LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Free Web Scanning Resources

04/25/2019

Report #: 201904251000

Agenda

- Introduction
  - What is a vulnerability?
  - How do web vulnerabilities fit into the big picture of enterprise risk management?
- Common web vulnerabilities/attacks
- EXAMPLE: SQL injection attacks
- Vulnerability Assessments
- Free scanning tools
- EXAMPLE: Securi
- DHS NCCIC
- Additional resources
- Outsourcing security
- Takeaways
- References
- Questions

WEB APP ATTACKS MADE UP

35%

OF ALL BREACHES IN 2013

Verizon 2014 Data Breach Investigations Report

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Introduction

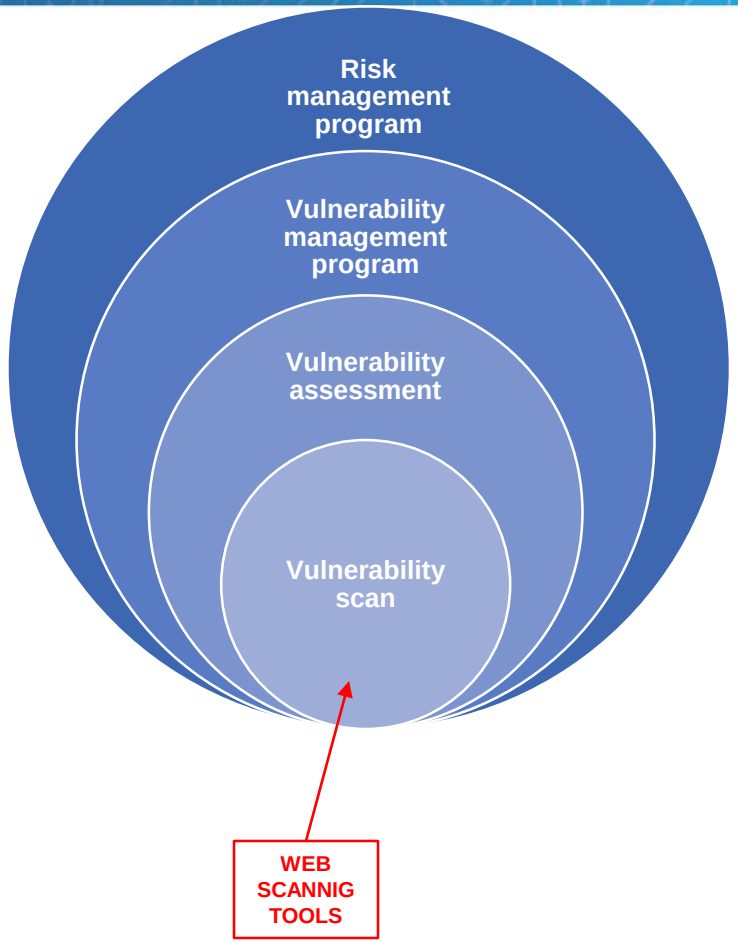
- What is web security?
  - Protecting a webserver and associated applications and services
- How are web assets vulnerable?
  - What is a vulnerability?
    - The state of being open of exposed to attack
    - Sometimes colloquially referred to as an exploit
    - Effects both hardware and software of all types
    - There is no finite limit; new vulnerabilities are being discovered all the time
  - What is a zero day? Why are zero days important?
    - An exploit/vulnerability that is not known to the vendors/developers
    - Because zero days are unknown, they offer the attacker the element of surprise and an opportunity to gain a critical time advantage against defenders during an attack
- What does a vulnerability scanner do?
  - Scans identify known vulnerabilities of their targeted systems
  - Scan is just one component of a vulnerability assessment

There are many ways to exploit a vulnerability

Source: Manufacturing Global

Introduction (continued)

- Vulnerability management vs. vulnerability assessment
  - Vulnerability management
    - Ongoing, continuous, repeatable program
    - Includes vulnerability assessment process
  - Vulnerability assessment
    - One-time project with defined start and stop dates
    - *NOT* simply a scan; comprehensive analysis of enterprise-wide vulnerabilities with recommended remediation's
- What is the vulnerability management lifecycle? (A critical part of vulnerability management and ultimately, risk management)
  - Asset inventory
  - Information Management
  - Risk Assessment
  - Vulnerability Assessment
  - Reporting and Remediation
  - Response Planning
- This presentation applies to HPH and other industries as well



Common web vulnerabilities

What types of vulnerabilities are associated with web resources?

