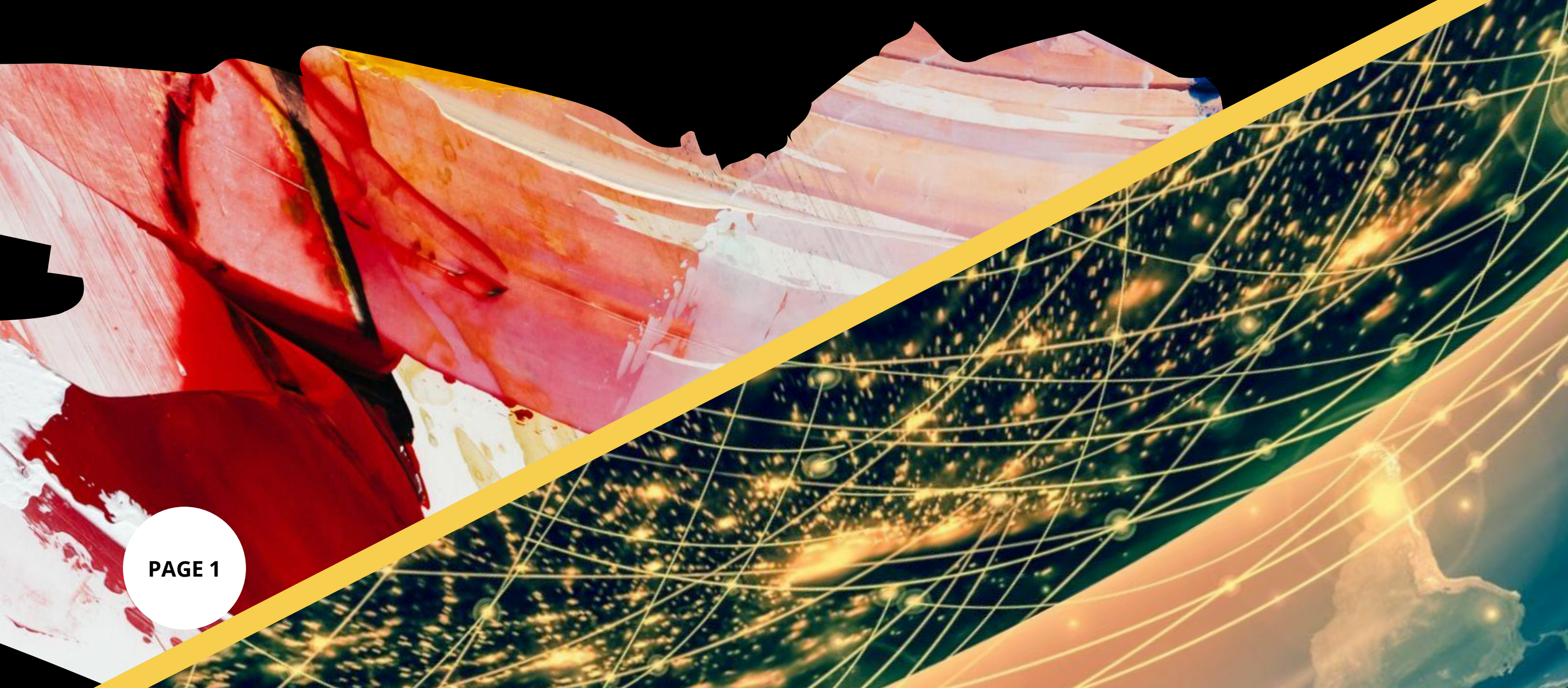
ALLENDEVAUX.COM

VULNERABILITY GUIDANCE



GETTING STARTED WITH VULNERABILITY MANAGEMENT

In this section, we will answer the following questions:

