Sécuriser un site web

3 Axes de travail

→ 08/12/2025

Sommaire

01 **Contexte**

02 **Durcissement de l’OS**

03 **Bonnes pratiques de configuration**

04 **Contrôles applicatifs**

05 **Aller plus loin**

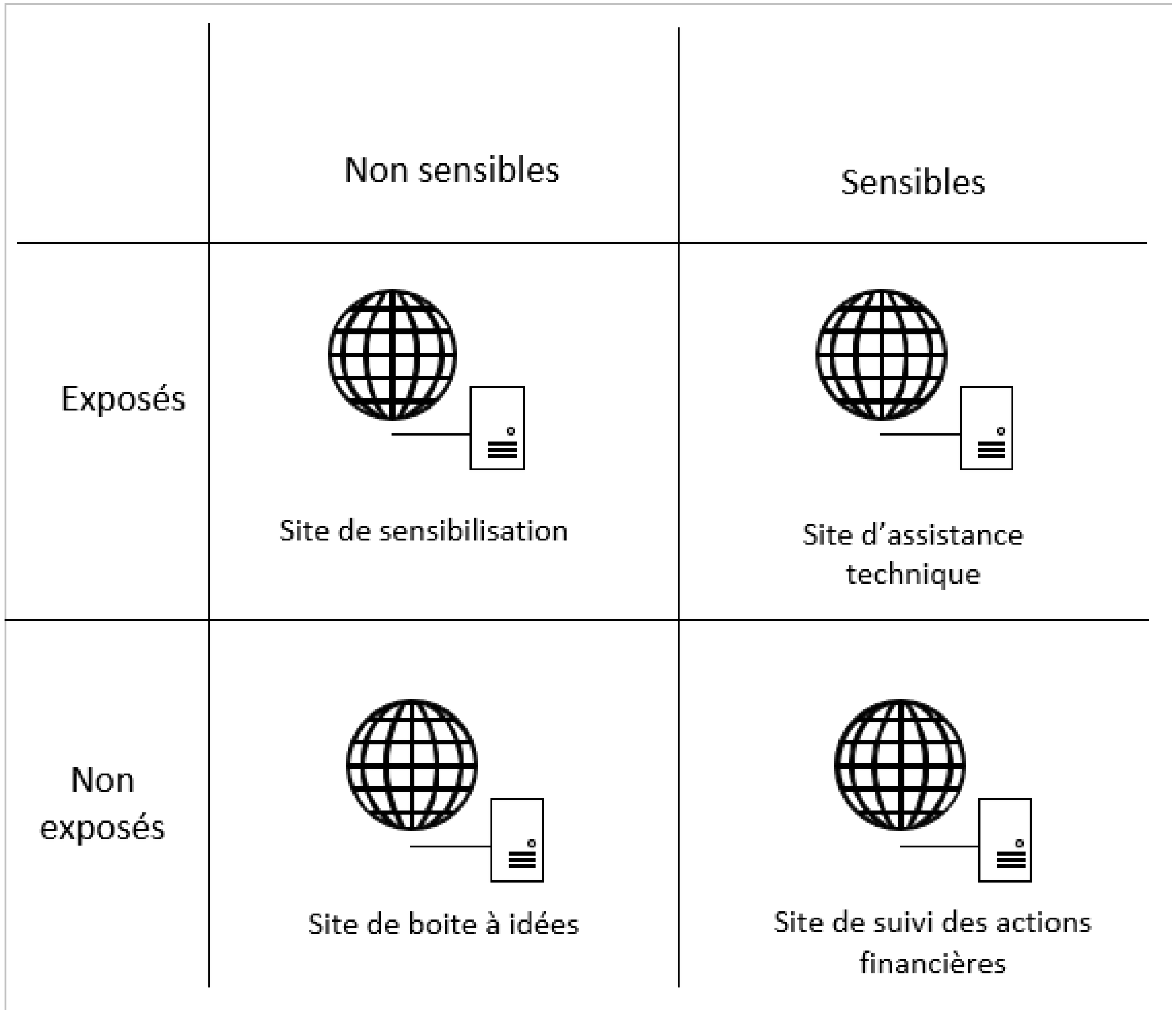
01 Mise en contexte

Contexte

Déploiement de nouveau service

Quatre cas possible :

- **Plateforme sensible exposée**
- **Plateforme non sensible exposée**
- **Plateforme sensible non exposée**
- **Plateforme non sensible non exposée**



	Non sensibles	Sensibles
Exposés	Site de sensibilisation	Site d’assistance technique
Non exposés	Site de boite à idées	Site de suivi des actions financières

02 Durcissement de l’OS

OpenScap

- **Open Source**

- **Utilisation des SCAP :** Security Content Automation Protocol

- **Utilisé par plusieurs types d’organismes : gouvernementaux, entreprise public et privé.**

- **Bases notables: NIST, SCAP, STIG, ANSSI**

- **Objectif :**
  - **Renforcer la partie OS**
  - **Vérifier les vulnérabilités**
  - **Valider les configurations**

OpenSCAP
Audit, Fix and be Merry

Government Users

Corporations and E-commerce

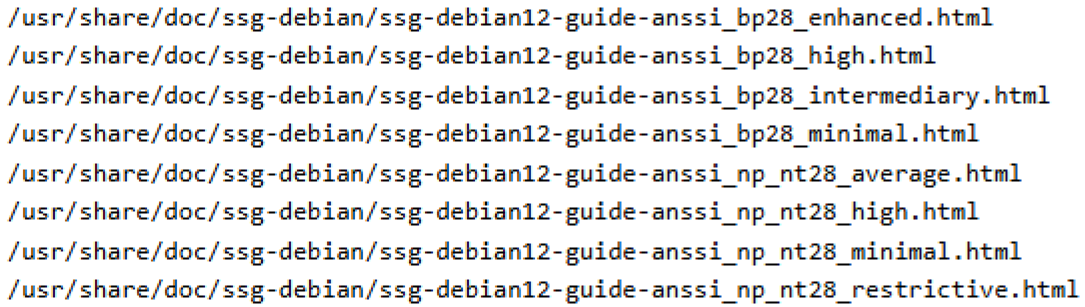
Open Source Community

OpenScap

Initialisation

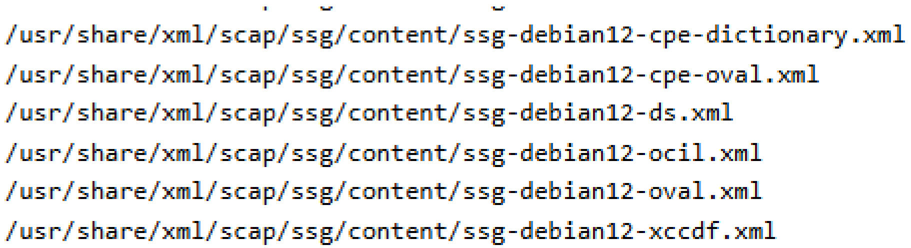
```
apt -y install openscap-scanner openscap-utils bzip2

apt –y install ssg-debian

wget https://www.debian.org/security/oval/oval-definitions-bookworm.xml.bz2

bzip2 -d oval-definitions-bookworm.xml.bz2
```

Documentation :



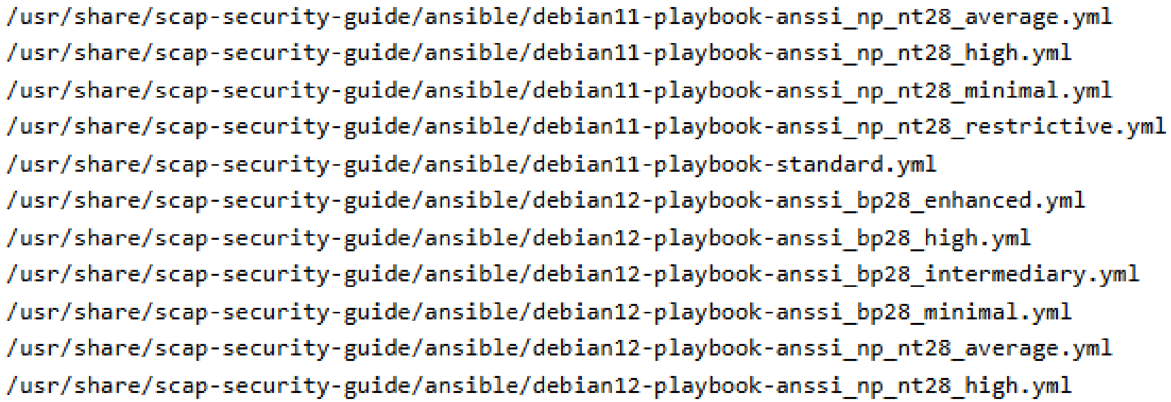
```
/usr/share/doc/ssg-debian/ssg-debian12-guide-anssi_bp28_enhanced.html
/usr/share/doc/ssg-debian/ssg-debian12-guide-anssi_bp28_high.html
/usr/share/doc/ssg-debian/ssg-debian12-guide-anssi_bp28_intermediary.html
/usr/share/doc/ssg-debian/ssg-debian12-guide-anssi_bp28_minimal.html
/usr/share/doc/ssg-debian/ssg-debian12-guide-anssi_np_nt28_average.html
/usr/share/doc/ssg-debian/ssg-debian12-guide-anssi_np_nt28_high.html
/usr/share/doc/ssg-debian/ssg-debian12-guide-anssi_np_nt28_minimal.html
/usr/share/doc/ssg-debian/ssg-debian12-guide-anssi_np_nt28_restrictive.html
```