- Cross site scripting (XSS)
  - Malicious code injected into websites and passed on to victims surfing the site via their browsers
- SQL injection (SQLi)
  - An attack on a SQL database via code being inserted into a SQL statement; execution of arbitrary code
- HTTP Header injection
  - Malicious code injected into an HTTP packet
- AJAX testing
  - Malicious code inserted in AJAX transmission
- File inclusion
  - Can allow for outputting contents of file or code execution; often results in unauthorized access to a system
- Information leakage
  - Application reveals sensitive technical information such as details about itself, the environment it runs in or user data

SQL Injection attacks

Injection attacks are commonly used to target web resources, so let's look at one of the most frequently used – a SQL injection:

SQL – Structured Query Language, used for manipulating and retrieving information in/from databases

What is a SQL injection attack?

When the user exploits a vulnerable user input within a webpage or application in order to submit input as a SQL command

Image source: Acunetix.com

Let's briefly look at a SQL Injection attack:

SQL database code

```
# Define POST variables
uname = request.POST['username']
passwd = request.POST['password']

# SQL query vulnerable to SQLi
sql = "SELECT id FROM users WHERE username='" + uname + "' AND password='" + passwd + "'"

# Execute the SQL statement
database.execute(sql)
```

Code source: Acunetix.com

User input

```
password' OR 1=1
```

Processed command

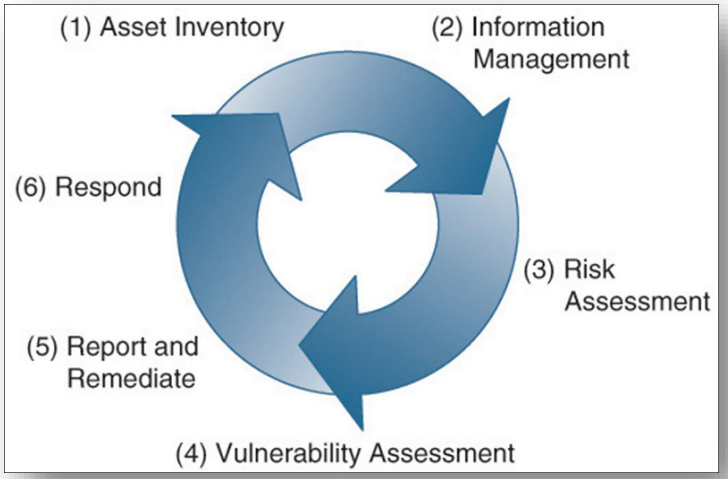
```
SELECT id FROM users WHERE username='username' AND password='password' OR 1=1'
```

A successful SQL inject attack will allow the attacker to view, modify or delete records in the database

TO BE CLEAR: Injection attacks, and SQL injections specifically, are only one of many types of cyberattacks against web resources.

Vulnerability Assessments

- Vulnerability management, which includes vulnerability assessment and remediation – is an iterative process
  - **Time is of the essence**; Goal: Reducing the attack surface
  - Sometimes a tradeoff between patching and operations
- Per NIST:
  - Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware. From a security perspective, patches are most often of interest because they are mitigating software flaw vulnerabilities; applying patches to eliminate these vulnerabilities significantly reduces the opportunities for exploitation. Patches serve other purposes than just fixing software flaws; they can also add new features to software and firmware, including security capabilities.



Vulnerability management model endorsed by SANS and Cisco

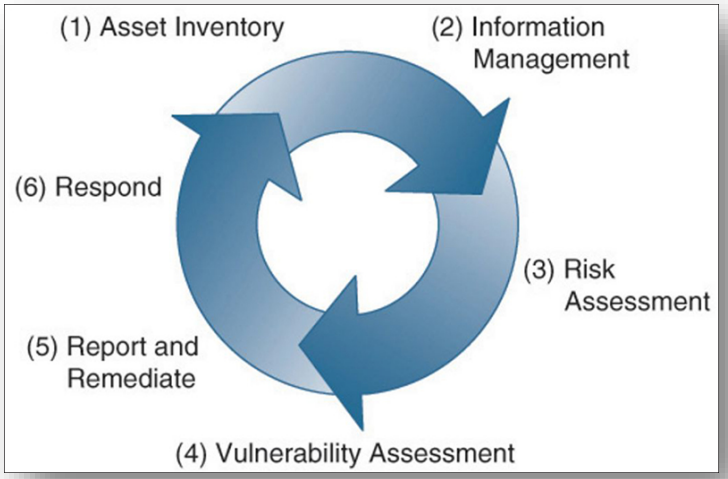
Cisco/SANS vulnerability management methodology:

- 6-step iterative process
- Self-feeding process (each iteration provides inputs for the next)
- Part of greater risk management program
- Goal: Reducing attack surface

Vulnerability Assessments (Cont.)