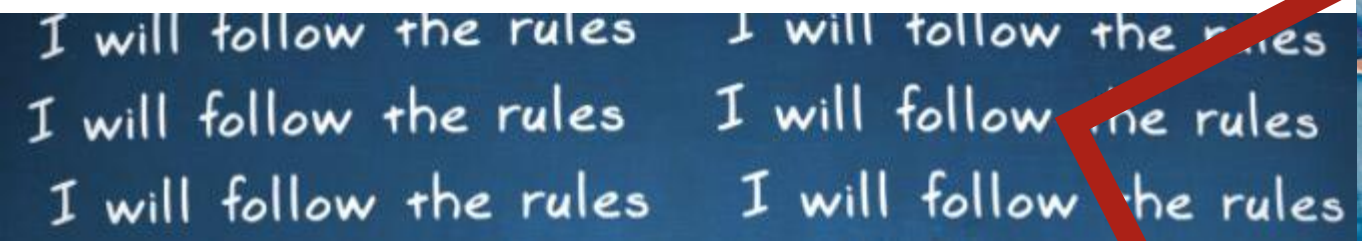
- What data is regulated that the enterprise collects and processes?
- What is a vulnerability scan and why is it important?
- What is the output of a vulnerability scan, and why does it matter?
- How can an enterprise perform a technical vulnerability scan?
- How often must technical vulnerability scans be performed?

When you collect and process regulated personal information from employees, customers, and others, there is a legal obligation to understand your responsibilities, with director liability for failure to do so. It is imperative for leadership to understand its obligations; extremely steep fines will be facing your organisation if there's a data breach and you failed to demonstrate due care and due diligence.

PART 1: WHAT DATA IS REGULATED THAT BUSINESSES COLLECT AND PROCESS?

Businesses around the world collect and process all kinds of information about individuals, including personal data regarding prospective customers, active customers, past customers, employees, and contractors. Information can come in various forms, such as:

- submitted employment applications,
- performance reports,
- financial information,
- health insurance information,
- identity data such as passport numbers,
- gender and sexual orientation,
- criminal record disclosure; and
- much more.



VULNERABILTY GUIDANCE

WHAT IS A VULNERABILITY SCAN?

Scanning an organisation's web portals, Internet firewalls and even its infrastructure (i.e., servers, if relevant) for hidden security "holes" or "gaps" is a foundational practice. This is a cybersecurity function termed technical vulnerability scanning. Scanning for technical vulnerabilities is important for many reasons:

- It uncovers hidden security holes that could be exploited by threats such as malware or hackers, resulting in a data breach;
- It reveals patches that have not been applied to firmware, operating systems and applications;
- It discovers insecure protocols in operation such as SNMPv1, SSLv3 or TLSv1.0, telnet, http vs https, and others;
- It satisfies a legal requirement in many parts of the world to demonstrate "sufficient guarantees to implement appropriate technical and organisation measures" of data protection (Article 28, the GDPR);
- It generates a list of remedial actions to address to tighten security and safeguard information entrusted to your organisation; and
- It demonstrates due care; and, when paired with correction action, it demonstrates due diligence.

Some regulations, such as those throughout the European Union, impose director liability to ensure organisations exercise due care and due diligence to protect the confidentiality of information. In essence, should a data breach occur, your organisation's senior management can be held legally and financially liable for your failure to understand the regulatory landscape, ensure approach technical measures were implemented, and technical vulnerability scanning was performed to measure the effectiveness of the safeguard's employed. In the European Union, fines of 20 million euros can be levied, an outcome the authors of this website aim to avoid.

WORLDWIDE REGULATIONS

Because this information would be highly damaging to the data subject if it was unlawfully disclosed (i.e. found through a Google search due to theft or other type of data breach), this data is regulated by governments around the world, and required to be protected. For instance, to quote a European law, organisations are required to "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk..." (Article 32 of the EU's GDPR). Other regulations around the world require similar measures. But what does this mean and how is it done?

ASSESSING & ADDRESSING VULNERABILITIES

Part 2: What is the Output of a Vulnerability Scan, and Why Does It Matter?

