

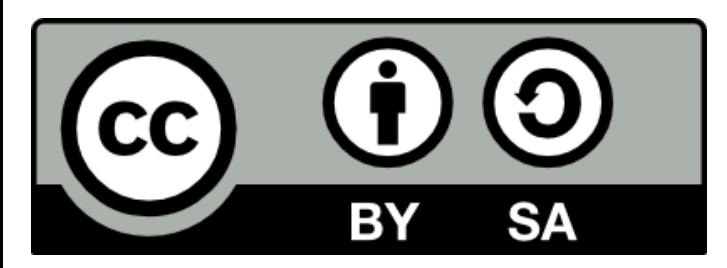
SitePassword

A Hybrid Password Manager

Alan H. Karp

alanhkarp@gmail.com

12 April 2023



“Passwords are terrible, and we won’t be using them in 10 years.”

“Passwords are terrible, and we won’t be using them in 10 years.”

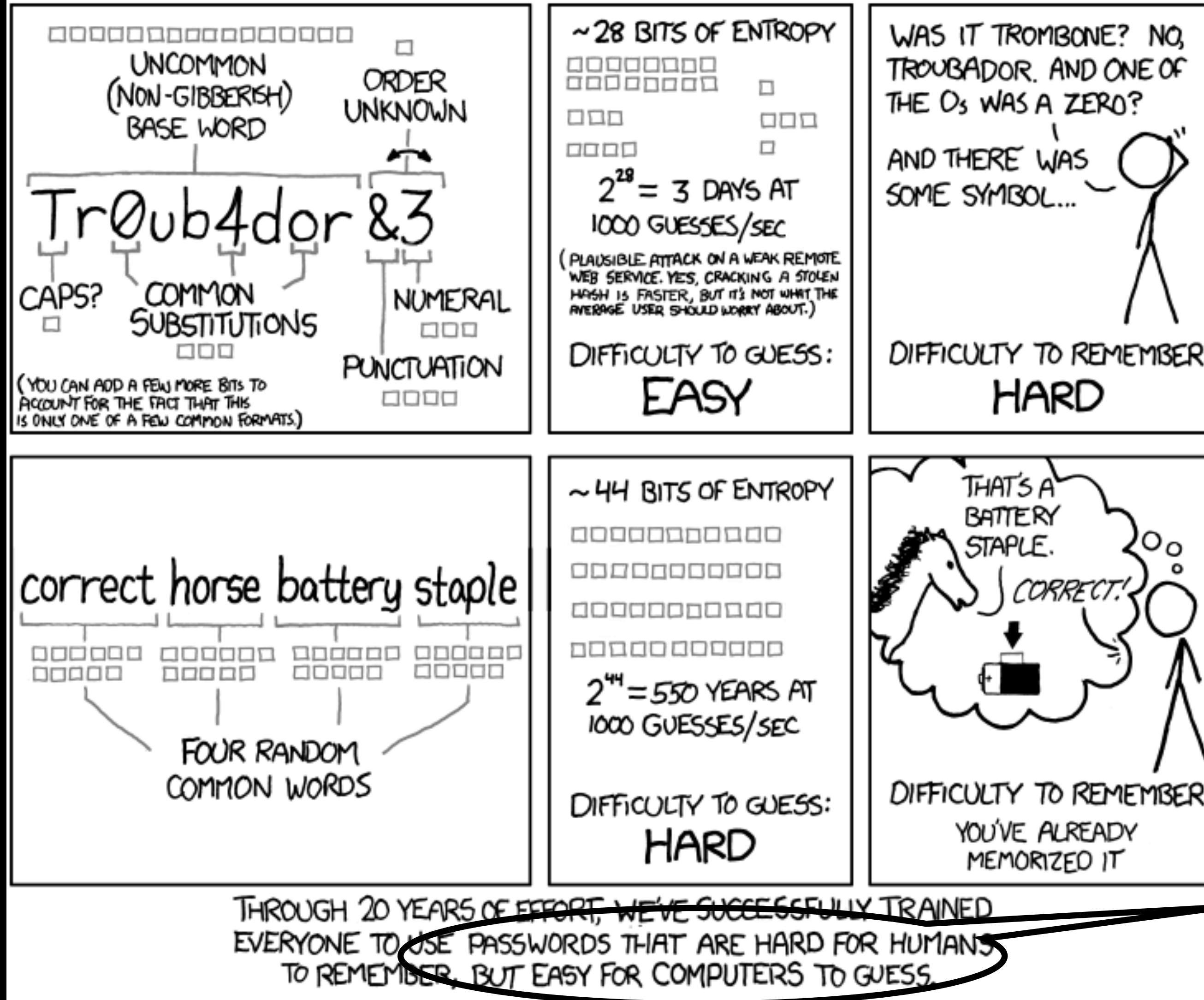
Everybody

“Passwords are terrible, and we won’t be using them in 10 years.”

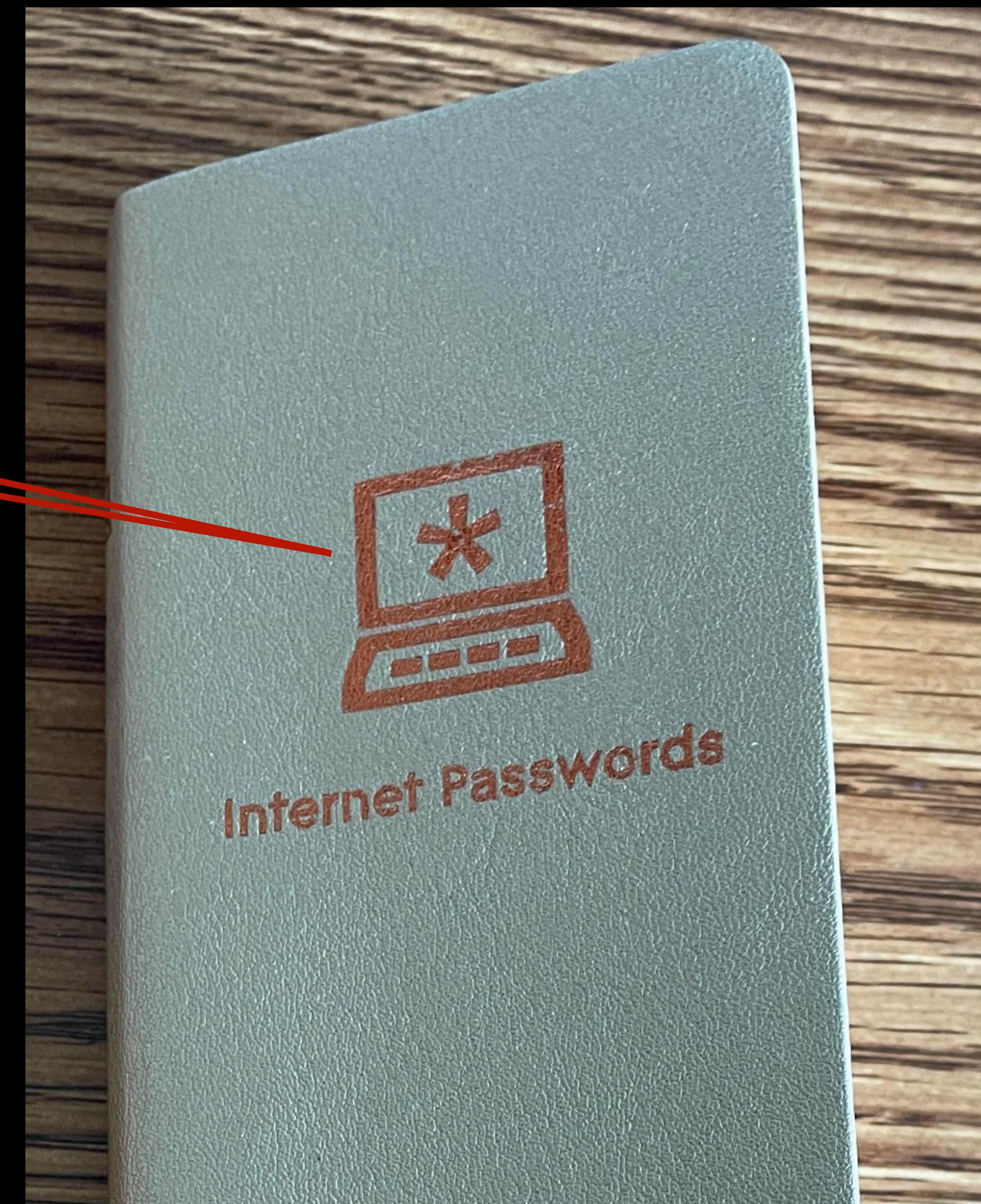
Everybody

2013 2003 1993 1983 1973 1963

What's So Bad about Passwords?