Cisco/SANS vulnerability management methodology:

- Asset inventory
  - Comprehensive inventory of all information systems
  - Preferably managed by a single authority
- Information Management
  - Track all hardware systems, operating systems, installed patches and new vulnerabilities
- Risk Assessment
  - Understanding threats and their potential impact on enterprise IT assets and business operations
- Vulnerability Assessment
  - Calculate vulnerabilities based on business operations value and technical specifics, including scanning
- Report and Remediate
  - Download, test and deploy and verify patches; Generate and disseminate reports
- Respond
  - Conduct incident response as necessary



Vulnerability management model endorsed by SANS and Cisco

Free Scanning Tools

HHS does not endorse any tool or company in particular

- Scan My Server – Free website test for security weaknesses and confidential report; Searches for issues with code structure and errors as well as issues with password-protected pages, if permission is granted; Multi-site accounts and PCI certification testing can be conducted for a fee.
  - https://scanmyserver.com/
- SUCURI – Free scan of website or blog for known malware, blacklisting status, website errors, injected spam, defacements and out-of-date software; For a fee, SUCIRI will remediate malware, blacklisting and bot spams, in addition to WAF protection, real-time monitoring and incident response.
  - https://sucuri.net/
- Qualys – Free Community Edition of cloud security platform which provides asset discovery, vulnerability assessment, secure configuration assessment, web application scanning, digital certificate and public cloud management and the ability to assess security and compliance postures; For a fee, Qualys will provide infrastructure, cloud, web and endpoint security as well as software development vulnerability testing and security compliance validation.
  - https://www.qualys.com
- Quttera – Free scanning against website, blog or SharePoint site with analysis for malicious or suspicious files and blacklisted status, among other features; For a fee, the offer various anti-malware services.
  - https://quttera.com/

Free Scanning Tools (Cont.)

HHS does not endorse any tool or company in particular

- Detectify – Free 14 day domain scan for 1000+ vulnerabilities, including OWASP Top 10, CORS and Amazon S3 Bucket misconfigurations; For a fee, the services can be extended beyond 14-day trial period.
  - https://detectify.com/
- SiteGuarding – Free website analysis for malware, blacklisting, spam and defacement; Similar to SUCURI; For a fee, full enterprise website security is offered with this service.
  - https://www.siteguarding.com
- WebInspector – Free website analysis for malware, blacklisting, backdoors and Trojans, and heuristic viruses; For a fee, the same services can be offered as automated in addition to immediate notifications, network security and dashboard capabilities.
  - https://app.webinspector.com/
- Acunetix – Free website analysis for Trojans, auditing of Internet-facing servers, identifying system and network vulnerabilities, identify vulnerable and upgradable applications, and discovering information leaks; For a fee, more robust and comprehensive offerings of the free services are available.
  - https://www.acunetix.com
- Google Safe Browsing – Free website analysis to determine if it has malware, is associated with phishing or for any other reason is not safe to visit; There is no pay service associated with this service.
  - https://transparencyreport.google.com/safe-browsing/search

Free Scanning Tools (Cont.)

HHS does not endorse any tool or company in particular

- MetaDefender – Free scanning of IP address against 12 anti-malware sites or files/hashes against 43 anti-malware engines; For a fee, various network security products and cybersecurity services are offered.
  - https://metadefender.opswat.com/#!/
- VirusTotal – Free scanning of files, URLs, domains and hashes against dozens of malware engines to determine if they are malicious or infected. There is no pay service associated with this service.
  - https://www.virustotal.com
- ReScan Pro – Free malware scanner that searches for hidden redirects, obfuscated malware injects, spam, resident malware, defacements, adware/spyware, blacklist status and website errors. There is no pay service associated with this service.
  - https://rescan.pro/
- TinFoil Security – Free API and web scanner; Also, free vulnerability-specific scans available. For a fee, various additional scanning services are offered.
  - https://www.tinfoilsecurity.com/free-website-security-scan
- Vega – Free/open source web scanner; Identifies and validates SQL injections, cross-site scripting (XSS), inadvertently disclosed sensitive information, and other vulnerabilities. For a fee, various threat modelling, code review and penetration testing services are offered.
  - https://subgraph.com/vega/