Fichiers Scap



```
/usr/share/xml/scap/ssg/content/ssg-debian12-cpe-dictionary.xml
/usr/share/xml/scap/ssg/content/ssg-debian12-cpe-oval.xml
/usr/share/xml/scap/ssg/content/ssg-debian12-ds.xml
/usr/share/xml/scap/ssg/content/ssg-debian12-ocil.xml
/usr/share/xml/scap/ssg/content/ssg-debian12-oval.xml
/usr/share/xml/scap/ssg/content/ssg-debian12-xccdf.xml
```

Ansible

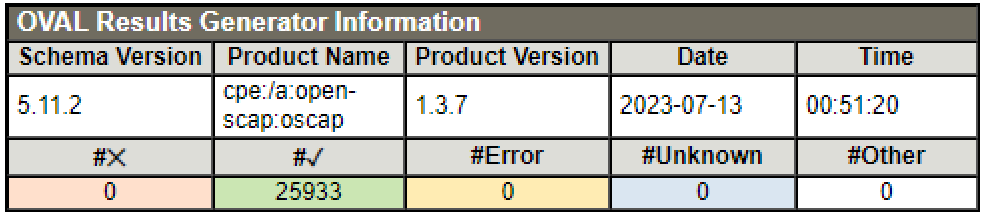


```
/usr/share/scap-security-guide/ansible/debian11-playbook-anssi_np_nt28_average.yml
/usr/share/scap-security-guide/ansible/debian11-playbook-anssi_np_nt28_high.yml
/usr/share/scap-security-guide/ansible/debian11-playbook-anssi_np_nt28_minimal.yml
/usr/share/scap-security-guide/ansible/debian11-playbook-anssi_np_nt28_restrictive.yml
/usr/share/scap-security-guide/ansible/debian11-playbook-standard.yml
/usr/share/scap-security-guide/ansible/debian12-playbook-anssi_bp28_enhanced.yml
/usr/share/scap-security-guide/ansible/debian12-playbook-anssi_bp28_high.yml
/usr/share/scap-security-guide/ansible/debian12-playbook-anssi_bp28_intermediary.yml
/usr/share/scap-security-guide/ansible/debian12-playbook-anssi_bp28_minimal.yml
/usr/share/scap-security-guide/ansible/debian12-playbook-anssi_np_nt28_average.yml
/usr/share/scap-security-guide/ansible/debian12-playbook-anssi_np_nt28_high.yml
```

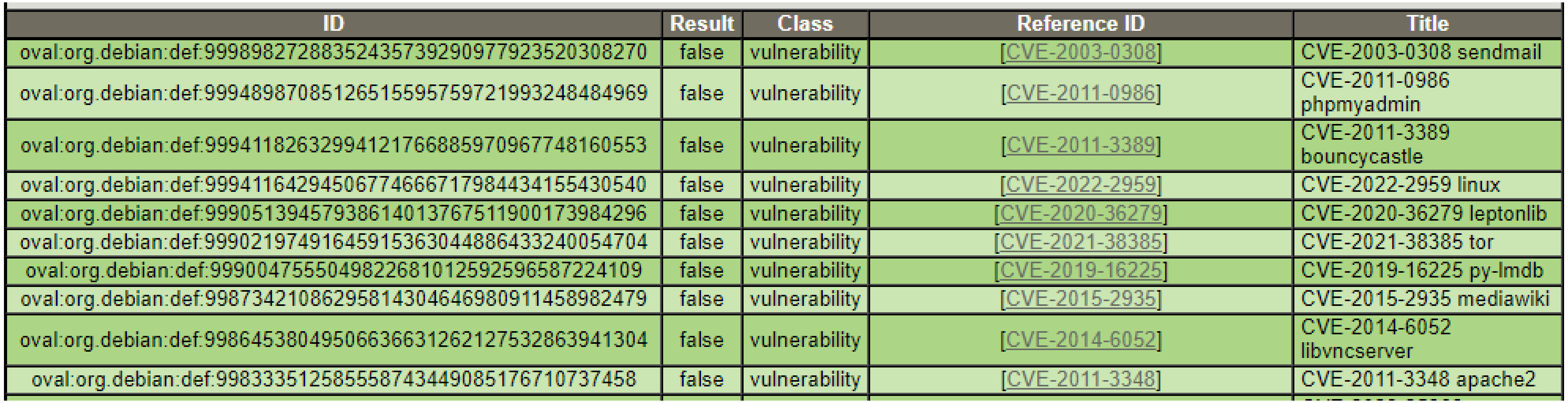
OpenScap

Scanning

```
oscap oval eval --report oval-bookworm.html
oval-definitions-bookworm.xml
```



OVAL Results Generator Information				
Schema Version	Product Name	Product Version	Date	Time
5.11.2	cpe:/a:open-scap:oscap	1.3.7	2023-07-13	00:51:20
#✗	#✓	#Error	#Unknown	#Other
0	25933	0	0	0

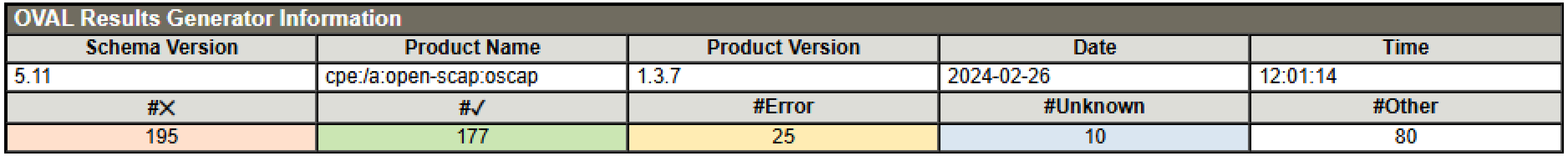


ID	Result	Class	Reference ID	Title
oval:org.debian:def:99989827288352435739290977923520308270	false	vulnerability	[CVE-2003-0308]	CVE-2003-0308 sendmail
oval:org.debian:def:99948987085126515595759721993248484969	false	vulnerability	[CVE-2011-0986]	CVE-2011-0986 phpmyadmin
oval:org.debian:def:99941182632994121766885970967748160553	false	vulnerability	[CVE-2011-3389]	CVE-2011-3389 bouncycastle
oval:org.debian:def:99941164294506774666717984434155430540	false	vulnerability	[CVE-2022-2959]	CVE-2022-2959 linux
oval:org.debian:def:99905139457938614013767511900173984296	false	vulnerability	[CVE-2020-36279]	CVE-2020-36279 leptonlib
oval:org.debian:def:99902197491645915363044886433240054704	false	vulnerability	[CVE-2021-38385]	CVE-2021-38385 tor
oval:org.debian:def:9990047555049822681012592596587224109	false	vulnerability	[CVE-2019-16225]	CVE-2019-16225 py-lmdb
oval:org.debian:def:99873421086295814304646980911458982479	false	vulnerability	[CVE-2015-2935]	CVE-2015-2935 mediawiki
oval:org.debian:def:99864538049506636631262127532863941304	false	vulnerability	[CVE-2014-6052]	CVE-2014-6052 libvncserver
oval:org.debian:def:9983335125855587434490851767107374 58	false	vulnerability	[CVE-2011-3348]	CVE-2011-3348 apache2

OpenScap

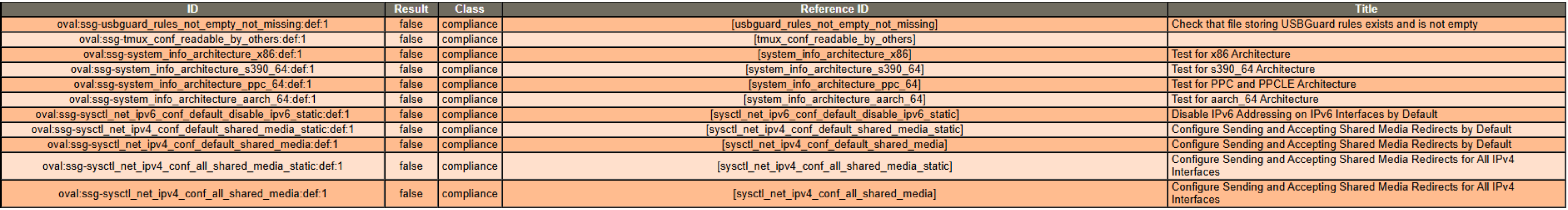
Scanning

```
oscap oval eval --report oval-bookworm.html ssg-debian12-oval.xml -> 100% automatique
oscap oval eval --report oval-bookworm.html ssg-debian12-ocil.xml -> Basé sur des questions
```



OVAL Results Generator Information

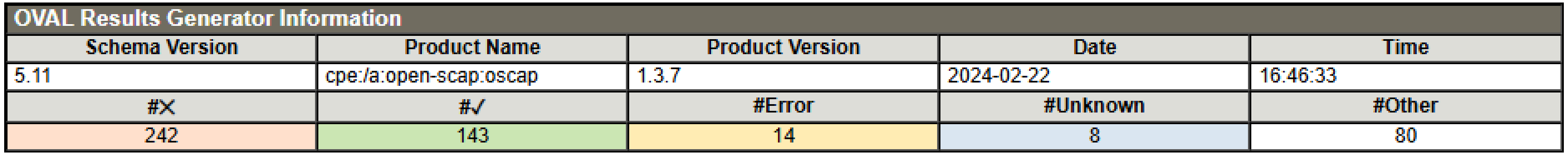
Schema Version	Product Name	Product Version	Date	Time
5.11	cpe:/a:open-scap:oscap	1.3.7	2024-02-26	12:01:14
#✗	#✓	#Error	#Unknown	#Other
195	177	25	10	80



