

The background image shows a panoramic view of a city skyline at night, likely New York City. The Empire State Building is prominently featured in the center, its Art Deco spire reaching towards a dark, cloudy sky. Other recognizable buildings like the Chrysler Building with its distinctive Art Deco spire are visible to the left. The city lights reflect off the water in the foreground.

MEET MAGENTO NEW YORK

Recent Magento security issues

!=

Magento issues

<https://tale.sh/mm22nyc>



Your code is secure, but what about everything else?

Talesh Seeparsan | Security Consultant



Problem 1: Human beings



Problem 4: Human beings



Problem 1: Human beings



**Who has access?
What do they have access to?**





Welcome, please sign in

* Username

* Password

[Forgot your password?](#)

[Sign in](#)

Past employees?



New employees?

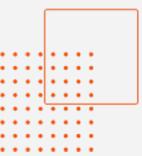


External resources?



A photograph showing two people from behind, sitting on a couch. The person on the left is wearing a bright green t-shirt and has curly hair. The person on the right is wearing a dark-colored shirt. They are both looking at a laptop screen which is visible in the foreground. The background shows a window with a view of a building and a lamp post outside.

Module support?



**Who has access?
What do they have access to?**



NEW YORK US

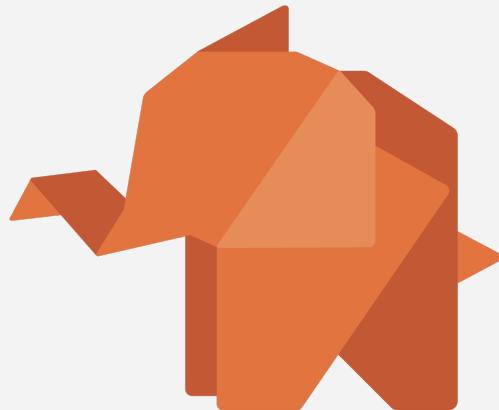
Meet Magento™
#MM22NYC



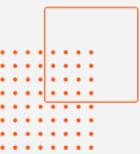


GitHub





Satis



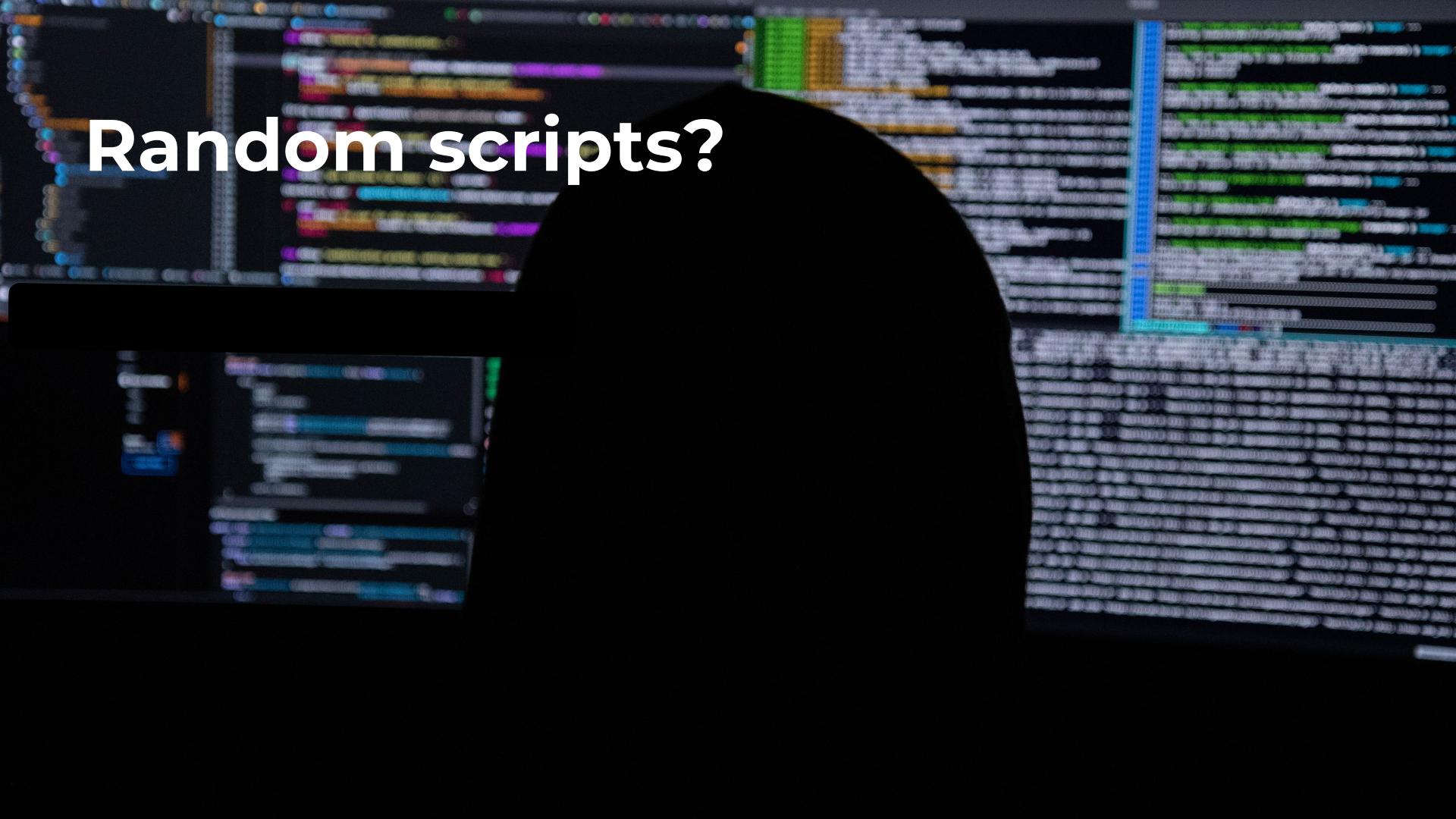