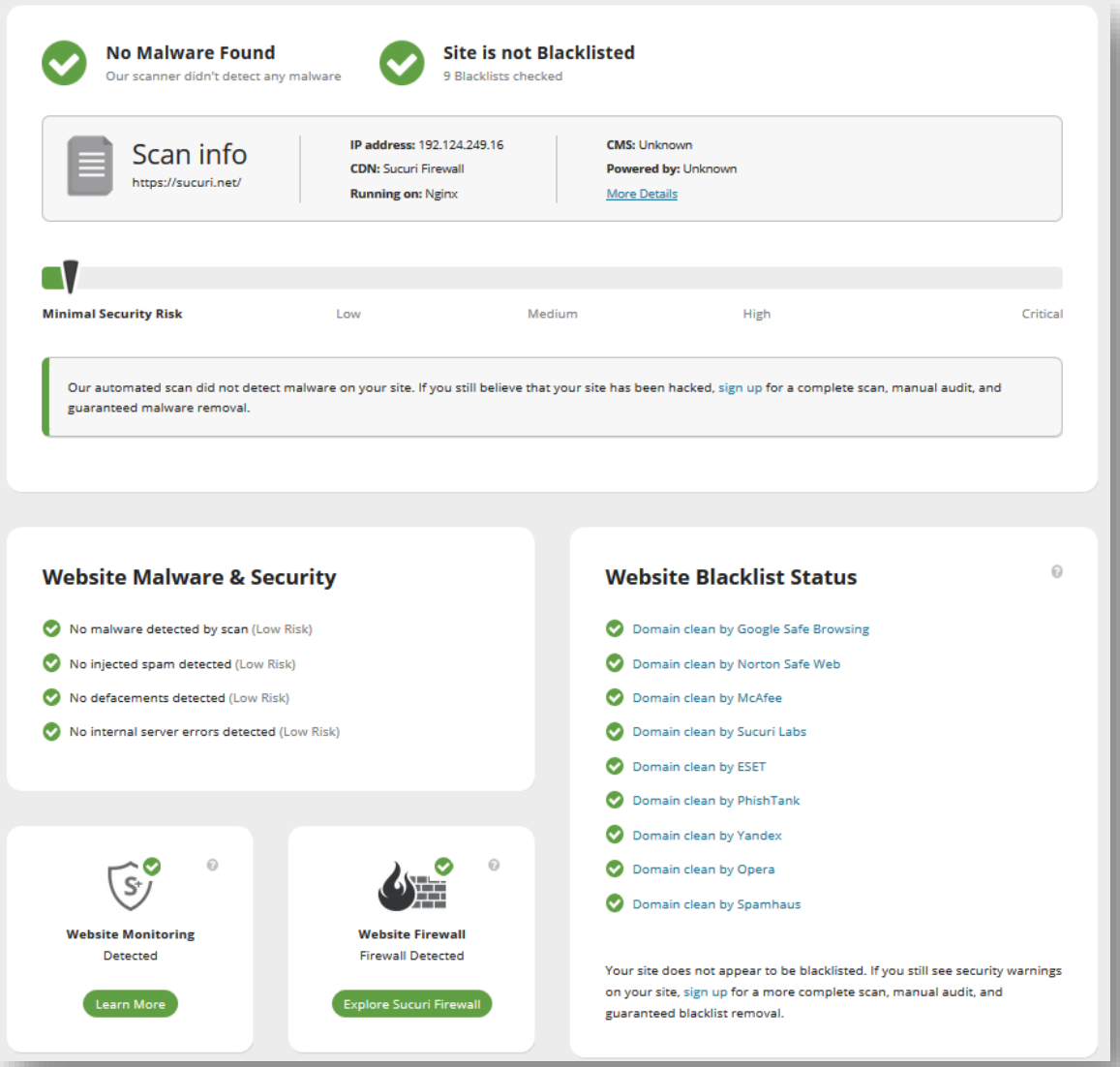
Free Scanning Tools (Cont.)