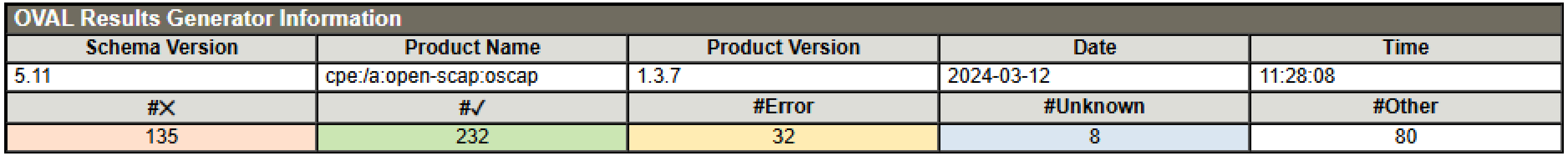
ID	Result	Class	Reference ID	Title
oval:ssg-usbguard_rules_not_empty_not_missing:def:1	false	compliance	[usbguard_rules_not_empty_not_missing]	Check that file storing USBGuard rules exists and is not empty
oval:ssg-tmux_conf_readable_by_others:def:1	false	compliance	[tmux_conf_readable_by_others]	
oval:ssg-system_info_architecture_x86:def:1	false	compliance	[system_info_architecture_x86]	Test for x86 Architecture
oval:ssg-system_info_architecture_s390_64:def:1	false	compliance	[system_info_architecture_s390_64]	Test for s390_64 Architecture
oval:ssg-system_info_architecture_ppc_64:def:1	false	compliance	[system_info_architecture_ppc_64]	Test for PPC and PPCLE Architecture
oval:ssg-system_info_architecture_aarch_64:def:1	false	compliance	[system_info_architecture_aarch_64]	Test for aarch_64 Architecture
oval:ssg-sysctl_net_ipv6_conf_default_disable_ipv6_static:def:1	false	compliance	[sysctl_net_ipv6_conf_default_disable_ipv6_static]	Disable IPv6 Addressing on IPv6 Interfaces by Default
oval:ssg-sysctl_net_ipv4_conf_default_shared_media_static:def:1	false	compliance	[sysctl_net_ipv4_conf_default_shared_media_static]	Configure Sending and Accepting Shared Media Redirects by Default
oval:ssg-sysctl_net_ipv4_conf_default_shared_media:def:1	false	compliance	[sysctl_net_ipv4_conf_default_shared_media]	Configure Sending and Accepting Shared Media Redirects by Default
oval:ssg-sysctl_net_ipv4_conf_all_shared_media_static:def:1	false	compliance	[sysctl_net_ipv4_conf_all_shared_media_static]	Configure Sending and Accepting Shared Media Redirects for All IPv4 Interfaces
oval:ssg-sysctl_net_ipv4_conf_all_shared_media:def:1	false	compliance	[sysctl_net_ipv4_conf_all_shared_media]	Configure Sending and Accepting Shared Media Redirects for All IPv4 Interfaces

OpenScap

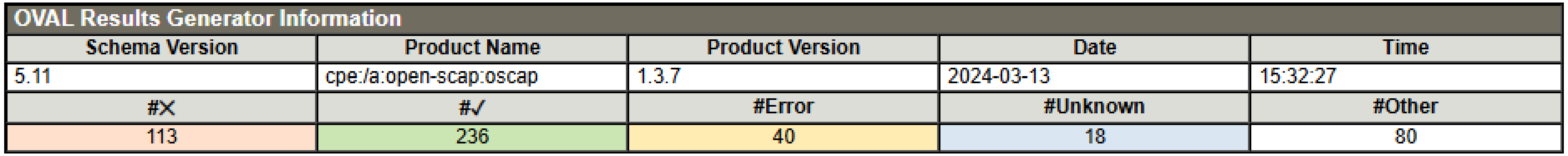
Remédiation



OVAL Results Generator Information				
Schema Version	Product Name	Product Version	Date	Time
5.11	cpe:/a:open-scap:oscap	1.3.7	2024-02-22	16:46:33
#✕	#✓	#Error	#Unknown	#Other
242	143	14	8	80



OVAL Results Generator Information				
Schema Version	Product Name	Product Version	Date	Time
5.11	cpe:/a:open-scap:oscap	1.3.7	2024-03-12	11:28:08
#✕	#✓	#Error	#Unknown	#Other
135	232	32	8	80

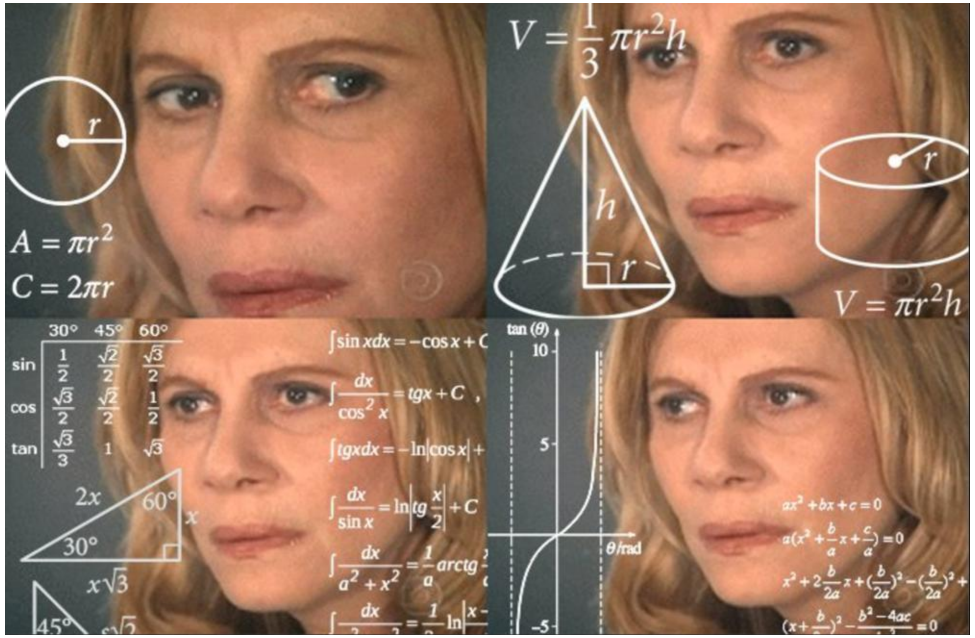


OVAL Results Generator Information				
Schema Version	Product Name	Product Version	Date	Time
5.11	cpe:/a:open-scap:oscap	1.3.7	2024-03-13	15:32:27
#✕	#✓	#Error	#Unknown	#Other
113	236	40	18	80

OpenScap

Remédiation

- ➔ **Installation d’applications : Antivirus, gestion de l’heure, journalisation, etc…**
- ➔ **Modification des droits sur les fichiers critiques**
- ➔ **Modification des accès Root**
- ➔ **Modification des paramétrages IP**
- ➔ **Durcissement du kernel**
- ➔ **Envoi d’alertes**
- ➔ **Paramétrage de l’audit de configuration**
- ➔ **Durcissement des configurations**


$A = \pi r^2$
$C = 2\pi r$
$V = \frac{1}{3}\pi r^2 h$
$V = \pi r^2 h$
r
h
30° 45° 60°
sin
cos
tan
2x
30°
60°
$x\sqrt{3}$
45°
$\int \sin x dx = -\cos x + C$
$\int \frac{dx}{\cos^2 x} = tgx + C$
$\int tgx dx = -\ln|\cos x| +$
tan (θ)
10
5
-5
θ/rad
$ax^2 + bx + c = 0$

Openscap

Ansible

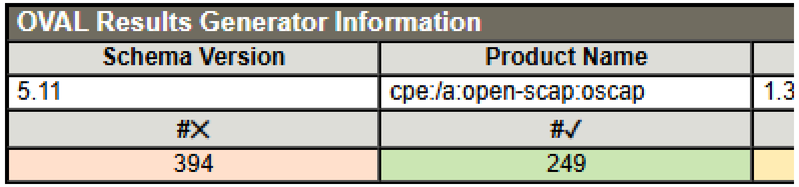
Apt –y ansible

Ansible-playbook debian12-playbook-anssi_bp28_*.yml

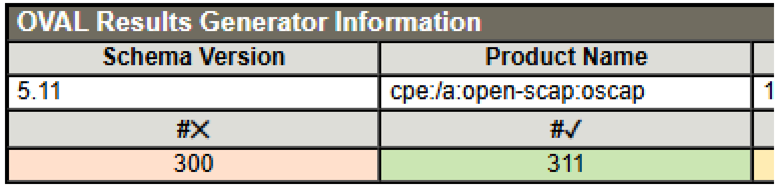
Ansible-playbook debian12-playbook-anssi_nt28_*.yml

Ansible-playbook debian12-playbook-anssi_np_nt28_*.yml

* : Niveau souhaité d'application de l'ansible : minimal, intermediary, high, enhanced



OVAL Results Generator Information		
Schema Version	Product Name	
5.11	cpe:/a:open-scap:oscap	1.3
#✕	#✓	
394	249	

