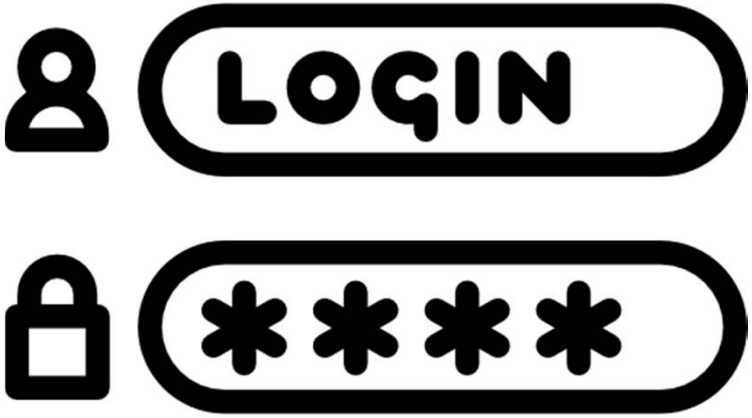
smarthouse | adesso financial solutions

Sicherer Austausch von Credentials

Ein Erfahrungsbericht

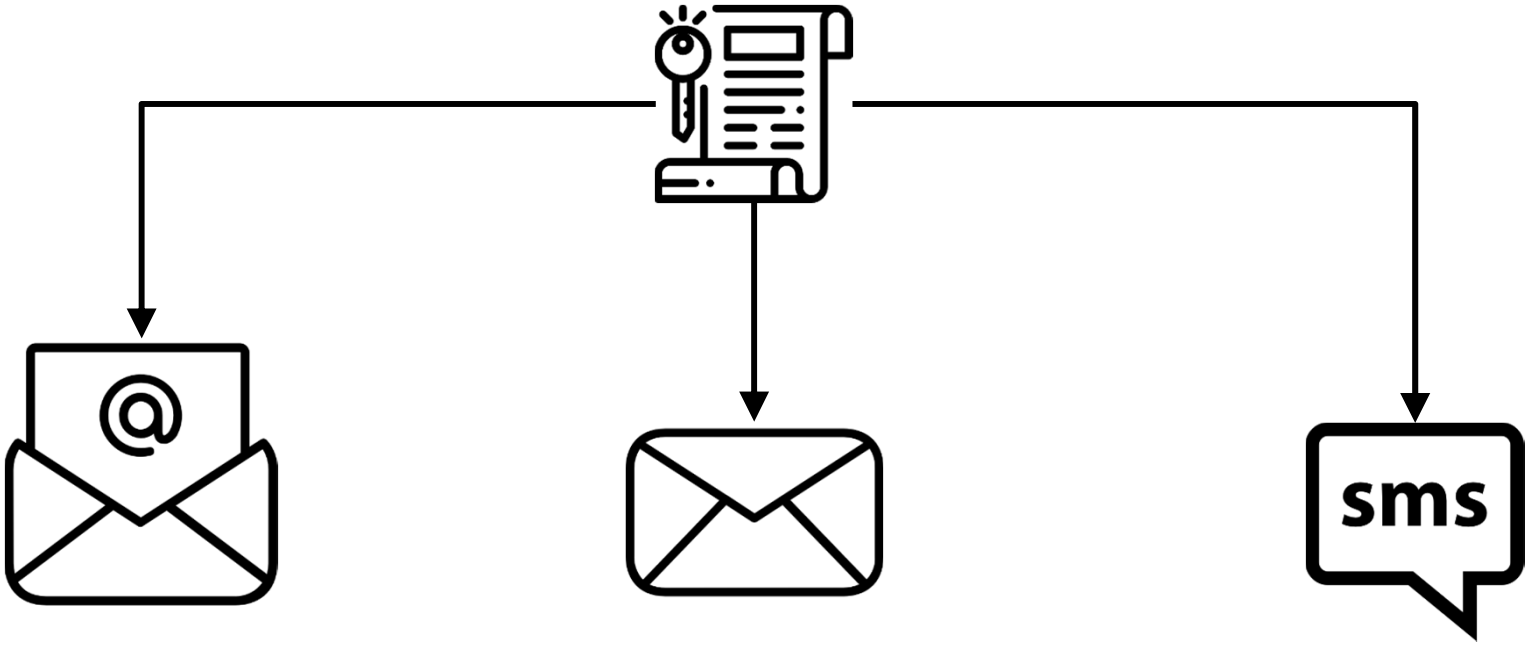
20.06.2018 Ives Laaf / Leonard Schönborn Karlsruher Entwicklertag 2018

Credential-Austausch



Login Password designed by Freepik from Flaticon

Gängige Methoden und Probleme



Mails designed by Good Ware / Speechbubble designed by Alfredo Hernandez / Keyword designed by Freepik from Flaticon

