



Your *vulnerability Management* Sucks

There's a lot more to vulnerability management than running scans, performing penetration tests, and patching systems.



Hi, my name is *@HollyGraceful*,

I break into computers for a living.



What are we talking about?



Vulnerability Management



Vulnerability Management is the process of optimising your organisation's ability to identify, triage, manage, and report on your exposure to vulnerabilities over time.

Identify, Triage, Manage, Report

Vulnerability Management



It's not just monitoring vulnerabilities, it's not just patching issues, it's not just running scans and penetration tests.



Your Vulnerability Management Sucks
Holly Grace Williams, MD at Akimbo

www.AkimboCore.com
@AkimboCore

System Integration

Vulnerability Management should tie in to:

- Vulnerability Scanning
- Penetration Testing
- Asset Management
- Risk Management

The Worst Case



A penetration tester finds a critical vulnerability during a test:

What happens next?

How are retests conducted?

How is a partial remediation reported?

The screenshot shows a report entry for CVE-2015-17513. The title is "5. Internal Infrastructure Assessment" and the sub-section is "5.1. Multicast Name Resolution Enabled". The risk rating is "Critical" with a CVSS v3.1 score of 9.3. The CVSS vector is "CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N". The description explains that Link-local Multicast Name Resolution (LLMNR) is enabled by default on Windows machines and is used as a fallback for DNS. It notes that LLMNR can be abused by threat actors to perform an interception attack, leading to credential theft or password hash disclosure. The recommendation is to disable Multicast Name Resolution. Two methods are provided: Centralised Configuration with Group Policy and Local Device Configuration. The local device configuration includes a registry path and a PowerShell command to set the registry value to 0.

5. Internal Infrastructure Assessment

5.1. Multicast Name Resolution Enabled

Risk Rating: Critical
CVSS v3.1: 9.3
CVSS Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N

Link-local Multicast Name Resolution (LLMNR) is enabled by default on Windows machines and is used as a fallback for DNS. If a machine requests a hostname, such as when attempting to connect to a file-share, and the DNS server doesn't have an answer – either because the DNS server is temporarily unavailable or the hostname was incorrectly typed – then a LLMNR request will be sent.

LLMNR can be abused by threat actors to perform an interception attack and this may lead to credential theft or password hash disclosure. Where SMB signing is disabled, which it is by default on Windows machines, these issues can often be combined to lead to command execution against vulnerable machines.

5.1.1. Recommendation

It is recommended that Multicast Name Resolution is disabled.

Centralised Configuration with Group Policy

To enforce this configuration centrally using Group Policy, set the following entry to Enabled:

Computer Configuration → Policies → Administrative Templates → Network → DNS Client → Turn off multicast name resolution

Local Device Configuration

If the device is not centrally managed with group policy you can configure this option by setting the following registry value to 0 with type REG_DWORD:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient:EnableMulticast
```

Alternatively, this policy can be enforced programmatically with the following PowerShell command executed with administrative privileges:

```
New-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient" -Name "EnableMulticast" -Value 0 -PropertyType "DWORD" -force
```

Handling Data



Sadly Microsoft Excel is one of the most common tools companies use for vulnerability management.

Outstanding Vulnerabilities					
No	Vulnerability Description	Exposure	Severity	Risk	Comments / Additional Info
V1	Open URL Redirect	3	3	1.8	Open Redirect vulnerabilities occur where a web application include a function that redirects to another site or page, and the destination is controlled by a variable that can be controlled by the user such as a URL parameter. Thereby allowing a threat actor to craft a link which when clicked will redirect a user to a malicious page.
V2	Stored Cross-site Scripting	3	4	2.4	Cross-site Scripting (XSS) issues occur where user supplied input is insecurely included within a server response, or insecurely processed by a client-side script. If the payload is included with the response that immediately follows the request containing the payload then this is known as Reflected XSS. It is also sometimes referred to as Non-persisted XSS. If the payload is stored by the server and returned in a later response, it is known as Stored XSS, or Persistent XSS.
V3	CBC Ciphers in Use	5	1	1	The use of CBC is now generally discouraged in favour of more secure options such as Galois/Counter Mode (GCM) and Counter with CBC-MAC (CCM).
V4	Information Disclosure: Internal IP Address	5	1	1	The remote web servers disclose their internal IP addresses in response to a crafted HTTP request. This information is not useful to users of the applications but may assist an attacker in launching further attacks into the internal network.

Improving Maturity



You need established secure communications between the tester, management, and the remediation team.

That could just be a slack chat but have the thought:
"Am I comfortable with the tester sharing sensitive information about our systems on this channel?"

The Worst Option

"Send me an encrypted email"

Encrypted using what mechanism?

How are we handling an follow up discussion?

How will this discussion be attached to the vulnerability and the asset?