Whilst the immense growth of the Internet has enriched the world's 4.1 billion collaborators (Statista 2018), including businesses like yours from all around the world, it has also become a theatre of peril for the ill-prepared. Countless Internet villains await to pilfer their victims, and data breaches do real damage; they can result in financial loss, reputation damage, emotional distress, physical injury, and entangled litigation.

Hackers & netbots never stop hunting for weakness to exploit, scanning your websites, attempting to login to your systems, attempting to find backdoors, attempting to create an error that pries open a trap door to permit rogue code to infect your systems undetected.

Performing a vulnerability scan is a safe way to uncover and detect system weakness so that issues may be identified, catalogued by type, and scored in terms of severity.
The outcome of this activity produces a specific, actionable list of remedial tasks, such as disabling ports, replacing insecure protocols with secure protocols, applying a missing software patch, and other remedial steps that a technical person can perform.

Below is an example from an average report Allendevaux & Company performs for organizations on a regular basis. The example issues identified below are associated with hosts inside of this example network, noting the IP address and description of each device, the vulnerability found, the ports affected, and the severity level.

Three Vectors of Vulnerability Scanning

1 Internet Facing Perimeter Devices

Things such as routers, firewalls, etc. that have public IP addresses or direct IP-to-IP routing from a public address to an internal address

2 Web Portals

It's not uncommon to have many web portals for larger organisations

3 Internet Hosts Across All Subnets

This includes servers, workstations, switches, wireless access points, printers, IoT devices, IP cameras, and anything else that has an IP address

VULNERABILITY GUIDANCE

VULNERABILITY RESULTS EXAMPLE

19 .1.240 (gateway1-chalet, -) Ubuntu / Tiny Core Linux / Linux 2.6.x

Vulnerabilities (6)

3	SSL/TLS Server supports TLSv1.0	port 443/tcp over SSL	New
2	SSL Certificate - Self-Signed Certificate	port 443/tcp over SSL	New
2	SSL Certificate - Subject Common Name Does Not Match Server FQDN	port 443/tcp over SSL	New
2	SSL Certificate - Improper Usage Vulnerability	port 443/tcp over SSL	New
2	SSL Certificate - Signature Verification Failed Vulnerability	port 443/tcp over SSL	New
2	HTTP Security Header Not Detected	port 443/tcp	New

19 .1.241 (commteam1, COMMTEAM1) Windows 10 Pro

Vulnerabilities (1)

2	NetBIOS Name Accessible		New

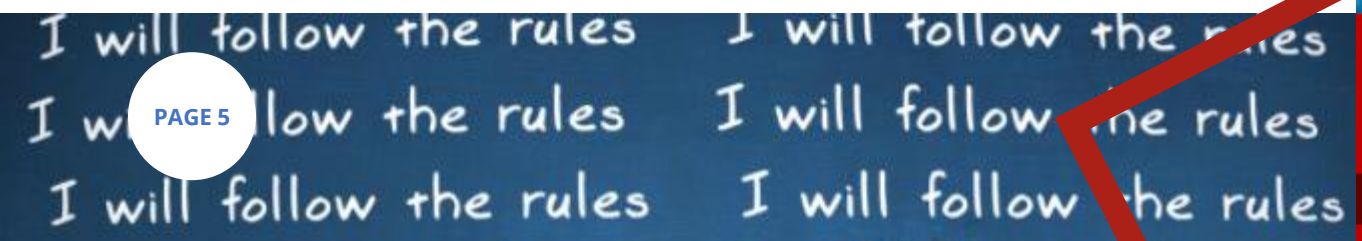
19 .1.243 (ysrv05, YSRV05) Ubuntu / Fedora / Tiny Core Linux / Linux 3.x

Vulnerabilities (36)

