



Data Security Best Practices

Or

“How to Manage Risk When Everything is Broken”

FAMIS Conference

June 25th, 2019

Eric Gray

Privacy Technical Assistance Center



FERPA & Data Security

- FERPA was written in 1974...
- Initially focused on the protection of paper records and information.
- This is both a blessing and a curse.
- FERPA deals addresses data security through the concept of "Reasonable Methods"

FERPA & Data Security

- Applies only to “education records”
- Applies to any agency / institution that receives US Department of Education funding
- Requires written consent to disclose PII from education records unless the disclosure is under one of the exceptions to FERPA:
 - ***School Officials***
 - ***Studies***
 - ***Audits & Evaluations***
 - ***Directory Information***
 - ***Health and Safety Emergency***

FERPA & Data Security

What specific technology controls does FERPA require for your IT systems?

FERPA & Data Security



Yup... Nada... Nothing... Zilch...

FERPA & Data Security

Why doesn't FERPA tell me how to protect student records?



FERPA & Data Security

rea·son·a·ble meth·od

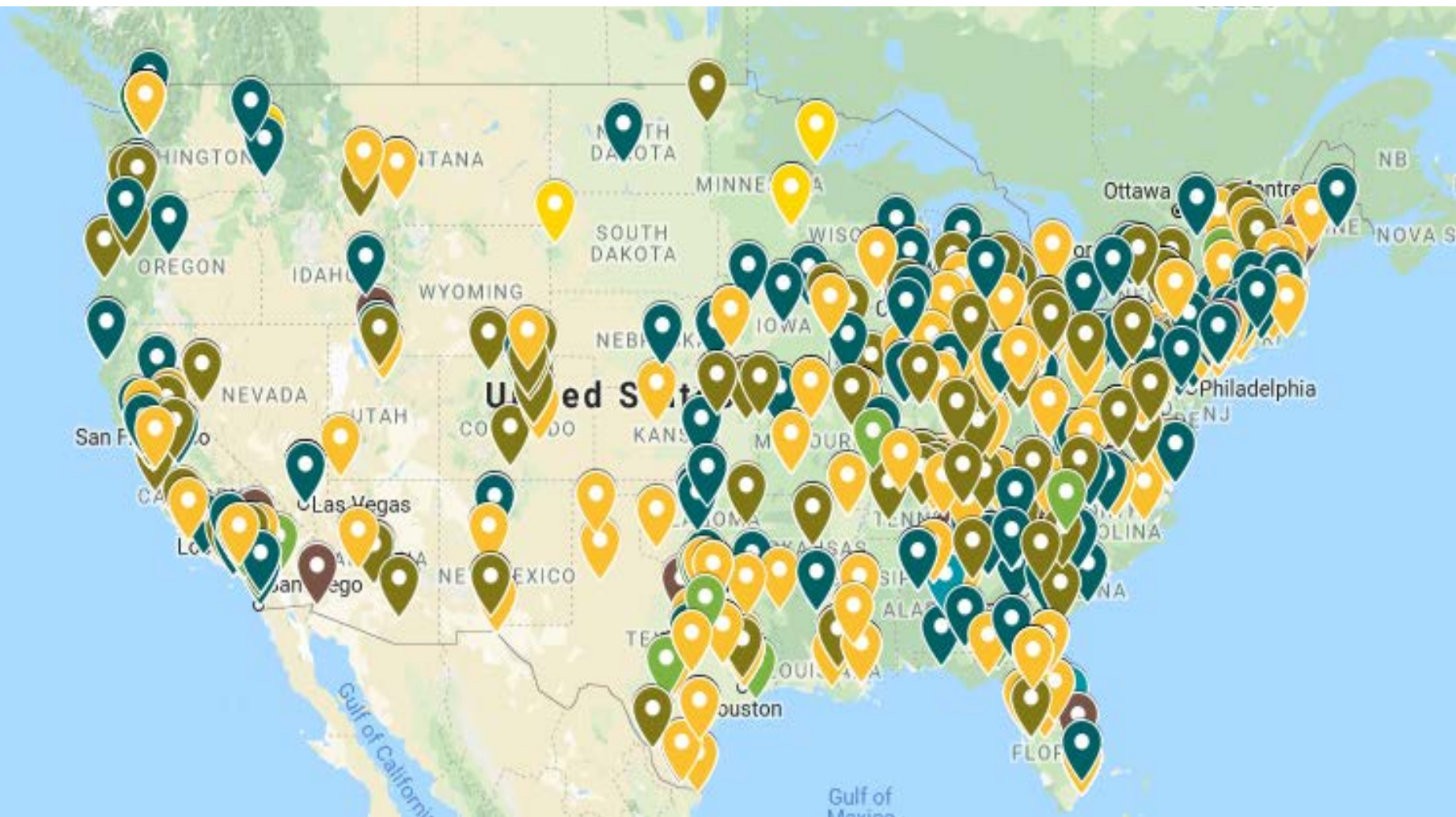
/ˈrēz(ə)nəb(ə)l/ /ˈmeTHəd/

We generally interpret reasonable methods to mean a set of security controls that are in line with current accepted security and privacy best practices for data of similar sensitivity.

