WOW SUCH PCI COMPLIANCE

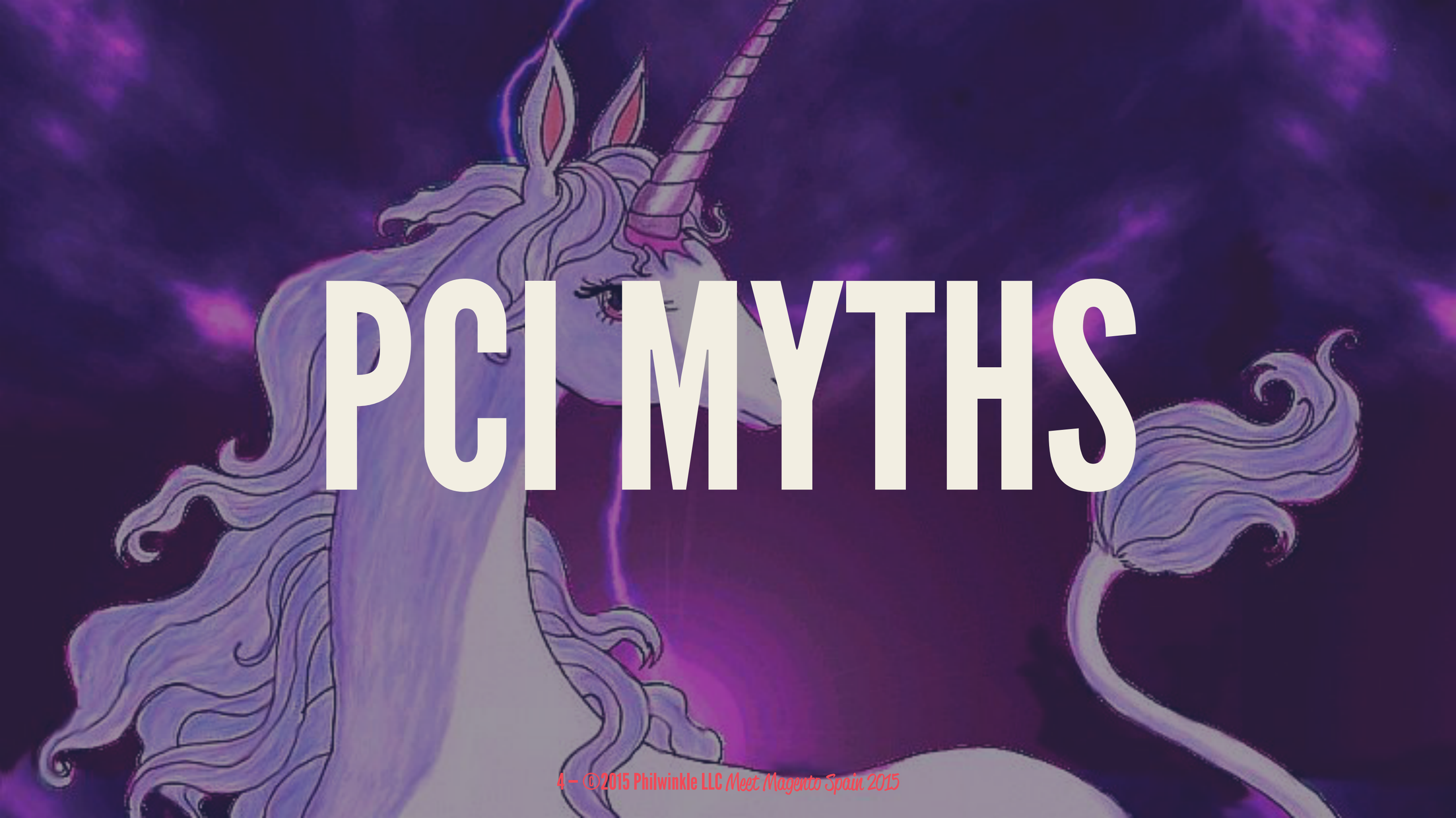
Very card, wow security wow

PHILLIP JACKSON
LEAD MAGENTO ARCHITECT, SOMETHING DIGITAL

@PHILWINKLE

GITHUB.COM/PHILWINKLE

@MAGETALK


PCI MYTHS

1. IF I don't store CREDIT CARDS PCI doesn't apply


FALSE

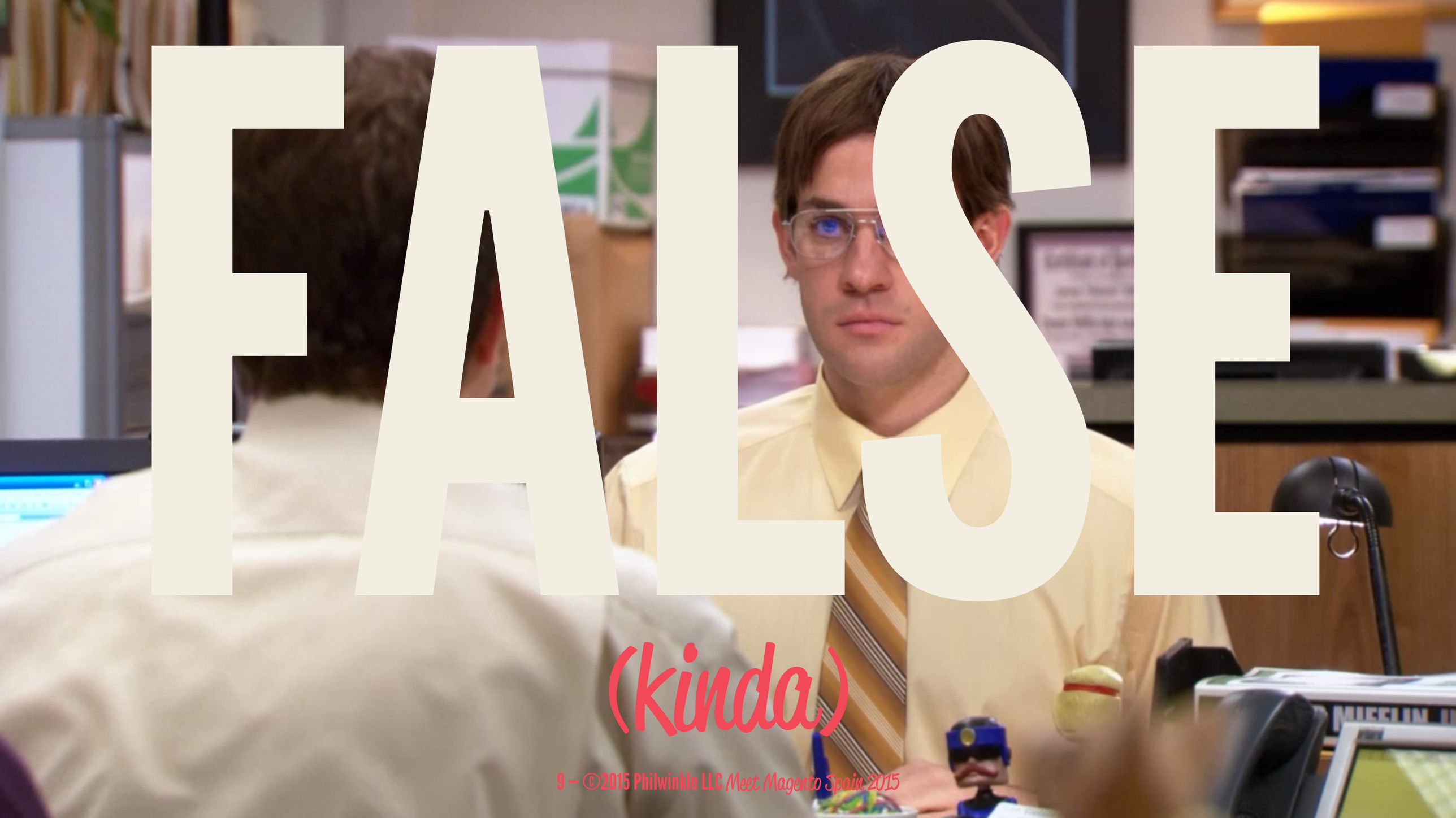
The only way to avoid PCI compliance is to transfer the risk entirely to someone else … where credit card information never traverses your own servers[1]

-- Focus on PCI

[1] http://www.focusonpci.com/site/index.php/articles/pci-misconceptions.html

2. MAGENTO IS PCI COMPLIANT, SO THEREFORE

I'm PCI compliant


FALSE
(kinda)

MAGENTO IS PCI DSS COMPLIANT ONLY WHEN USED IN CONJUCTION WITH SECURE PAYMENT BRIDGE[2]

[2] http://magento.com/resources/pci

WHY ISN'T MAGENTO ITSELF PCI COMPLIANT?

- Magento is monolithic
- Swift update deployment
- Limit the scope of feature impact
- $$$$

3. I AM IN THE EU/AUS/ ANTARCTICA AND I DON'T NEED TO ABIDE BY PCI

FALSE

YOU CAN'T UN-HACK YOUR SITE

HOW LONG UNTIL A DEFAULT MAGENTO CE 1.9.0.0 IS *hacked*?

