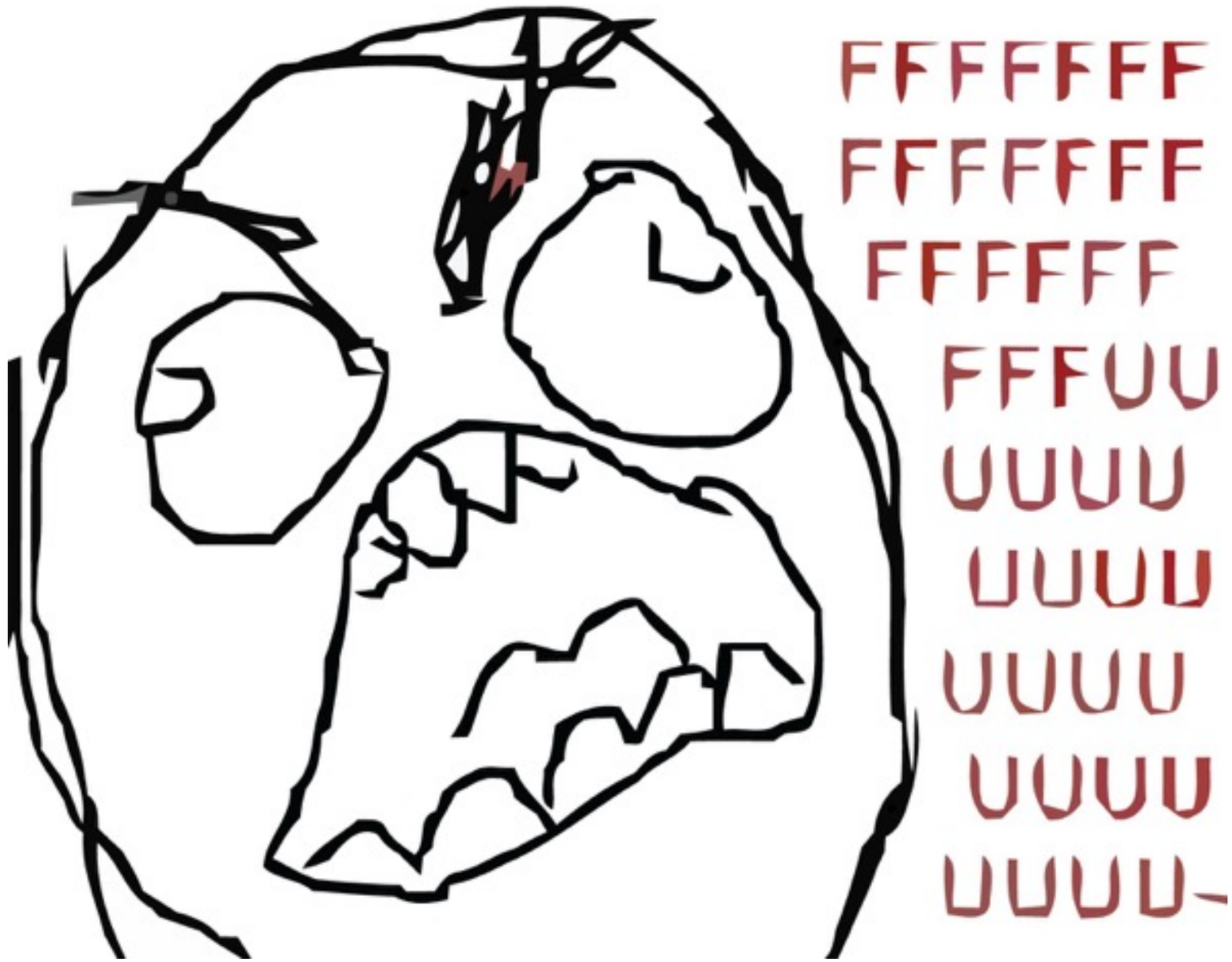
KELLEY BLUE BOOK®
Buying or Selling a Used Car? Get Vehicle Values & More at KBB.com®!
www.KBB.com

About 2 results (0.33 seconds)

Buggy K-Meleon prefs.js - Pastebin.com
pastebin.com/WFqi5tUv
Sep 16, 2014 ... homeHkMods", "control alt"); user_pref("extensions.lastpass.language", "en-US"); user_pref("extensions.lastpass.loginpws", ...

prefs.js mkdante381.18.March.2015 - Pastebin.com
pastebin.com/a2Ym5HAs
Mar 18, 2015 ... user_pref("extensions.lastpass.loginpws", "mkdante381%40gmail.com=QDpa% 2Fdz3a1kVPbP9GaxZolkQ1E50brYjhpYgn0Hz54%3D");





Stop sharing your LastPass credentials with the entire world!!!!

Hardening LastPass

Hardening LastPass

- Use the binary version of the plugin
- Do not store your master password
- Disable “Account recovery”
- Do not use “Password reminder”
- Activate 2-factor auth
- Prompt for master password to make passwords visible
- Add country restriction
- Update/Randomize PBKDF2 iterations
- Disallow TOR logins

Thank you!

Questions?

@martin_vigo
martinvigo.com
martinvigo@gmail.com