Data Security - Why

- FERPA requires it.
- Students deserve it.
- A breach could cause reputational harm.
- Electronic records are more prevalent than ever.
- We collect more, move more, use more & lose more data than ever before.

Data Breaches in ED



Problems in ED Data Systems

- A ton of old or unpatched software
- IoT devices in schools include:
 - Server room cameras & sensors
 - School surveillance systems
 - Access card readers
 - Modems (UPnP hackable)
 - HVAC / Boilers
- Hundreds of forgotten servers / computers

Problems in ED Data Systems for one state found in an afternoon

- 626 machines with no firewall
- 2 SIS breaches affecting thousands of students
- Hundreds of anonymous FTP servers
- 143 Windows XP machines (some already hacked)
- 10 VPNs running out of date Windows 2003 Server
- 835 Web servers running IIS 6 or earlier

But I
don't
work in
IT?

- **Most breaches start with social engineering**
- **Attackers target YOU, not the technology first**
- **Most successful large breaches use stolen credentials**

Education Data Security in the News

WSU Social & Economic Sciences Center loses an unencrypted hard drive in a theft containing personally identifiable information.

- More than 1 million people affected
- Data was stored in an unencrypted fashion in a safe locked in a rented storage unit
- Data included names, SSNs, education status, employment data

Education Data Security in the News

In March, the Department of Justice sanctioned nine Iranian hackers over attacks on more than 300 universities in the United States and abroad.

- *31 Terabytes of data stolen*
- *Estimated value of \$3 billion dollars*
- *Began with phishing attacks*
- *Targeted 100k users, successfully compromised ~8k*

How a School is Vulnerable

**Most phishing e-mails are easy to notice.
Here are some things an attacker might do to
gain access to your systems.**

1. Locate Staff Directory (yes, it's there)
2. Send Phishing E-mail to targeted employees, infecting the unwary user
3. Locate and exfiltrate data
4. Profit!

Default Initial Setup Interface

Services

9999
tcp
telnet

*** Siemens AEM200 ***

Serial Number 1221349 MAC address 00204A125365

Software version 05.2 (030725) DLX SIE



Press Enter to go into Setup Mode

LUTRON

Enter your login and password

Login Incorrect.

Login:

Password:

Enter



Data Security Dragnet

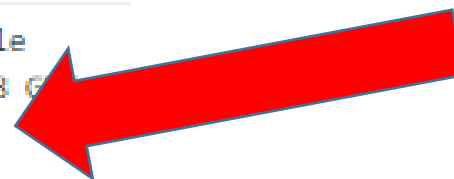


80
tcp
http



Apache httpd Version: 2.2.15

HTTP/1.1 503 Service Unavailable
Date: Fri, 21 Jun 2019 06:17:08 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.37
Content-Length: 2452
Connection: close
Content-Type: text/html; charset=UTF-8



Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2010-2068	mod_proxy_http.c in mod_proxy_http in the Apache HTTP Server 2.2.9 through 2.2.15, 2.3.4-alpha, and 2.3.5-alpha on Windows, NetWare, and OS/2, in certain configurations involving proxy worker pools, does not properly detect timeouts, which allows remote attackers to obtain a potentially sensitive response intended for a different client in opportunistic circumstances via a normal HTTP request.
CVE-2011-4317	The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an @ (at sign) character and a : (colon) character in invalid positions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.
CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
CVE-2011-3368	The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.
CVE-2011-3348	The mod_proxy_ajp module in the Apache HTTP Server before 2.2.21, when used with mod_proxy_balancer in certain configurations, allows remote attackers to cause a denial of service (temporary "error state" in the backend server) via a malformed HTTP request.
CVE-2012-3499	Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs in the (1) mod_imagemap, (2) mod_info, (3) mod_ldap, (4) mod_proxy_ftp, and (5) mod_status modules.
CVE-2012-4558	Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.
CVE-2011-3607	Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvif directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.