PasswordPusher – Die Lösung?

smarthouse | adesso financial solutions

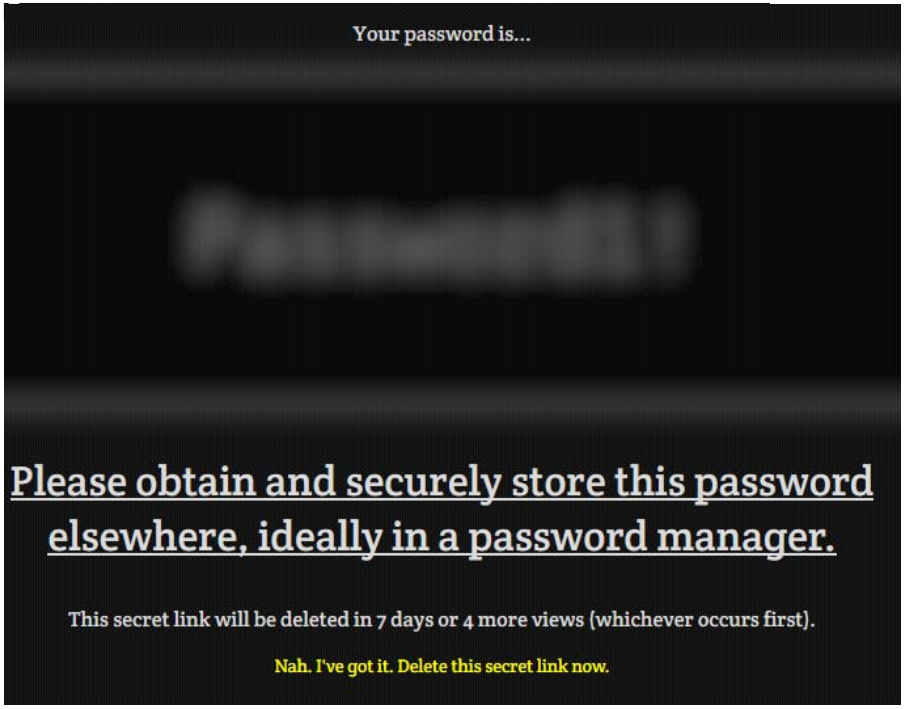
created by Peter Giacomo Lombardo

PasswordPusher – Die Lösung?