HHS does not endorse any tool or company in particular

- Hacker Combat – Free scanner for malware, blacklisting, back doors and many other forms of suspicious code. For a fee, various additional scanning services are offered.
  - https://hackercombat.com/website-malware-scanner/
- Arachni – Multi-platform, vulnerability detection engine in both command-line and web-based versions. No fee is charged unless the tool is used for commercial purposes.
  - https://www.arachni-scanner.com/
- Wapiti – Free command-line tool for auditing of websites and web applications including analysis for vulnerabilities, malware; Donations accepted
  - http://wapiti.sourceforge.net/
- Zed Attack Proxy (ZAP) – Free vulnerability detection tool; Donations accepted
  - https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Securi

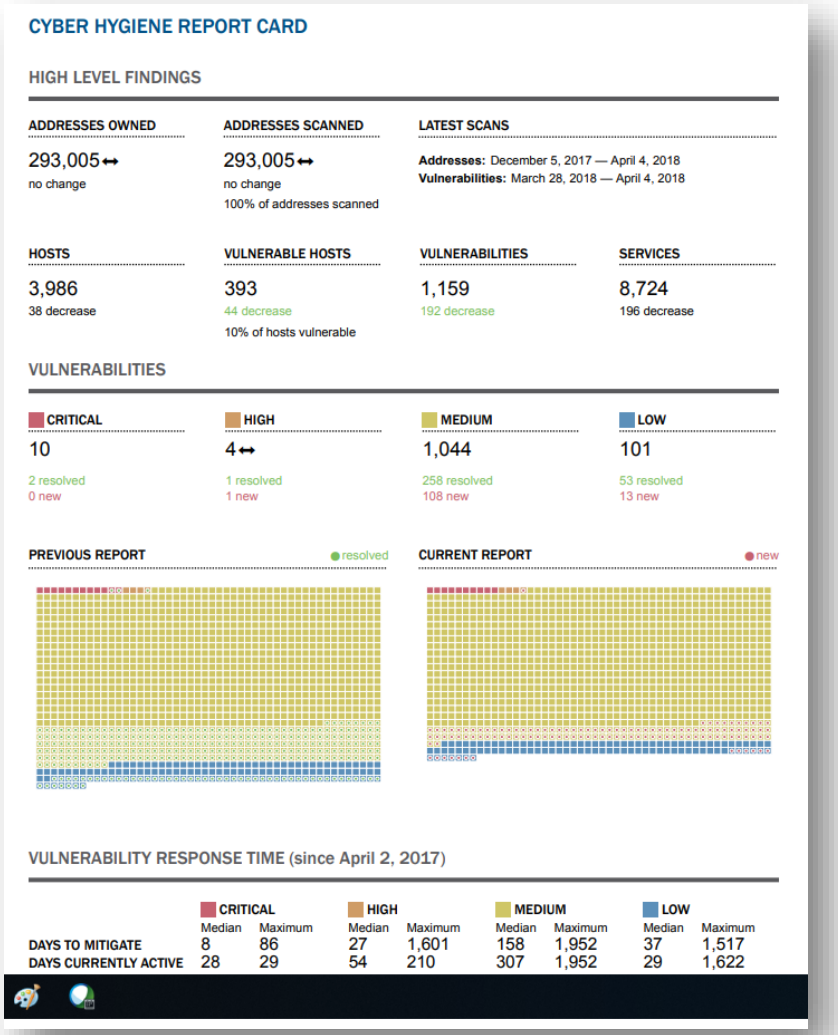
- **To reiterate: HHS does not endorse any tool in particular**
- A Securi scan was run against the Securi site as an example. The following data points were identified:
  - IP address
  - Type of firewall; firewall platform
  - Presence of malware, spam or defacements
  - Internal server errors
  - Blacklist status
  - Website monitoring services



DHS NCCIC

- Cyber Hygiene Assessment
  - Located here: https://www.us-cert.gov/resources/ncats
  - Sample (website) on right
  - Report includes:
    - Vulnerabilities (with rating)
    - Changes since last scan
    - Most frequently found vulnerabilities across enterprise
    - Most vulnerable systems across enterprise (based on quantity and severity of vulnerabilities)

- **We *DO* recommend the use of this resource**



CYBER HYGIENE REPORT CARD

HIGH LEVEL FINDINGS

ADDRESSES OWNED	ADDRESSES SCANNED	LATEST SCANS
293,005 ↔	293,005 ↔	**Addresses:** December 5, 2017 — April 4, 2018
no change	no change	**Vulnerabilities:** March 28, 2018 — April 4, 2018
	100% of addresses scanned	