CVE-2016-8612	Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.
CVE-2018-19935	ext/imap/php_imap.c in PHP 5.x and 7.x before 7.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty string in the message argument to the imap_mail function.
CVE-2014-0098	The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.
CVE-2012-4557	The mod_proxy_ajp module in the Apache HTTP Server 2.2.12 through 2.2.21 places a worker node into an error state upon detection of a long request-processing time, which allows remote attackers to cause a denial of service (worker consumption) via an expensive request.
CVE-2019-9639	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the data_len variable.
CVE-2019-9638	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the maker_note->offset relationship to value_len.
CVE-2017-7668	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.
CVE-2013-6438	The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.
CVE-2019-9021	An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A heap-based buffer over-read in PHAR reading functions in the PHAR extension may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse the file name, a different vulnerability than CVE-2018-20783. This is related to phar_detect_phar_fname_ext in ext/phar/phar.c.
CVE-2012-2687	Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.
CVE-2019-9637	An issue was discovered in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly available with wrong permissions while the rename is ongoing, thus enabling unauthorized users to access the data.





CVE-2011-4415	The <code>ap_pregsub</code> function in <code>server/util.c</code> in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the <code>mod_setenvif</code> module is enabled, does not restrict the size of values of environment variables, which allows local users to cause a denial of service (memory consumption or NULL pointer dereference) via a <code>.htaccess</code> file with a crafted <code>SetEnvif</code> directive, in conjunction with a crafted HTTP request header, related to (1) the <code>"len +="</code> statement and (2) the <code>apr_pccalloc</code> function call, a different vulnerability than CVE-2011-3607.
CVE-2012-0031	<code>scoreboard.c</code> in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the <code>free</code> function.
CVE-2013-2249	<code>mod_session_dbd.c</code> in the <code>mod_session_dbd</code> module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.
CVE-2010-1452	The (1) <code>mod_cache</code> and (2) <code>mod_dav</code> modules in the Apache HTTP Server 2.2.x before 2.2.16 allow remote attackers to cause a denial of service (process crash) via a request that lacks a path.
CVE-2013-1896	<code>mod_dav.c</code> in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the <code>mod_dav_svn</code> module, but a certain href attribute in XML data refers to a non-DAV URI.
CVE-2017-3167	In Apache <code>httpd</code> 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the <code>ap_get_basic_auth_pw()</code> by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.
CVE-2012-0053	<code>protocol.c</code> in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.
CVE-2012-0883	<code>envvars</code> (aka <code>envvars-std</code>) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the <code>LD_LIBRARY_PATH</code> , which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of <code>apachectl</code> .
CVE-2017-3169	In Apache <code>httpd</code> 2.2.x before 2.2.33 and 2.4.x before 2.4.26, <code>mod_ssl</code> may dereference a NULL pointer when third-party modules call <code>ap_hook_process_connection()</code> during an HTTP request to an HTTPS port.
CVE-2011-3639	The <code>mod_proxy</code> module in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x before 2.2.18, when the Revision 1179239 patch is in place, does not properly interact with use of (1) <code>RewriteRule</code> and (2) <code>ProxyPassMatch</code> pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests





Drupal 6.27, 2012-12-19

- Fixed security issues (multiple vulnerabilities), see SA-CORE-2012-004.

Drupal 6.26, 2012-05-02

- Fixed a small number of bugs.
- Made code documentation improvements.

Drupal 6.25, 2012-02-29

- Fixed regressions introduced in Drupal 6.24 only.

Drupal 6.24, 2012-02-01

- Improved performance of search indexing and user operations by adding indexes.
- Fixed issues with themes getting disabled due to missing locking in `system_theme_data()`.
- Fix issue with blocks being disabled on updates in `_block_rehash()`.
- Further improvements to PHP 5.3, PHP 4 and PostgreSQL compatibility.
- Improved code documentation at various places.
- Fixed a variety of other bugs.



A New Challenger Appears!!!!

80
tcp
http



Apache httpd Version: 1.3.39

HTTP/1.1 302 Found

Date: Sat, 15 Jun 2019 22:39:58 GMT

Server: Apache/1.3.39 (Unix) PHP/4.4.7

X-Powered-By: PHP/4.4.7

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Last-Modified: Sat, 15 Jun 2019 22:39:58 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

Set-Cookie: PHPSESSID=60711d633a20c21e2d8f7061e64d644e; path=/

Location: <http://earobics.broward.k12.fl.us/?module=Auth&action=Logout&exp=true>

Transfer-Encoding: chunked

Content-Type: text/html; charset=UTF-8

Apache 2 Test Page

powered by **CentOS**

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page it means that the Apache HTTP server installed at this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

You are free to use the images below on Apache and CentOS Linux powered HTTP servers. Thanks for using Apache and CentOS!



About CentOS:

The Community ENTERprise Operating System (CentOS) Linux is a community-supported enterprise distribution derived from sources freely provided to the public by Red Hat. As such, CentOS Linux aims to be functionally compatible with Red Hat Enterprise Linux. The CentOS Project is the organization that builds CentOS. We mainly change packages to remove upstream vendor branding and artwork.

