Ecole Supérieure Privée des Technologies et de l'Ingénierie

Spécialité : SSIR-2D

Rapport de Projet de owasp

Realisé par : Nasri wissem

Encadrant académique : oussema riahi

Année universitaire : 2023 2024

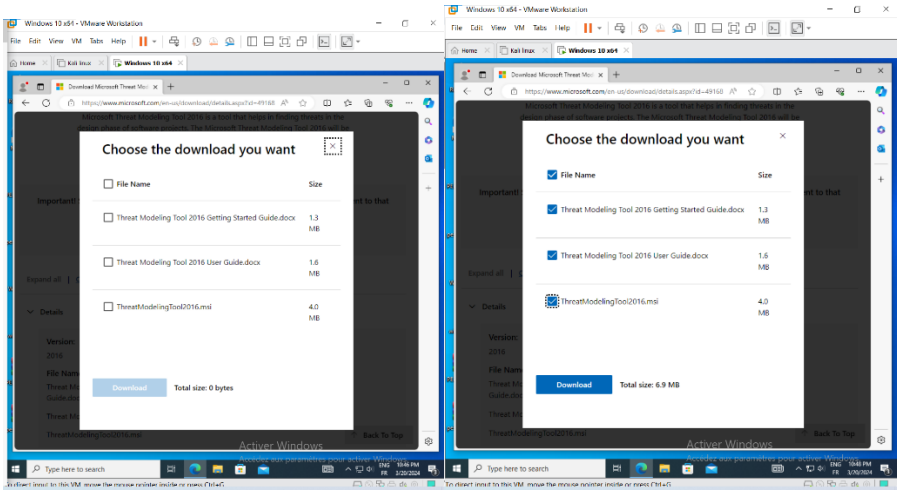
Table des matiéres :

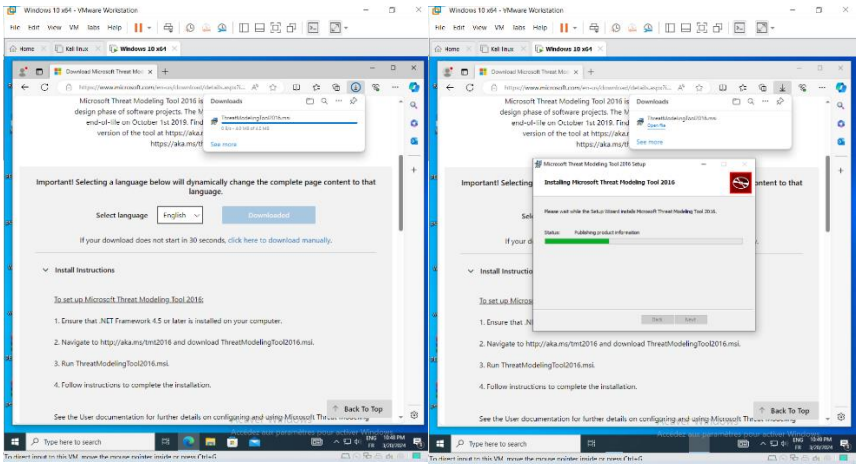
1.Modélisation des menaces

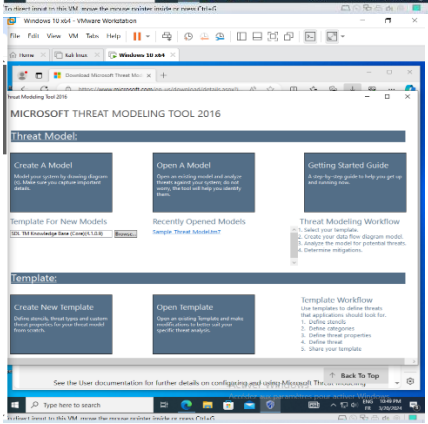
Modélisation des menaces Le modèle de menace est un processus par lequel des menaces potentielles, telles que les vulnérabilités structurelles peuvent être identifiées, énumérées et classées par ordre de priorité. Lorsqu'elle est effectuée correctement, la modélisation des menaces peut fournir une ligne de vue claire sur un projet logiciel, aidant à justifier les efforts de sécurité. Le processus de modélisation des menaces aide une organisation à documenter les menaces de sécurité connues pour une application et à prendre des décisions rationnelles sur la manière de les traiter

1.1.Modélisation des menaces avec « Microsoft Threat Modeling Tool 2016 »

1-Telecharger l'outil « Microsoft Threat Modeling Tool 2016 » depuis son source officiel

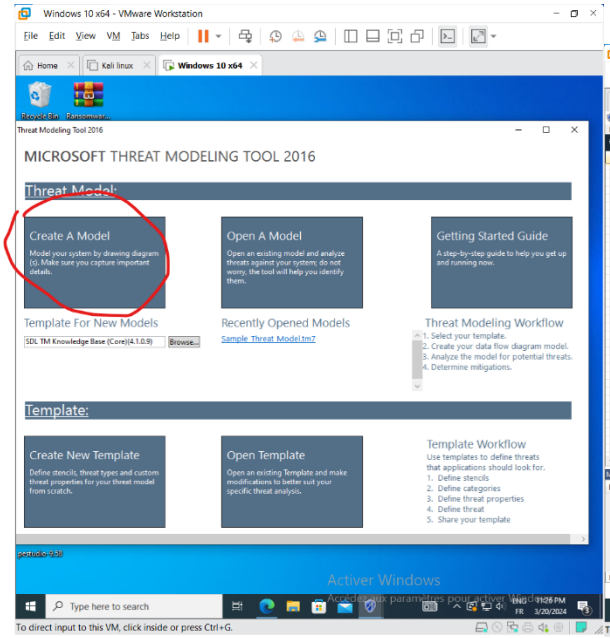


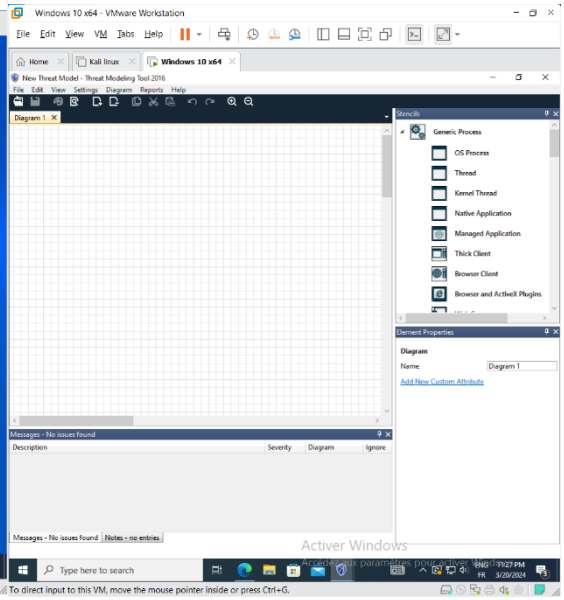


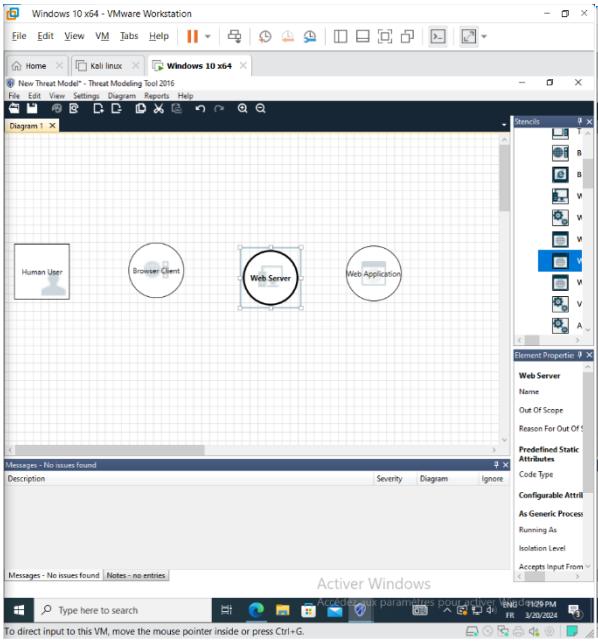


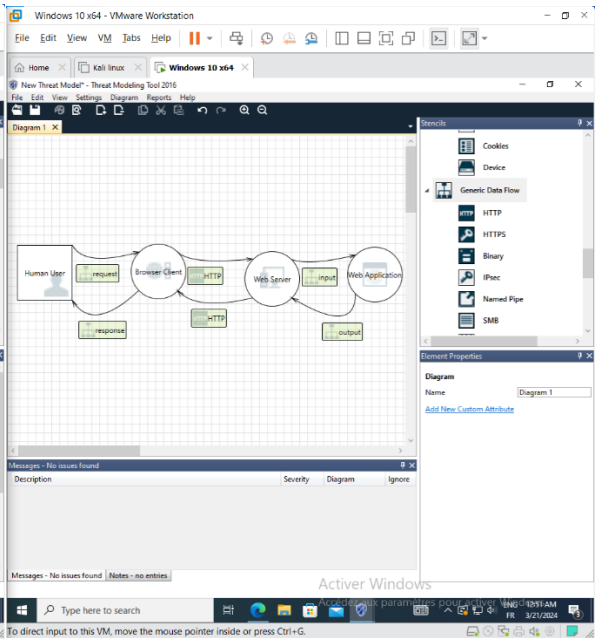
3- Reproduire l’architecture suivante et créer sa modèle de menace :