4	Remote User List Disclosure Using NetBIOS		New
4	Null Session/Password NetBIOS Access		New
3	NetBIOS Shared Folder List Available		New
3	WINS Domain Controller Spoofing Vulnerability - Zero Day		New
3	NetBIOS Name Conflict Vulnerability		New
3	NetBIOS Release Vulnerability		New
3	PhpMyAdmin Multiple Vulnerabilities (PMASA-2018-3,PMASA-2018-4)	port 80/tcp	New
3	PhpMyAdmin Cross-Site Scripting Vulnerability (PMASA-2018-5)	port 80/tcp	New
3	Web Server Uses Plain-Text Form Based Authentication	port 80/tcp	New

A severity level of 5 is usually given emergency status, meaning intruders can easily gain control of the host and compromise the system.

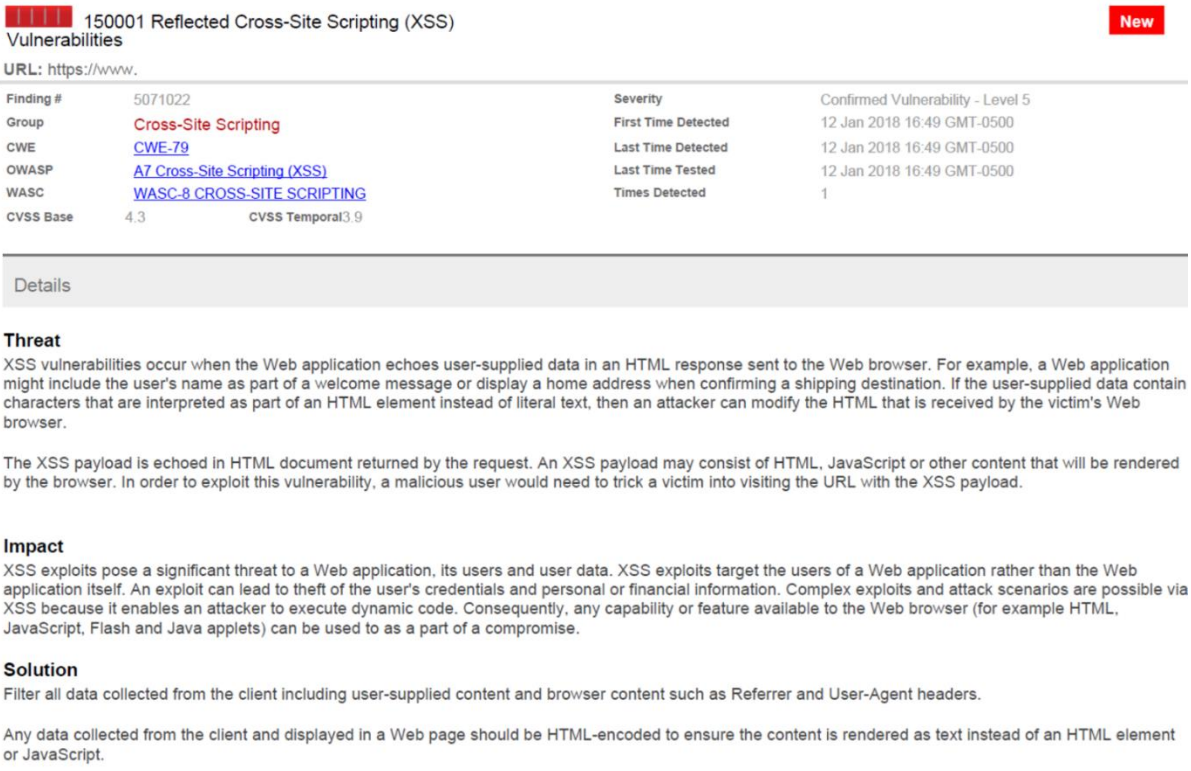
A severity rating of 4 is critical, because intruders can likely gain control of the host and compromise the system.