Passwords are hard for people to remember and easy for computers to guess.



Do You Use a Password Manager?

One of the top recommended security practices but only 40% use them

Do You Use a Password Manager?

One of the top recommended security practices but only 40% use them

- 1Password (\$36)
- LastPass (\$36)
- DashLane (\$60)
- Keeper (\$35)
- ZohoVault (Free or \$54)
- Avira (\$32)
- RememBear (Shutting down)
- PassBolt (Free if you host)
- Bitwarden (Free or \$40)
- LogMeOnce (\$48)
- NordPass (Free or \$36)
- PasswordBoss (Free?)
- RoboForm (\$24)
- Your Browser (Free)

Password Manager Characteristics

- Requirements
 - Easy to use
 - Engenders trust
 - Use from anywhere
 - Secure
- Other desirable features
 - Strong passwords
 - Different for every site
 - Easy to change (Ask me why that's bad)

What is a Password Manager?

A software application designed to **store** and manage online credentials. It also generates passwords. Usually, the passwords are stored in an encrypted database locked behind a master password. — malwarebytes.com

A password manager is an app on your phone, tablet, or computer that **stores** your passwords, so you don't have to remember them. — ncsc.gov

A password manager is a service that helps you generate and **store** long, unique passwords for all your online accounts. — consumerreports.org

So What's So Bad about That?

- Where are your passwords stored?
 - On your machine?
 - In the cloud? Who's cloud?
- How are they stored?
- It costs money
 - To manage your account
 - To pay for the cloud resources

And then There's This to Worry About



We recently detected unusual activity within a third-party cloud storage service, ...

We have determined that an unauthorized party, ...was able to gain access to certain elements of our customers' information. **Our customers' passwords remain safely encrypted due to LastPass's Zero Knowledge architecture.**

A Different Approach

A Different Kind of Password Manager

Don't Remember Your Passwords, Calculate Them

- It can be free
 - No accounts to manage
 - No password storage needed
- Can even be used without network access
- **You are in control**
 - Carry a piece of paper with everything you need to get your passwords.
 - It's not great if you lose it, but it isn't terrible either.