Etapes pour reproduire l’architecture

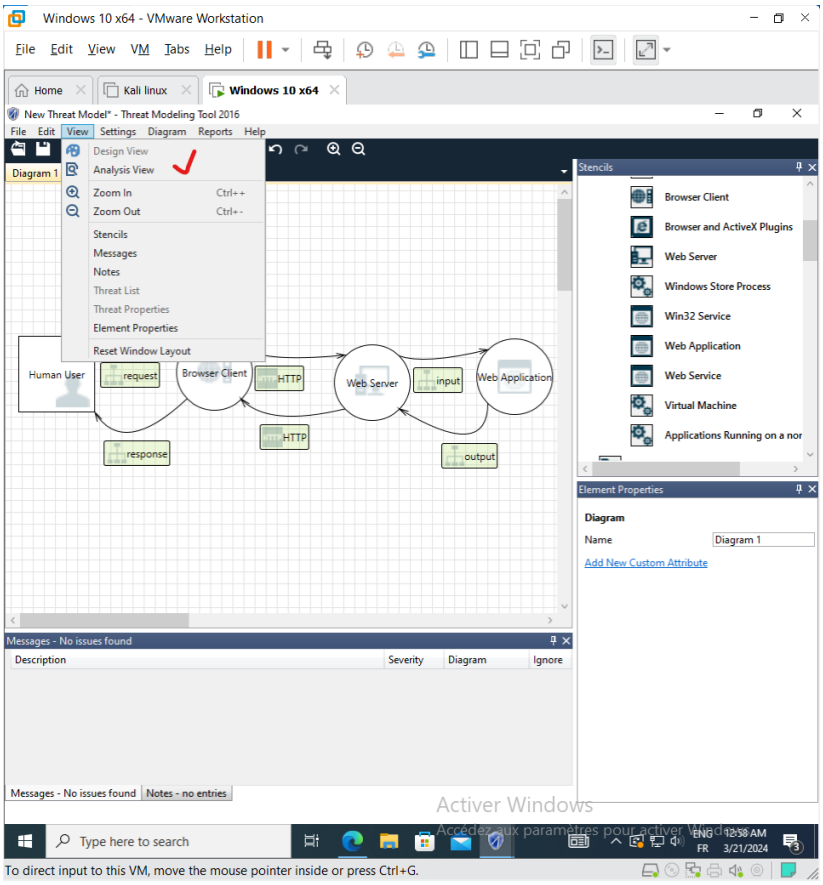


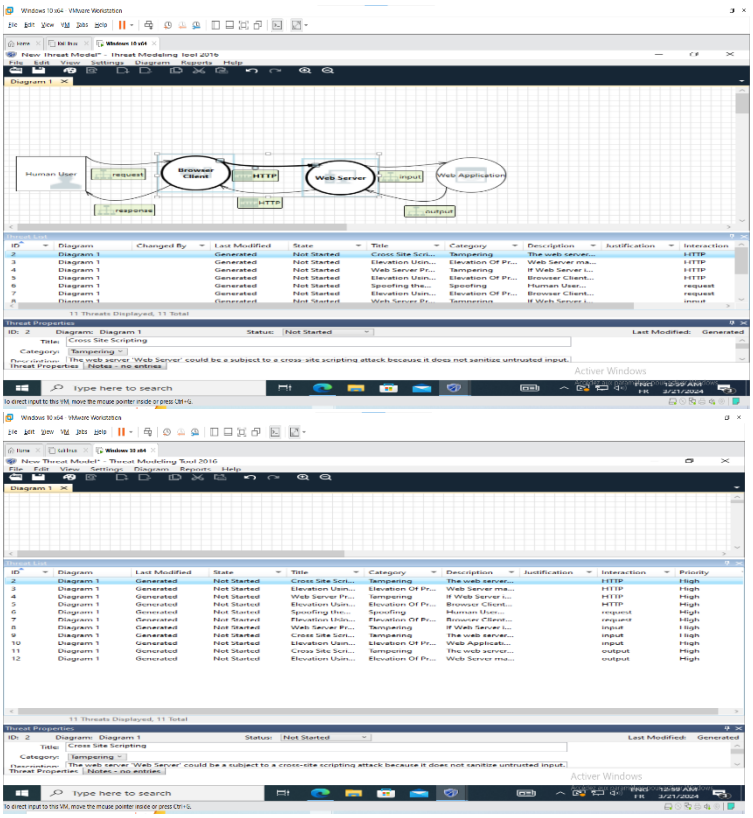




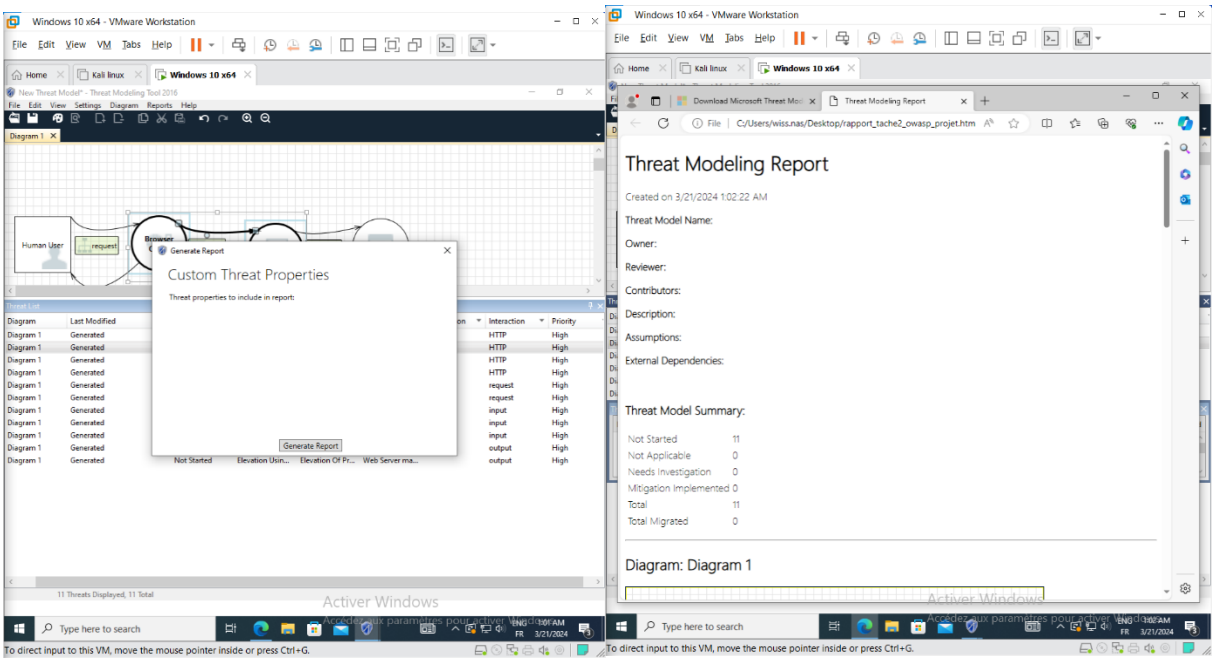


4- l’outil Microsoft Threat Modeling Tool possède deux vues : Vue de conception et Vue d'analyse, utiliser la vue d’analyse pour déterminer les vulnérabilités liée à cette architecture


Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
Windows 10 x64
New Threat Model* - Threat Modeling Tool 2016
File Edit View Settings Diagram Reports Help
Design View
Analysis View
Zoom In Ctrl++
Zoom Out Ctrl+-
Stencils
Messages
Notes
Threat List
Threat Properties
Element Properties
Reset Window Layout
Diagram 1
Human User
request
Browser Client
HTTP
Web Server
input
Web Application
response
HTTP
output
Stencils
Browser Client
Browser and ActiveX Plugins
Web Server
Windows Store Process
Win32 Service
Web Application
Web Service
Virtual Machine
Applications Running on a nor
Element Properties
Diagram
Name
Diagram 1
Add New Custom Attribute
Messages - No issues found
Description
Severity
Diagram
Ignore
Messages - No issues found
Notes - no entries
Activer Windows
Accédez aux paramètres pour activer Windows.
Type here to search
ENG
FR
12:58 AM
3/21/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Threat modeling report :



Voir le lien qui comporte se rapport du 2eme partie

les vulnérabilités liée à cette architecture :