VULNERABILITY GUIDANCE

VULNERABILITY RESULTS EXAMPLE

Here's another look at a finding from a website scan. In this example below, we'll look at a fictitious university web portal (based on some real findings we did in a real engagement). Here we see a reflected cross-site scripting (XSS) vulnerability was found within the organization's website. When this vulnerability is exploited, a rogue hacker can reflect all the information someone types into the university portal. For instance, if someone fills out an application for a class, provides sensitive data, provides credentials or any other data into the portal, it can be reflected elsewhere in the Internet to capture all the text without the knowledge of the user or the university.



150001 Reflected Cross-Site Scripting (XSS) Vulnerabilities

New

URL: https://www.

Finding #	5071022	Severity	Confirmed Vulnerability - Level 5
Group	Cross-Site Scripting	First Time Detected	12 Jan 2018 16:49 GMT-0500
CWE	CWE-79	Last Time Detected	12 Jan 2018 16:49 GMT-0500
OWASP	A7 Cross-Site Scripting (XSS)	Last Time Tested	12 Jan 2018 16:49 GMT-0500
WASC	WASC-8 CROSS-SITE SCRIPTING	Times Detected	1
CVSS Base	4.3	CVSS Temporal	3.9

Details

Threat

XSS vulnerabilities occur when the Web application echoes user-supplied data in an HTML response sent to the Web browser. For example, a Web application might include the user's name as part of a welcome message or display a home address when confirming a shipping destination. If the user-supplied data contain characters that are interpreted as part of an HTML element instead of literal text, then an attacker can modify the HTML that is received by the victim's Web browser.

The XSS payload is echoed in HTML document returned by the request. An XSS payload may consist of HTML, JavaScript or other content that will be rendered by the browser. In order to exploit this vulnerability, a malicious user would need to trick a victim into visiting the URL with the XSS payload.

Impact

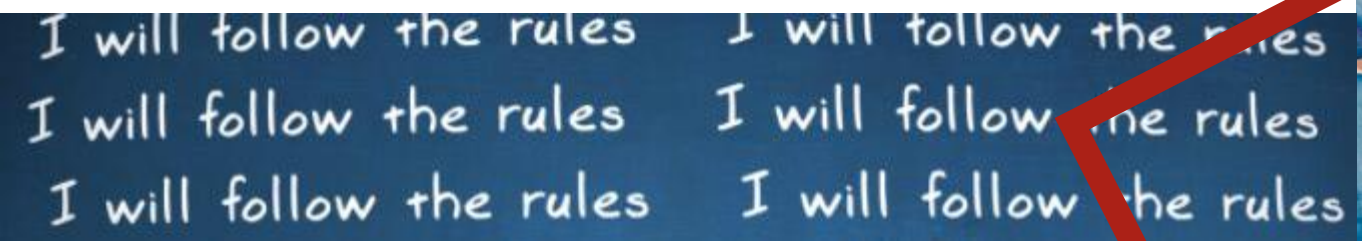
XSS exploits pose a significant threat to a Web application, its users and user data. XSS exploits target the users of a Web application rather than the Web application itself. An exploit can lead to theft of the user's credentials and personal or financial information. Complex exploits and attack scenarios are possible via XSS because it enables an attacker to execute dynamic code. Consequently, any capability or feature available to the Web browser (for example HTML, JavaScript, Flash and Java applets) can be used to as a part of a compromise.

Solution

Filter all data collected from the client including user-supplied content and browser content such as Referrer and User-Agent headers.

Any data collected from the client and displayed in a Web page should be HTML-encoded to ensure the content is rendered as text instead of an HTML element or JavaScript.

The final output of a comprehensive scan results in a report that provides overall findings and actionable recommendations. The report's executive summary provides a comprehensive, independent auditor's report, usually addressed to the highest levels of leadership per regulatory requirements.



PART 3: HOW CAN MY BUSINESS PERFORM A TECHNICAL VULNERABILITY SCAN?