Vulnerability Management

AKIMBOCORE



The screenshot shows a dashboard with a red header containing navigation links: Platform, Services, Articles, and About Us. Below the header, there are buttons for 'Published', 'Medium', 'Edit', and 'Workflow'. The main content area is titled 'Stored Cross-site Scripting (XSS)'. It contains three paragraphs of text describing XSS, its types (Reflected, Non-persisted, Stored), and how it is exploited. To the right of the main content is a 'Vulnerability Notes' section with a light blue background, containing the author's name, the date and time the issue was noted, and a detailed description of the issue's status and impact.

Vulnerability Notes

Author: HollyGraceful (Holly)

Noted: 2022-03-11 11:05:53

This issue was partially remediated. It originally impacted the `Address.Line1`, `Address.Line2`, and `Address.Town` parameters, however it has been partially fixed but is still outstanding in `Address.Town` - the original payload can still exploit this issue using that parameter.

Your Vulnerability Management Sucks
Holly Grace Williams, MD at Akimbo

www.AkimboCore.com
@AkimboCore

The Worst Option

AKIMBOCORE



We think we've fixed Vuln #7, can you retest it?

Vuln #7 from the last test or the one before?

From the retest report or the original report?

From the infrastructure or the web app?

Your Vulnerability Management Sucks

Holly Grace Williams, MD at Akimbo



www.AkimboCore.com

@AkimboCore

Vulnerability Management

AKIMBOCORE



Platform Services Articles About Us  

Platform | Notifications | Thread

Reply

Vulnerability Assigned
From: Test.User1
To: HollyGraceful (Holly)
Sent: 2022-03-11 11:13:15

Heya, I reckon I've fixed this one.
I implemented `htmlspecialchars()` before the text is sent to `print()` so it should HTML Entity encode the output like you suggested.
Can you take a look?

Impact

Critical

High

Medium

Low

Info

Hardening

Accepted

Fixed

Your Vulnerability Management Sucks
Holly Grace Williams, MD at Akimbo

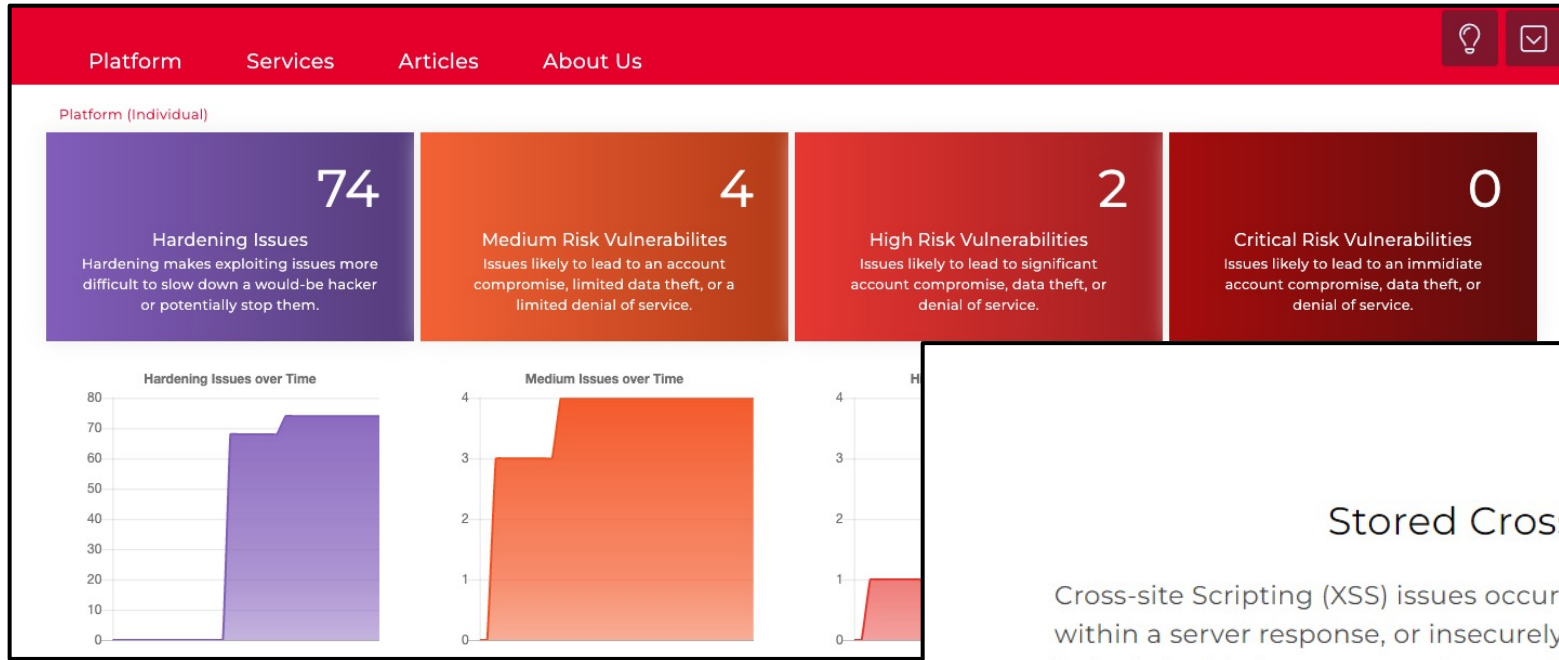
www.AkimboCore.com
@AkimboCore

The Worst Option