interaction http

1.elevation using impersonation

2.Cross site scripting

interaction http

3.web server process memory tampered

4.elevation using impersonation

Interaction input

5. webserver process memory tampered

6.cross site scripting

7.elevation using impersonation

Interaction output

8.cross site scripting

9.elevation using impersonation

Interaction request

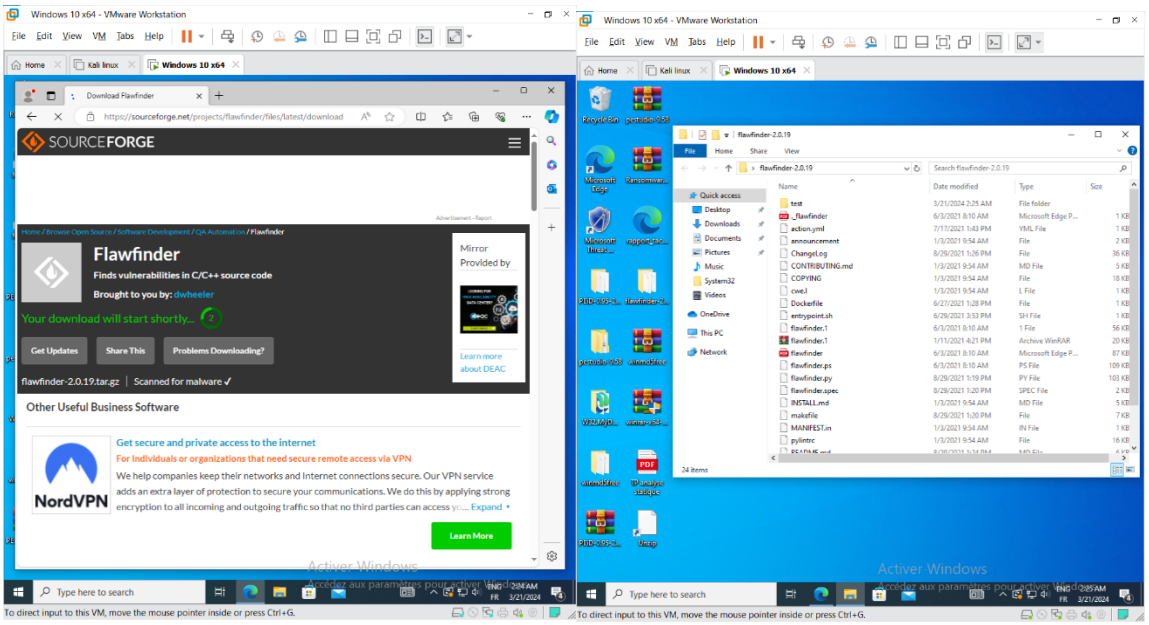
10.spoofing using impersonation

11.elevation using impersonation

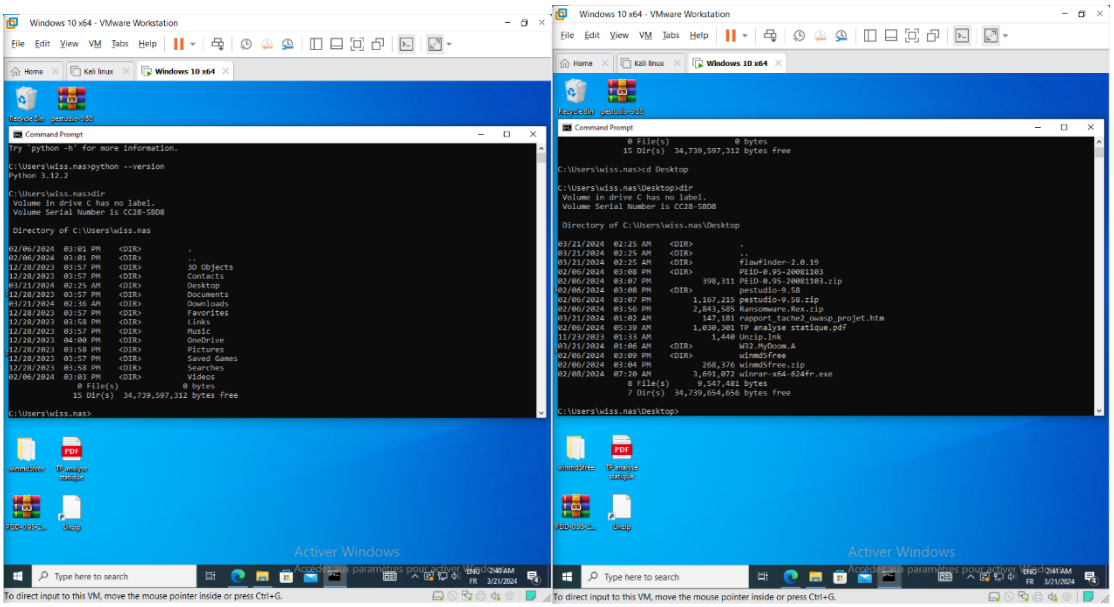
2.Tests statiques de sécurité des applications (SAST)

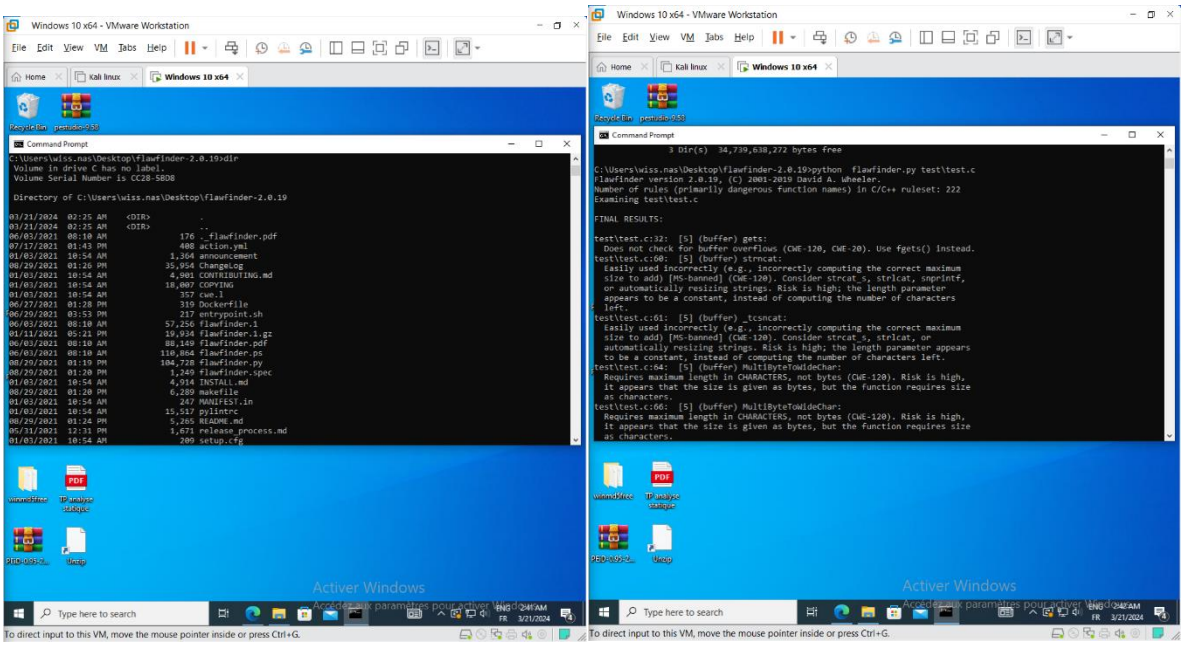
2.1.Analyse du code c à l'aide de l'outil « flaw finder »

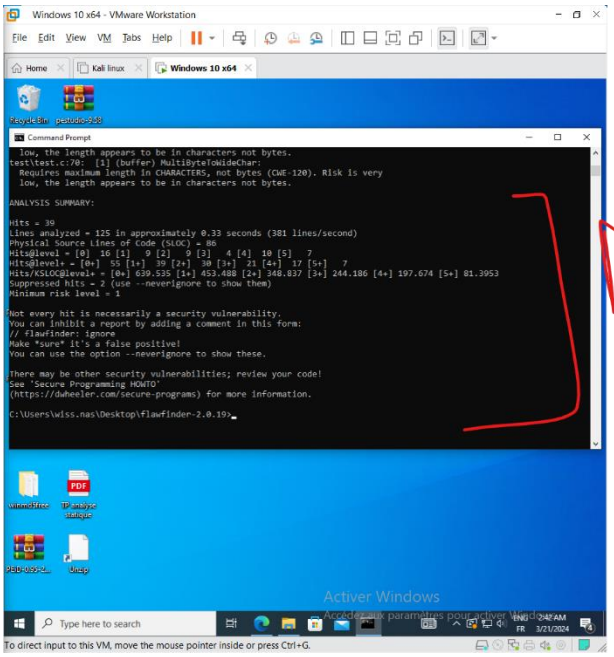
Exercie1 :

1. 

2.





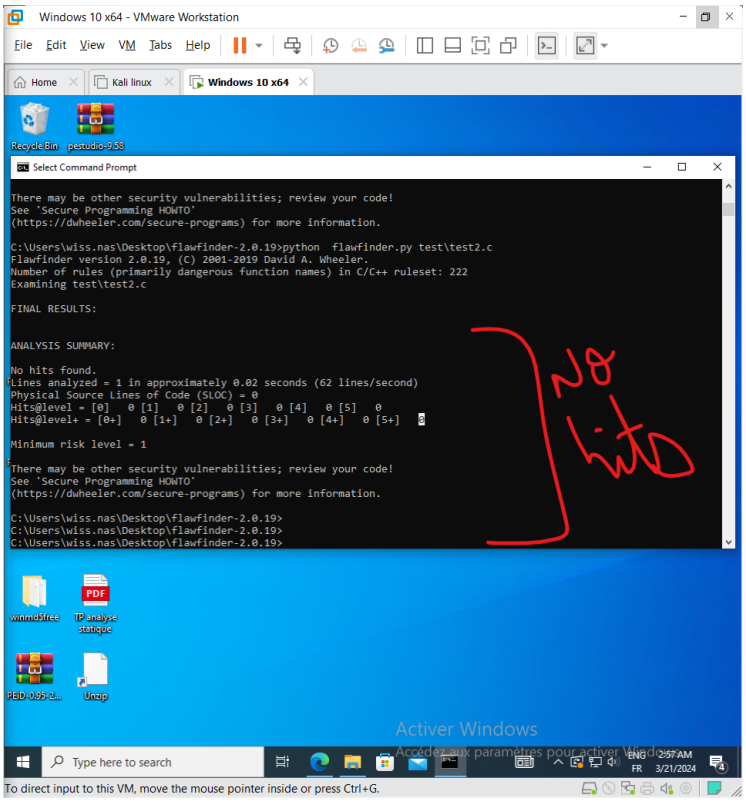


→ Hits=39

3.

Il existe 39 vulnerabilite au niveau de code c du fichier test.c →le code est vulnerable

4.