HOSTS	VULNERABLE HOSTS	VULNERABILITIES	SERVICES
3,986	393	1,159	8,724
38 decrease	44 decrease	192 decrease	196 decrease
	10% of hosts vulnerable		

VULNERABILITIES

CRITICAL	HIGH	MEDIUM	LOW
10	4 ↔	1,044	101
2 resolved	1 resolved	258 resolved	53 resolved
0 new	1 new	108 new	13 new

PREVIOUS REPORT ● resolved

CURRENT REPORT ● new

VULNERABILITY RESPONSE TIME (since April 2, 2017)

	CRITICAL		HIGH		MEDIUM		LOW	
	Median	Maximum	Median	Maximum	Median	Maximum	Median	Maximum
DAYS TO MITIGATE	8	86	27	1,601	158	1,952	37	1,517
DAYS CURRENTLY ACTIVE	28	29	54	210	307	1,952	29	1,622

DHS NCCIC (Cont.)

7 Vulnerability Scan Results

For this period, CyHy detected 1,159 occurrences of 63 distinct vulnerabilities (10 critical, 4 high, 1,044 medium, and 101 low). SAMPLE should review the vulnerabilities detected and report any false positives back to NCATS so these can be excluded from future reports (see the Frequently Asked Questions section for more about false positives).

The scanning detected 393 vulnerable hosts—364 hosts with one to five vulnerabilities were identified; 24 hosts had between six and nine vulnerabilities; 4 hosts had ten or more vulnerabilities identified.

Severity	Distinct Vulnerabilities		Total Vulnerabilities	
Critical	5%	3	1%	10
High	5%	3	0%	4
Medium	68%	43	90%	1,044
Low	22%	14	9%	101
Total		63		1,159

Table 5: Number of Vulnerabilities by Severity Level

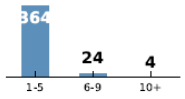


Figure 9: Vulnerability Count per Host

The CVSS scores for all active vulnerabilities can be found in Figure 10.

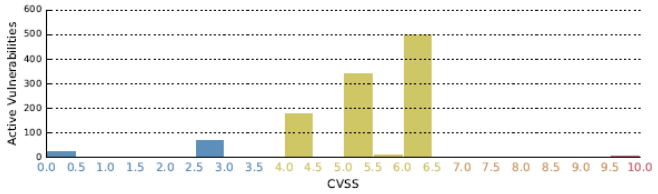


Figure 10: CVSS Histogram for Active Vulnerabilities

The top vulnerabilities according to CVSS score are represented in Table 6.

Vulnerability Name	Severity	Hosts	CVSS Score
MikroTik RouterOS < 6.41.3 SMB Buffer Overflow	Critical	4	10.0
MikroTik RouterOS HTTP Server Arbitrary Write RCE (ChimayRed)	Critical	3	10.0
Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE	Critical	3	10.0
PHP 5.6.x < 5.6.34 Stack Buffer Overflow	High	2	7.5
FTP Privileged Port Bounce Scan	High	1	7.5
SNMP Agent Default Community Name (public)	High	1	7.5
Apache Tomcat Default Files	Medium	2	6.8
AXIS gSOAP Message Handling RCE (ACV-116267) (Devil's Ivy)	Medium	1	6.8
SSL Certificate Cannot Be Trusted	Medium	319	6.4
SSL Self-Signed Certificate	Medium	180	6.4

Table 6: Top Vulnerabilities by CVSS

A complete list of distinct vulnerabilities detected, including severity level and number of hosts having the vulnerability can be found in Appendix A: Vulnerability Summary. Full details on every detected vulnerability can be found in Appendix C: Detailed Findings and Recommended Mitigations by Vulnerability. Every critical and high finding detected, along with the hosts that have these findings, are listed in Appendix D: Critical and High Vulnerability Mitigations by IP Address.

The top high-risk hosts are identified in Table 7 by combining the total number of vulnerabilities, the severity of the vulnerabilities, and a weighted CVSS score for vulnerabilities detected. For more information on the formula, please refer to Table 8: Risk Rating System.