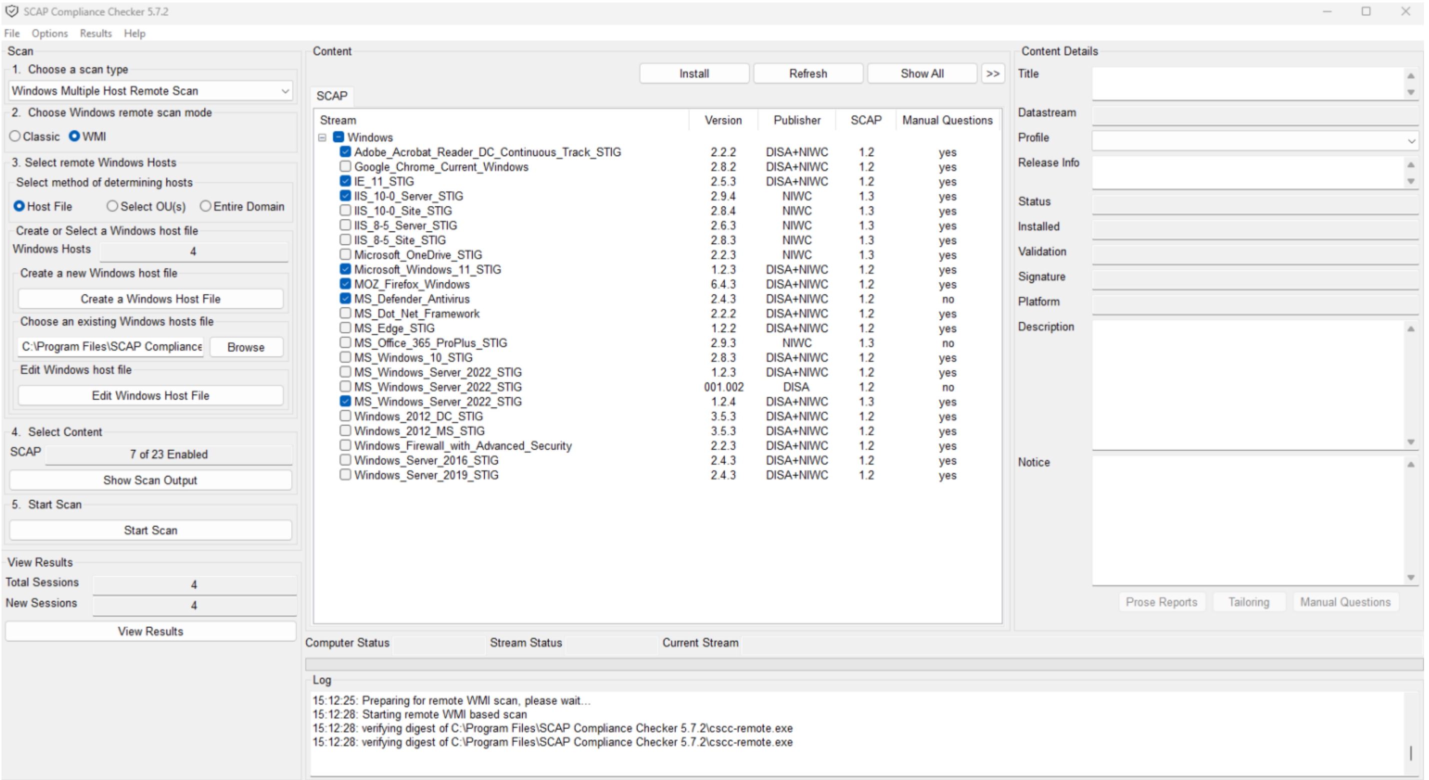


OVAL Results Generator Information		
Schema Version	Product Name	
5.11	cpe:/a:open-scap:oscap	1
#✕	#✓	
300	311	

SCC : Scap compliance checker

NIWC ATLANTIC

Pour Windows



1. Choose a scan type: Windows Multiple Host Remote Scan
2. Choose Windows remote scan mode: ○ Classic ● WMI
3. Select remote Windows Hosts
   - Select method of determining hosts: ● Host File ○ Select OU(s) ○ Entire Domain
   - Create or Select a Windows host file: Windows Hosts 4
   - Create a new Windows host file: Create a Windows Host File
   - Choose an existing Windows hosts file: C:\Program Files\SCAP Compliance | Browse
   - Edit Windows host file: Edit Windows Host File
4. Select Content: SCAP 7 of 23 Enabled | Show Scan Output
5. Start Scan: Start Scan

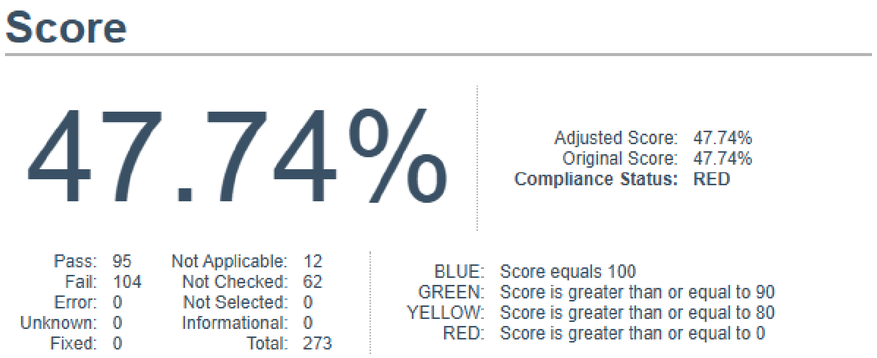
View Results: Total Sessions 4 — New Sessions 4 — View Results

Stream	Version	Publisher	SCAP	Manual Questions
⊟ Windows				
☑ Adobe_Acrobat_Reader_DC_Continuous_Track_STIG	2.2.2	DISA+NIWC	1.2	yes
☐ Google_Chrome_Current_Windows	2.8.2	DISA+NIWC	1.2	yes
☑ IE_11_STIG	2.5.3	DISA+NIWC	1.2	yes
☑ IIS_10-0_Server_STIG	2.9.4	NIWC	1.3	yes
☐ IIS_10-0_Site_STIG	2.8.4	NIWC	1.3	yes
☐ IIS_8-5_Server_STIG	2.6.3	NIWC	1.3	yes
☐ IIS_8-5_Site_STIG	2.8.3	NIWC	1.3	yes
☐ Microsoft_OneDrive_STIG	2.2.3	NIWC	1.3	yes
☑ Microsoft_Windows_11_STIG	1.2.3	DISA+NIWC	1.2	yes
☑ MOZ_Firefox_Windows	6.4.3	DISA+NIWC	1.2	yes
☑ MS_Defender_Antivirus	2.4.3	DISA+NIWC	1.2	no
☐ MS_Dot_Net_Framework	2.2.2	DISA+NIWC	1.2	yes
☐ MS_Edge_STIG	1.2.2	DISA+NIWC	1.2	yes
☐ MS_Office_365_ProPlus_STIG	2.9.3	NIWC	1.3	no
☐ MS_Windows_10_STIG	2.8.3	DISA+NIWC	1.2	yes
☐ MS_Windows_Server_2022_STIG	1.2.3	DISA+NIWC	1.2	yes
☐ MS_Windows_Server_2022_STIG	001.002	DISA	1.2	no
☑ MS_Windows_Server_2022_STIG	1.2.4	DISA+NIWC	1.3	yes
☐ Windows_2012_DC_STIG	3.5.3	DISA+NIWC	1.2	yes
☐ Windows_2012_MS_STIG	3.5.3	DISA+NIWC	1.2	yes
☐ Windows_Firewall_with_Advanced_Security	2.2.3	DISA+NIWC	1.2	yes
☐ Windows_Server_2016_STIG	2.4.3	DISA+NIWC	1.2	yes
☐ Windows_Server_2019_STIG	2.4.3	DISA+NIWC	1.2	yes

```
15:12:25: Preparing for remote WMI scan, please wait...
15:12:28: Starting remote WMI based scan
15:12:28: verifying digest of C:\Program Files\SCAP Compliance Checker 5.7.2\cscc-remote.exe
15:12:28: verifying digest of C:\Program Files\SCAP Compliance Checker 5.7.2\cscc-remote.exe
```

SCC

SCC : Scap compliance checker



Score

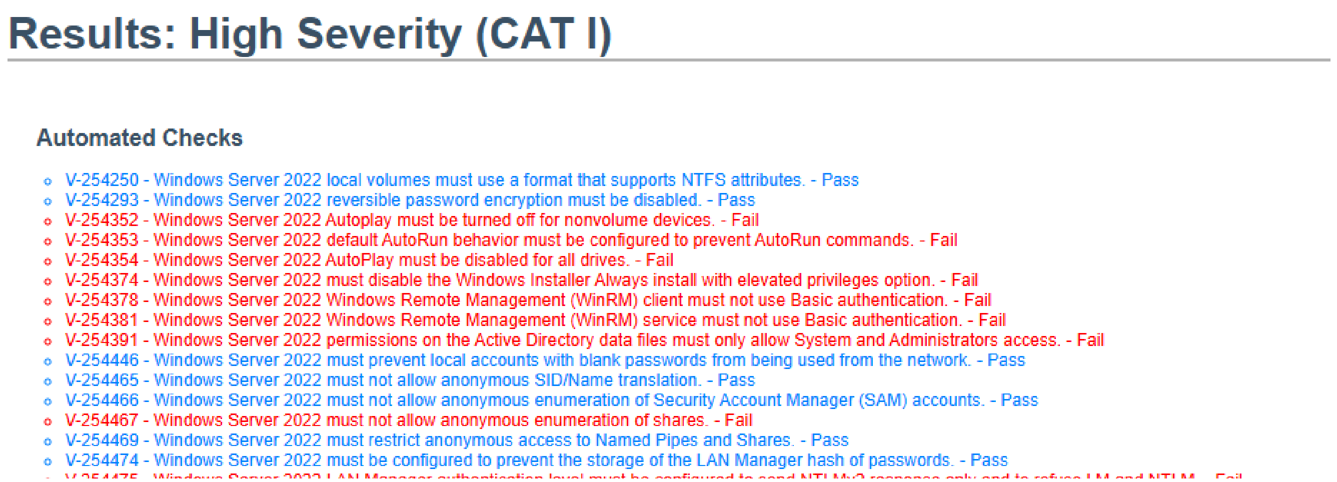
47.74%

Adjusted Score:	47.74%
Original Score:	47.74%
Compliance Status:	**RED**

Pass:	95	Not Applicable:	12
Fail:	104	Not Checked:	62
Error:	0	Not Selected:	0
Unknown:	0	Informational:	0
Fixed:	0	Total:	273

BLUE:	Score equals 100
GREEN:	Score is greater than or equal to 90
YELLOW:	Score is greater than or equal to 80
RED:	Score is greater than or equal to 0