For information on CentOS please visit the [CentOS website](http://www.centos.org).



intitle:"Workspace Login" intext:"WinOcular WorkSpace"

Powered by [WinOcular](#) Software

WinOcular WorkSpace

Version 1.0.15, Copyright © 2008-2013, Combined Computer Resources, Inc.

WinOcular Workspace Login portals.

Decoy

Still using IIS 6.0? Stop right now – the latest zero-day won't be patched

03 APR 2017 2

Vulnerability

✕ Don't show me this again

Get the latest security news in your inbox.

you@example.com


Subscribe





untitled



Added on 2019-06-18 19:44:29 GMT


 United States, Sebring


HTTP/1.1 200 OK
Content-Length: 454
Content-Type: text/html
Content-Location: /Default.htm
Last-Modified: Wed, 21 Feb 2018 13:46:50 GMT
Accept-Ranges: none
ETag: "9751df6c1aabd31:3f0"
Server: Microsoft-IIS/6.0
PICS-Label: (PICS-1.0 "http: 

Under Construction



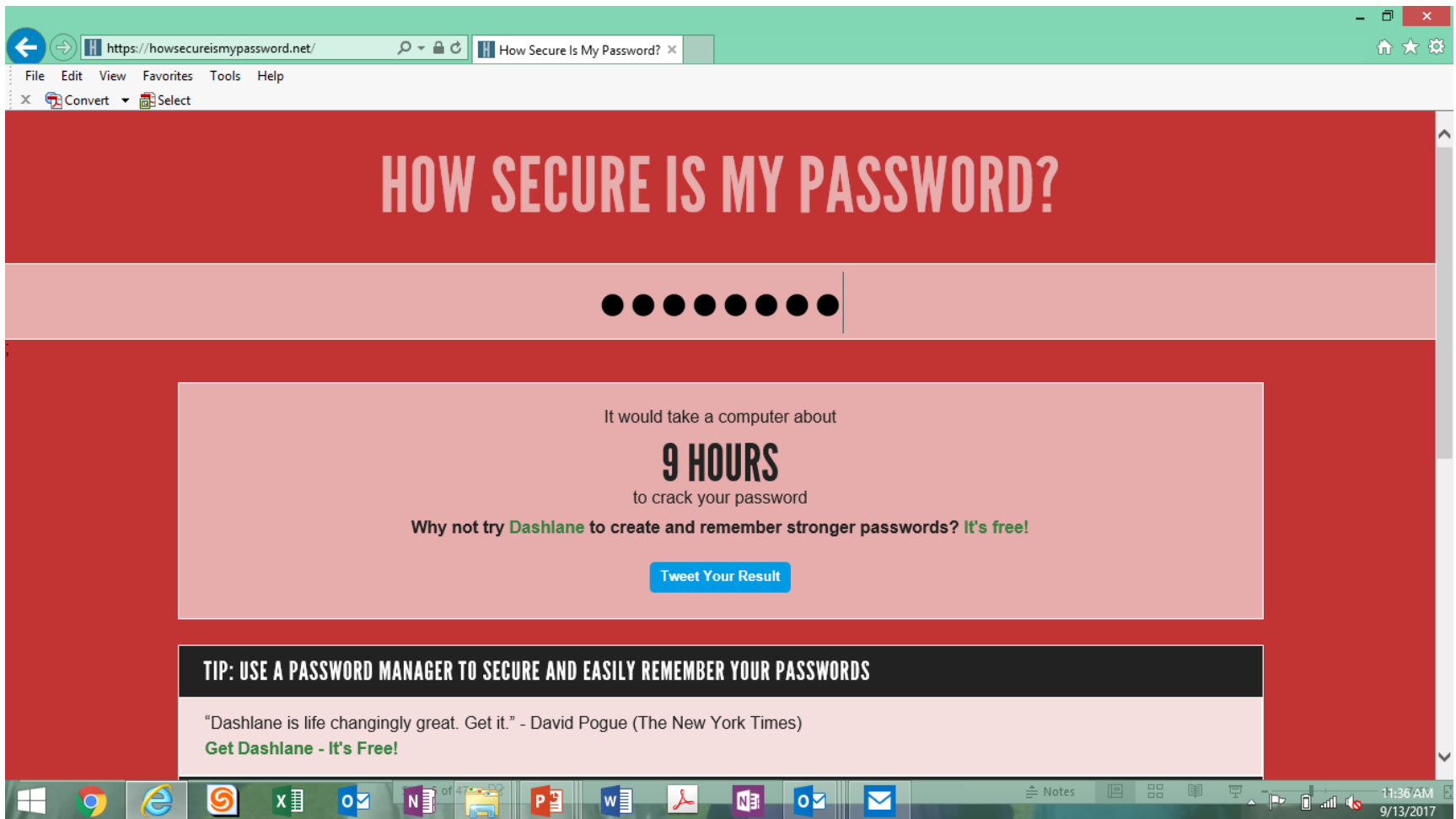
Added on 2019-06-14 03:25:06 GMT

 United States, Sebring

HTTP/1.1 200 OK
Content-Length: 1433
Content-Type: text/html
Content-Location: fl.us/iisstart.htm
Last-Modified: Fri, 21 Feb 2003 23:48:30 GMT
Accept-Ranges: none
ETag: "09b60bc3dac21:473"
Server: Microsoft-IIS/6.0
Date: Fri, 14 Jun 2019 03:25:06 GMT