➔ **NO hits found**

Le code c du fichier test2.c n'est pas vulnerable

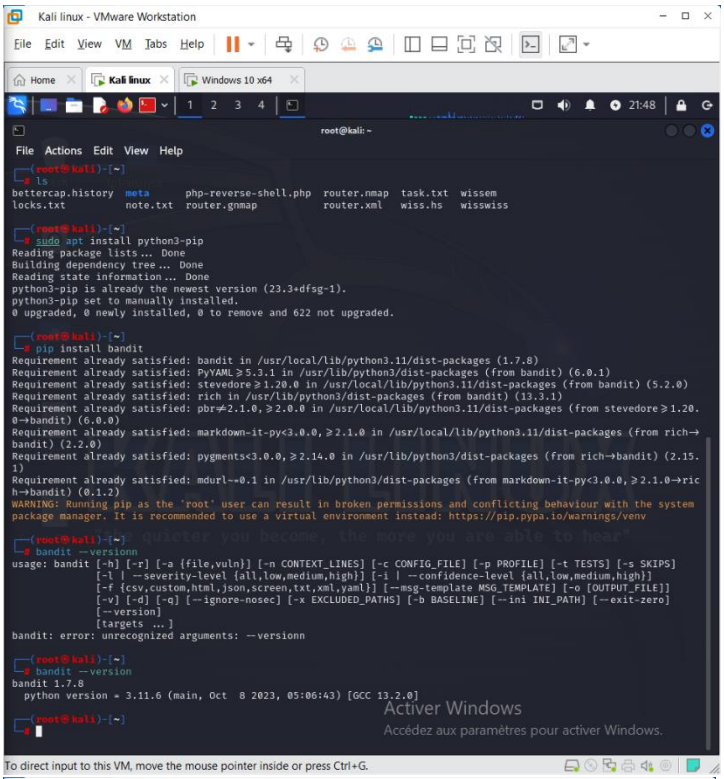
5.

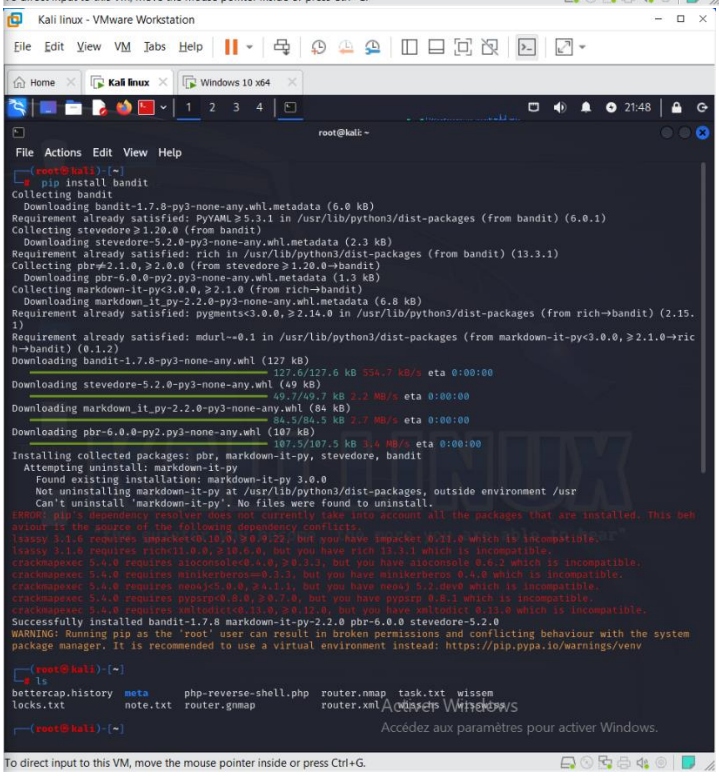
Flawfinder utilise une méthode de recherche de motifs pour analyser le code source à la recherche de constructions potentiellement dangereuses ou sujettes à des vulnérabilités de sécurité. Il recherche des chaînes de caractères correspondant à des appels de fonctions ou à des motifs de code qui sont souvent associés à des problèmes de sécurité connus, tels que les dépassements de tampon, les vulnérabilités de format de chaîne, etc. Il repose sur une base de données de vulnérabilités connues pour identifier ces motifs.

2.2.Analyse du code Python à l’aide de l’outil « Bandit »

Bandit est un outil open source d'analyse statique de code pour Python, conçu pour détecter les vulnérabilités de sécurité potentielles dans les applications Python. Son objectif principal est d'identifier les pratiques de programmation dangereuses qui pourraient conduire à des failles de sécurité, en se concentrant principalement sur les erreurs liées à l'exécution de commandes potentiellement dangereuses, à l'utilisation de fonctions ou de modules non sécurisés, et à d'autres vulnérabilités courantes.

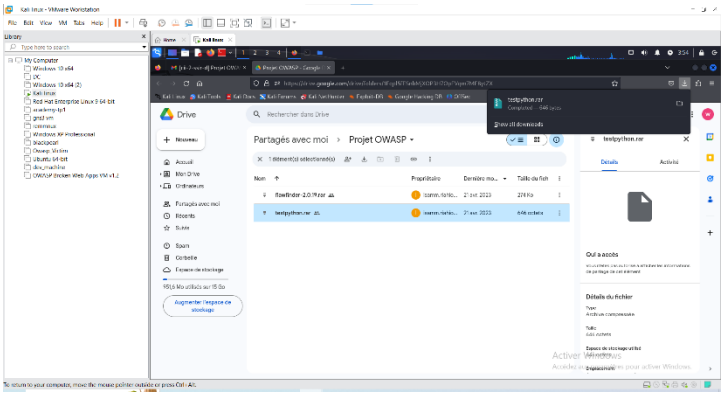
L’instalation de l’outil <<bandit>> en utilisant la commande : pip install bandit

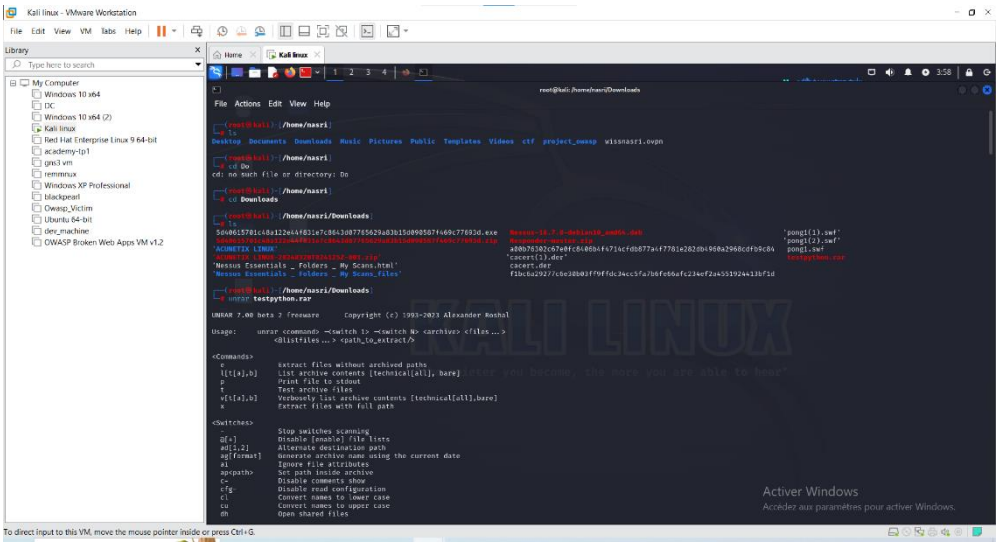




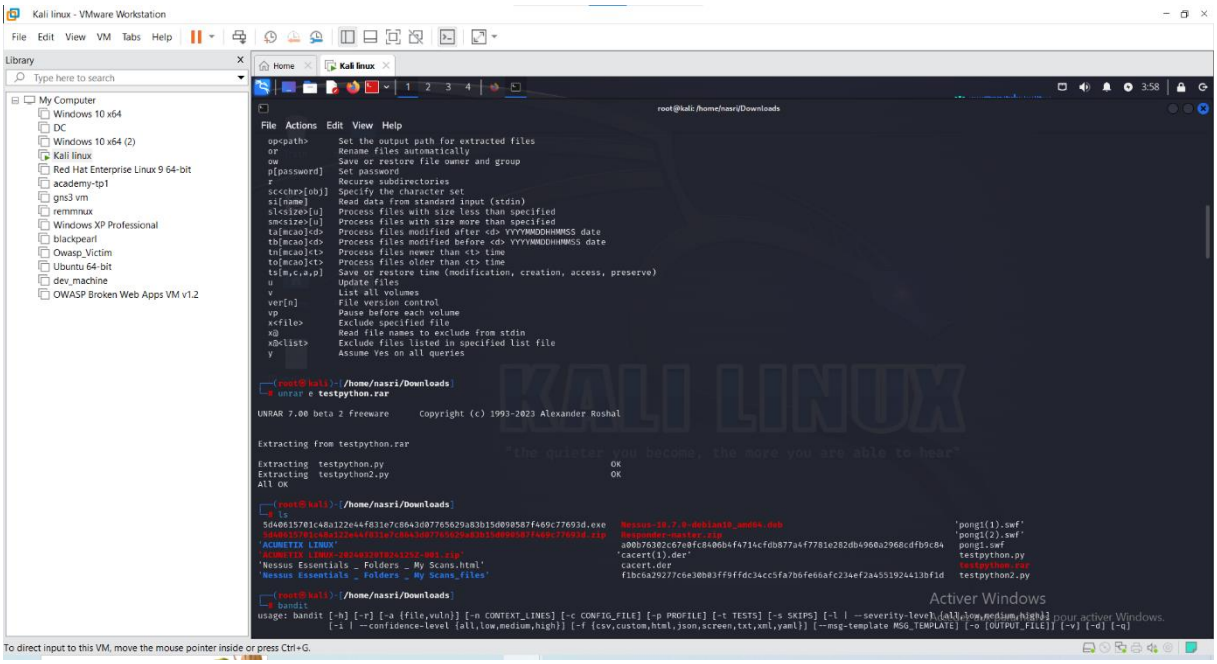
-Télécharger et copier le « fichier testpython.py » dans la machine kali linux