18 MINUTES

Report.com

About Contact Sign

N ALL

.165.79.121

emo.magentocommerce.com

ve your site list.

et notified about new vulnerabilities.

Register using Byte

Register using Github

Register using Google

Register using LinkedIn

HYPERNODE by byte

nt to you by Hypernode: The advanced Magento
nosting platform from the experts at Byte

Shop URL (e.g. "myshop.com")

SCAN

RISK LEVEL: HIGH for **54.165.79.121**

RE

Security patch 6788 (secrets leak) — **not installed**

Risk rating — **Medium**

Patch SUPEE-6788 fixes multiple issues: in some cases hackers can steal your passwords and customer data. Released October 27th, 2015

Patch not detected *or* your registration form is broken.

Security patch 6482 (XSS) — **not insta**

Risk rating — **Med**

Patch SUPEE-6482 fixes a leak where hackers can take control c customer's sessions in the Enterprise edition and some smaller security risks in the Community edition. Released Aug 4th, 2015

This patch was not detected, you are vulnerable.

How do I fix it?.

GuruInc Javascript Hack? — **safe**

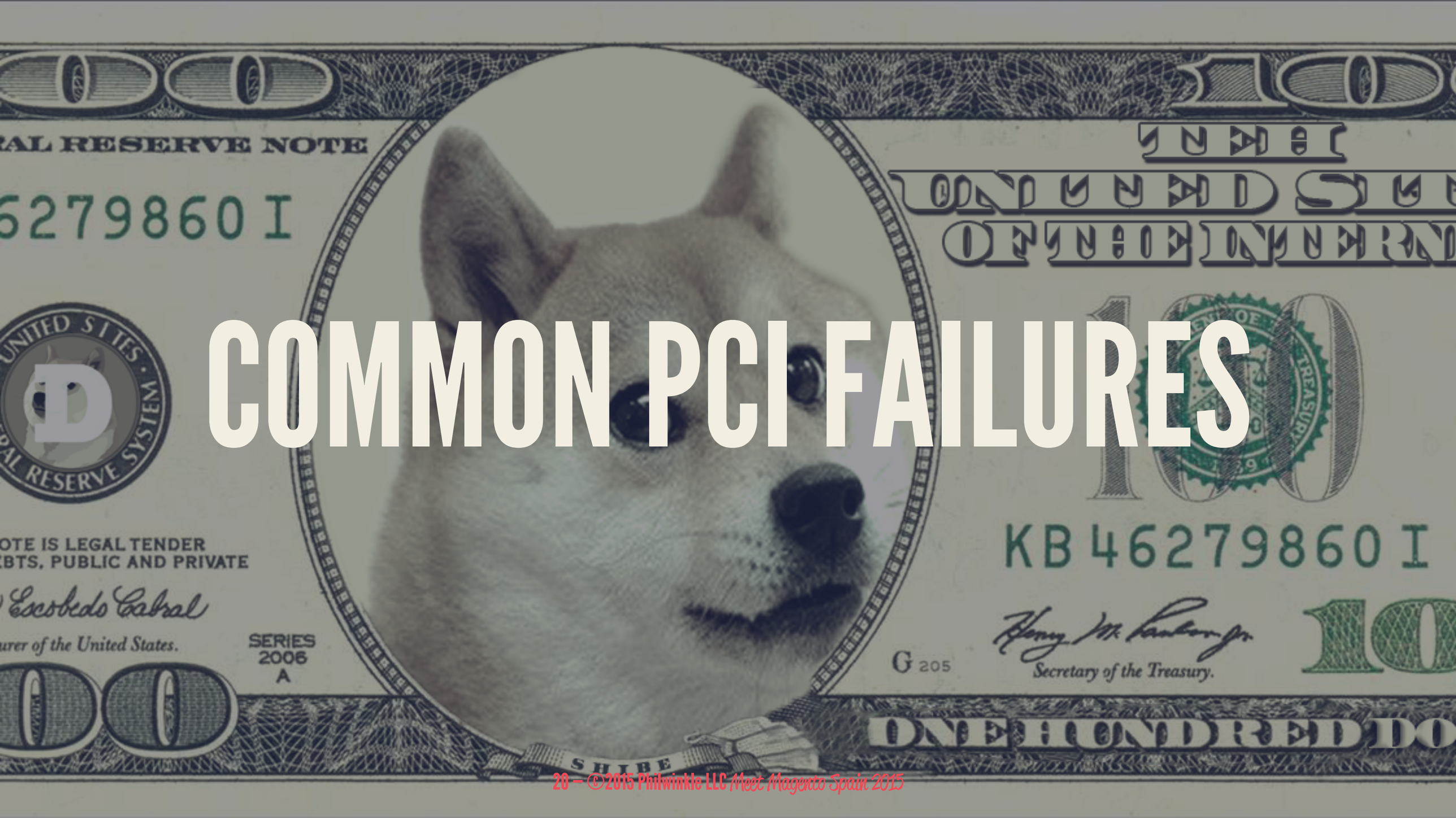
GuruInc is malware that targets Magento shops. Once a shop is infected, it will try to infect visitors as well.