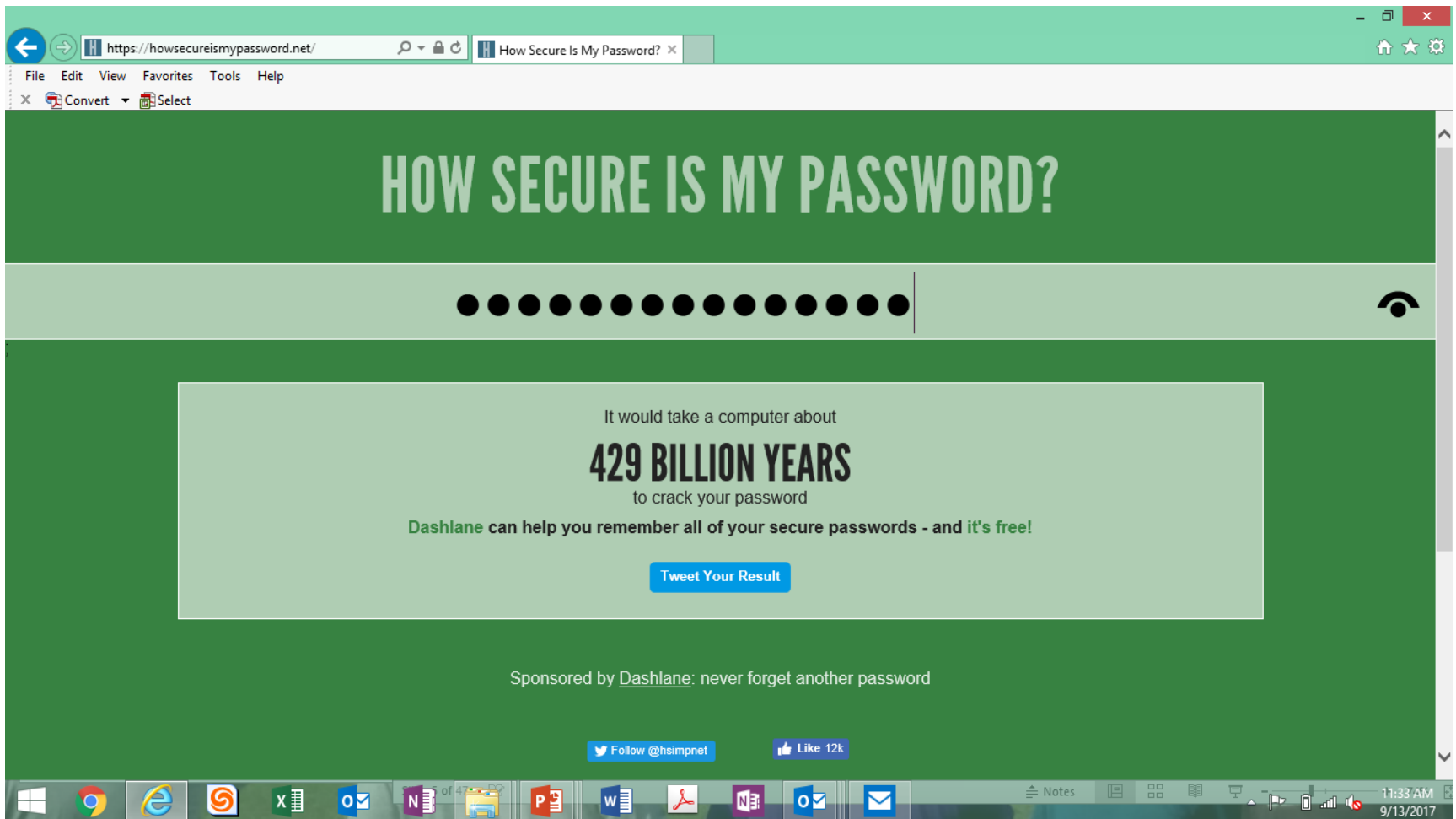
Passwords: How good is this password?

- zQ4ab!ui



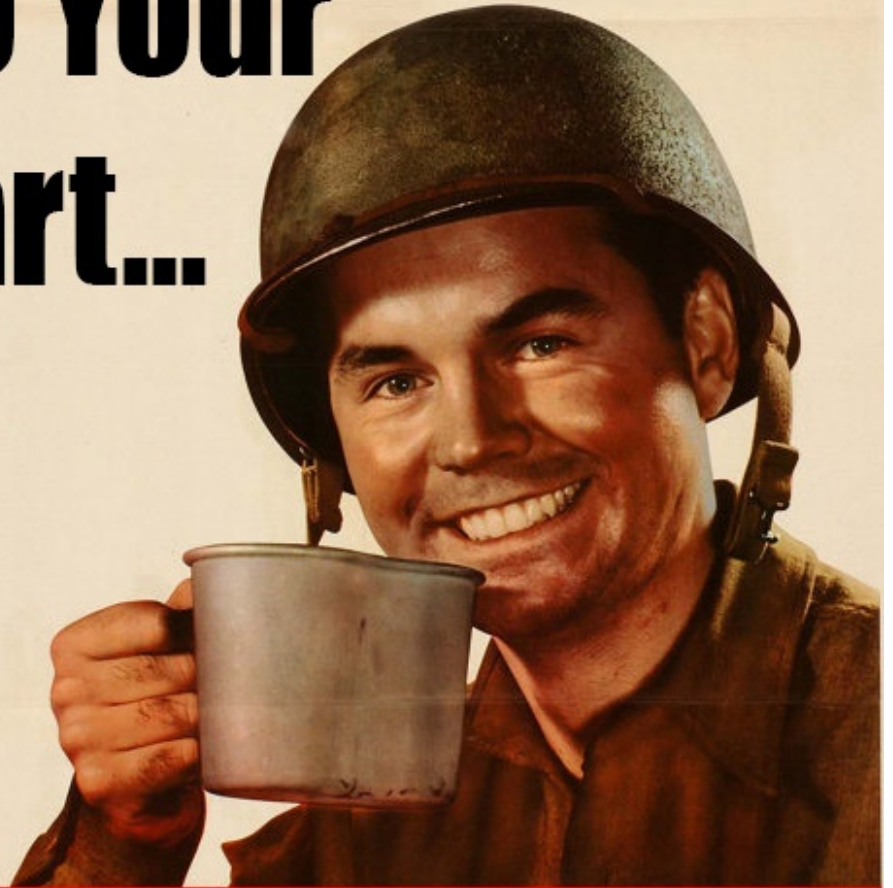
How about this Password?

- I L0ve my M0m!



Let's Start
With This

**Do Your
Part...**

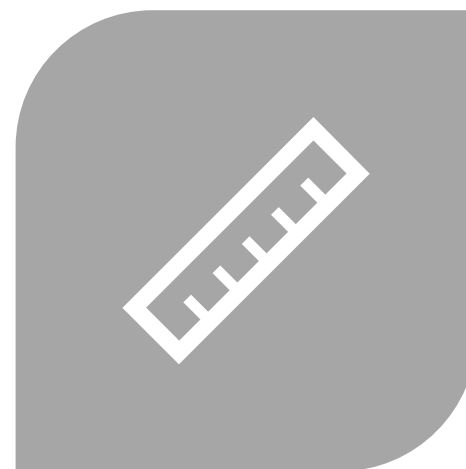


STOP CLICKING ON STUFF

How to Operationalize Security?

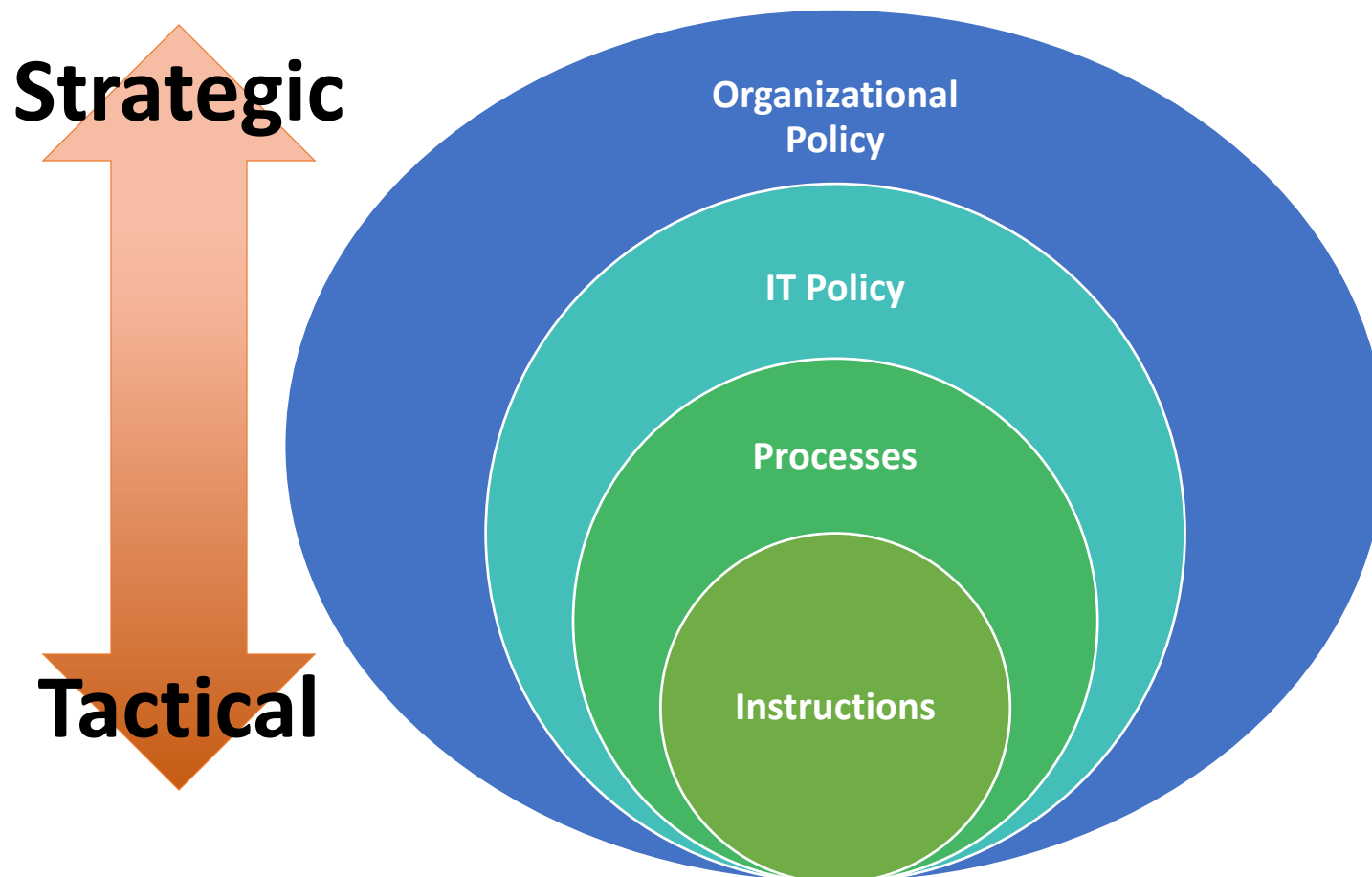


***DOCUMENTED, REPEATABLE PROCESSES
DRIVEN BY SOLID ORGANIZATIONAL
POLICY***



METRICS

(Groan) Start With Policy



Bare Bones Must Haves

- Privacy & IT security Training annually
- Vulnerability Tracking & Mitigation
- Risk Assessment / Management
- Incident Response Plan
- Account Management
- Data & System Standards
- Enforcement

Data Security is a Shared Responsibility

IT

- Vulnerability Mgmt
- Account Mgmt
- Boundary Control
- Performance Metrics

Shared

- Privacy & Security Training
- Incident Response
- Risk Management
- Data Accountability

Standards Are Your Friends

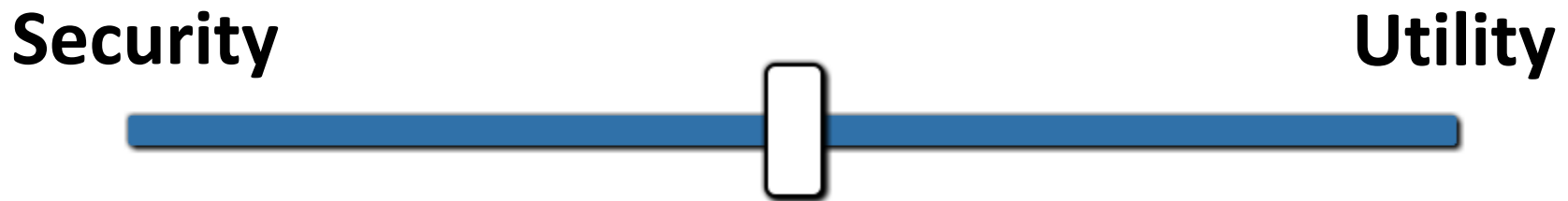
Reliable data security programs all have one thing in common... control:

- *Create standard software loads & enforce them*
- *Same applies to Boundary Control (fw rules)*
- *Police for compliance*

Process changes through CCB or similar process

Tailor Data Security to Your Business

**Do not forget that the purpose of the systems
is to enable the business of educating
children!**



Perform Annual Risk Assessments

“The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact.”

-National Institute of Standards and Technology (NIST)

What is a Risk Assessment?