SSH Keys?

```
l@T490s
OS: Debian GNU/Linux bookworm/sid
Host: 20NY000JNZ.ThinkPad.TW
Kernel: 5.15.0-2-amd64
Uptime: 6 days, 34 mins
Packages: 2887 (dpkg)
Shell: zsh 5.8
Resolution: 2560x1440
DE: GNOME 3.38.6
WM: Mutter
WM Theme: Materia-dark-compact
Theme: Materia-dark-compact (GNOME)
Icons: Papirus-Dark (GTK2/3)
Terminal: tilix
CPU: Intel i7-8565U (8) @ 4.60GHz
GPU: Intel WhiskeyLake-U GT2 (HMD Graphics) (0)
Memory: 5025MiB / 7641MiB
```

Admin APIs?*



Random scripts?





HashiCorp
Terraform



ANSIBLE



CHEF™



puppet

A close-up, low-angle shot of the rear side of a silver Uber car at night. The word "Uber" is prominently displayed in white on the dark roof. The car's body is mostly in shadow, with highlights from streetlights reflecting off the windows and door. In the background, the blurred lights of other vehicles are visible.

Uber

Uber Hack

Passwordless?



Problem 2: Access Control





Magento Admin

[← Back](#) [Delete Role](#) [Reset](#)

ROLE INFORMATION

Role Info

Role Resources

Role Users

Roles Resources

Resource Access

Custom

Resources

- Dashboard
- Analytics
- API
- Custom Menu
 - Create
 - Delete
- Sales
- Catalog
- Customers
- Carts
- My Account
- Marketing
- Content
- Reports
- Stores
- System
 - Data Transfer
 - Import
 - Export
 - Import/Export Tax Rates
 - Import History
 - Magento Connect
 - Connect Manager
 - Package Extensions
 - System Extensions

**Who has access?
What do they have access to?**





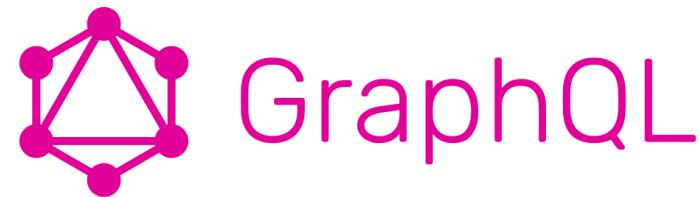
Sloppy tutorials

Browser?