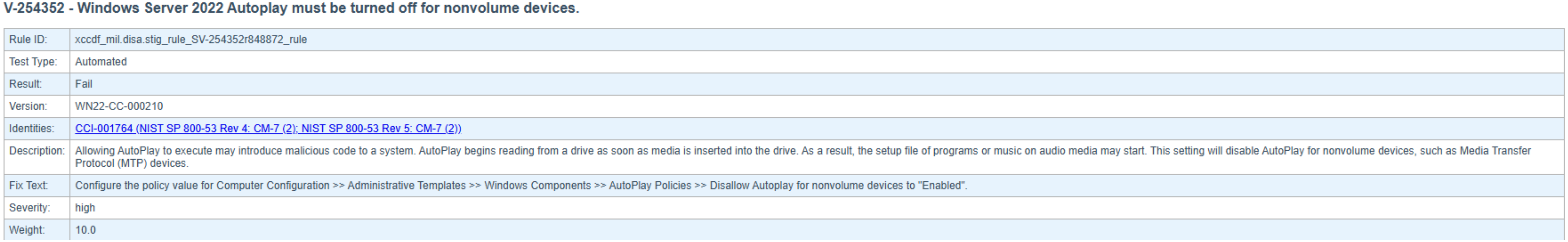
Pour Windows



Results: High Severity (CAT I)

Automated Checks

- V-254250 - Windows Server 2022 local volumes must use a format that supports NTFS attributes. - Pass
- V-254293 - Windows Server 2022 reversible password encryption must be disabled. - Pass
- V-254352 - Windows Server 2022 Autoplay must be turned off for nonvolume devices. - Fail
- V-254353 - Windows Server 2022 default AutoRun behavior must be configured to prevent AutoRun commands. - Fail
- V-254354 - Windows Server 2022 AutoPlay must be disabled for all drives. - Fail
- V-254374 - Windows Server 2022 must disable the Windows Installer Always install with elevated privileges option. - Fail
- V-254378 - Windows Server 2022 Windows Remote Management (WinRM) client must not use Basic authentication. - Fail
- V-254381 - Windows Server 2022 Windows Remote Management (WinRM) service must not use Basic authentication. - Fail
- V-254391 - Windows Server 2022 permissions on the Active Directory data files must only allow System and Administrators access. - Fail
- V-254446 - Windows Server 2022 must prevent local accounts with blank passwords from being used from the network. - Pass
- V-254465 - Windows Server 2022 must not allow anonymous SID/Name translation. - Pass
- V-254466 - Windows Server 2022 must not allow anonymous enumeration of Security Account Manager (SAM) accounts. - Pass
- V-254467 - Windows Server 2022 must not allow anonymous enumeration of shares. - Fail
- V-254469 - Windows Server 2022 must restrict anonymous access to Named Pipes and Shares. - Pass
- V-254474 - Windows Server 2022 must be configured to prevent the storage of the LAN Manager hash of passwords. - Pass
- V-254475 - Windows Server 2022 LAN Manager authentication level must be configured to send NTLMv2 response only and to refuse LM and NTLM. - Fail



V-254352 - Windows Server 2022 Autoplay must be turned off for nonvolume devices.

Rule ID:	xccdf_mil.disa.stig_rule_SV-254352r848872_rule
Test Type:	Automated
Result:	Fail
Version:	WN22-CC-000210
Identities:	CCI-001764 (NIST SP 800-53 Rev 4: CM-7 (2); NIST SP 800-53 Rev 5: CM-7 (2))
Description:	Allowing AutoPlay to execute may introduce malicious code to a system. AutoPlay begins reading from a drive as soon as media is inserted into the drive. As a result, the setup file of programs or music on audio media may start. This setting will disable AutoPlay for nonvolume devices, such as Media Transfer Protocol (MTP) devices.
Fix Text:	Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> AutoPlay Policies >> Disallow Autoplay for nonvolume devices to "Enabled".
Severity:	high
Weight:	10.0

03

Bonnes pratiques de configuration

Les fichiers de configuration

La partie immergée de l’iceberg

- **Les fichiers de configurations sont :**
  - **Absolument partout : Routeur, switch , équipement de sécurité, serveur, application, bornes wifi, etc…**
  - **Faiblement exposés (pour la plupart)**
  - **Faiblement priorisés pour la sécurisation**
  - **Facilement exploitables**

37000

Organisations public victimes de cyberattaque en 2022

73%

Des cyberattaques commencent par du phishing

53%

Des cyberattaques utilisent des défauts de configurations

16

Les fichiers de configuration

Objectifs visés :

NTP :

- **Conserver une heure précise afin de conserver une précision dans les détections et dans les logs.**

Cryptographie :

- **Permettre une confidentialité des données stockées et échangées**

Mailing :

- **Permet l’envoi d’alerte et de notifications**

Advanced Intrusion Detection Environnement (AIDE) :

- **Permet de définir une base de l’existant et d’alerter en cas de changement**

Audit et logging :

- **Permet de définir les politiques d’audit et de suivi des actions**
- **Permet un meilleur suivi des actions qui ont été effectué sur la machine**
- **Permet de retrouver plus rapidement les actions en cas d’incident**

Les fichiers de configuration

Objectifs visés :

DUMP :

- **Permet de se protéger des attaques basées sur l’extraction de la mémoire**

SSH :

- **Permet de mieux régulier les accès à la machine et sécurise les échanges de données**

Kernel :

- **Permet de sécuriser les risques de corruptions de la mémoire**

Module :

- **Désactive les modules non utilisés et non nécessaire**

Grub :

- **Permet de limiter certaines interactions à risques entre la machine physique et le système d’exploitation**

Les fichiers de configuration

Objectifs visés :

Droits par défaut :

- **Limiter les accès et les modifications sur les fichiers critiques**

Polyinstantiation :

- **Permet de diviser les répertoires utilisés pour éviter les mises à disposition involontaires de données**

Mot de passe :

- **Permet de mettre une politique sur la gestion des mots de passe, évitant les problèmes de sécurité**

Les fichiers de configuration

Focus sur certains fichiers

- rsylog
- Aide
- sysctl
- IPV6
- boot
- grub
- Auditd
- faillock
- chrony
- ssh
- etc…

Est-ce qu’on pourrait faire un script ?

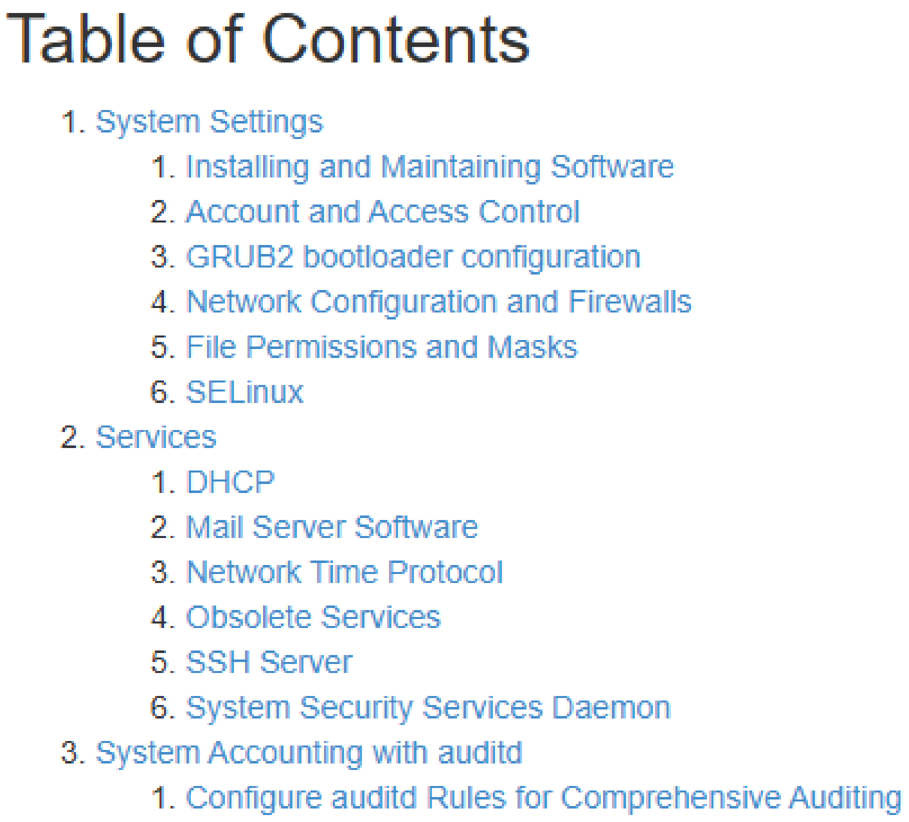


Table of Contents

1. System Settings
    1. Installing and Maintaining Software
    2. Account and Access Control
    3. GRUB2 bootloader configuration
    4. Network Configuration and Firewalls
    5. File Permissions and Masks
    6. SELinux
2. Services
    1. DHCP
    2. Mail Server Software
    3. Network Time Protocol
    4. Obsolete Services
    5. SSH Server
    6. System Security Services Daemon
3. System Accounting with auditd
    1. Configure auditd Rules for Comprehensive Auditing