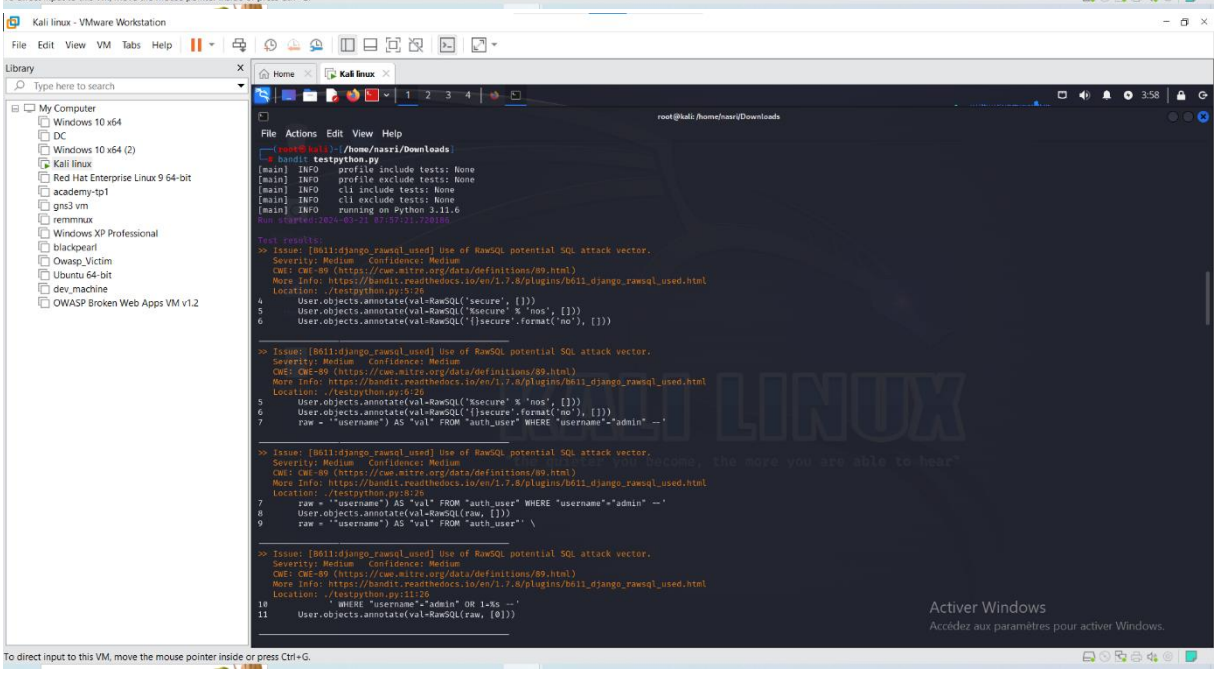
- Télécharger et copier le « fichier testpython2.py » dans la machine kali linux

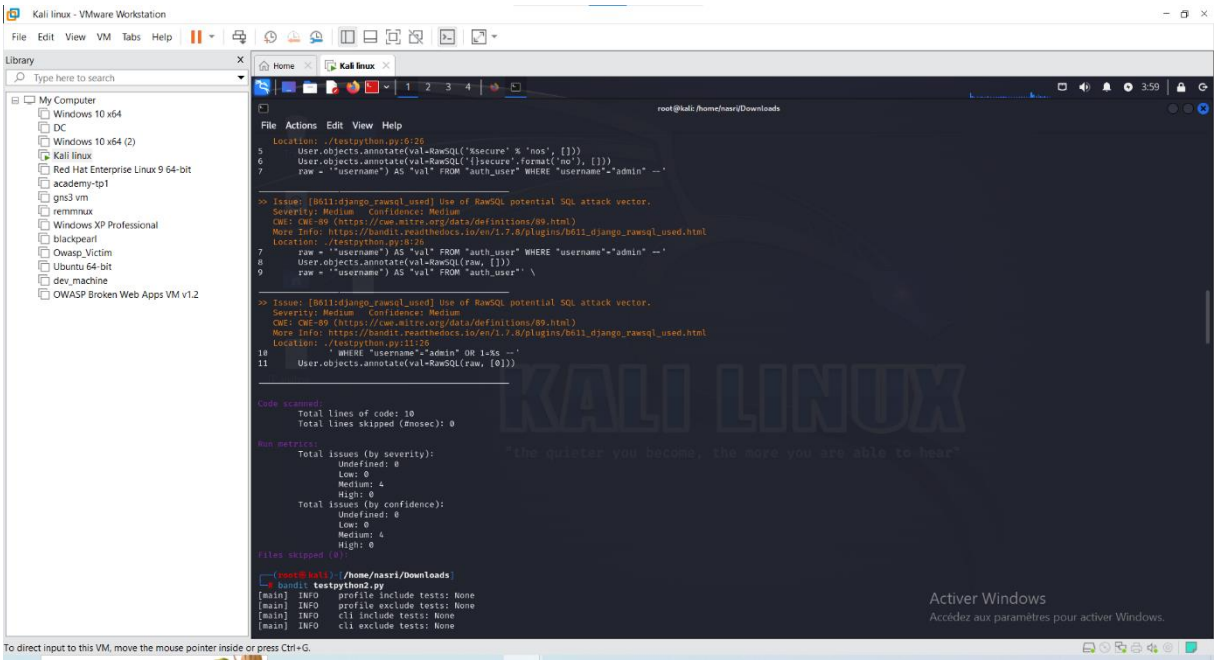


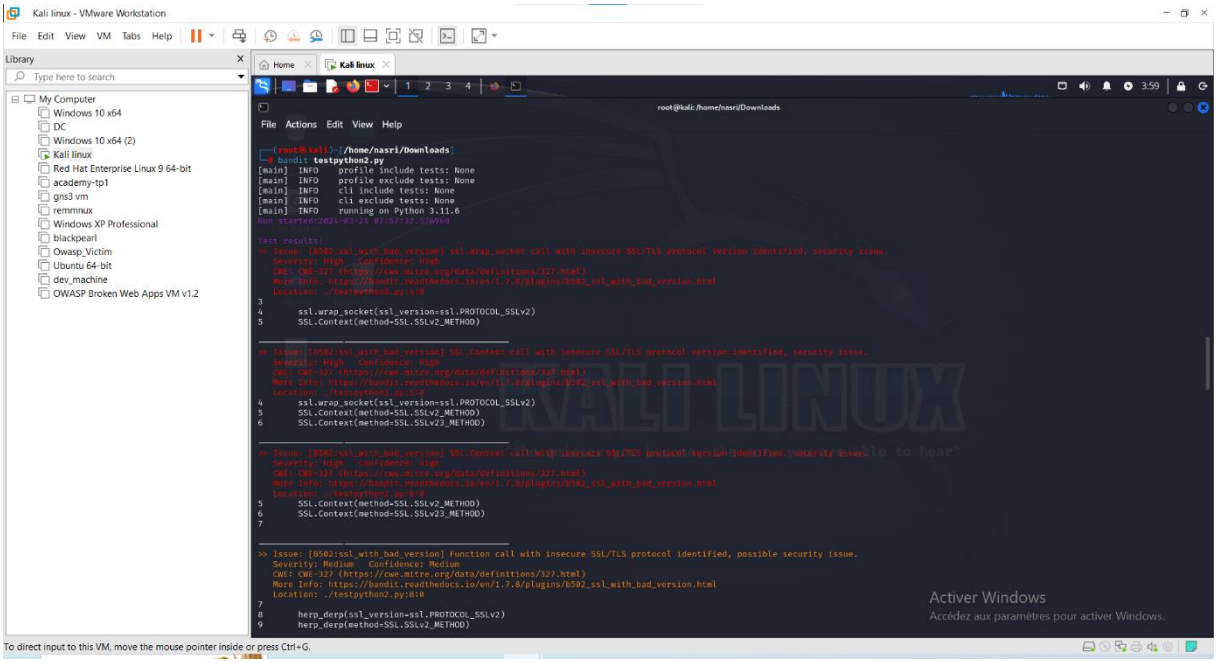


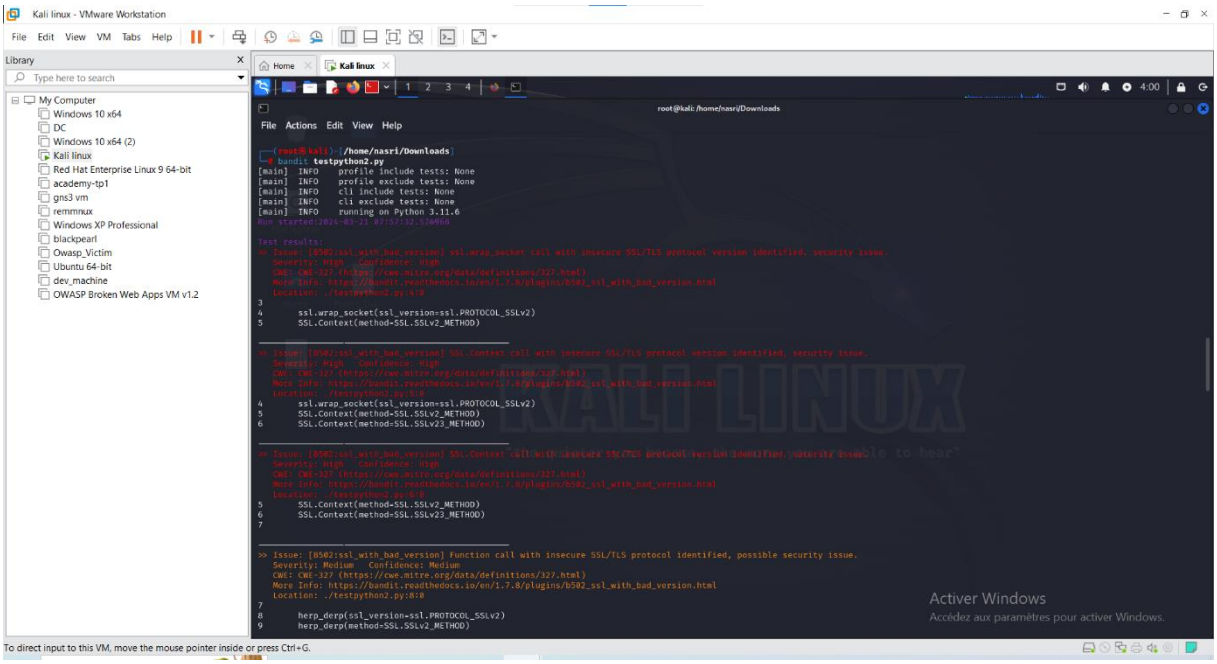
Evaluation de la sécurité des codes« testpython.py », « testpython2.py » en utilisant la commande **bandit tespython.py** et **bandit testpython2.py** et la retour de l'analyse effectué