"Your Penetration Test report is ready, I have attached it to the email in an encrypted ZIP file, I will text you the password".

Vulnerability Management

AKIMBOCORE



Published Medium Edit

Stored Cross-site Scripting (XSS)

Cross-site Scripting (XSS) issues occur where user supplied input is insecurely included within a server response, or insecurely processed by a client-side script. If the payload is included with the response that immediately follows the request containing the payload then this is known as Reflected XSS. It is also sometimes referred to as Non-persisted XSS. If the payload is stored by the server and returned in a later response, it is known as Stored XSS, or Persistent XSS.

Exploitation typically allows for confidential data theft, virtual defacement, malicious software distribution or account takeover.

Your Vulnerability Management Sucks
Holly Grace Williams, MD at Akimbo

www.AkimboCore.com
@AkimboCore

Vulnerability Management

AKIMBOCORE



Download Documents



[PenetrationTest_Acme_20220217.pdf](#)

Penetration Test report for Acme Infrastructure and Web App, 16-17

Feb 2022

2022-02-18 11:31



**That was a lot of words,
Just give me the
summary.**



Summary

- If your vulnerability management system is copying vulnerabilities from a PDF into an Excel spreadsheet. You are doing it wrong.

Summary

AKIMBOCORE

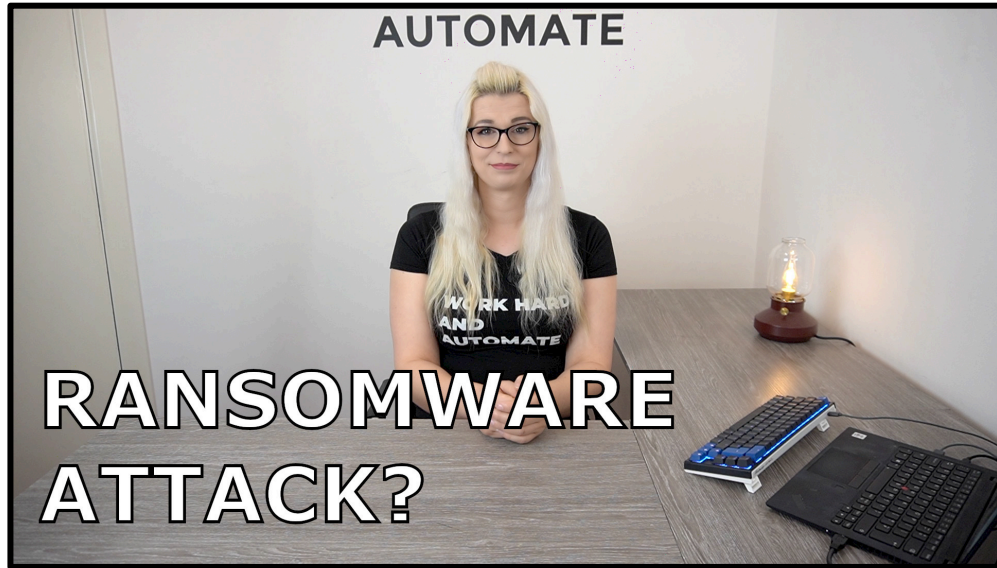


Your vulnerability management system should:

- Enable you to share vulnerability information quickly and securely.
- Allow you to discuss vulnerabilities.
- Mark risk on a per-asset level.
- Assign vulnerabilities for remediation.
- Track a vulnerability from detection, to fix, to retest, to second remediation, to oh no it's come back, to phew we finally fixed it.

Thanks for Watching!

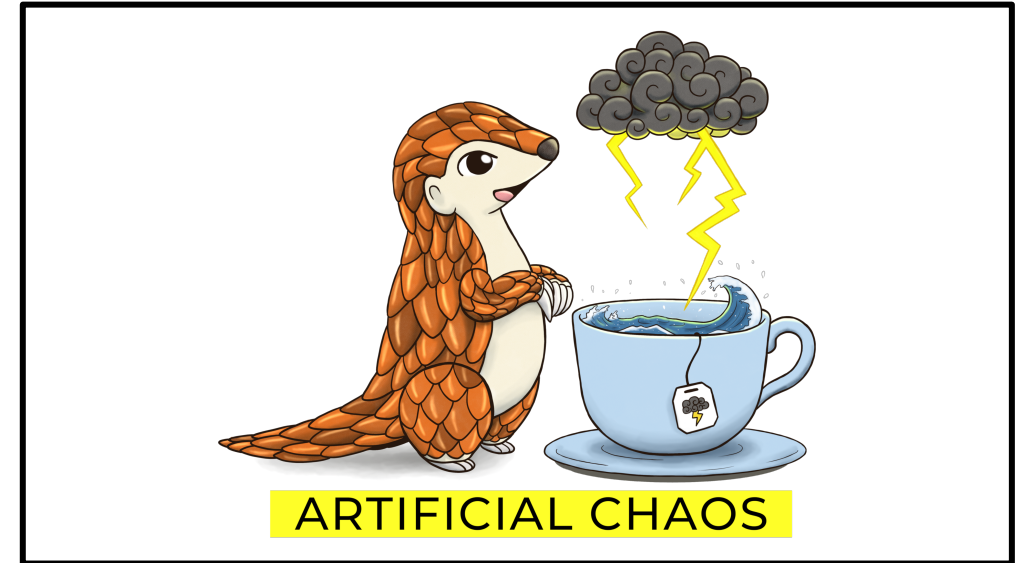
AKIMBOCORE



 [AkimboCore.com/youtube](https://www.akimboCore.com/youtube)

 [AkimboCore.com/linkedin](https://www.akimboCore.com/linkedin)

 [AkimboCore.com/twitter](https://www.akimboCore.com/twitter)



 Listen on
Apple Podcasts

 Listen on
Spotify

 Listen on
Overcast

Your Vulnerability Management Sucks
Holly Grace Williams, MD at Akimbo

www.akimboCore.com
@AkimboCore