04 Contrôles applicatifs

OWASP

Top 10 OWASP

A01:2025 - Broken Access Control

A02:2025 - Security Misconfiguration

A03:2025 - Software Supply Chain Failures

A04:2025 - Cryptographic Failures

A05:2025 – Injection

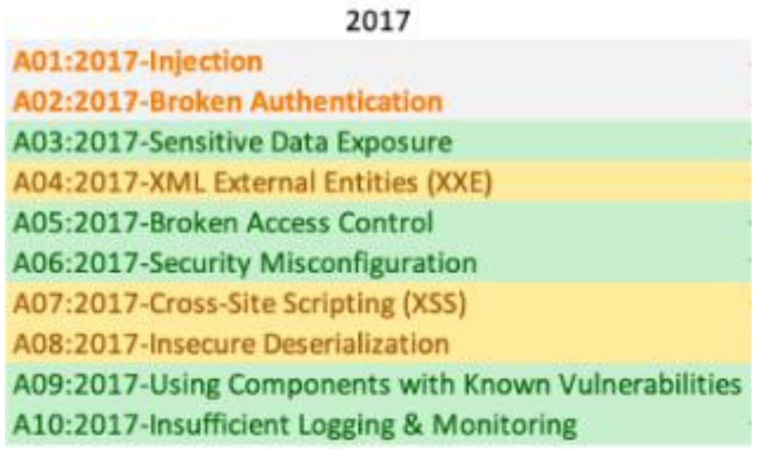
A06:2025 - Insecure Design

A07:2025 - Authentication Failures

A08:2025 - Software or Data Integrity Failures

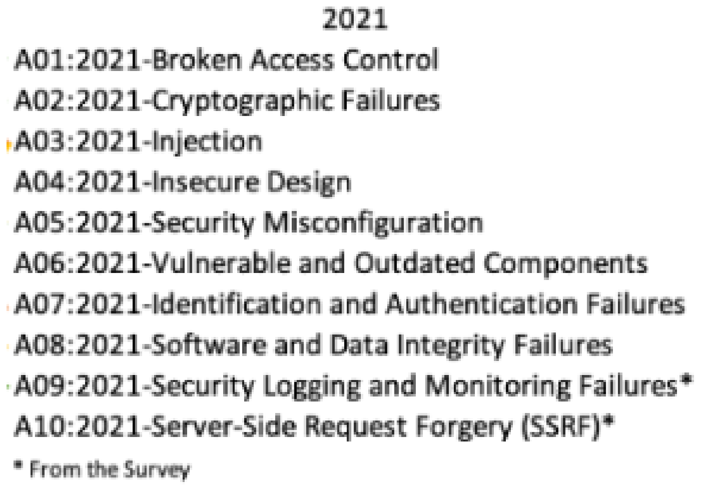
A09:2025 - Logging & Alerting Failures

A10:2025 - Mishandling of Exceptional Conditions



2017

A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring



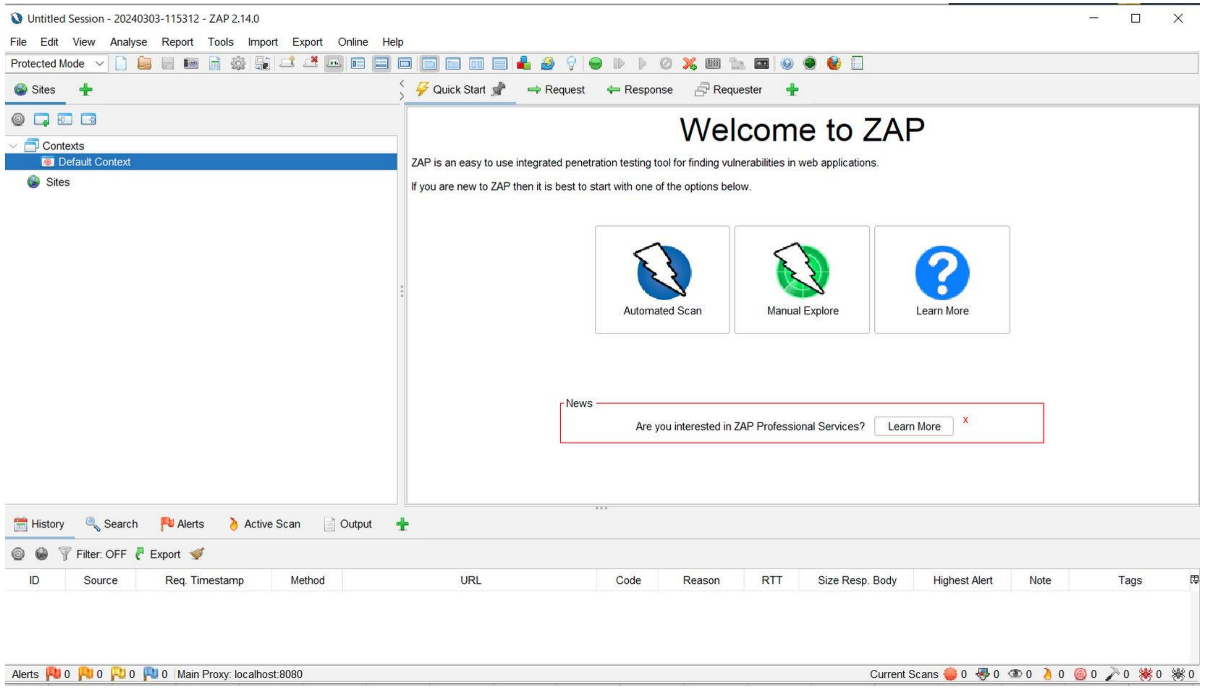
2021

A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

ZAP by Checkmarx

Projet OpenSource



Untitled Session - 20240303-115312 - ZAP 2.14.0

Welcome to ZAP

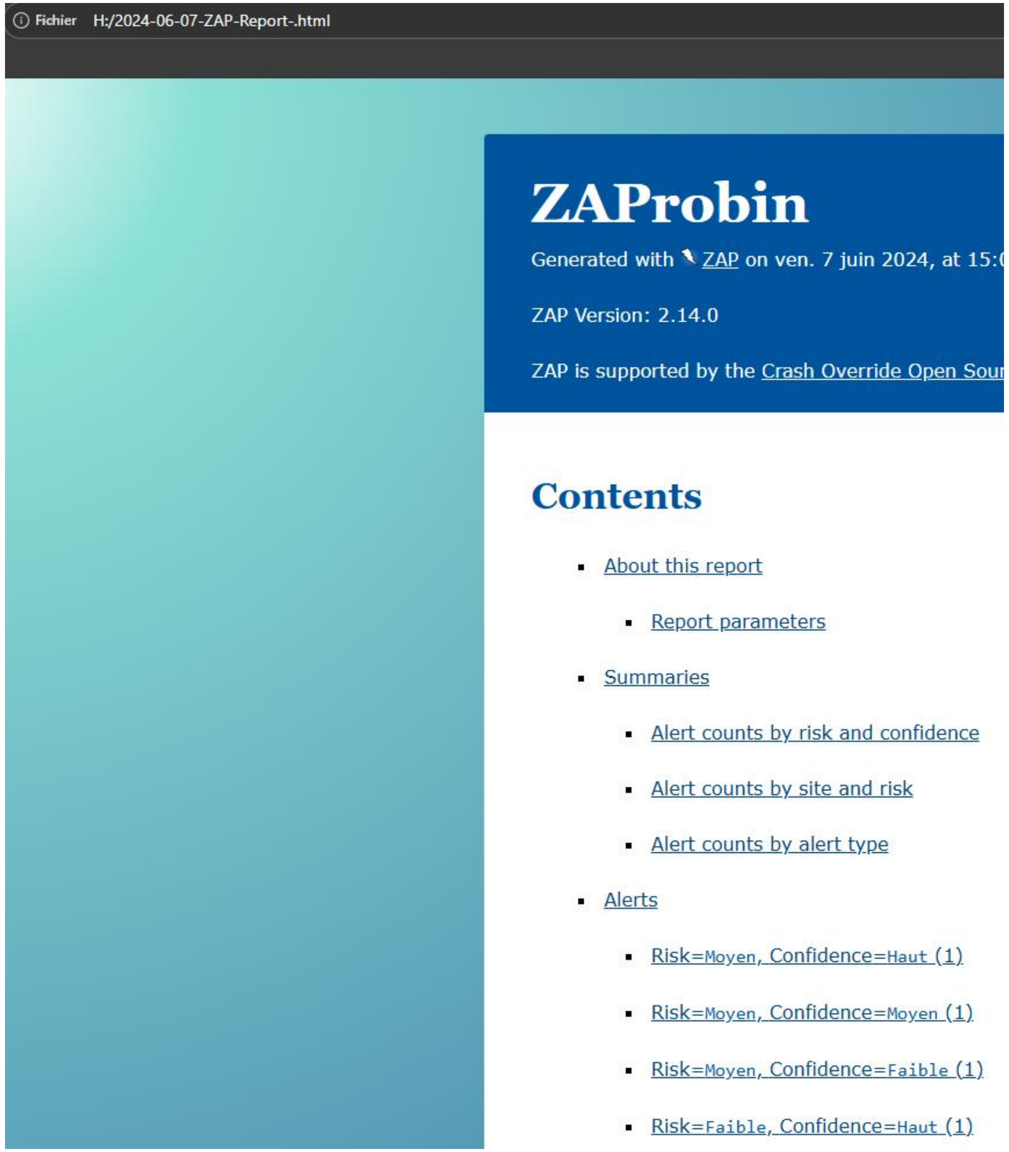
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

News

Are you interested in ZAP Professional Services?