This is a question that's commonly asked, and usually the advice given is this: don't try this yourself. Technical staff at your business might try to convince management that they can download a free scanner, initiate a scan, and produce a report. But the report won't be trustworthy; in fact, it will give false confidence. Most regulations require strict guidelines of competency and experience, requiring cybersecurity activities to be overseen by certified practitioners.

Seek the assistance of a certified cybersecurity firm; yes, it will require funding to do, but this is not an area in which to skimp. **Send an email to infosec@allendevaux.com for help.**

HOW WE CAN HELP

If your business or organization wants the service of Allendevaux & Company, we can help; we approach cybersecurity activities in conformance with ISO/IEC 27032 international best practices. The highlights of the process are as follows:

- Initiate communication by sending an email to infosec@allendevaux.com, stating your business/organization name, and a contact person with whom we can work.
- Setup a discussion via phone, Skype, Zoom, BlueJeans, or another compatible way of communication; face-to-face video conversations are best, where screensharing is permitted.
- Generate an inventory of websites used by your business. For instance, when recently working with a university, just one of their campuses had 10 different web domains with hosted websites.
- Generate an inventory of Internet-facing devices, such as firewalls or routers.
- Determine if an internal scan will be conducted; if so, generate an IP list, or discuss setting up a discovery scan by network.
- Choose the scan date/time.
- Conduct the scan.
- Generate the report.
- Review the report with key stakeholders.

Activities will be performed by a team of professionals and overseen by an accredited ISO/ANSI and/or IBITGQ certified professional. As noted above, the output of these activities result in a proper report with actionable recommendations.

PART 4: HOW OFTEN MUST TECHNICAL VULNERABILITY SCANS BE PERFORMED?

At the very minimum, scanning should be performed annually. Without regular vulnerability scanning, scoring and incident mitigation, exploits cannot be mitigated, resulting in an increased risk of attack. Gartner Group recommends an enterprise establish and practice a monthly model to discover and remediate vulnerabilities that would otherwise accumulate (Chuvakin & Barros, 2015). Qualys recommends an enterprise establish a systematic model to regularly scan its information assets (Qualys, 2016). The Centre for Internet Security as reported by Tripwire recommends monthly scanning as a minimum baseline (Khimji, 2016).
The reason professionals push for frequent scanning is this: When a vulnerability is first released, it may have a lower vulnerability score (i.e. SEV2 or SEV3) because there is no known exploit. But as time passes, exploits often become available and the severity increases further underscoring the need for regularly vulnerability management.

Ultimately, the decision as to the frequency of performing a scan is up to each organisation, a function of risk appetite and affordability. Set your schedule and document your decision in terms of your technical vulnerability management policy.

REFERENCES

Chuvakin, A., & Barros, A. (2015, November 17). How to Implement Enterprise Vulnerability Assessment. Gartner. Retrieved February 1, 2017, from https://www.gartner.com/doc/3169219

Khimji, I. (2016, January 10). Vulnerability Management Program Best Practices -- Part 1. Tripwire. Retrieved February 1, 2017, from https://www.tripwire.com/state-of-security/vulnerability-management/vulnerability-management-program-best-practices-part-1/

Palmaers, T. (2013, March 23). Implementing a Vulnerability Management Process. (D. Distler, Ed.) SANS Institute InfoSec Reading Room. Retrieved January 30, 2017, from https://www.sans.org/reading-room/whitepapers/threats/implementing-vulnerability-management-process-34180

Qualys. (2016, February 4). Best Practices for Scanning. Qualys Community. Retrieved February 1, 2017, from https://community.qualys.com/docs/DOC-3814

Statista. (2018, October 1). Global digital population as of October 2018. Retrieved January 4, 2019, from https://www.statista.com/statistics/617136/digital-population-worldwide/

CONTACT US

info@allendevaux.com

US East: +1 513 401 7107
US West: +1 213 279 1055

UK: +44 2038 802 321
CH: +41 44 585 91 15

www.allendevaux.com

ALLENDEVAUX.COM