Very card, wow security wow

PHILLIP JACKSON

LEAD MAGENTO ARCHITECT, SOMETHING DIGITAL

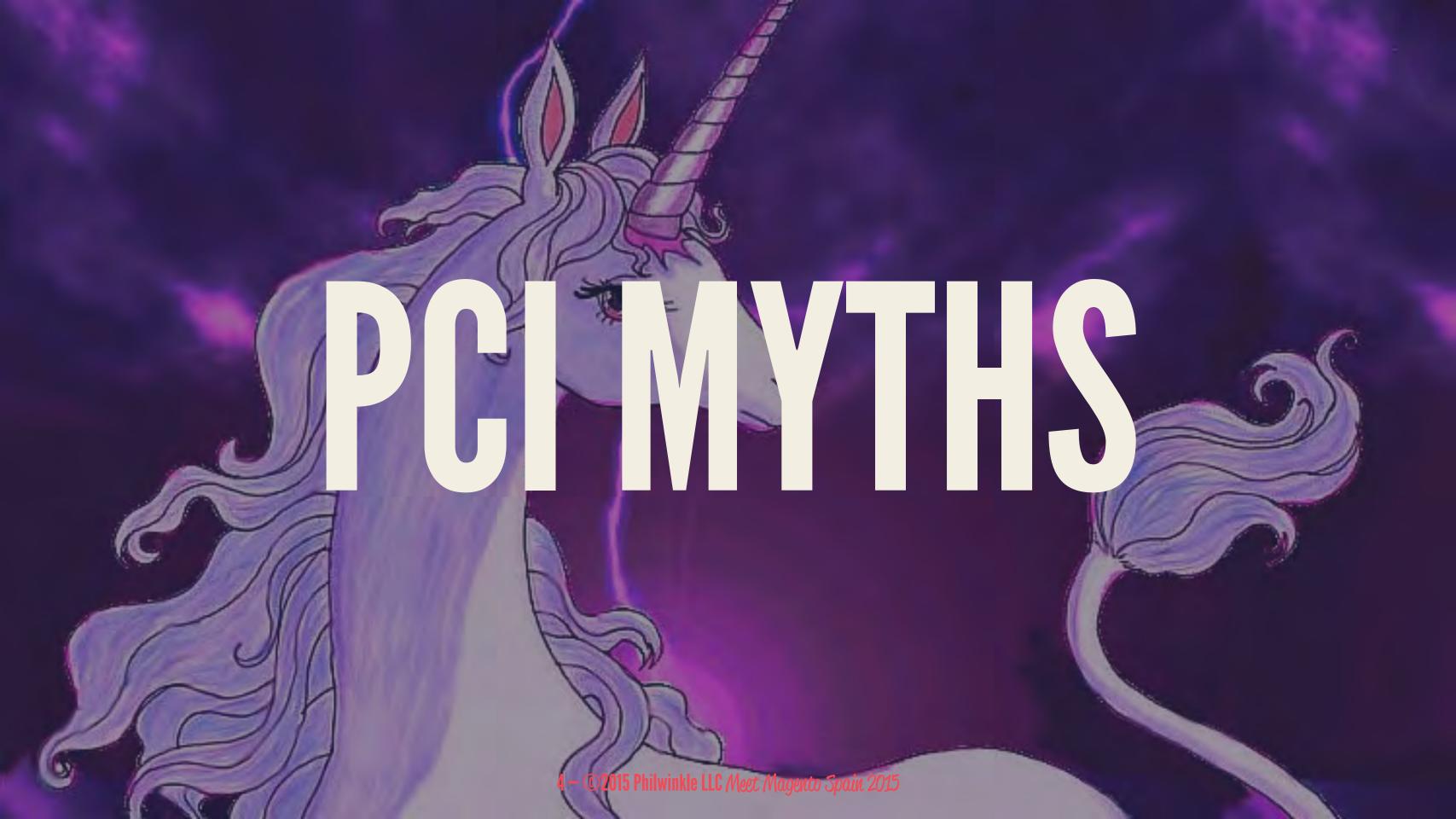
1 – © 2015 Philwinkle LLC Meet Magento Spain 2015