Main Proxy: localhost:8080



Fichier H:/2024-06-07-ZAP-Report-.html

ZAProbin

Generated with ZAP on ven. 7 juin 2024, at 15:(

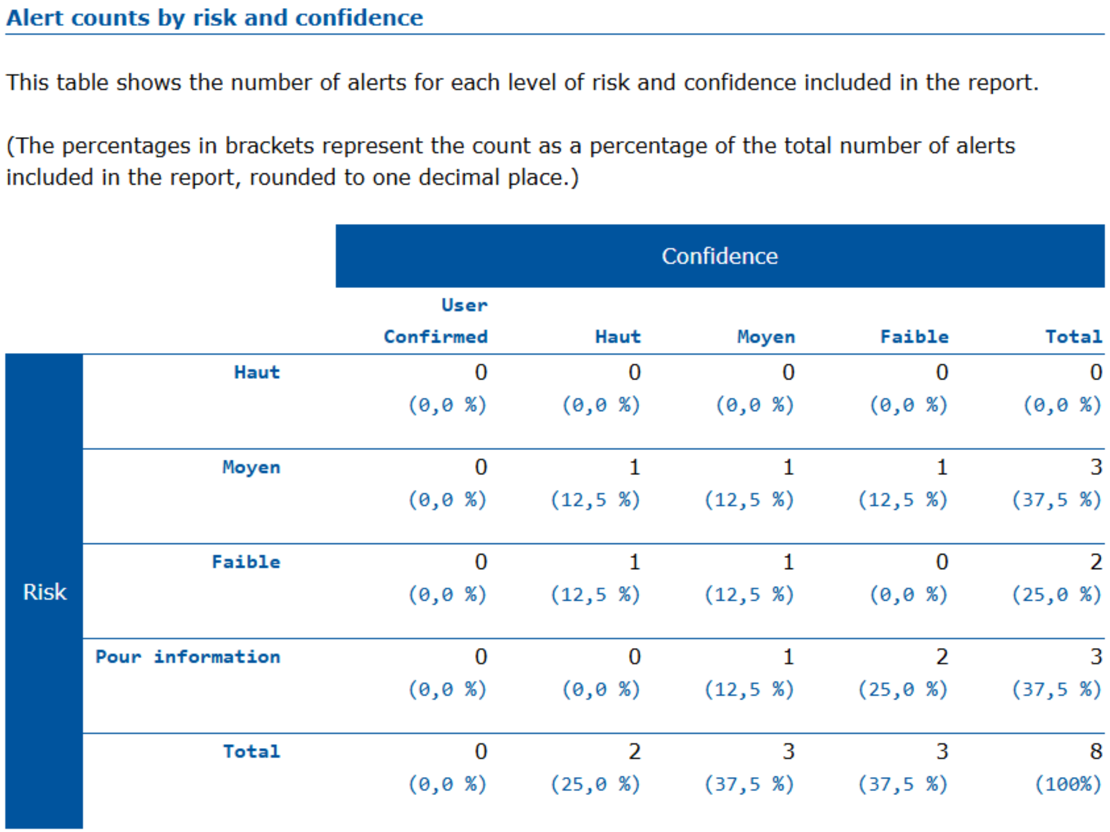
ZAP Version: 2.14.0

ZAP is supported by the Crash Override Open Sour

Contents

ZAP

Rapport

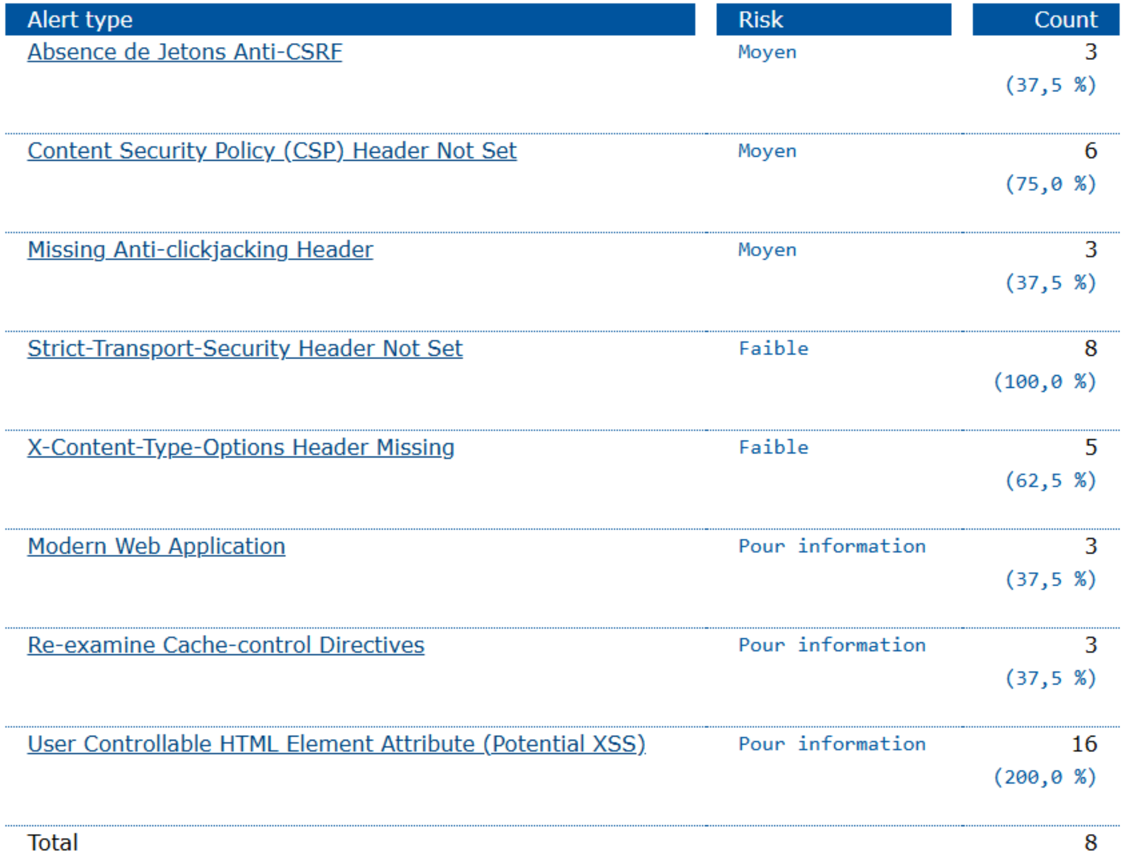


Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

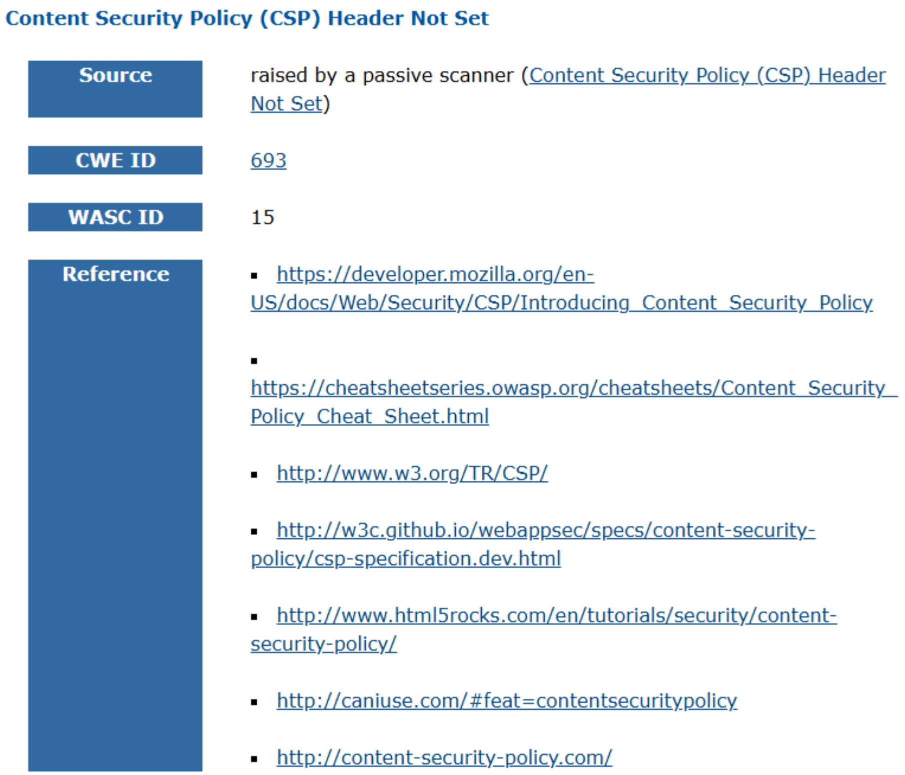
		Confidence				
		User Confirmed	Haut	Moyen	Faible	Total
Risk	Haut	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)
	Moyen	0 (0,0 %)	1 (12,5 %)	1 (12,5 %)	1 (12,5 %)	3 (37,5 %)
	Faible	0 (0,0 %)	1 (12,5 %)	1 (12,5 %)	0 (0,0 %)	2 (25,0 %)
	Pour information	0 (0,0 %)	0 (0,0 %)	1 (12,5 %)	2 (25,0 %)	3 (37,5 %)
	Total	0 (0,0 %)	2 (25,0 %)	3 (37,5 %)	3 (37,5 %)	8 (100%)



Alert type	Risk	Count
Absence de Jetons Anti-CSRF	Moyen	3 (37,5 %)
Content Security Policy (CSP) Header Not Set	Moyen	6 (75,0 %)
Missing Anti-clickjacking Header	Moyen	3 (37,5 %)
Strict-Transport-Security Header Not Set	Faible	8 (100,0 %)
X-Content-Type-Options Header Missing	Faible	5 (62,5 %)
Modern Web Application	Pour information	3 (37,5 %)
Re-examine Cache-control Directives	Pour information	3 (37,5 %)
User Controllable HTML Element Attribute (Potential XSS)	Pour information	16 (200,0 %)
Total		8