A Brief History of SitePassword

The Earliest Days

2003

The Earliest Days

2003

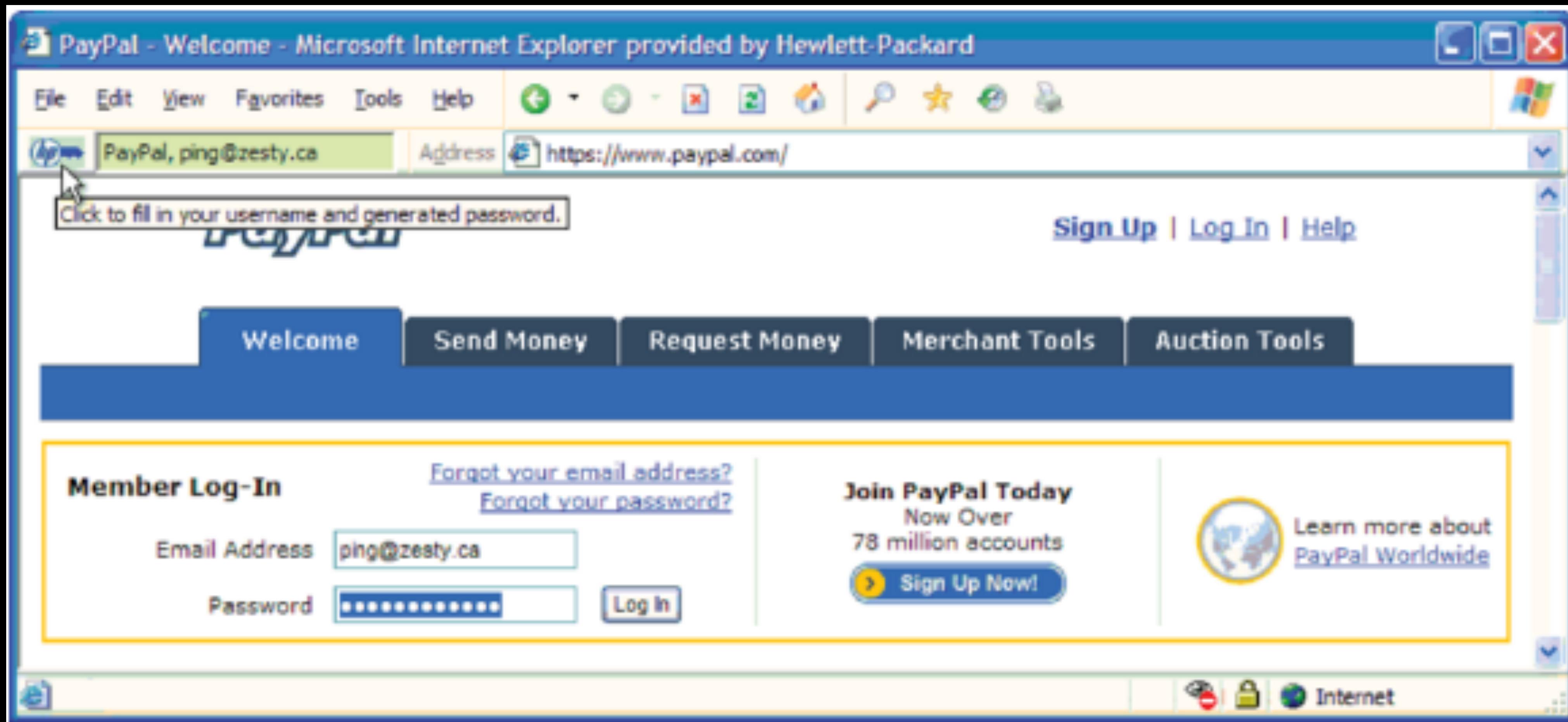


HP Anti-Phishing Toolbar for IE

2005

HP Anti-Phishing Toolbar for IE

2005



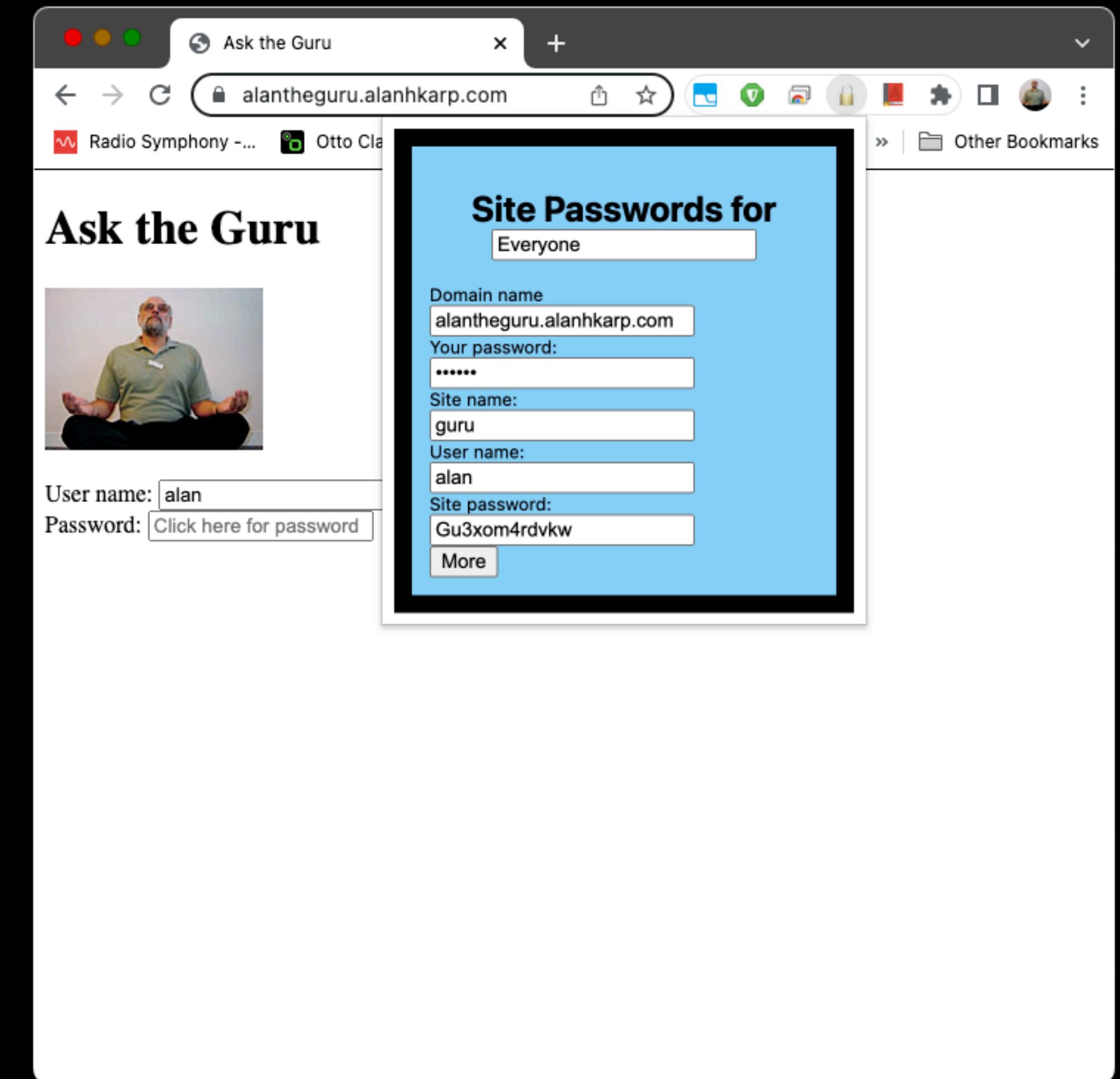
Chrome Extension

2012

Chrome Extension

2012

- Some Problems
 - No sync across machines
 - Unhappy with personas
 - Only finds 60% of password fields
 - Only available for testers
 - Only I used it for the next 10 years



And Then

2021

- Google says I have to update it.
- “No problem,” I say to myself. “It’ll only take a week or so.”
- A year later

Why It Took So Long

- Google's changes
 - From a persistent background page to a transient service worker
 - Everything is async
- Fixed what I didn't like
 - Always(?) finds password field
 - Synchronizes across machines
 - Handles different personas



Let Google Do the Heavy Lifting

- Store settings in bookmarks
 - Every browser syncs bookmarks
 - But Google doesn't merge duplicates
- Supporting personas with Google Profiles
 - Switch Profile without logging out
 - Each Profile has its own bookmarks

A Taste of SitePassword

Ask the Guru

alanthege... alanthe... Other Bookmarks

Radio Symphony -... Otto Classical Pandora

Ask the Guru



User name:

Password: Click SitePassword

Ask the Guru

alanthe guru.alanhkarp.com

Radio Symphony -... Otto

Ask the Guru



User name:

Password: Click SitePassword

SitePassword.info

alanthe guru.alanhkarp.com

..... 

Too Weak

A unique nickname for this account

Your user-id for this account 

pvQhUS2xVu0I  

 Clear Clipboard 

Provide your own site password.

Clear master password on use.

Hide site password by default.

Password is **12** characters long

Starts with letter

Requires at least **1** lowercase letter(s)

Requires at least **1** uppercase letter(s)

Requires at least **1** number(s)

Allows special characters

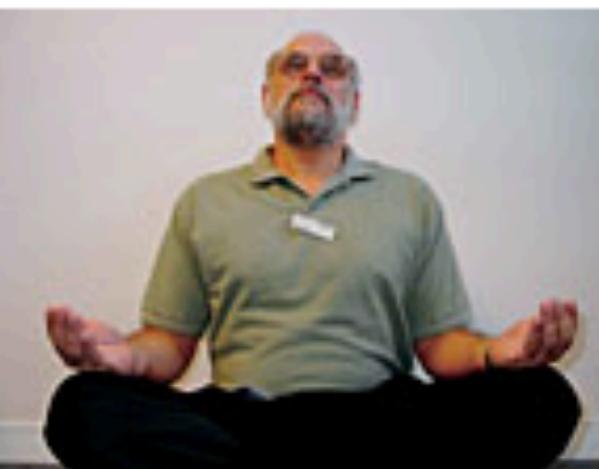
Download Site Data

Ask the Guru

alanthe guru.alanhkarp.com

Radio Symphony -... Otto

Ask the Guru



User name:

Password: Click SitePassword

SitePassword.info

alanthe guru.alanhkarp.com

..... 

Too Weak

Guru

alan 

to3X9g55EK8C 

 Clear Clipboard 

Provide your own site password.

Clear master password on use.

Hide site password by default.

Password is **12** characters long

Starts with letter

Requires at least **1** lowercase letter(s)

Requires at least **1** uppercase letter(s)

Requires at least **1** number(s)

Allows special characters

Download Site Data

Ask the Guru

alanthege... alanthe... Other Bookmarks

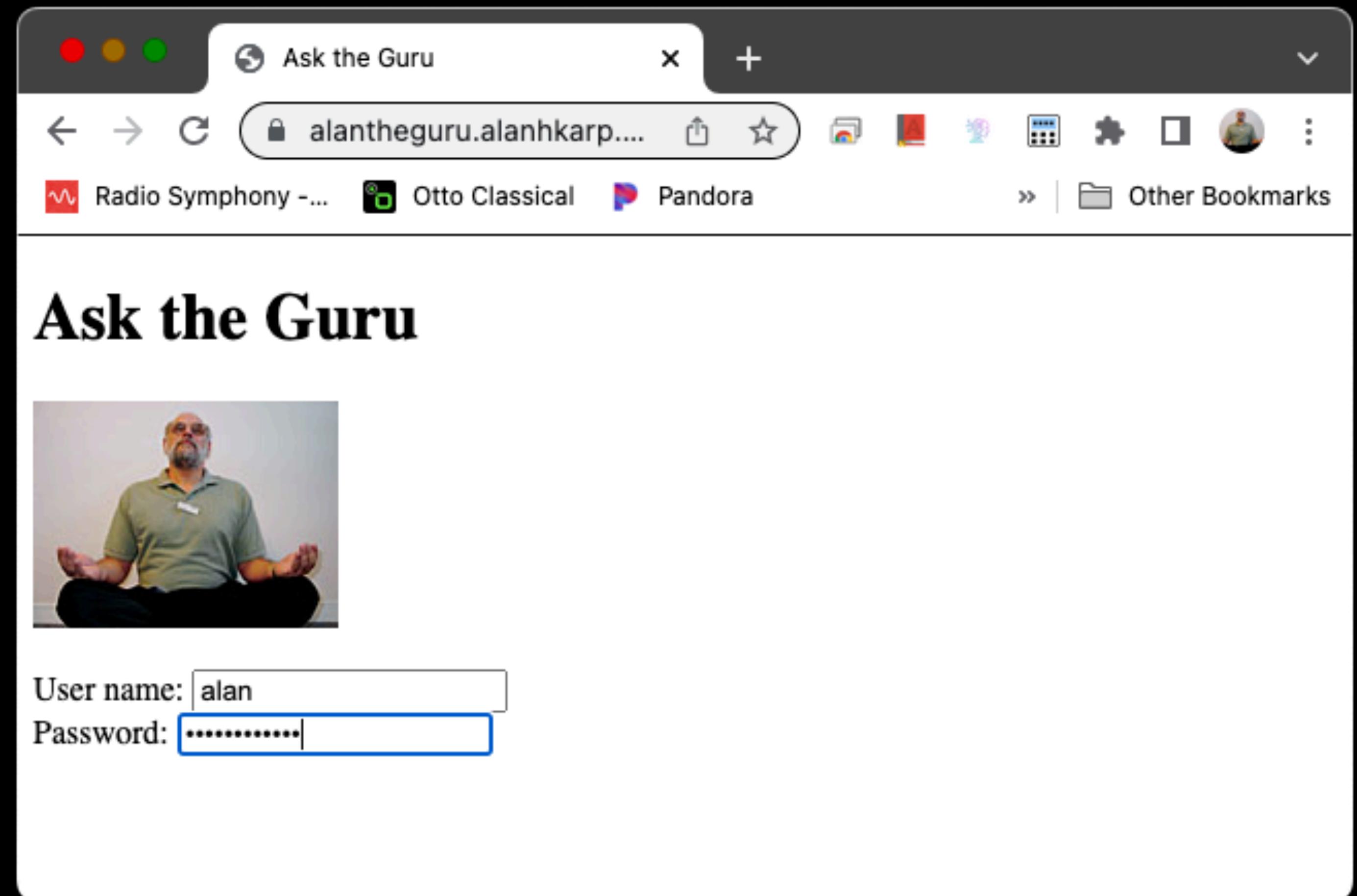
Radio Symphony -... Otto Classical Pandora