smarthouse | adesso financial solutions

User Experience

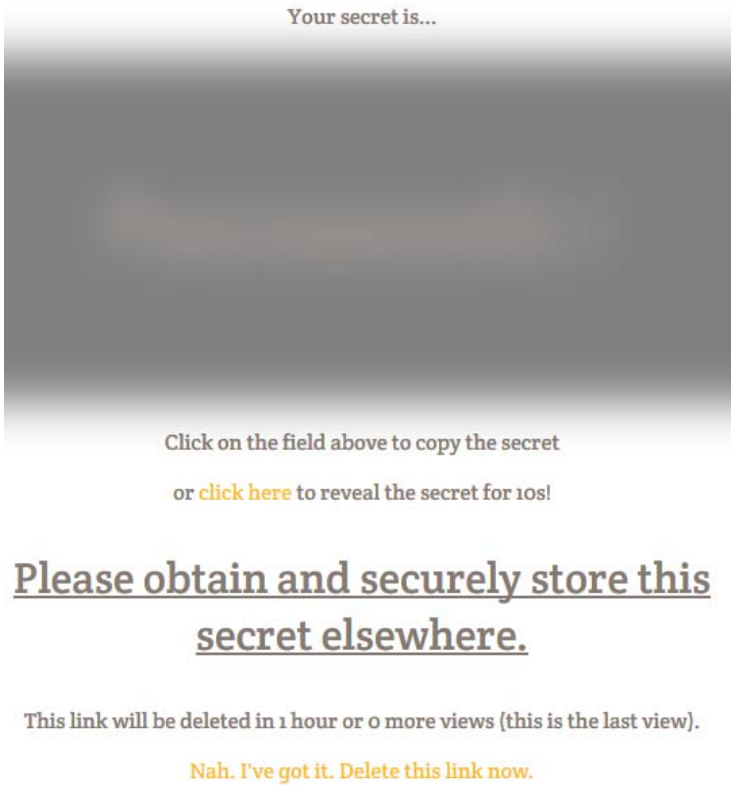
smarthouse | adesso financial solutions



smarthouse | adesso financial solutions

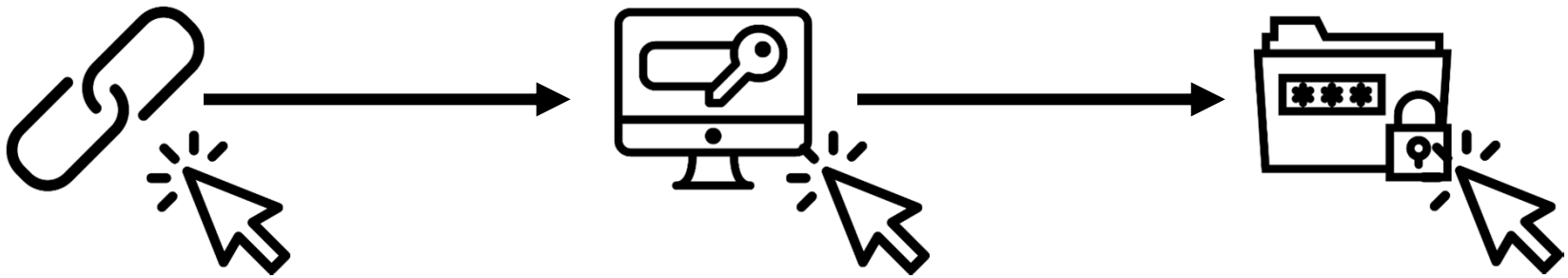
User Experience: Secure-by-default

smarthouse | adesso financial solutions



User Experience: Easy-2-Use

smarthouse | adesso financial solutions



Link designed by Gregor Cresnar / Cursor designed by Freepik / Password designed by Those Icons / Folder designed by Nikita Golubev from Flaticon

smarthouse | adesso financial solutions

Security Header

smarthouse | adesso financial solutions

Scan Summary

B

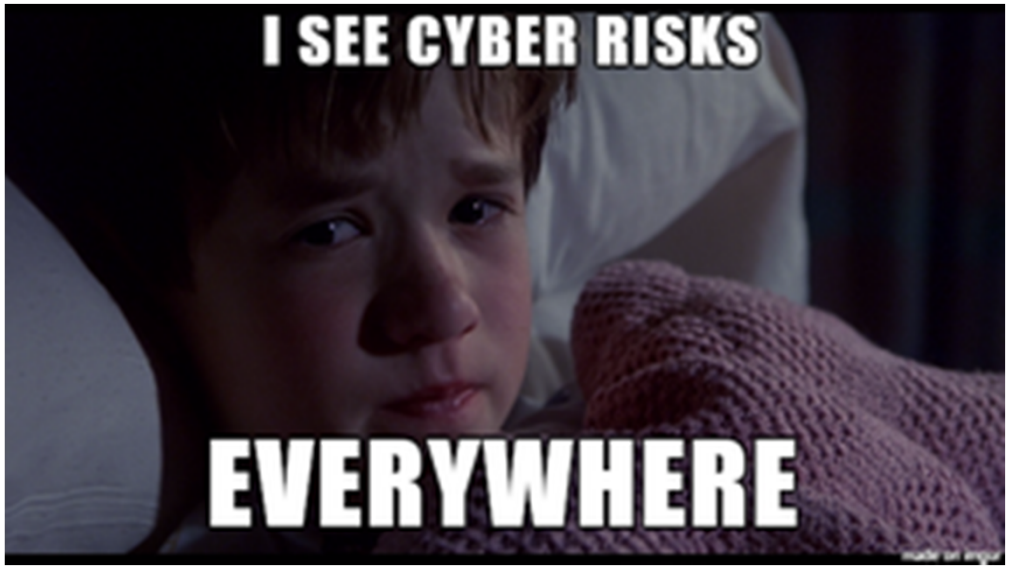
Host:	pwpush.com
Scan ID #:	7709838
Start Time:	June 19, 2018 1:14 PM
Duration:	4 seconds
Score:	75/100
Tests Passed:	10/11

Test Scores

Test	Pass	Score	Explanation
Content Security Policy	✖	-25	Content Security Policy (CSP) header not implemented
Cookies	✔	0	All cookies use the `Secure` flag and all session cookies use the `HttpOnly` flag
Cross-origin Resource Sharing	✔	0	Content is not visible via cross-origin resource sharing (CORS) files or headers
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)
HTTP Strict Transport Security	✔	0	HTTP Strict Transport Security (HSTS) header set to a minimum of six months (15768000)
Redirection	✔	0	Initial redirection is to HTTPS on same host, final destination is HTTPS
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)
Subresource Integrity	–	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin
X-Content-Type-Options	✔	0	X-Content-Type-Options header set to `"nosniff"`
X-Frame-Options	✔	0	X-Frame-Options (XFO) header set to `SAMEORIGIN` or `DENY`
X-XSS-Protection	✔	0	X-XSS-Protection header set to `"1; mode=block"`

Adding a CSP

smarthouse | adesso financial solutions



Scene from The Sixth Sense

Unser Ergebnis

smarthouse | adesso financial solutions

Scan Summary

A+

Host:	secpush.smarthouse.de
Scan ID #:	7709145 (unlisted)
Start Time:	June 19, 2018 10:25 AM
Duration:	9 seconds
Score:	130/100
Tests Passed:	11/11