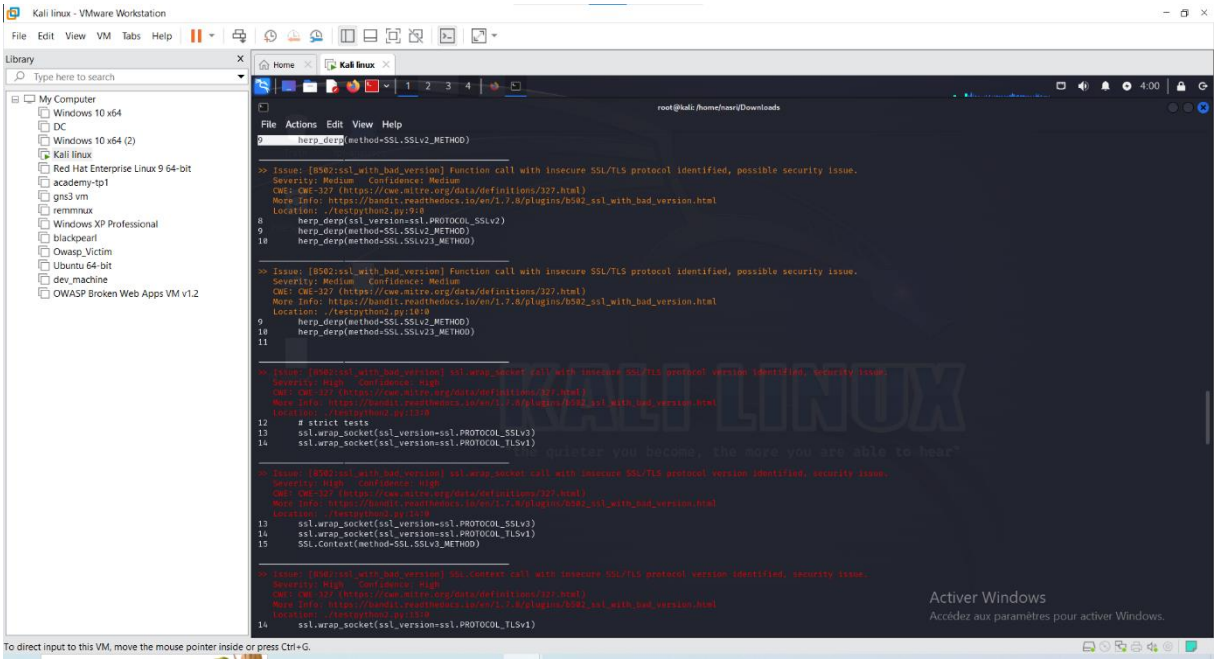


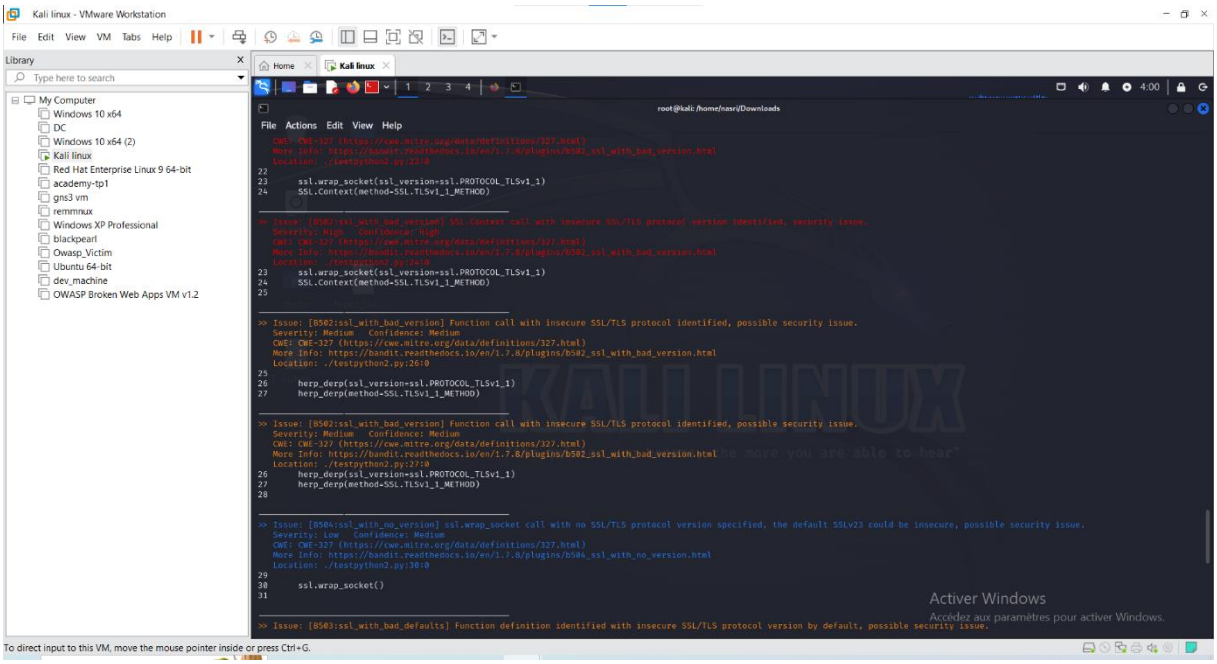


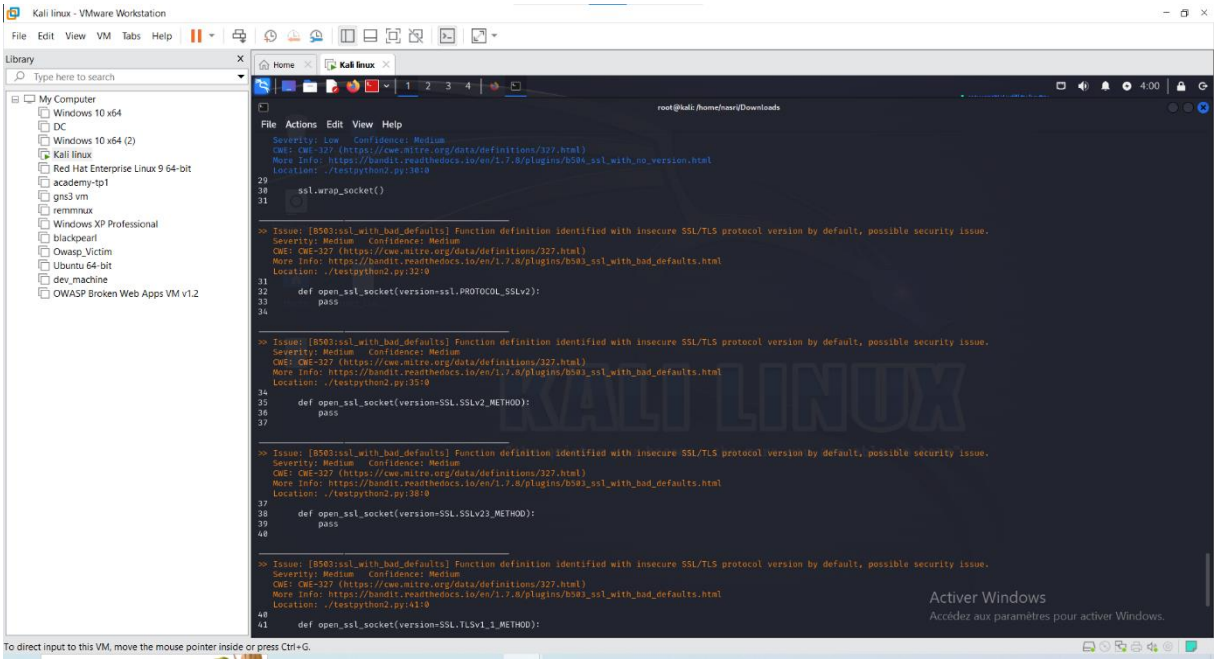

Kali linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 10 x64
DC
Windows 10 x64 (2)
Kali linux
Red Hat Enterprise Linux 9 64-bit
academy-tp1
gns3 vm
remmnux
Windows XP Professional
blackpearl
Owasp_Victim
Ubuntu 64-bit
dev_machine
OWASP Broken Web Apps VM v1.2
Home
Kali linux
root@kali: /home/nasri/Downloads
File Actions Edit View Help
Location: ./testpython.py:6:26
5 User.objects.annotate(val=RawSQL('%secure' % 'nos', []))
6 User.objects.annotate(val=RawSQL('{}secure'.format('no'), []))
7 raw = '"username") AS "val" FROM "auth_user" WHERE "username"="admin" --'
>> Issue: [B611:django_rawsql_used] Use of RawSQL potential SQL attack vector.
Severity: Medium Confidence: Medium
CWE: CWE-89 (https://cwe.mitre.org/data/definitions/89.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b611_django_rawsql_used.html
Location: ./testpython.py:8:26
7 raw = '"username") AS "val" FROM "auth_user" WHERE "username"="admin" --'
8 User.objects.annotate(val=RawSQL(raw, []))
9 raw = '"username") AS "val" FROM "auth_user"' \
>> Issue: [B611:django_rawsql_used] Use of RawSQL potential SQL attack vector.
Severity: Medium Confidence: Medium
CWE: CWE-89 (https://cwe.mitre.org/data/definitions/89.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b611_django_rawsql_used.html
Location: ./testpython.py:11:26
10 ' WHERE "username"="admin" OR 1=%s --'
11 User.objects.annotate(val=RawSQL(raw, [0]))
Code scanned:
Total lines of code: 10
Total lines skipped (#nosec): 0
Run metrics:
Total issues (by severity):
Undefined: 0
Low: 0
Medium: 4
High: 0
Total issues (by confidence):
Undefined: 0
Low: 0
Medium: 4
High: 0
Files skipped (0):
(root㉿kali)-[/home/nasri/Downloads]
bandit testpython2.py
[main] INFO profile include tests: None
[main] INFO profile exclude tests: None
[main] INFO cli include tests: None
[main] INFO cli exclude tests: None
"the quieter you become, the more you are able to hear"
Activer Windows
Accédez aux paramètres pour activer Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