Unprotected Magmi?

Magmi is a Magento mass importer. It's an alternative product importer offering better performance over the default Magento importer. It doesn't have authentication of its own, making it a dangerous tool as it effectively offers full access to your Magent database.

Cacheleak vulnerability? — **safe**

A misconfigured webserver can leak cachefiles containing database


COMMON PCI FAILURES
SHIBE

DO YOU USE *3rd party* MODULES?

DO YOU USE SOURCE CONTROL FOR DEPLOYMENTS?

CHECK YOURSITE.COM/.GIT AND YOURSITE.COM/VAR RIGHT AWAY

WHAT HAPPENS IF *an employee* TAKES A CREDIT CARD OVER THE PHONE?

DO YOU HAVE WIFI?
I BET YOU DO.

WHEN WAS YOUR LAST SECURITY SCAN?

WHAT IS YOUR LOG RETENTION POLICY AND IS IT STORED *offsite*, AND FOR *how long*?

WHAT IS YOUR PASSWORD POLICY?

WHAT DO YOU DO IN CASE OF A DATA BREACH?

WHAT IS YOUR BACKUP STRATEGY?

DO YOU HAVE A STAGING ENVIRONMENT?

DO YOU HAVE SEPARATE DEVELOPMENT ENVIRONMENTS?

DO YOU COPY LIVE CUSTOMER DATA TO YOUR DEVELOPMENT OR STAGING ENVIRONMENTS?

ARE YOU SCARED YET?

HOW DO I GET COMPLIANT?

CONVENIENT 12-STEP PROGRAM

BUILD AND *Maintain* A SECURE NETWORK

1. Install and maintain a firewall
2. Do not use vendor-supplied defaults

PROTECT CARDHOLDER DATA

1. Protect stored cardholder data
2. Encrypt transmission of cardholder data

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

1. Use and regularly update anti-virus software
2. Develop and maintain secure systems and applications

YES, AUDITORS WILL REQUIRE AV ON PRODUCTION HARDWARE

YES THIS IS DUMB

LOOK INTO THESE: CLAMAV (FREE), SOPHOS (INEXPENSIVE)

TO DEVELOP SECURE SYSTEMS

TOOLS TO ASSIST IN SECURE CODE DELIVERY

- FOSS tools[3]
- RIPS for PHP
- SQLmap
- OWASP Xenotix XSS Exploit Framework

[3] http://www.isaca.org/Groups/Professional-English/pci-compliance/GroupDocuments/Meet%20PCI%20DSS%20Requirements%20with%20FOSS.pdf

IMPLEMENT STRONG ACCESS CONTROL MEASURES

1. Restrict employee access to cardholder data
2. Assign a unique ID to each person
3. Restrict physical access

REGULARLY MONITOR AND TEST NETWORKS

1. Track and monitor all access to network resources and cardholder data
2. Regularly test security systems and processes

MAINTAIN AN INFORMATION SECURITY POLICY

1. Maintain a policy that addresses information security

SAMPLE POLICIES AVAILABLE ONLINE[4][5]

[4] https://www.dmoz.org/Computers/Security/Policy/Sample_Policies/

[5] https://github.com/catalyzeio/policies


FREEDOM

CONCLUSION

THIS SOUNDS HARD

LET'S MAKE IT EASIER

WAYS WE CAN *contribute* AS A COMMUNITY

- Security Stackexchange
- Magento Stackexchange
- Magento Subreddit (r/magento)

WAYS WE CAN *stay secure*

- OWASP mailing list
- Magento security mailing list
- Managed hosting
- Policy reminders

PERFORM AN ASSESSMENT

MAGENTO ECG CODING STANDARD

- anywhere you see `$_GET`, be scared
- anywhere you see direct SQL, be scared

RUN MAGEREPORT

- Byte.nl
- Scans for patch vulnerability and other issues

THANK YOU!

SOMETHINGDIGITAL.COM

@PHILWINKLE

GITHUB.COM/PHILWINKLE