Ask the Guru



User name:

Password:



Ask the Guru

alanthege... alanthe... Other Bookmarks

Radio Symphony -... Otto Classical Pandora

Ask the Guru



User name:

Password:

Ask the Guru

allanthe guru.alanhkarp....

Radio Symphony -... Other Bookmarks

Ask the Guru



User name:

Password: Click SitePassword

SitePassword.info

allanthe guru.alanhkarp.com

..... Too Weak

guru

Your user-id for this account

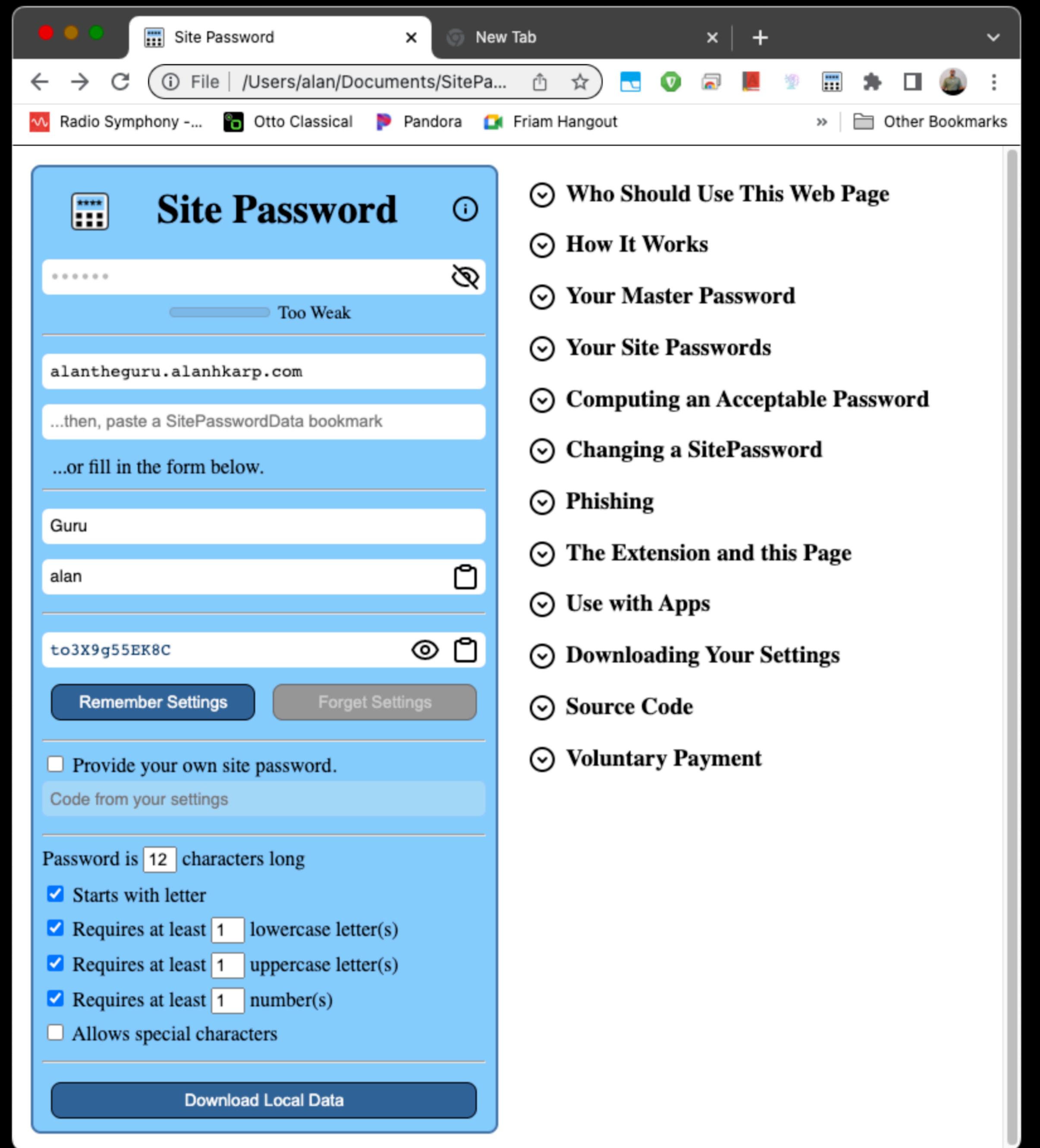
Generated site password

Warning: You may be at a fake site that is trying to steal your password. You previously used this nickname for
alanthe guru.alanhkarp.com
but the domain name asking for your password is
allanthe guru.alanhkarp.com
It is common to see different domain names for the same account login. Click the top (green) button if that's not the case or the middle (red) button if it is. You can also pick a new nickname if this page is for a different account.

Get me to safety!

This page is for the same account.

Pick a new nickname.



Ask the Guru

alanthe guru.alanhkarp.com

Radio Symphony -... Otto

Ask the Guru



User name: alan

Password: Click here for password

SitePassword.info

alanthe guru.alanhkarp.com

.....

Too Weak

Guru

alan

MyStrongPassword

Clear Clipboard

Provide your own site password.

Clear master password on use.

Hide site password by default.

Password is 12 characters long

Starts with letter

Requires at least 1 lowercase letter(s)

Requires at least 1 uppercase letter(s)

Requires at least 1 number(s)

Allows special characters

Download Site Data

Usability

Usable Security

No system can be secure if users don't understand the implications of their actions.

Ping's 10 Principles for a Secure UX

1. Path of Least Resistance: Make the easy way the secure way.
2. Appropriate Boundaries: Make distinctions matter to the user.
3. Explicit Authorization: Authorize only by explicit user action.
4. Visibility: All security related decisions must be viewable.
5. Revocability: Make it easy to revoke granted permissions.
6. Expected Ability: Don't make user think the tool will do what it can't
7. Trusted Path: It should not be possible to spoof the UI.
8. Identifiability: Give each object an identifier that the user understands.
9. Expressiveness: Allow users to express policies that they want.
10. Clarity. Make effects of actions apparent to the user before acting.

Ping's 10 Principles for a Secure UX

1. Path of Least Resistance: Make the easy way the secure way.
2. Appropriate Boundaries: Make distinctions matter to the user.
3. Explicit Authorization: Authorize only by explicit user action.
4. Visibility: All security related decisions must be viewable.
5. Revocability: Make it easy to revoke granted permissions.
6. Expected Ability: Don't make user think the tool will do what it can't
7. Trusted Path: It should not be possible to spoof the UI.
8. Identifiability: Give each object an identifier that the user understands.
9. Expressiveness: Allow users to express policies that they want.
10. Clarity. Make effects of actions apparent to the user before acting.