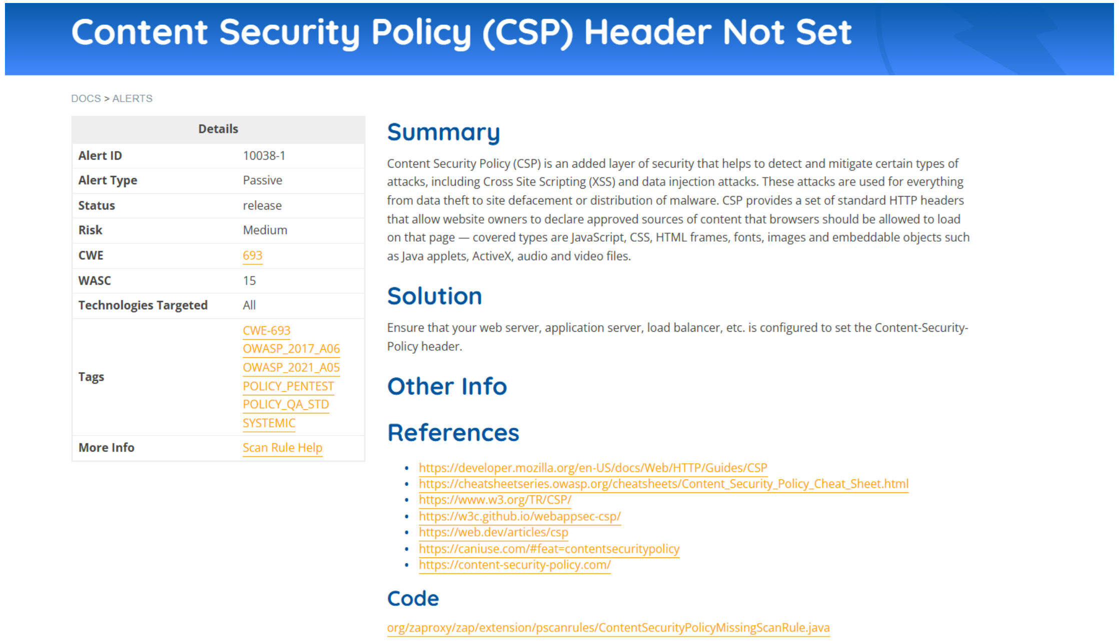
ZAP

Rapport



Content Security Policy (CSP) Header Not Set

Source	raised by a passive scanner (Content Security Policy (CSP) Header Not Set)
CWE ID	693
WASC ID	15
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy ▪ https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html ▪ http://www.w3.org/TR/CSP/ ▪ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html ▪ http://www.html5rocks.com/en/tutorials/security/content-security-policy/ ▪ http://caniuse.com/#feat=contentsecuritypolicy ▪ http://content-security-policy.com/



Content Security Policy (CSP) Header Not Set

DOCS > ALERTS

Details	
Alert ID	10038-1
Alert Type	Passive
Status	release
Risk	Medium
CWE	693
WASC	15
Technologies Targeted	All
Tags	CWE-693 OWASP_2017_A06 OWASP_2021_A05 POLICY_PENTEST POLICY_QA_STD SYSTEMIC
More Info	Scan Rule Help

Summary

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Other Info

References

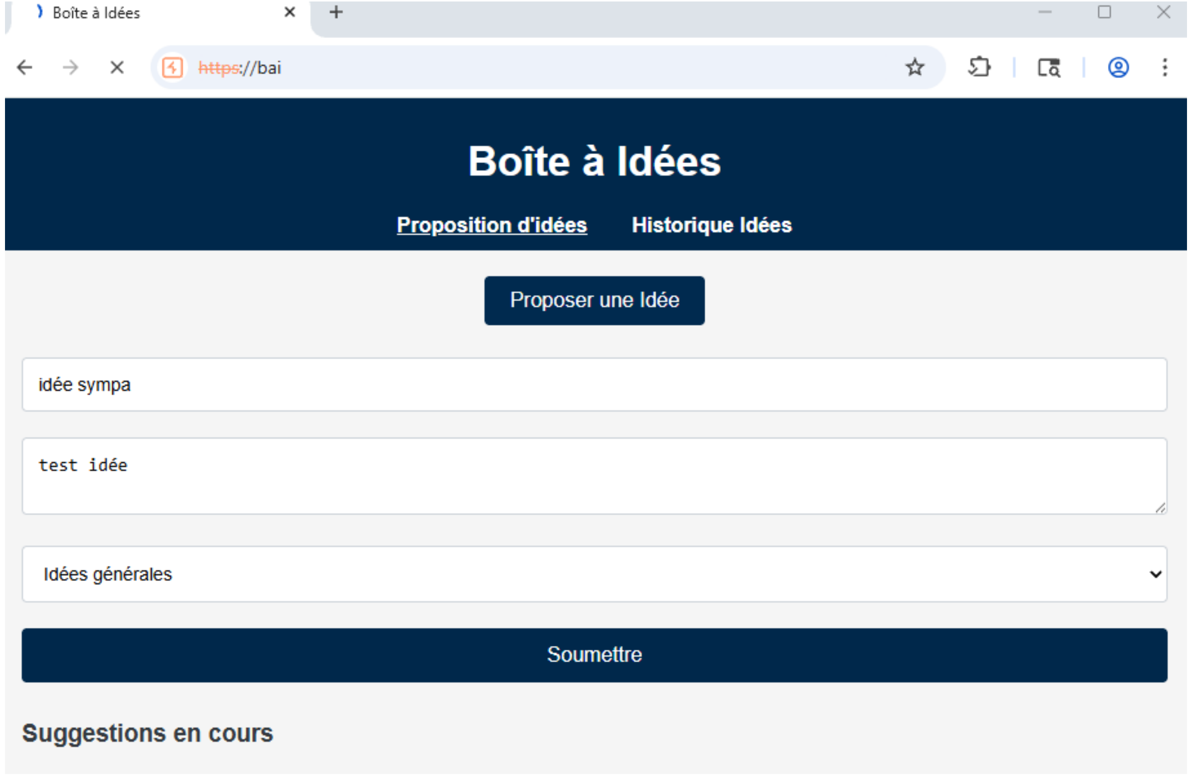
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP
- https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
- https://www.w3.org/TR/CSP/
- https://w3c.github.io/webappsec-csp/
- https://web.dev/articles/csp
- https://caniuse.com/#feat=contentsecuritypolicy
- https://content-security-policy.com/

Code

org/zaproxy/zap/extension/pscanrules/ContentSecurityPolicyMissingScanRule.java

Burp Community

Pousser un peu les tests :

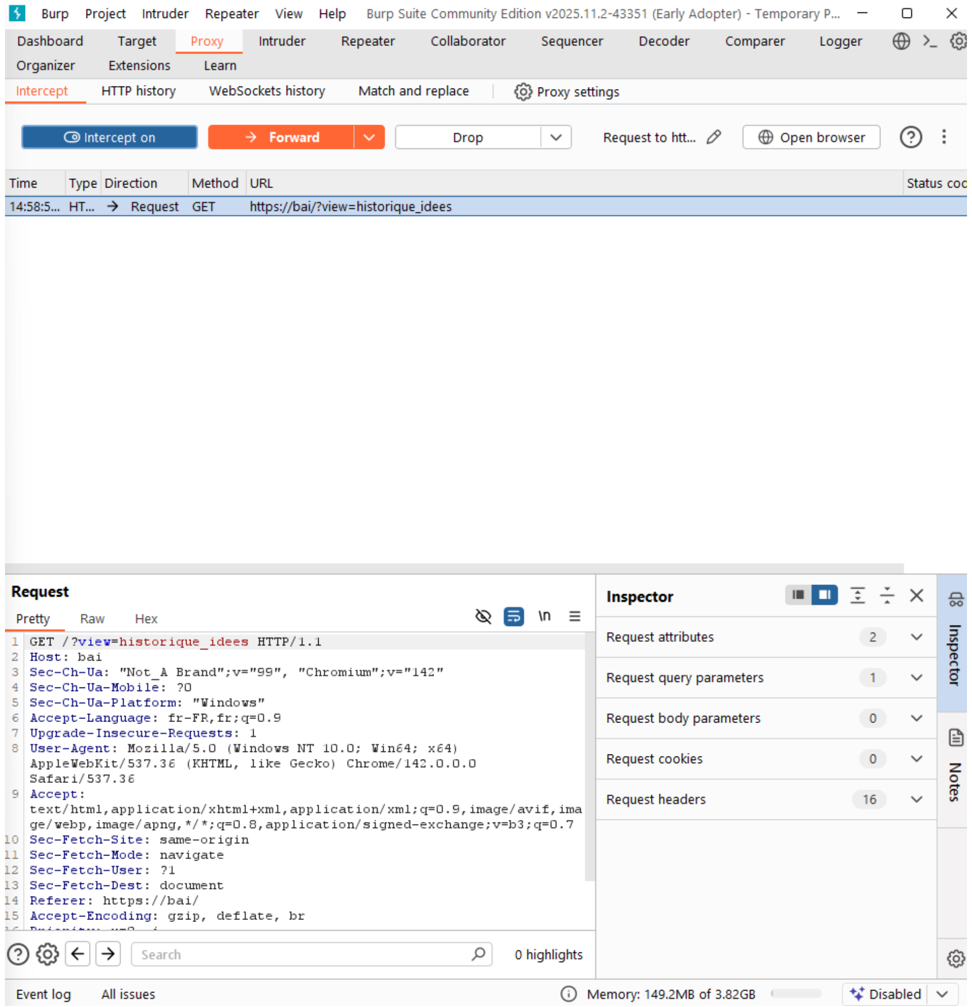


idée sympa

test idée

Idées générales

Suggestions en cours



Time	Type	Direction	Method	URL	Status coc
14:58:5...	HT...	→ Request	GET	https://bai/?view=historique_idees	

```
GET /?view=historique_idees HTTP/1.1
Host: bai
Sec-Ch-Ua: "Not_A Brand";v="99", "Chromium";v="142"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
ge/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://bai/
Accept-Encoding: gzip, deflate, br
```

Request attributes	2
Request query parameters	1
Request body parameters	0
Request cookies	0
Request headers	16

05 Aller plus loin

accès
architecture
segmentation
multi-tiers
filtrage
analyse
audit
traçabilité
contrôle
journaux