APIs?





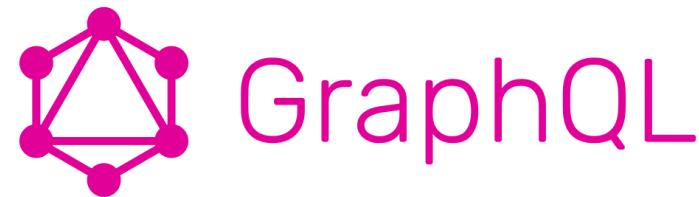
GraphQL Authorization

[Edit on GitHub](#)[Log an Issue](#)

Adobe Commerce and Magento Open Source provide two mechanisms for authorizing GraphQL calls:

- **Authorization tokens.** Commerce generates a JSON Web Token (JWT), a set of cryptographically signed credentials. All calls that perform an action on behalf of a logged-in customer or admin provide an authorization token. Authorization tokens are stateless. Commerce does not need to know the state of a client to execute a request—the token contains all of the information needed for authorization and authentication.
- **Session cookies.** A session cookie is information generated by Commerce that is stored in the client's browser. It contains details about the session, including the time period the user can access resources. Cookies are stateful, thereby increasing complexity and possibly latency.

Adobe recommends that you use authorization tokens instead of session cookies for GraphQL requests. By default, session cookies are enabled. As of Commerce 2.4.5, you can disable session cookies, eliminating the chances of encountering problems caused by the differences between the two authorization methods. However, merchants with existing implementations that rely on cookies can continue using this method. [Session cookies](#) describes how to enable or disable cookies for GraphQL.



Guest user API access





Sloppy tutorials

Guest user API access



Layered Defense aka Swiss Cheese model



Principle of Least Access



Problem 3: Supply Chain





Sansec
@sansecio

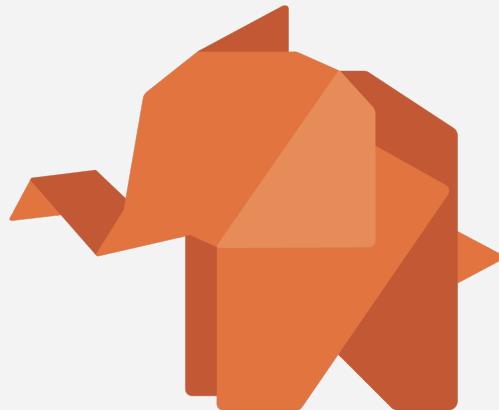
...

Fishpig, a vendor of popular Magento/Wordpress modules, has been breached. The [#Rekoobe](#) Linux trojan was found in paid extensions and on its licensing server.

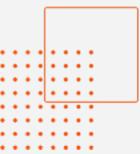
Magento store owners should disable any paid Fishpig software and run a malware scan.

sansec.io/research/rekoo...





Satis



Tempting targets





kubernetes



HashiCorp

Vault

Principle of Least Access



LastPass ••• |



Problem 4: Human beings



Weak passwords not a problem



A collection of various metal keys, including standard notched profile keys and some with notched heads, are scattered across a dark, solid-colored surface. The keys are silver-colored and vary in size and shape.

Duplicated passwords

Weak passwords not a problem



Recent Magento security issues

!=

Magento issues

Weak passwords not a problem



MFA isn't a perfect solution



A close-up, low-angle shot of the rear side of a silver Uber car at night. The word "Uber" is prominently displayed in white on the dark roof. The license plate area also has "Uber" printed on it. The background is dark, showing other blurred lights of a city street.

Uber

Uber Hack

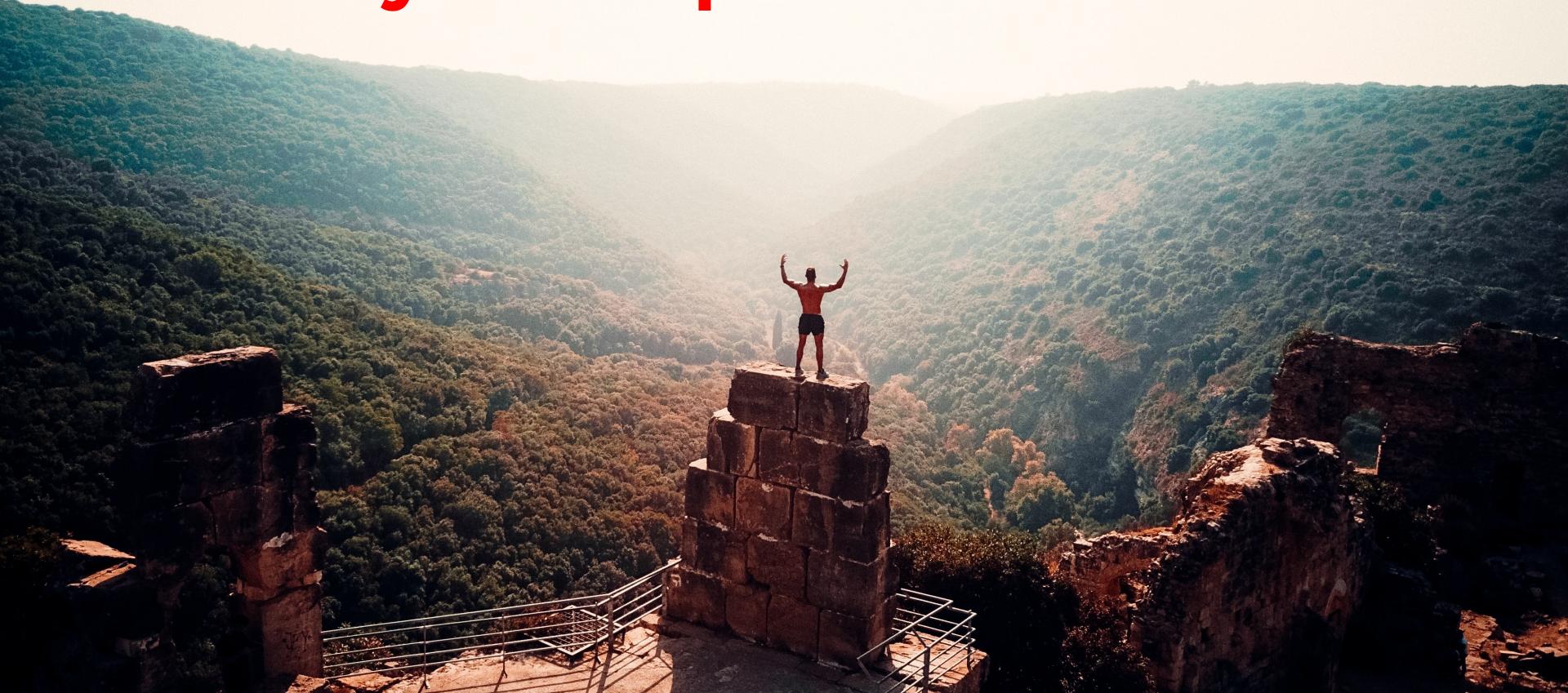
Human beings are the problem



Recurring training

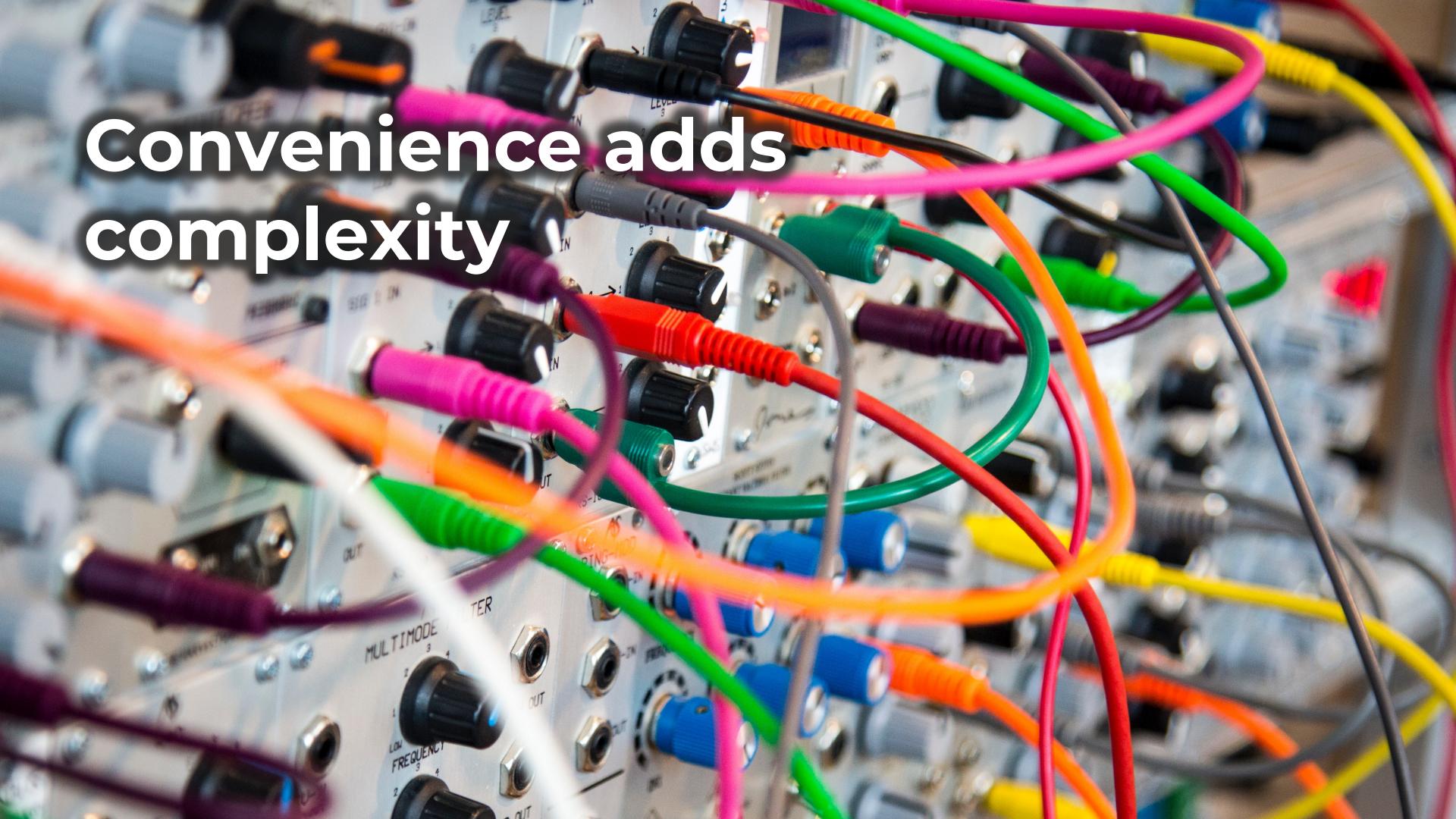


Security Champion



Security Bouncer

more

A close-up photograph of a modular synthesizer. The image shows several silver metal modules with various knobs, switches, and ports. Numerous colorful patch cables (in shades of pink, green, red, orange, yellow, and black) are plugged into the modules, creating a complex web of connections. The modules have labels like "LEVEL", "IN", "OUT", "MULTIMODE", and "CUTTER".

Convenience adds
complexity

Security implications



Security Bouncer

more

Problem 1: Human beings



Problem 2: Access Control



Problem 3: Supply Chain



Problem 4: Human beings





Talesh Seeparsan

<https://tale.sh/mm22nyc>



@_Talesh



talesh@bit79.ca