GPHILWINKLE GITHUB.COM/PHILWINKLE



CMAGETALK



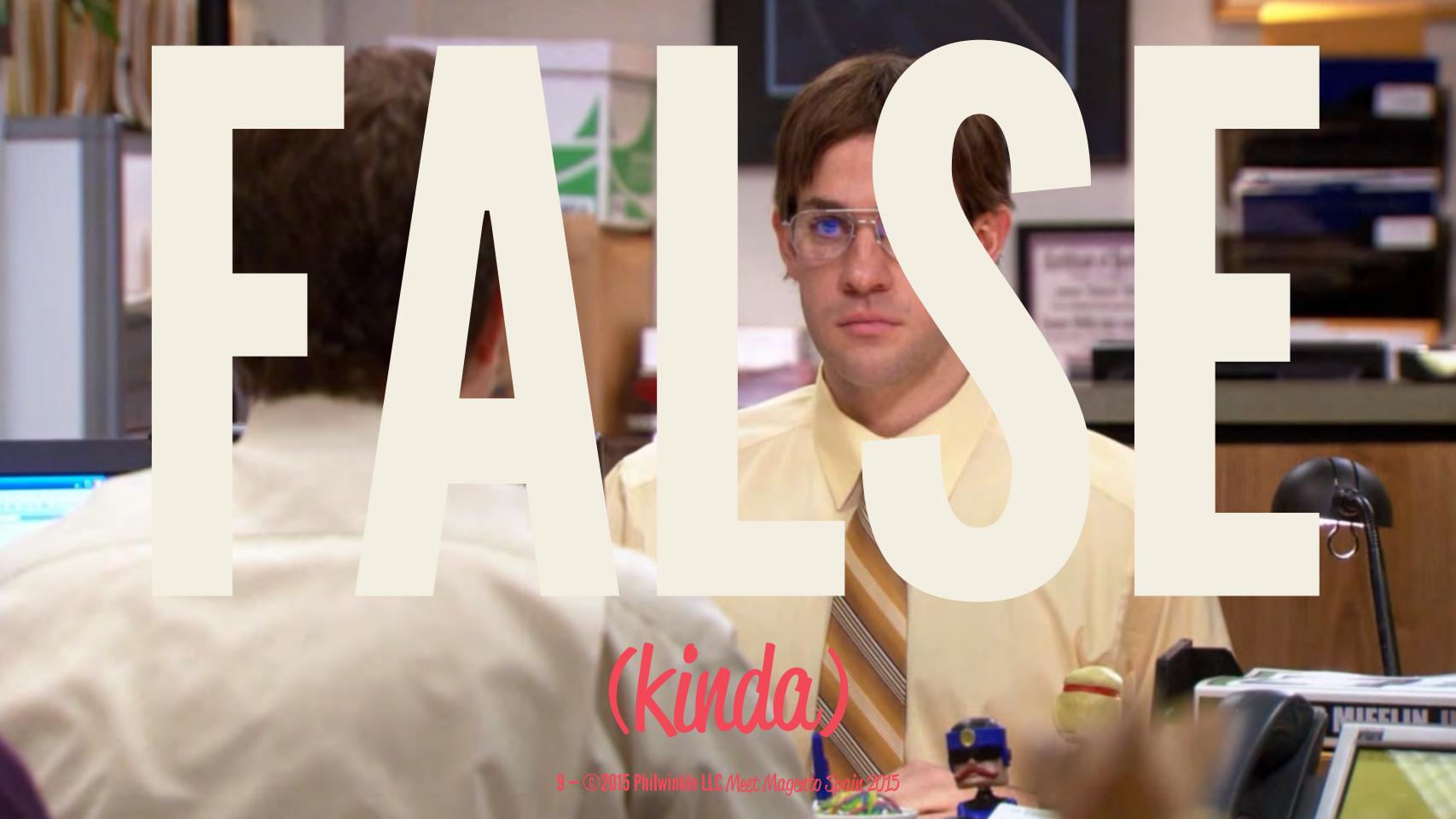
1. IF I don't store CREDIT CARDS PCI doesn't apply



The only way to avoid PCI compliance is to transfer the risk entirely to someone else ... where credit card information never traverses your own servers¹