IP Address	Critical	High	Medium	Low	Total
x.x.192.34	2	0	6	0	8
x.x.157.83	2	0	3	4	9
x.x.105.90	2	0	1	2	5
x.x.194.150	1	0	3	1	5
x.x.196.96	1	0	2	1	4
x.x.196.200	1	0	2	1	4
x.x.236.156	1	0	0	3	4
x.x.124.231	0	2	10	2	14
x.x.59.83	0	0	9	1	10
x.x.124.236	0	1	9	1	11

Table 7: Top Hosts by Weighted Risk

The Risk Rating System (RRS) emphasizes higher-rated CVSS scores to ensure that hosts with a large number of lower-risk vulnerabilities do not outweigh hosts with a smaller number of high-risk vulnerabilities, while ensuring that hosts with an extreme number of low-risk vulnerabilities are not overshadowed by hosts with a single higher-risk issue. The RRS also ensures that hosts with a significant number of high-risk vulnerabilities will not be overshadowed by a host with only a single critical vulnerability.

Table 8 illustrates the base and weighted CVSS scores and shows the equivalent number of lower-risk vulnerabilities to weigh evenly with a single critical (CVSS score of 10) vulnerability.

Base CVSS Score	Weighted CVSS Score	Equivalent to CVSS Score 10
1.0	1×10^{-06}	10,000,000.0
2.0	0.000,128	78,125.0
3.0	0.002,187	4,572.47
4.0	0.016,384	610.35
5.0	0.078,125	128.0
6.0	0.279,936	35.72
7.0	0.823,543	12.14
8.0	2.097,152	4.77
9.0	4.782,969	2.09
10.0	10.0	1.0

Table 8: Risk Rating System

As an example, a host having 400 vulnerabilities with a base CVSS score of 1.0 would get a weighted RRS score of 4×10^{-04}, which is considered lower-risk than a host with a single critical vulnerability (RRS score of 10.0). Similarly, a host having 4 vulnerabilities with a base CVSS score of 8 would get a RRS score of 8.39 and still be considered a lower risk than a host with a single critical vulnerability (RRS score of 10.0).

Additional Resources

- Remediation resources for web attacks
  - MITRE: Common Vulnerabilities and Exposures (https://cve.mitre.org/)
    - Standardized identifiers for cybersecurity vulnerabilities in order to avoid variation among solutions and resulting gaps in security coverage as well as lack of interoperability between security databases and tools.
  - NIST: National Vulnerability Database (https://nvd.nist.gov/)
    - U.S. government repository of standardized vulnerability management data represented using the Security Content Automation Protocol (SCAP) which enables automation of vulnerability management, security management and compliance efforts.
  - NIST: Special Publication 800-40 (Rev. 3) Guide to Enterprise Patch Management Technologies (https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final)
    - Provides assistance in understanding enterprise patch management technologies and relevant metrics as part of an overall risk management program.
  - Open Web Application Security Project (OWASP): is a not-for-profit international organization and an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. They advocate approaching application security through people, process, and technology solutions. (https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project)

Additional Resources (Cont.)

- Remediation resources for web attacks
  - SANS Reading Room: Patch Management (paper)
    - https://www.sans.org/reading-room/whitepapers/iso17799/paper/2064
  - A Practical Methodology for Implementing a Patch management Process (paper)
    - https://www.sans.org/reading-room/whitepapers/bestprac/paper/1206
  - Reducing Organizational Risk Through Virtual Patching
    - https://www.sans.org/reading-room/whitepapers/intrusion/paper/33589
  - Patch Management and the Need for Metrics
    - https://www.sans.org/reading-room/whitepapers/bestprac/paper/1461
  - Building a Vulnerability Management Program - A project management approach
    - https://www.sans.org/reading-room/whitepapers/projectmanagement/paper/35932
  - Agile Security Patching
    - https://www.sans.org/reading-room/whitepapers/bestprac/paper/38410

Outsourcing Cybersecurity

- A few recommendations for HPH organizations that outsource cybersecurity
  - Small business does not mean small target; often quite the opposite
  - There is no such thing as 100% security – not in the physical world and not in cyberspace
  - As much as possible, develop in-house talent and knowledge for quality assurance/quality control over vendors; maintain consistent POCs for vendors
  - The tools and resources available in this brief can be used to assist security vendors in doing their job and holding them accountable
  - Develop in-house policies and procedures to augment outsourced security such as:
    - Phishing training
    - Prompt account termination for departing employees
    - Principle-of-least-privilege policies towards access to IT resources