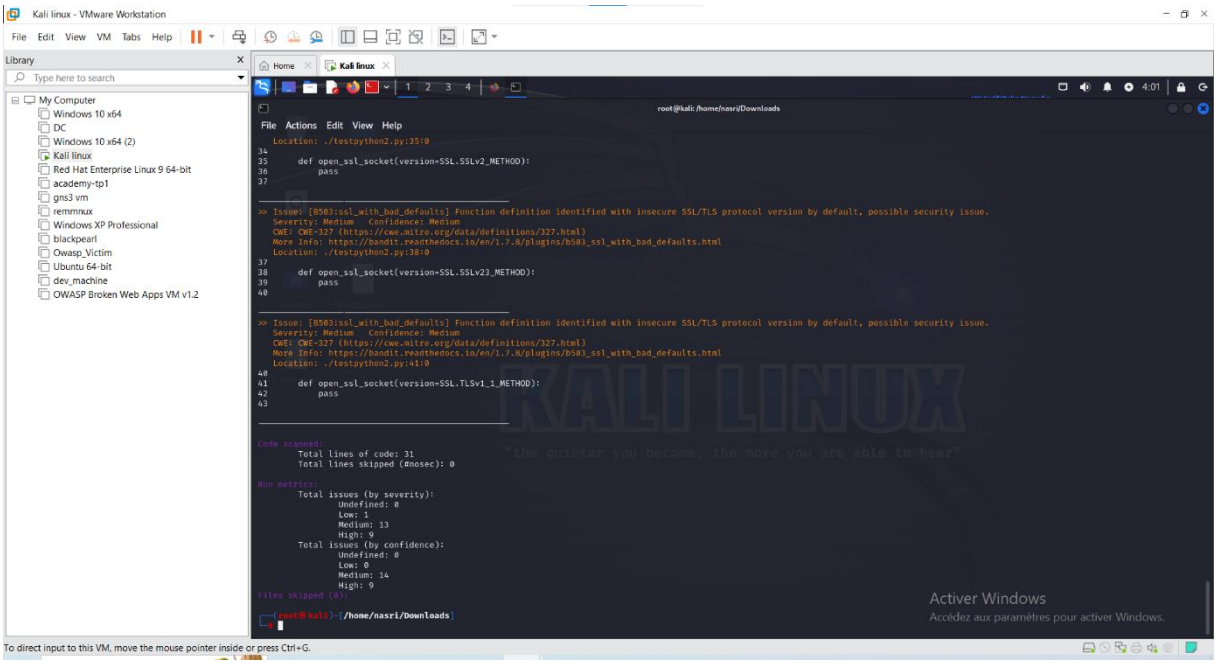

Kali linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 10 x64
DC
Windows 10 x64 (2)
Kali linux
Red Hat Enterprise Linux 9 64-bit
academy-tp1
gns3 vm
remmnux
Windows XP Professional
blackpearl
Owasp_Victim
Ubuntu 64-bit
dev_machine
OWASP Broken Web Apps VM v1.2
Home
Kali linux
root@kali: /home/nasri/Downloads
File Actions Edit View Help
(root㉿kali)-[/home/nasri/Downloads]
bandit testpython2.py
[main] INFO profile include tests: None
[main] INFO profile exclude tests: None
[main] INFO cli include tests: None
[main] INFO cli exclude tests: None
[main] INFO running on Python 3.11.6
Run started:2026-03-21 07:57:32.178960
Test results:
>> Issue: [B502:ssl_with_bad_version] ssl.wrap_socket call with insecure SSL/TLS protocol version identified, security issue.
Severity: High Confidence: High
CWE: CWE-327 (https://cwe.mitre.org/data/definitions/327.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b502_ssl_with_bad_version.html
Location: ./testpython2.py:4:0
3
4 ssl.wrap_socket(ssl_version=ssl.PROTOCOL_SSLv2)
5 SSL.Context(method=SSL.SSLv2_METHOD)
>> Issue: [B502:ssl_with_bad_version] SSL.Context call with insecure SSL/TLS protocol version identified, security issue.
Severity: High Confidence: High
CWE: CWE-327 (https://cwe.mitre.org/data/definitions/327.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b502_ssl_with_bad_version.html
Location: ./testpython2.py:5:0
4 ssl.wrap_socket(ssl_version=ssl.PROTOCOL_SSLv2)
5 SSL.Context(method=SSL.SSLv2_METHOD)
6 SSL.Context(method=SSL.SSLv23_METHOD)
>> Issue: [B502:ssl_with_bad_version] SSL.Context call with insecure SSL/TLS protocol version identified, security issue.
Severity: High Confidence: High
CWE: CWE-327 (https://cwe.mitre.org/data/definitions/327.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b502_ssl_with_bad_version.html
Location: ./testpython2.py:6:0
5 SSL.Context(method=SSL.SSLv2_METHOD)
6 SSL.Context(method=SSL.SSLv23_METHOD)
7
>> Issue: [B502:ssl_with_bad_version] Function call with insecure SSL/TLS protocol identified, possible security issue.
Severity: Medium Confidence: Medium
CWE: CWE-327 (https://cwe.mitre.org/data/definitions/327.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b502_ssl_with_bad_version.html
Location: ./testpython2.py:8:0
7
8 herp_derp(ssl_version=ssl.PROTOCOL_SSLv2)
9 herp_derp(method=SSL.SSLv2_METHOD)
"the quieter you become, the more you are able to hear"
Activer Windows
Accédez aux paramètres pour activer Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 10 x64
DC
Windows 10 x64 (2)
Kali linux
Red Hat Enterprise Linux 9 64-bit
academy-tp1
gns3 vm
remmnux
Windows XP Professional
blackpearl
Owasp_Victim
Ubuntu 64-bit
dev_machine
OWASP Broken Web Apps VM v1.2
Home
Kali linux
root@kali: /home/nasri/Downloads
File Actions Edit View Help
(root㉿kali)-[/home/nasri/Downloads]
bandit testpython2.py
[main] INFO profile include tests: None
[main] INFO profile exclude tests: None
[main] INFO cli include tests: None
[main] INFO cli exclude tests: None
[main] INFO running on Python 3.11.6
Run started:2024-03-21 07:57:32.530958
Test results:
>> Issue: [B502:ssl_with_bad_version] ssl.wrap_socket call with insecure SSL/TLS protocol version identified, security issue.
Severity: High Confidence: High
CWE: CWE-327 (https://cwe.mitre.org/data/definitions/327.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b502_ssl_with_bad_version.html
Location: ./testpython2.py:4:0
3
4 ssl.wrap_socket(ssl_version=ssl.PROTOCOL_SSLv2)
5 SSL.Context(method=SSL.SSLv2_METHOD)
>> Issue: [B502:ssl_with_bad_version] SSL.Context call with insecure SSL/TLS protocol version identified, security issue.
Severity: High Confidence: High
CWE: CWE-327 (https://cwe.mitre.org/data/definitions/327.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b502_ssl_with_bad_version.html
Location: ./testpython2.py:5:0
4 ssl.wrap_socket(ssl_version=ssl.PROTOCOL_SSLv2)
5 SSL.Context(method=SSL.SSLv2_METHOD)
6 SSL.Context(method=SSL.SSLv23_METHOD)
>> Issue: [B502:ssl_with_bad_version] SSL.Context call with insecure SSL/TLS protocol version identified, security issue.
Severity: High Confidence: High
CWE: CWE-327 (https://cwe.mitre.org/data/definitions/327.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b502_ssl_with_bad_version.html
Location: ./testpython2.py:6:0
5 SSL.Context(method=SSL.SSLv2_METHOD)
6 SSL.Context(method=SSL.SSLv23_METHOD)
7
>> Issue: [B502:ssl_with_bad_version] Function call with insecure SSL/TLS protocol identified, possible security issue.
Severity: Medium Confidence: Medium
CWE: CWE-327 (https://cwe.mitre.org/data/definitions/327.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b502_ssl_with_bad_version.html
Location: ./testpython2.py:8:0
7
8 herp_derp(ssl_version=ssl.PROTOCOL_SSLv2)
9 herp_derp(method=SSL.SSLv2_METHOD)
Activer Windows
Accédez aux paramètres pour activer Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 10 x64
DC
Windows 10 x64 (2)
Kali linux
Red Hat Enterprise Linux 9 64-bit
academy-tp1
gns3 vm
remmnux
Windows XP Professional
blackpearl
Owasp_Victim
Ubuntu 64-bit
dev_machine
OWASP Broken Web Apps VM v1.2
Home
Kali linux
root@kali: /home/nasri/Downloads
File Actions Edit View Help
8 herp_derp(method=SSL.SSLv2_METHOD)
>> Issue: [B502:ssl_with_bad_version] Function call with insecure SSL/TLS protocol identified, possible security issue.
Severity: Medium Confidence: Medium
CWE: CWE-327 (https://cwe.mitre.org/data/definitions/327.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b502_ssl_with_bad_version.html
Location: ./testpython2.py:9:0
8 herp_derp(ssl_version=ssl.PROTOCOL_SSLv2)
9 herp_derp(method=SSL.SSLv2_METHOD)
10 herp_derp(method=SSL.SSLv23_METHOD)
>> Issue: [B502:ssl_with_bad_version] Function call with insecure SSL/TLS protocol identified, possible security issue.
Severity: Medium Confidence: Medium
CWE: CWE-327 (https://cwe.mitre.org/data/definitions/327.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b502_ssl_with_bad_version.html
Location: ./testpython2.py:10:0
9 herp_derp(method=SSL.SSLv2_METHOD)
10 herp_derp(method=SSL.SSLv23_METHOD)
11
>> Issue: [B502:ssl_with_bad_version] ssl.wrap_socket call with insecure SSL/TLS protocol version identified, security issue.
Severity: High Confidence: High
CWE: CWE-327 (https://cwe.mitre.org/data/definitions/327.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b502_ssl_with_bad_version.html
Location: ./testpython2.py:12:0
12 # strict tests
13 ssl.wrap_socket(ssl_version=ssl.PROTOCOL_SSLv3)
14 ssl.wrap_socket(ssl_version=ssl.PROTOCOL_TLSv1)
>> Issue: [B502:ssl_with_bad_version] ssl.wrap_socket call with insecure SSL/TLS protocol version identified, security issue.
Severity: High Confidence: High
CWE: CWE-327 (https://cwe.mitre.org/data/definitions/327.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b502_ssl_with_bad_version.html
Location: ./testpython2.py:13:0
13 ssl.wrap_socket(ssl_version=ssl.PROTOCOL_SSLv3)
14 ssl.wrap_socket(ssl_version=ssl.PROTOCOL_TLSv1)
15 SSL.Context(method=SSL.SSLv3_METHOD)
>> Issue: [B502:ssl_with_bad_version] SSL.Context call with insecure SSL/TLS protocol version identified, security issue.
Severity: High Confidence: High
CWE: CWE-327 (https://cwe.mitre.org/data/definitions/327.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b502_ssl_with_bad_version.html
Location: ./testpython2.py:14:0
14 ssl.wrap_socket(ssl_version=ssl.PROTOCOL_TLSv1)
Activer Windows
Accédez aux paramètres pour activer Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 10 x64
DC
Windows 10 x64 (2)
Kali linux
Red Hat Enterprise Linux 9 64-bit
academy-tp1
gns3 vm
remmnux
Windows XP Professional
blackpearl
Owasp_Victim
Ubuntu 64-bit
dev_machine
OWASP Broken Web Apps VM v1.2
Home
Kali linux
root@kali: /home/nasri/Downloads
File Actions Edit View Help
>> Issue: [B502:ssl_with_bad_version] Function call with insecure SSL/TLS protocol identified, possible security issue.
Severity: Medium Confidence: Medium
CWE: CWE-327 (https://cwe.mitre.org/data/definitions/327.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b502_ssl_with_bad_version.html
Location: ./testpython2.py:26:0
>> Issue: [B504:ssl_with_no_version] ssl.wrap_socket call with no SSL/TLS protocol version specified, the default SSLv23 could be insecure, possible security issue.
Severity: Low Confidence: Medium
CWE: CWE-327 (https://cwe.mitre.org/data/definitions/327.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b504_ssl_with_no_version.html
Location: ./testpython2.py:30:0
>> Issue: [B503:ssl_with_bad_defaults] Function definition identified with insecure SSL/TLS protocol version by default, possible security issue.
Activer Windows
Accédez aux paramètres pour activer Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 10 x64
DC
Windows 10 x64 (2)
Kali linux
Red Hat Enterprise Linux 9 64-bit
academy-tp1
gns3 vm
remmnux
Windows XP Professional
blackpearl
Owasp_Victim
Ubuntu 64-bit
dev_machine
OWASP Broken Web Apps VM v1.2
Home
Kali linux
root@kali: /home/nasri/Downloads
File Actions Edit View Help
>> Issue: [B503:ssl_with_bad_defaults] Function definition identified with insecure SSL/TLS protocol version by default, possible security issue.
Severity: Medium Confidence: Medium
CWE: CWE-327 (https://cwe.mitre.org/data/definitions/327.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b503_ssl_with_bad_defaults.html
Location: ./testpython2.py:32:0
>> Issue: [B503:ssl_with_bad_defaults] Function definition identified with insecure SSL/TLS protocol version by default, possible security issue.
Severity: Medium Confidence: Medium
CWE: CWE-327 (https://cwe.mitre.org/data/definitions/327.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b503_ssl_with_bad_defaults.html
Location: ./testpython2.py:35:0
>> Issue: [B503:ssl_with_bad_defaults] Function definition identified with insecure SSL/TLS protocol version by default, possible security issue.
Severity: Medium Confidence: Medium
CWE: CWE-327 (https://cwe.mitre.org/data/definitions/327.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b503_ssl_with_bad_defaults.html
Location: ./testpython2.py:38:0
>> Issue: [B503:ssl_with_bad_defaults] Function definition identified with insecure SSL/TLS protocol version by default, possible security issue.
Severity: Medium Confidence: Medium
CWE: CWE-327 (https://cwe.mitre.org/data/definitions/327.html)
More Info: https://bandit.readthedocs.io/en/1.7.8/plugins/b503_ssl_with_bad_defaults.html
Location: ./testpython2.py:41:0
Activer Windows
Accédez aux paramètres pour activer Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Le fichier « testpython2.py » est plus vulnerable que l'autre fichier « testpython.py »