Ping's 10 Principles for a Secure UX

1. Path of Least Resistance: Make the easy way the secure way.
2. Appropriate Boundaries: Make distinctions matter to the user.
3. **Explicit Authorization:** Authorize only by explicit user action.
4. Visibility: All security related decisions must be viewable.
5. Revocability: Make it easy to revoke granted permissions.
6. Expected Ability: Don't make user think the tool will do what it can't
7. Trusted Path: It should not be possible to spoof the UI.
8. Identifiability: Give each object an identifier that the user understands.
9. Expressiveness: Allow users to express policies that they want.
10. Clarity. Make effects of actions apparent to the user before acting.

Ping's 10 Principles for a Secure UX

1. Path of Least Resistance: Make the easy way the secure way.
2. Appropriate Boundaries: Make distinctions matter to the user.
3. Explicit Authorization: Authorize only by explicit user action.
4. Visibility: All security related decisions must be viewable.
5. Revocability: Make it easy to revoke granted permissions.
6. Expected Ability: Don't make user think the tool will do what it can't
7. Trusted Path: It should not be possible to spoof the UI.
8. Identifiability: Give each object an identifier that the user understands.
9. Expressiveness: Allow users to express policies that they want.
10. Clarity. Make effects of actions apparent to the user before acting.

Ping's 10 Principles for a Secure UX

1. Path of Least Resistance: Make the easy way the secure way.
2. Appropriate Boundaries: Make distinctions matter to the user.
3. Explicit Authorization: Authorize only by explicit user action.
4. Visibility: All security related decisions must be viewable.
5. Revocability: Make it easy to revoke granted permissions.
6. Expected Ability: Don't make user think the tool will do what it can't
7. Trusted Path: It should not be possible to spoof the UI.
8. Identifiability: Give each object an identifier that the user understands.
9. Expressiveness: Allow users to express policies that they want.
10. Clarity. Make effects of actions apparent to the user before acting.

My User Experience Goals

Make it as easy to use as Candy Crush

- Can't break anything by experimenting
- A Help button is a crutch for developers
- Encourage good practices
 - Warn on weak master/site password
- Choose a readable font, particularly for site password
- Focus the field the user will be needing next

My User Experience Goals

Where I failed

- Can't always make "Click here for password" show up
 - Resorted to tooltip, but it takes a second or so to appear
- Forgetting settings for a domain
 - Delete the corresponding bookmark
- Closing the popup

Password Manager Security

Mobile Devices

Situation is Really Bad

- Too easy to spoof app identity
- iframes inside Android WebView can spoof messages
- One password manager pulled their app

Built into the Browser

- Pluses
 - Better than not using a password manager
 - Never resorts to the clipboard
 - Always finds password field
- Minuses
 - Not as secure
 - Some don't generate passwords, only store them
 - Many don't consider the password policy

Chrome Browser Password Manager

As Bad as it Gets

- Autofills with no user action – Makes it easy to steal passwords
- Can't customize generated password – Might not be able to use password
- Passwords not encrypted by default
- Warns on weak passwords only after you check
- Assumes any field of type “password” holds a password
- Uses same password for smile.amazon.com and amazon.com
 - but not amazon.co.uk

It's More than Just Passwords Strength

- Autofill with no user action
 - Put the password into a form controlled by an attacker
- Storage Security
 - Stolen, didn't get the passwords but got the metadata
- User Communication
 - Inform on weak/reused passwords
 - Generated passwords sometimes weak (oMMMMMMMT?m*m)

It's More than Just the Passwords

- Phishing sites and phishing the password manager password
- Domain name errors – google.evil.com vs google.com
- Accessibility features
- Code size - one password manager is over 250,000 lines of code
 - SitePassword 1,500 lines of JavaScript, 750 HTML, 250 CSS
- jQuery on the login page
- Worst of all - Not using a password manager due to lack of trust

SitePassword Security

The Good

- Require click on password field
- Callback registered only on visible password fields
- Use iframe domain name if its password field clicked
- Use zxcvbn() from Dropbox for password strength meter
- Site name and user name act as salt to defeat pre-computation attacks
- Warn if password might still be on the clipboard

The Not So Good But for Good Reasons

- Settings in bookmarks
 - Settings not encrypted
 - Stored on disk and in Google cloud
- Site password visible by default
 - Gives you a sense of how random looking the site passwords are
 - Don't often open the popup
- 12-character passwords by default

The Ugly

An offline attack against master password

1. You create an account at a bad guy's site
 2. Bad guy knows site password and username and can guess site name
 3. Bad guy starts guessing master passwords
- Mitigations
 - Strong master password
 - Hash a minimum of 100 times to get site password
 - Multiple master passwords

War Stories

Finding the Password Field

Websites do some weird #%^@

- Put password field in an iframe with a different domain name than page
- Add password field dynamically
- Add password field with type=text and change to type=password
- Many password fields on page but only one visible
- Make password field visible only after you click a button
- Some sites add CSS at runtime that make the password field visible

Finding the Password Field

Websites do some weird #%^@

- Change contents of page based on the fragment
- Password field in a shadow root (shadow DOM)
- Clears the field after I set it (Who the %#^@ knows why)
- Don't want to update password field at sitepassword.info

Is the Password Field Visible?

Harder to figure out than you may think.

- Does `windowComputedStyle(element)` say it's visible?
 - Correct most of the time but not always
- Is parent visible?
 - `offsetParent != null` **if position != 'fixed'**
- One clickjacking trick
 - `element.style.opacity = "0"` reported visible

Finding the UserID Field

Heuristic Used by Many Password Managers

- UserID field is the one immediately before the password field
 - Except when it's not
- Sometimes to the left
 - Arabic, Hebrew to the right?
- Sometimes intervening fields
 - Some of them not visible

Crazy #%^@

Done by big companies with professional programmers

- Multiple domain names for the same login form
- Login form at a completely different domain
- Username and password fields have the same id
- A bunch of errors when the page loads
 - Took 30 seconds to time out on 4 bad GETs

How Bad Is It?

One password manager has
special cases for over 200 sites.

Summary

Future Work

- User studies
- Security review
- Other browsers
 - Works on Safari, Firefox and most Chromium browsers, e.g., Brave, Chrome, Edge
- iOS and Android apps — Monitoring security issues

References

Slides at <https://github.com/alanhkarp/SitePassword>

- Ping's 10 Principles - <http://zesty.ca/pubs/icics-2002-uidss.pdf>
- Oesch Thesis - https://trace.tennessee.edu/cgi/viewcontent.cgi?article=7785&context=utk_graddiss
- Oesch Paper - https://www.usenix.org/system/files/sec20-oesch_0.pdf
- [https://eprints.whiterose.ac.uk/158056/8/
Revisiting Security Vulnerabilities in Commercial Password Managers 2.pdf](https://eprints.whiterose.ac.uk/158056/8/Revisiting%20Security%20Vulnerabilities%20in%20Commercial%20Password%20Managers%202.pdf)
- <https://www.usenix.org/system/files/soups2019-pearman.pdf>
- <https://crypto.stanford.edu/~dabo/pubs/papers/pwdmgrBrowser.pdf>

Takeaways

- Use a password manager - a bad one is better than none at all
- Turn off any setting that fills in the password without a user action
- Prepare for the worst - Some have gone out of business
- Use it wisely - use strong passwords even if you don't have to

OR

Take control and use SitePassword

Demo

Ask the Guru

alantheguru.alanhkarp.com

Radio Symphony -... Otto Classical Pandora Friam Hangout Other Bookmarks

Ask the Guru



User name:

Password: Click SitePassword

Ask the Guru

alanthe guru.alanhkarp.com

Radio Symphony -... Otto Classical Pandora

SitePassword.info

alanthe guru.alanhkarp.com

A strong master password

Too Weak

A unique nickname for this account

Your user-id for this account

Generated site password

User name:

Password: Click SitePassword

Provide your own site password.

Clear master password on use.

Hide site password by default.