-- Focus on PCI

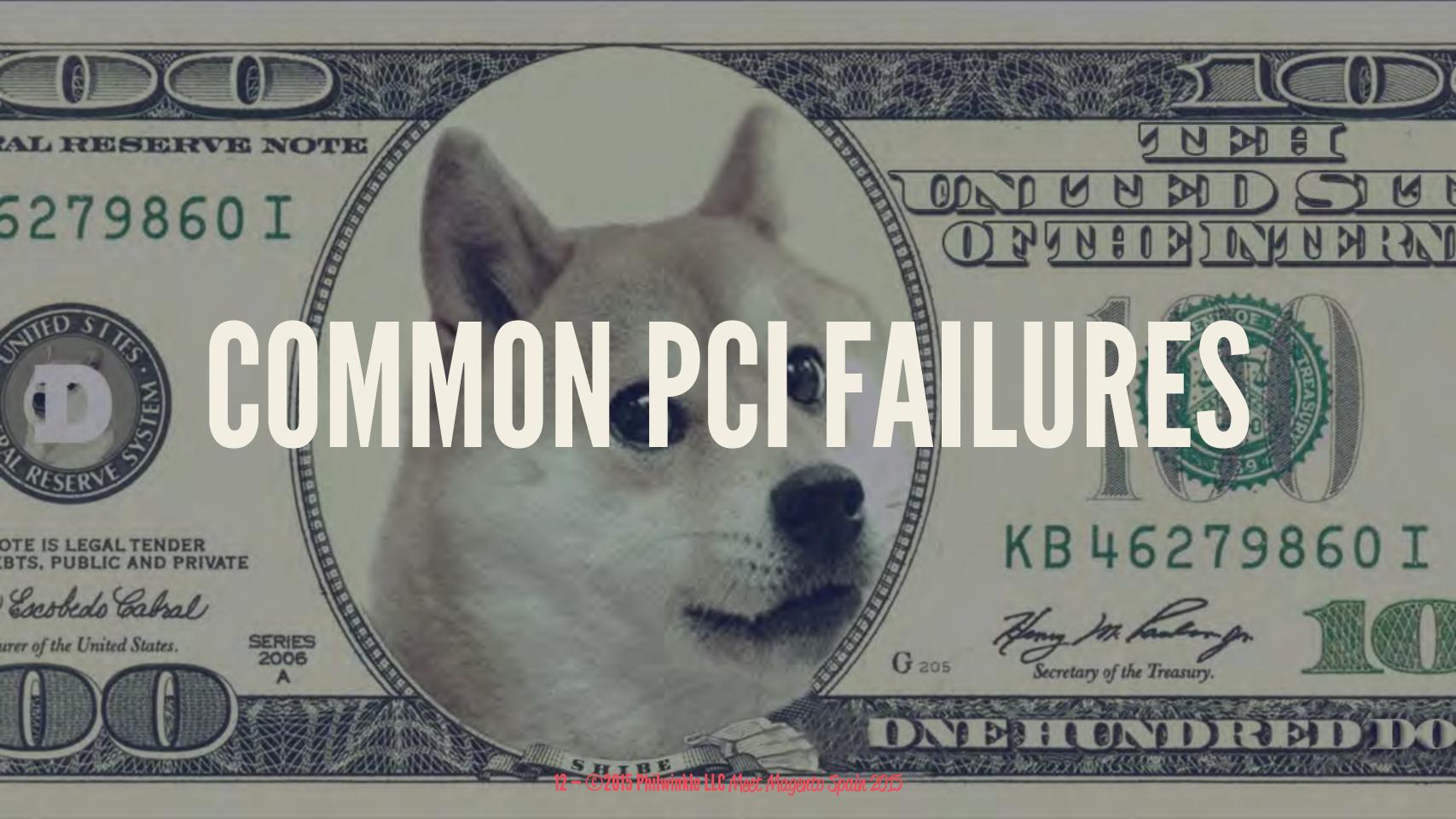
2. MAGENTO IS PCI COMPLIANT, SO THEREFORE I'm PCI compliant



MAGENTO IS PCI DSS COMPLIANT ONLY WHEN USED IN CONJUCTION WITH SECURE PAYMENT BRIDGE²

WHY ISN'T MAGENTO ITSELF PCI COMPLIANT?

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



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 ISIT STORED offsite, AND FOR how ONG

WHAT IS YOUR PASSWORD POLICY?

WHAT DO YOU DO IN CASE OF A DATA BREACH?

WHAT IS YOUR BACKUP STRATEGY?



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 tools³
 - ► 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 %20F0SS.pdf

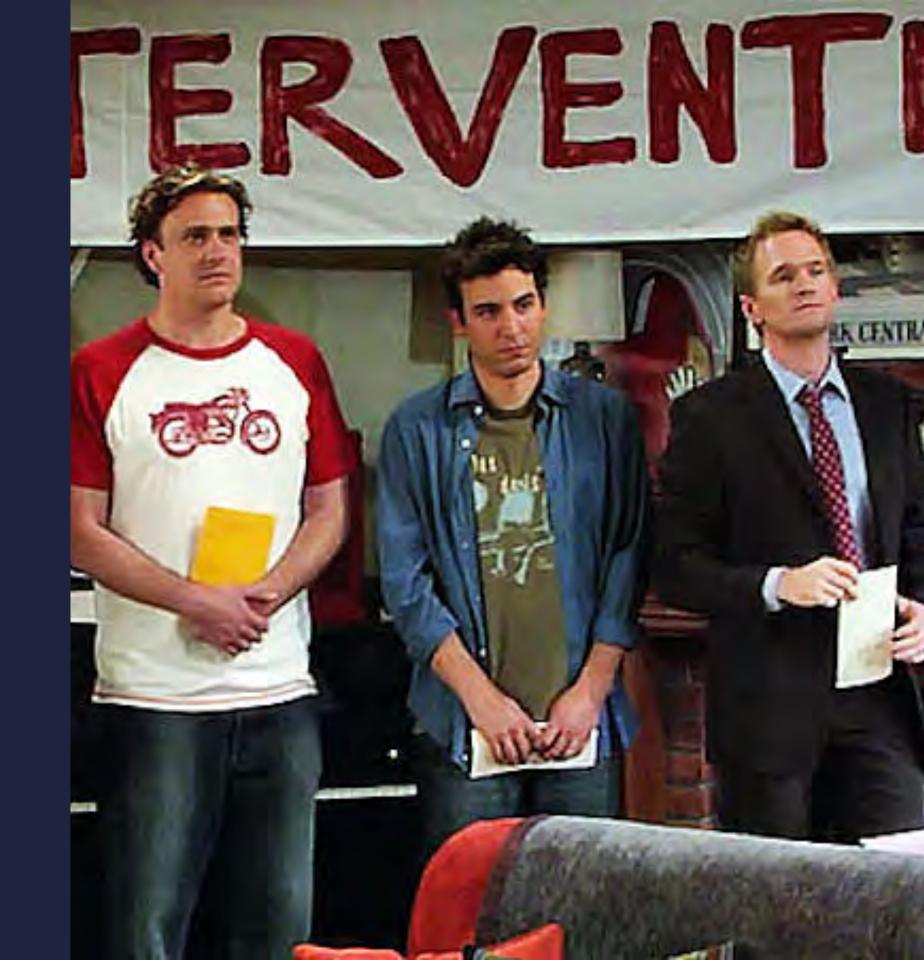


IMPLEMENT STRONG ACCESS CONTROL MEASURES

- 1. Restrict 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 ONLINE⁴⁵

⁴ https://www.dmoz.org/Computers/Security/Policy/Sample_Policies/
⁵ https://github.com/catalyzeio/policies

34 - © 2015 Philwinkle LLC Meet Magento Spain 2015



CONGLUSION

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

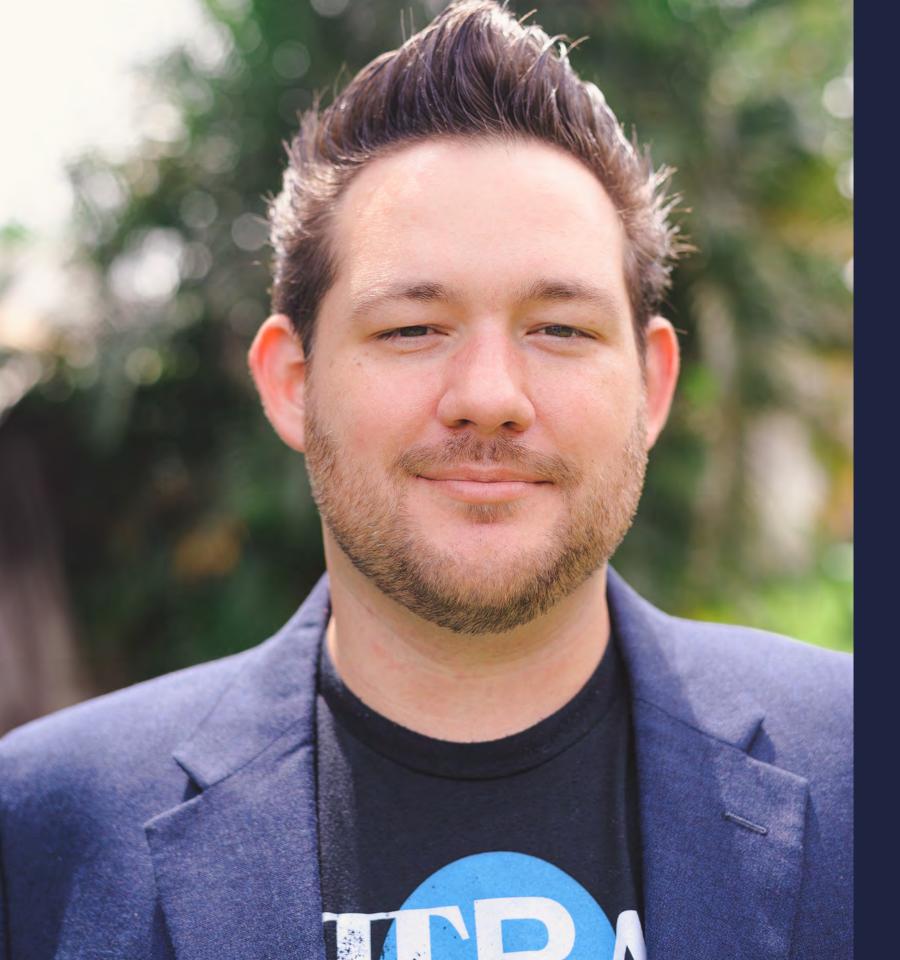
PERFORM AN ASSESSMENT

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 OPHILWINKLE GITHUB.COM/PHILWINKLE