Takeaways

- Vulnerability management is a necessary but not sufficient component to a cybersecurity program, which is a part of an organization's risk management program; web security is part of all this
- Vulnerability management is an ongoing, never ending process
- Vulnerability management includes both scanning and remediation – both are critical
- Many free web scanning services and tools exist; it is imperative on the leadership for each organization to leverage their assets and resources as efficiently and effectively as possible
- We strongly recommend considering DHS's vulnerability scanning program
- We recommend examining the free tools that exist, including but not limited to the ones in this presentation, and consider how they can help your organization
- Cost-based vulnerability scanning tools can also be valuable. We recommend any consideration of such tools include a full risk assessment and cost analysis.
- There are consequences to small healthcare providers who do not protect their data:

BUSINESS StarTribune

All of records erased, doctor's office closes after ransomware attack

Michigan ransomware attack is worst-case scenario for providers.

By Joe Carlson Star Tribune | APRIL 6, 2019 — 6:33PM

Reference Materials

References

- Kumar, Chandan, 12 Online Free Tools to Scan Website Security Vulnerabilities & Malware, GeekFlare, January 14, 2019, https://geekflare.com/online-scan-website-security-vulnerabilities/
- 14 Best Open Source Web Application Vulnerability Scanners [Updated for 2019], Infosec Institute, January 21, 2019, https://resources.infosecinstitute.com/14-popular-web-application-vulnerability-scanners/#gref
- Open Web Application Security Project Vulnerability Scanning Tools, https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools
- Qualys Community Edition, https://www.qualys.com/community-edition/#/freescan
- Admin, Top 10 Vulnerability Assessment Scanning Tools, cWatch, March 16, 2018, https://cwatch.comodo.com/blog/website-security/top-10-vulnerability-assessment-scanning-tools/
- Ranger, Steve, At $30,000 for a flaw, bug bounties are big and getting bigger, ZDNet, July 5, 2017, https://www.zdnet.com/article/at-30000-for-a-flaw-bug-bounties-are-big-and-getting-bigger/
- Symantec Internet Security Threat Report Trends for July – December 07 (Volume XII), Symantec, April 2008, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf
- Brodkin, Jon, The top 10 reasons Web sites get hacked, Network World, October 4, 2007, https://www.networkworld.com/article/2286560/the-top-10-reasons-web-sites-get-hacked.html
- Patch Management Life Cycle, Manage Engine, https://www.manageengine.com/products/desktop-central/help/patch_management/patch_management_life_cycle.html
- MITRE - Common Vulnerabilities and Exposures database, https://cve.mitre.org/
- National Institute of Standards and Technology, National Vulnerability Database, https://nvd.nist.gov/
- Ruppert, Brad, Patch Management (white paper), SANS, January 24, 2008, https://www.sans.org/reading-room/whitepapers/iso17799/paper/2064
- Voldal, Daniel, A Practical Methodology for Implementing a Patch management Process (white paper), SANS, April 17, 2019, https://www.sans.org/reading-room/whitepapers/bestprac/paper/1206
- Souppaya , Murugiah and Scarfone, Karen, Special Publication 800-40 (Rev. 3) Guide to Enterprise Patch Management Technologies, National Institute of Standards and Technology, https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final
- Scan My Server, Beyond Security, https://scanmyserver.com/
- Securi, https://sucuri.net/
- Qualys Community Edition, https://www.qualys.com/community-edition/
- Quttera free scan: https://quttera.com/
- Detectify free trial: https://detectify.com/createaccount
- SiteGuarding free trial, https://www.siteguarding.com/en/signup
- WebInspector free website malware scanner: https://app.webinspector.com/
- Acunetix demo: https://www.acunetix.com/web-vulnerability-scanner/us-demo/
- Google Safe Browsing malware and phishing scanner: https://transparencyreport.google.com/safe-browsing/search
- OPSWAT site analyzer: https://metadefender.opswat.com/#!/
- VirusTotal URL and file analyzer: https://www.virustotal.com
- https://rescan.pro/
- https://www.tinfoilsecurity.com/free-website-security-scan
- https://subgraph.com/vega/

References

- Rescan Pro free web scanner: https://rescan.pro/
- TinFoil Security free website scanner: https://www.tinfoilsecurity.com/free-website-security-scan
- Vega free web security scanner: https://subgraph.com/vega/

Questions

Questions

Upcoming Briefs

- The Dark Overlord
- Attack Surface

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV