
MEET MAGENTO NEW YORK

Recent Magento security issues

!=

Magento issues

https://tale.sh/mm22nyc

NEW YORK US
Meet Magento™
#MM22NYC

Your code is secure, but what about everything else?

Talesh Seeparsan | Security Consultant

Bit79

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?
2
EXIT

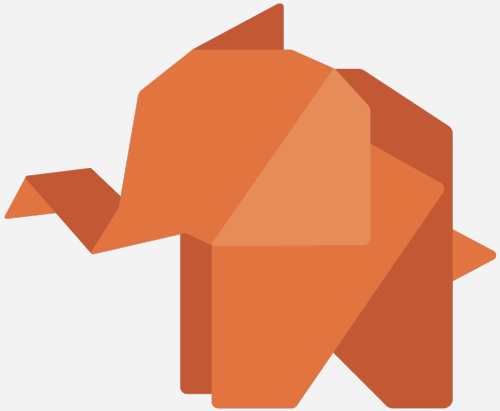
New employees?

External resources?

Module support?

Who has access?
What do they have access to?

GitHub



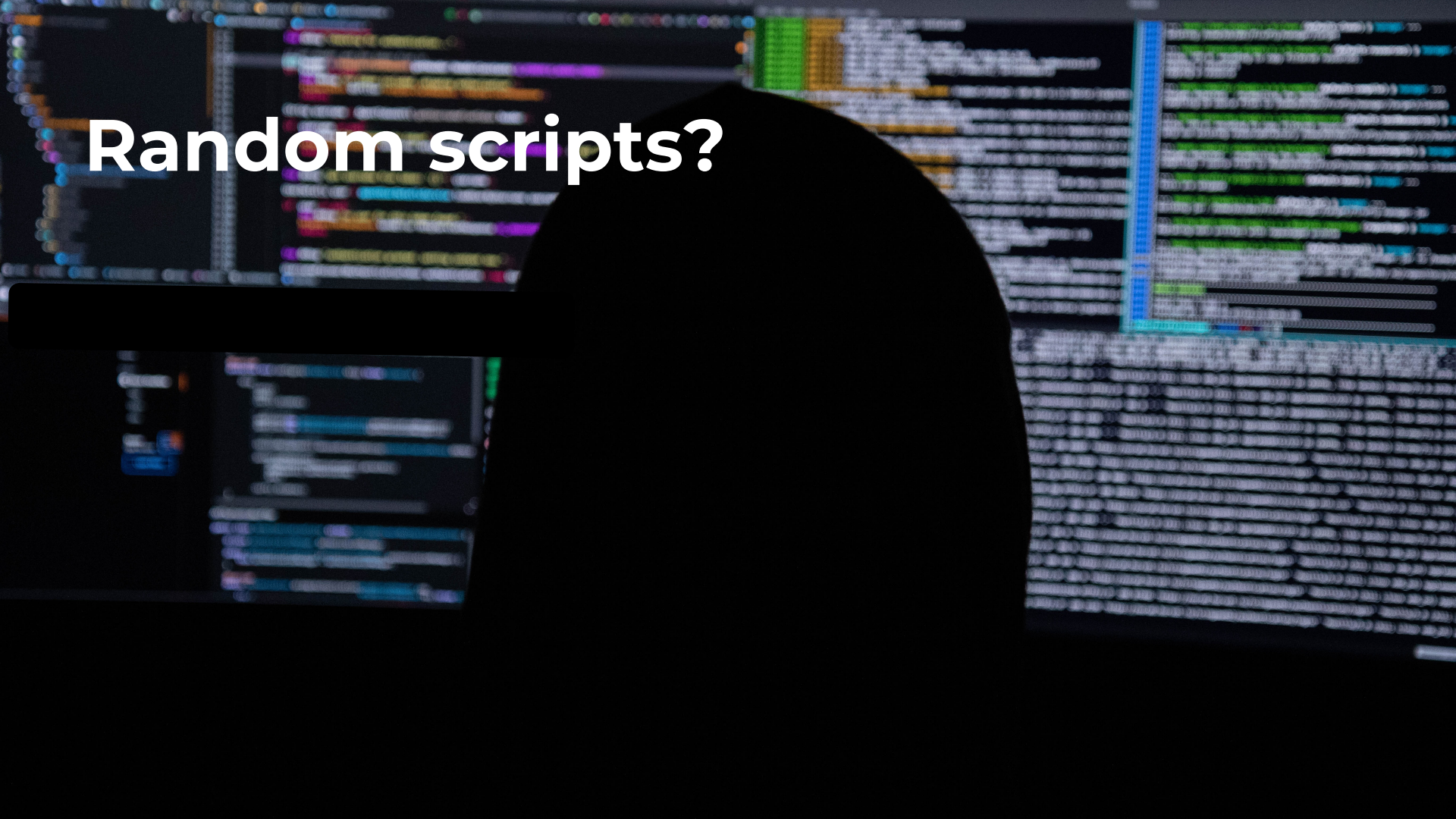
Satis

JFrog

SSH Keys?


lh@T490s
OS: Debian GNU/Linux
Host: 20NY000JMZ ThinkPad
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 [GTK2/3]
Icons: Papirus-Dark [GTK2/3]
Terminal: tilix
CPU: Intel i7-8565U (8) @ 4.600GHz
GPU: Intel WhiskeyLake-U GT2 [UHD Graphics 620]
Memory: 5025MiB / 7641MiB


Admin APIs?*


Random scripts?

HashiCorp
Terraform

ANSIBLE

CHEF™

puppet


Uber Hack
Uber

Passwordless?


Problem 2: Access Control

Magento Admin

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

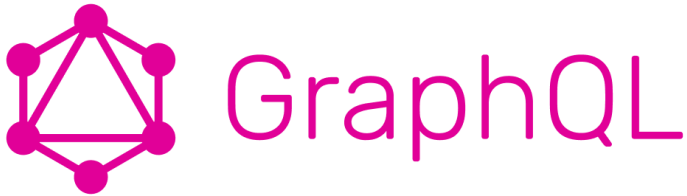
Who has access?
What do they have access to?


Sloppy tutorials

Browser?


APIs?


REST
API


GraphQL

GraphQL Authorization

Edit on GitHub Log an Issue

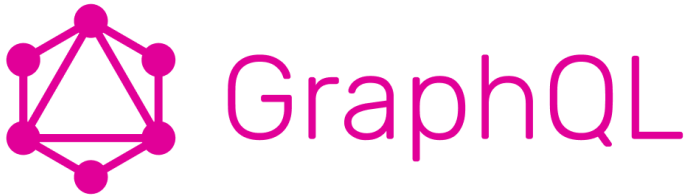
Adobe Commerce and Magento Open Source provide two mechanisms for authorizing GraphQL calls:

- **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.


REST
API


GraphQL

Guest user API access


Sloppy tutorials

Guest user API access

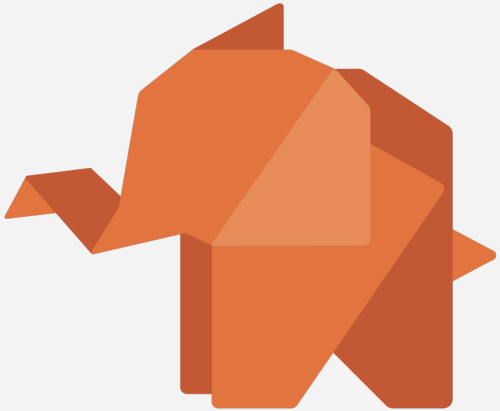

Layered Defense
aka Swiss Cheese model

Principle of Least Access


Problem 3: Supply Chain
EVERGREEN
CMA CGM
PA TRIUMPH
ZP BISON
VALLETTA

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

JFrog

Tempting targets

kubernetes

HashiCorp
Vault

Principle of Least Access


LastPass

Problem 4: Human beings

Weak passwords not a problem


Duplicated passwords

Weak passwords not a problem

Recent Magento security issues

!=

Magento issues

Weak passwords not a problem

MFA isn’t a perfect solution

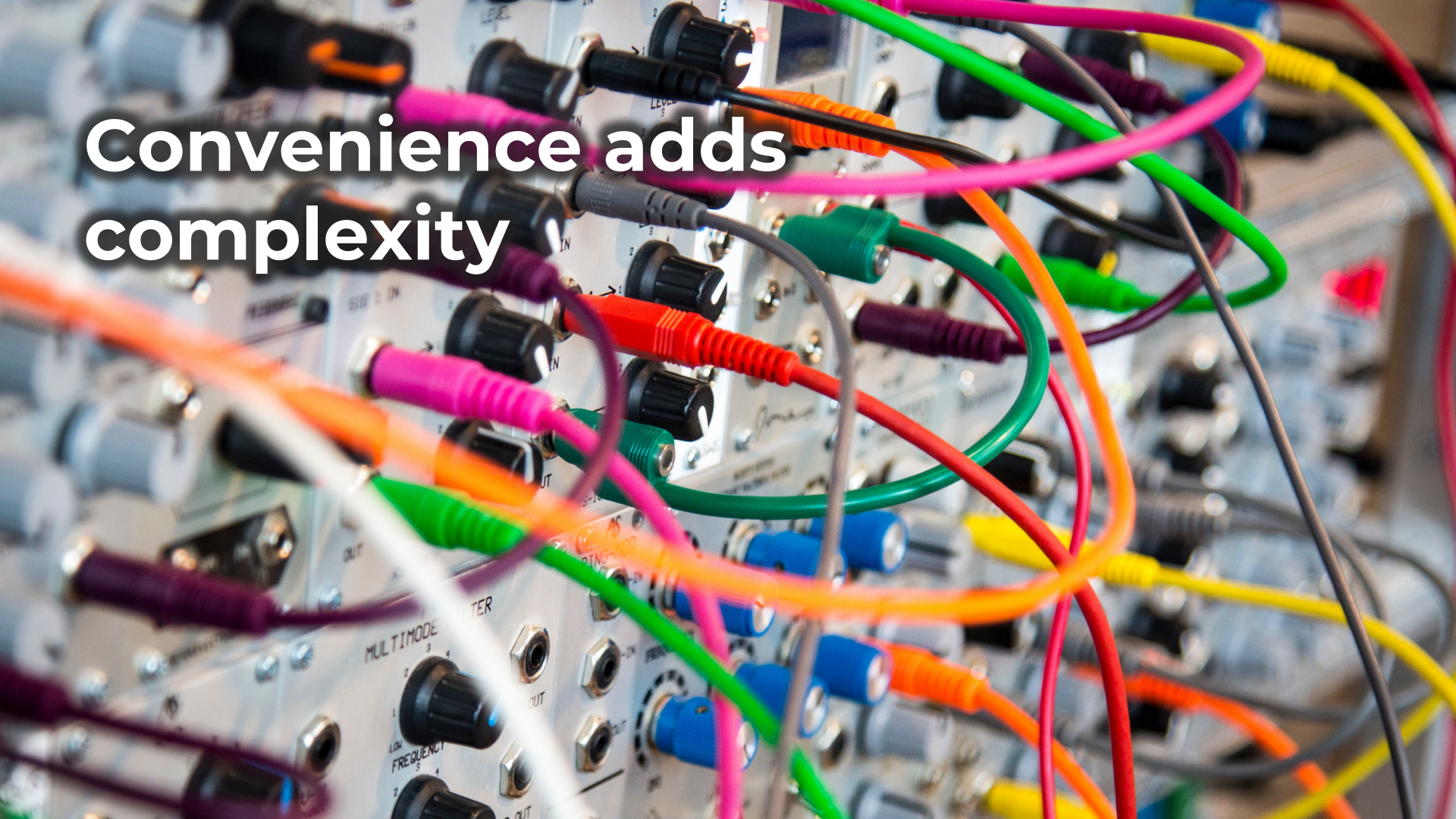

Uber Hack
Uber


Human beings are the problem


Recurring training

Security Champion


Security Bouncer
nope.


Convenience adds complexity

Security implications


Security Bouncer
nope.

Problem 1: Human beings


Problem 2: Access Control


Problem 3: Supply Chain
EVERGREEN
CMA CGM
PA TRIUMPH
ZP BISON
VALLETTA

Problem 4: Human beings

Talesh Seeparsan

https://tale.sh/mm22nyc

@_Talesh

talesh@bit79.ca