>Password is 12 characters long

Starts with letter

Requires at least 1 lowercase letter(s)

Requires at least 1 uppercase letter(s)

Requires at least 1 number(s)

Allows special characters

Download Site Data

Ask the Guru

alanthe guru.alanhkarp.com

Radio Symphony -... Otto Classical Pandora

SitePassword.info

alanthe guru.alanhkarp.com

..... Too Weak

guru

alan

to3X9g55EK8C

User name:

Password: Click SitePassword

Clear Clipboard

Provide your own site password.

Clear master password on use.

Hide site password by default.

Password is 12 characters long

Starts with letter

Requires at least 1 lowercase letter(s)

Requires at least 1 uppercase letter(s)

Requires at least 1 number(s)

Allows special characters

Download Site Data

Ask the Guru

alanthege... alanhkarp.com Radio Symphony -... Otto Classical Pandora Friam Hangout Other Bookmarks

Ask the Guru



User name:

Password: [Click here for password](#)

Ask the Guru

alanthege... alanhkarp.com Radio Symphony -... Otto Classical Pandora Friam Hangout Other Bookmarks

Ask the Guru



User name:

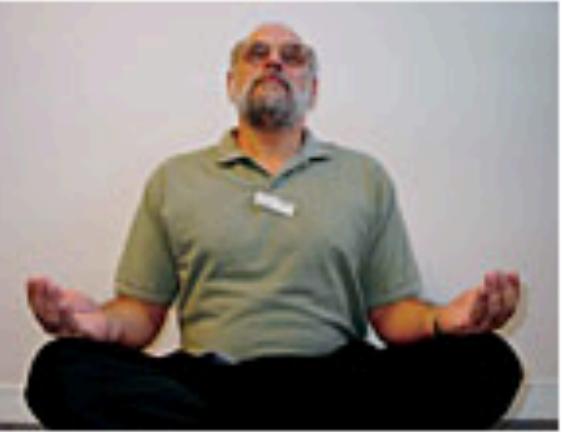
Password: [Click here for password](#)

Ask the Guru

alanthege... alanhkarp.com

Radio Symphony -... Otto Classical Pandora Friam Hangout Other Bookmarks

Ask the Guru



User name:

Password:

Ask the Guru

alanthege... alanhkarp.com Radio Symphony -... Otto Classical Pandora Friam Hangout Other Bookmarks

Ask the Guru



User name:

Password: [Click here for password](#)

Site Password

sitepassword.info

Radio Symphony -... Otto Classical Other Bookmarks

Site Password

Choose a strong master password Too Weak

Paste the login page URL here

...then, paste a SitePasswordData bookmark

...or fill in the form below.

A unique nickname for this account

Your user-id for this account

Generated site password Eye Copy

Remember Settings Forget Settings

Provide your own site password.

Code from your settings

Password is 12 characters long

Starts with letter

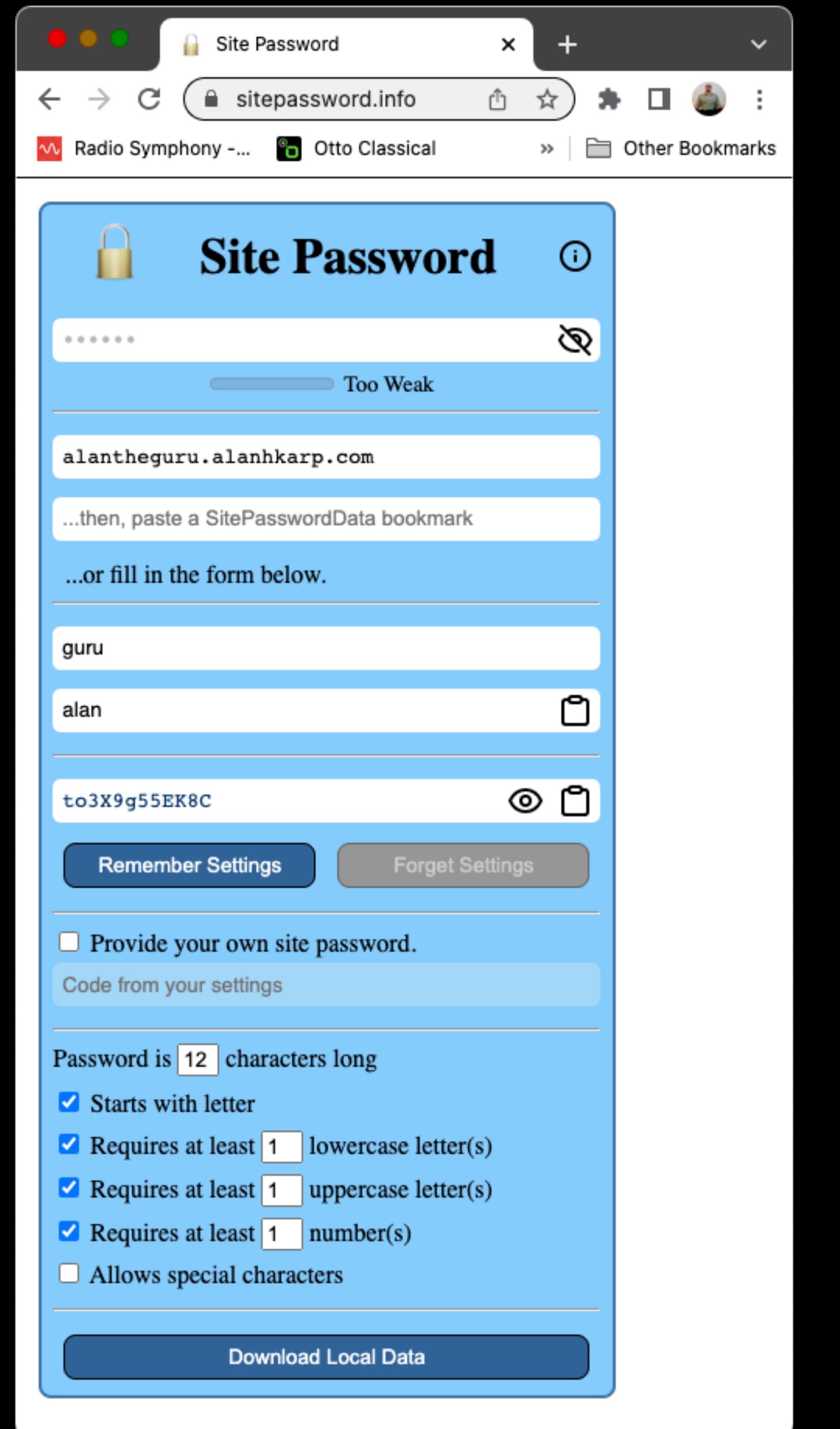
Requires at least 1 lowercase letter(s)