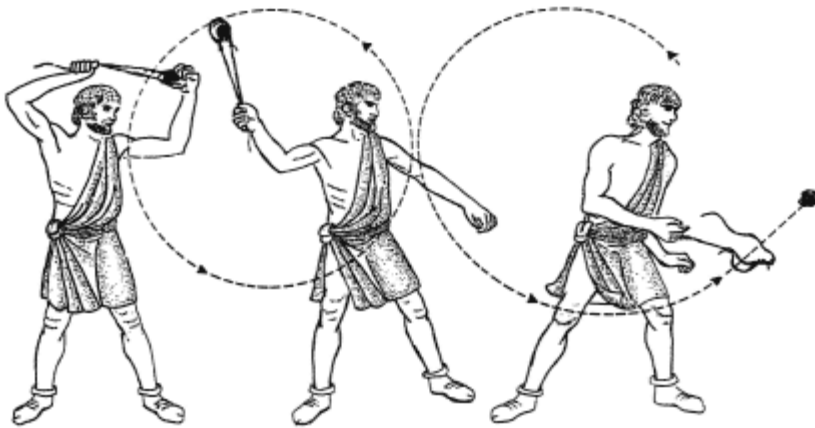
Formal organizational process involving leadership, IT, and organizational stakeholders

Four stages:

- **Identification** – *finding, documenting, and categorizing risks*
- **Analysis** – *ascertaining the nature of the risks and determining their potential impact and effects*
- **Evaluation** – *applying organizational risk tolerance and existing controls to the risk to determine significance*
- **Control** – identifying and applying mitigating controls to reduce the risk based on analysis

The Reality is

Attackers only have to get lucky once...



Reducing
the Risk

News Flash:

***You can hack yourselves for your
own good!!!!***

Footholds (57)

Examples of queries that can help an attacker gain a foothold into a web server

Sensitive Directories (123)

Googles collection of web sites sharing sensitive directories. The files contained in here will vary from sensitive to über-secret!

Vulnerable Files (62)

HUNDREDS of vulnerable files that Google can find on websites.

Vulnerable Servers (83)

These searches reveal servers with specific vulnerabilities. These are found in a different way than the searches found in the "Vulnerable Files" section.

Error Messages (94)

Really verbose error messages that say WAY too much!

Network or Vulnerability Data (70)

These pages contain such things as firewall logs, honeypot logs, network information, IDS logs... All sorts of fun stuff!

Various Online Devices (317)

This category contains things like printers, video cameras, and all sorts of cool things found on the web with Google.

Web Server Detection (80)

These links demonstrate Googles awesome ability to profile web servers.

Files Containing Usernames (17)

These files contain usernames, but no passwords... Still, Google finding usernames on a web site.

Files Containing Passwords (200)

PASSWORDS!!! Google found PASSWORDS!

Sensitive Online Shopping Info (11)

Examples of queries that can reveal online shopping information like customer data, suppliers, orders, credit card numbers, credit card info, etc

Files Containing Juicy Info (374)

No usernames or passwords, but interesting stuff none the less.

Pages Containing Login Portals (383)

These are login pages for various services. Consider them the front door of a websites more sensitive functions.

Advisories and Vulnerabilities (1996)

These searches locate vulnerable servers. These searches are often generated from various security advisory posts, and in many cases are product or version-specific.

Security Self-Assessment

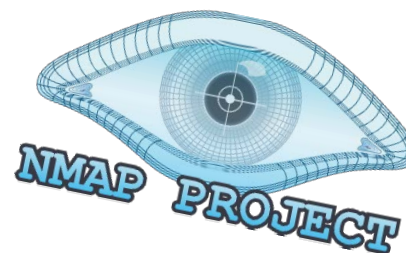


a hacker's best friend:

OK Google.... Find me some passwords

Security Self-Assessment

- Lot's of cheap and free tools out there to assist in finding things that slip through the cracks





SHODAN

Com

Web ser

- E
- A
- L
- in

city: find devices in a particular city

country: find devices in a particular country

geo: you can pass it coordinates

hostname: find values that match the hostname

net: search based on an IP or /x CIDR

os: search based on operating system

port: find particular ports that are open

before/after: find results within a timeframe

ormation.

ners

access)



SHODAN



Security Self-Assessment

- Leverage automated tools like SIEM to correlate logs across the environment and identify anomalies
- Look for architectural and logical improvements that you can implement cheaply to make an attacker's life harder
- Leverage users to identify permissions issues and spot incongruities in security or privacy. Implement a bounty program where users are rewarded in some way for identifying issues

Questions?



Contact information

United States Department of Education,
Privacy Technical Assistance Center



(855) 249-3072
(202) 260-3887



privacyTA@ed.gov



<http://studentprivacy.ed.gov>



(855) 249-3073