Test Scores

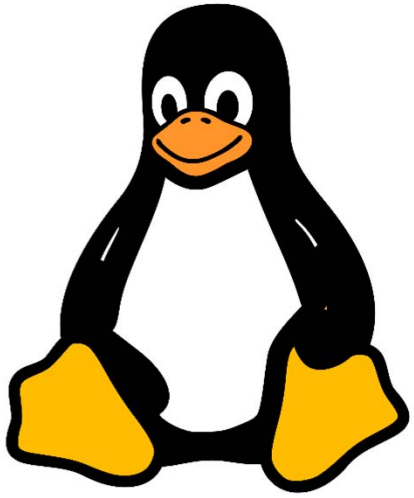
Test	Pass	Score	Explanation
Content Security Policy	✔	+10	Content Security Policy (CSP) implemented with `default-src 'none'` and no `'unsafe'`
Cookies	✔	+5	All cookies use the `Secure` flag, session cookies use the `HttpOnly` flag, and cross-origin restrictions are in place via the `SameSite` flag
Cross-origin Resource Sharing	✔	0	Content is not visible via cross-origin resource sharing (CORS) files or headers
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)
HTTP Strict Transport Security	✔	+5	Preloaded via the HTTP Strict Transport Security (HSTS) preloading process
Redirection	✔	0	Not able to connect via HTTP, so no redirection necessary
Referrer Policy	✔	+5	Referrer-Policy header set to `"no-referrer"`, `"same-origin"`, `"strict-origin"` or `"strict-origin-when-cross-origin"`
Subresource Integrity	–	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin
X-Content-Type-Options	✔	0	X-Content-Type-Options header set to `"nosniff"`
X-Frame-Options	✔	+5	X-Frame-Options (XFO) implemented via the CSP `frame-ancestors` directive
X-XSS-Protection	✔	0	X-XSS-Protection header set to `"1; mode=block"`

Datenverwaltung

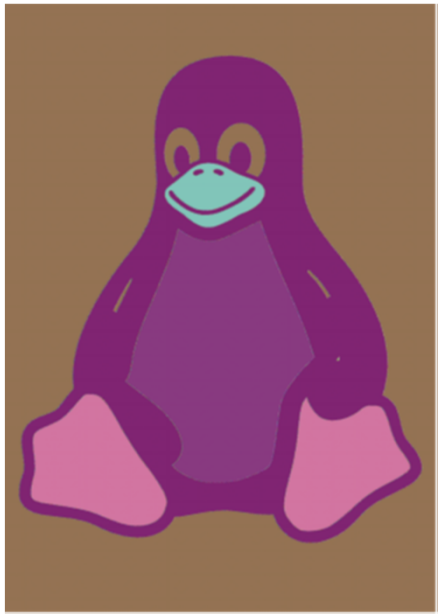
smarthouse | adesso financial solutions

Keyword designed by Freepik / Lock designed by turkkub / Database designed by Smashicons from Flaticon

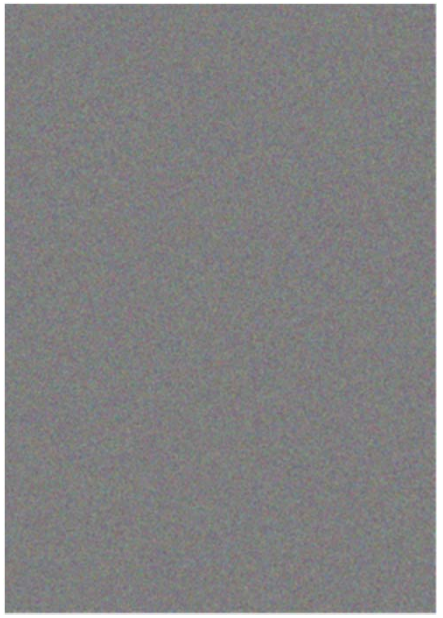
smarthouse | adesso financial solutions



Original



Deterministisch



Probabilistisch

Datenverwaltung: Forgetting your Secret

smarthouse | adesso financial solutions

Scene from Men in Black

smarthouse | adesso financial solutions

Evaluation	?
User Experience	?
Updating	?
Security Header	?
Datenverwaltung	?
Sonstiges	?
Total	**?**

smarthouse | adesso financial solutions

Evaluation	~5h
User Experience	~15h
Updating	~16h
Security Header	~8h
Datenverwaltung	~9h
Sonstiges	~15h
Total	**~68h / ~8.5 Arbeitsage**

smarthouse | adesso financial solutions

Vielen Dank!

https://github.com/smarthouse/PasswordPusher/