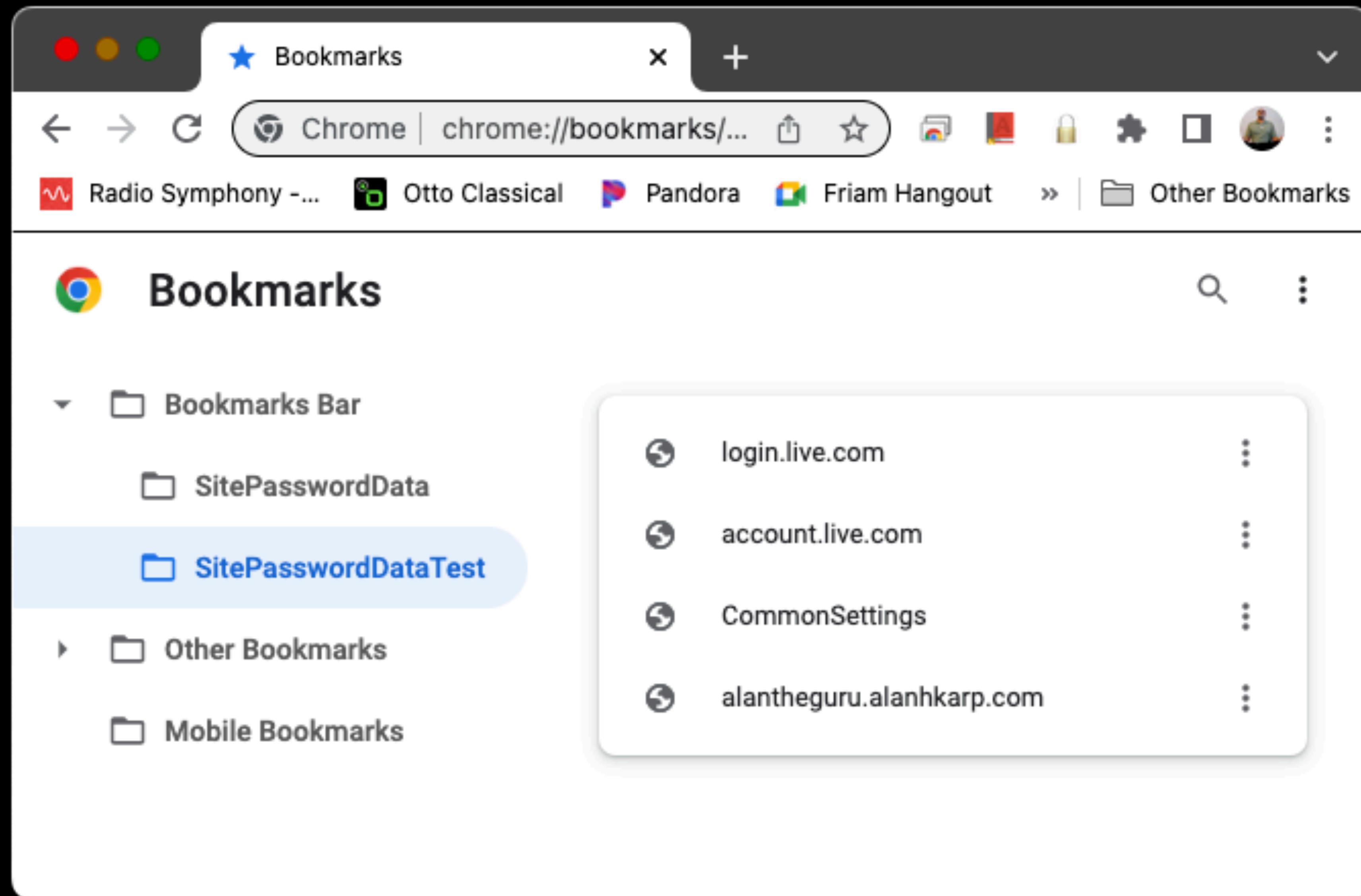
Requires at least 1 uppercase letter(s)

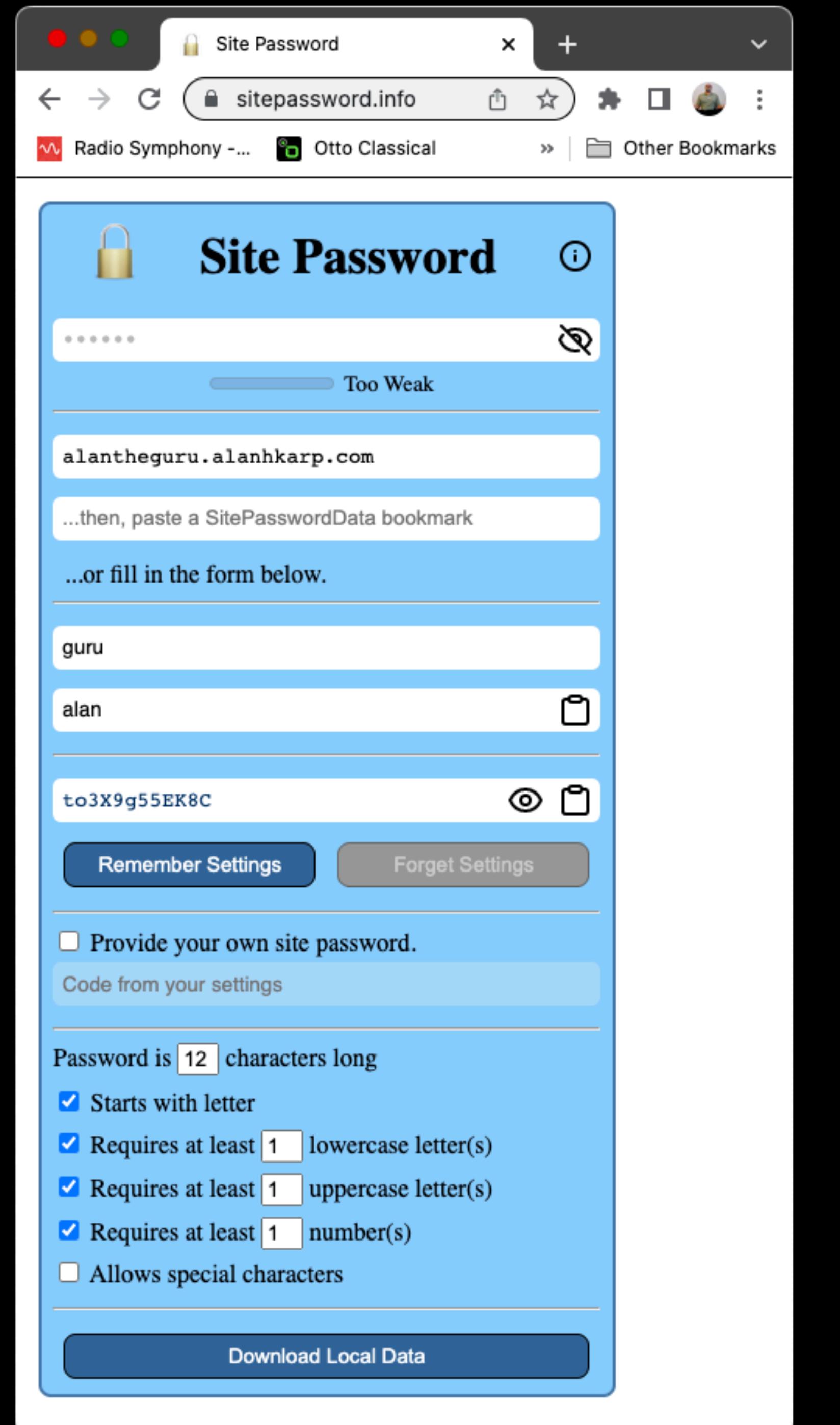
Requires at least 1 number(s)

Allows special characters

Download Local Data







Did you approve this \$1,000 pu x

mail.google.com/mail/u/0/?zx=de96ru64x1pi#label/Demo... 35 ...

Radio Symphony -... Otto Classical Pandora Friam Hangout My Personal Web... » | Other Bookmarks

Gmail label:demo X ? ⚙️ ⋮ Profile Picture

Compose ← 🔗 ! Delete Email Clock Checkmark Folder Open ⋮ < >

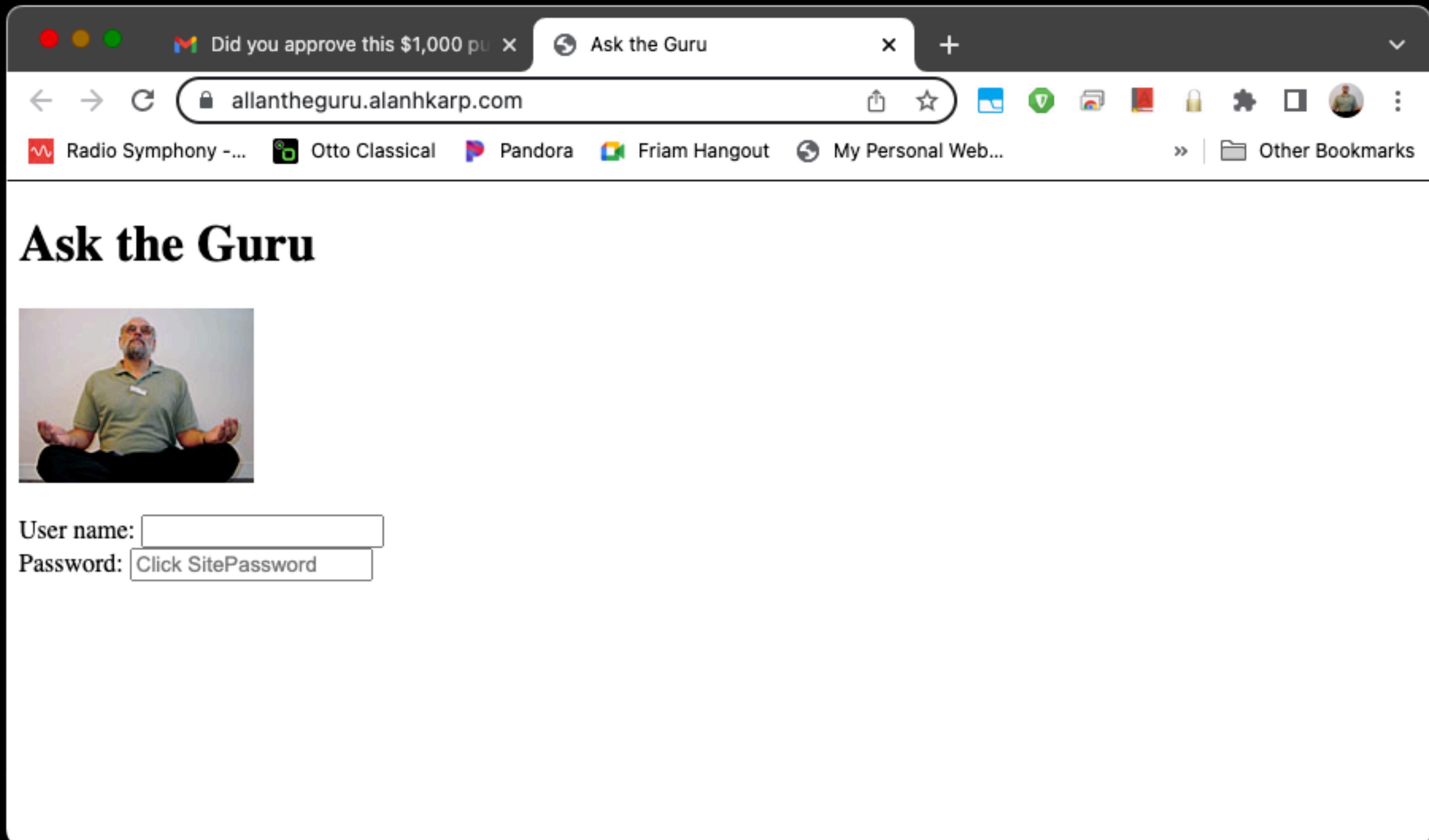
Inbox 99 Starred Snoozed Important Sent Drafts Categories More

Labels + Best Buy C.A.R.

Did you approve this \$1,000 purchase?
Alan Karp <alanhkarp@gmail.com> Nov 11, 2022, 2:02PM Star Reply Forward

to me ▾
Log into <https://alantheguru.alanhkarp.com> if you did not place this order.

Alan Karp

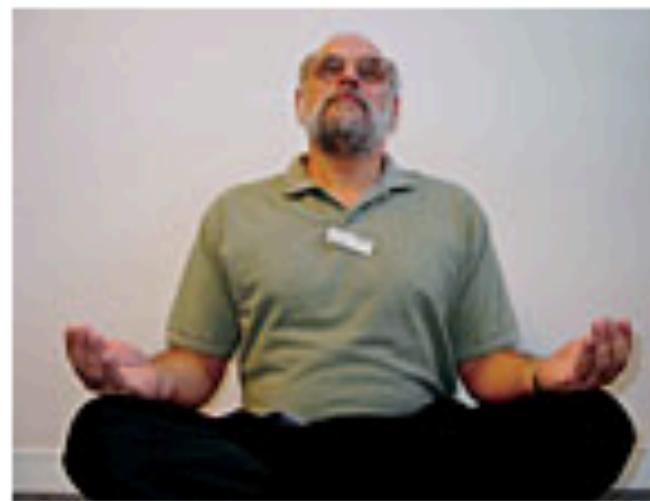


Did you approve this \$1,000 pu X Ask the Guru

◀ ▶ C allanthe guru.alanhkarp.com

Radio Symphony -... Otto Classical Pandora Friam Han

Ask the Guru



User name:

Password: Click SitePassword

SitePassword.info

allanthe guru.alanhkarp.com

.....

Too Weak

guru

Your user-id for this account

Generated site password

Warning: You may be at a fake site that is trying to steal your password. You previously used this nickname for
alanthe guru.alanhkarp.com
but the domain name asking for your password is
alanthe guru.alanhkarp.com
It is common to see different domain names for the same account login. Click the top (green) button if that's not the case or the middle (red) button if it is. You can also pick a new nickname if this page is for a different account.

Get me to safety!

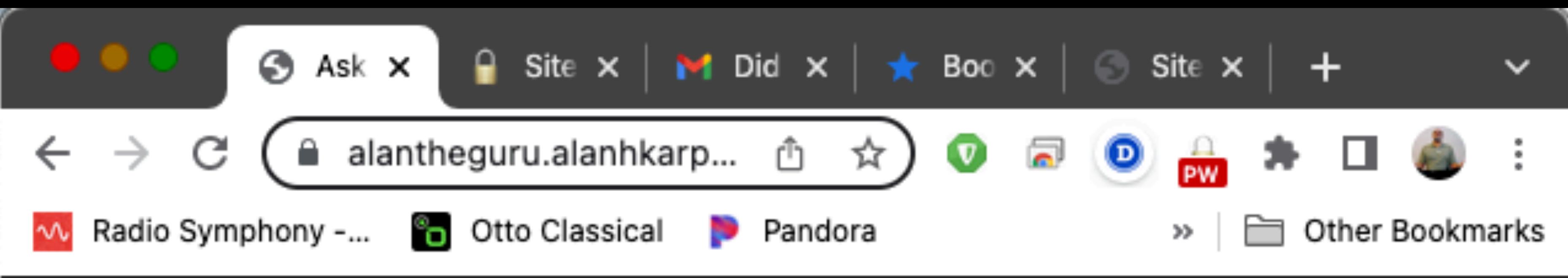
This page is for the same account.

Other Bookmarks

Screenshot of a web browser window showing SiteData.html. The browser has a dark theme with a light gray header bar. The title bar says "SiteData.html". The address bar shows the file path "/Users/alan/Downloads/SiteData.html". Below the address bar is a toolbar with various icons for file operations and bookmarks.

The main content area displays a table of site data:

Site Name	Domain Name	User Name	Password Length	Start with Letter	Allow Lower	Min Lower	Allow Upper	Min Upper	Allow Numbers	Min Numbers	Allow Specials	Min Specials	Specials
Guru	alantheguru.alanhkarp.com	Alan	12	true	true	1	true	1	true	1	false	0	/!=@?._-
microsoft login.live.com		alanhkarp@outlook.com	12	true	true	1	true	1	true	1	false	0	/!=@?._-
microsoft account.live.com		alanhkarp@outlook.com	12	true	true	1	true	1	true	1	false	0	/!=@?._-



Ask the Guru



User name:

Password:

[Click here for password](#)

Backup Slides

The Evil Coffee Shop Attack

Autofill with no user action

1. The user sets up several sites with a password manager.
2. User connects to a rogue router in a coffee shop.

The attacker can inject, block, and change network packets.

3. Attacker directs user's browser to a vulnerable page at the target site.
4. Attacker injects login form into the vulnerable page by modifying packets.
5. Your password manager fills it in.
6. Repeats for another site with a vulnerable page.

How to Inject a Password Field

- HTTP login page - submits forms with HTTPS
 - Doesn't happen much now but (Schwab, eBay)
- Broken HTTPS
 - Usually an expired certificate (HP)
- HTTPS with active content fetched over HTTP
- XSS (Cross Site Scripting) on any page at the victim site
- Unnecessary dependencies
 - Many use jQuery on their login pages