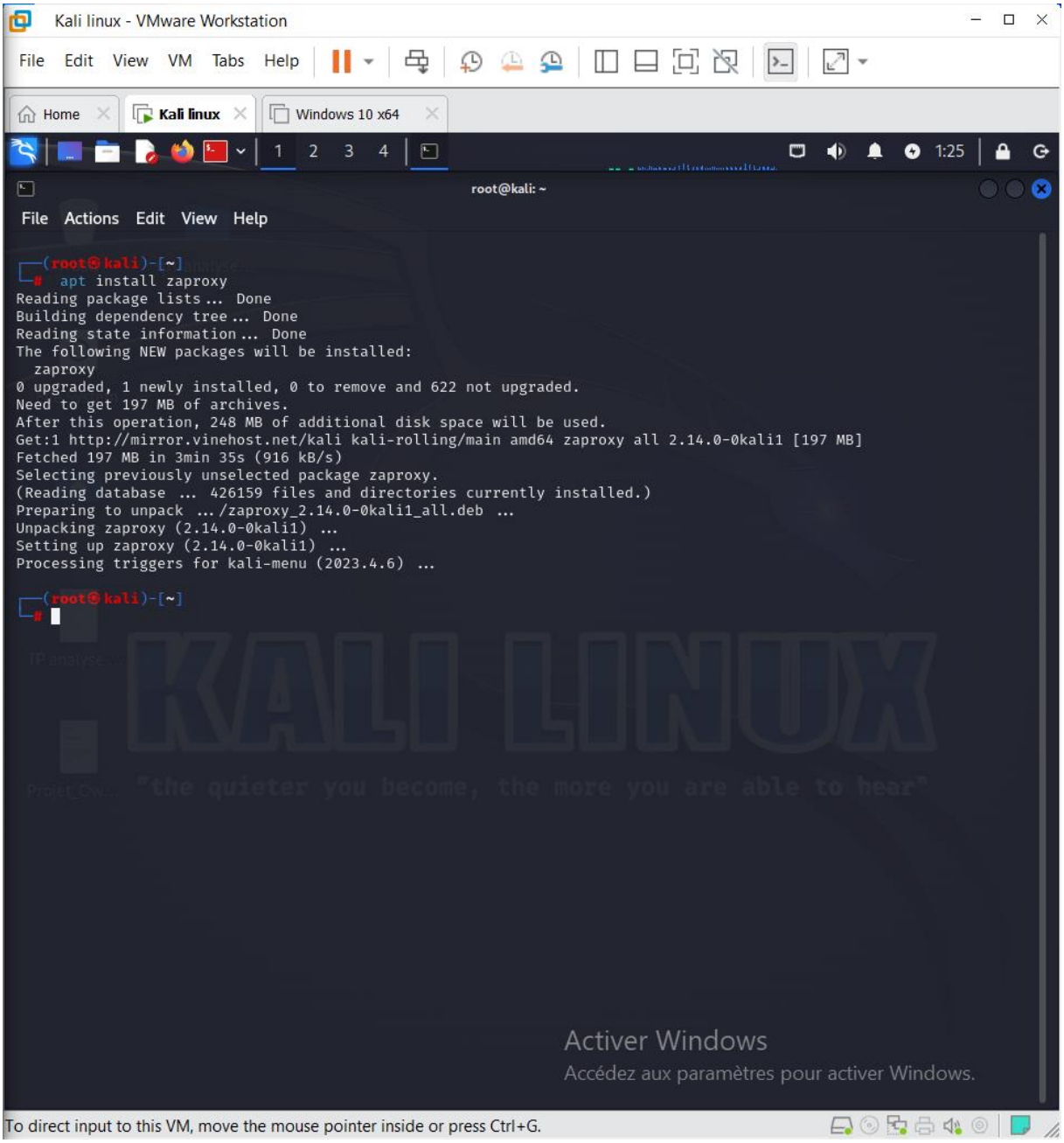
« testpython2.py »

« testpython.py »

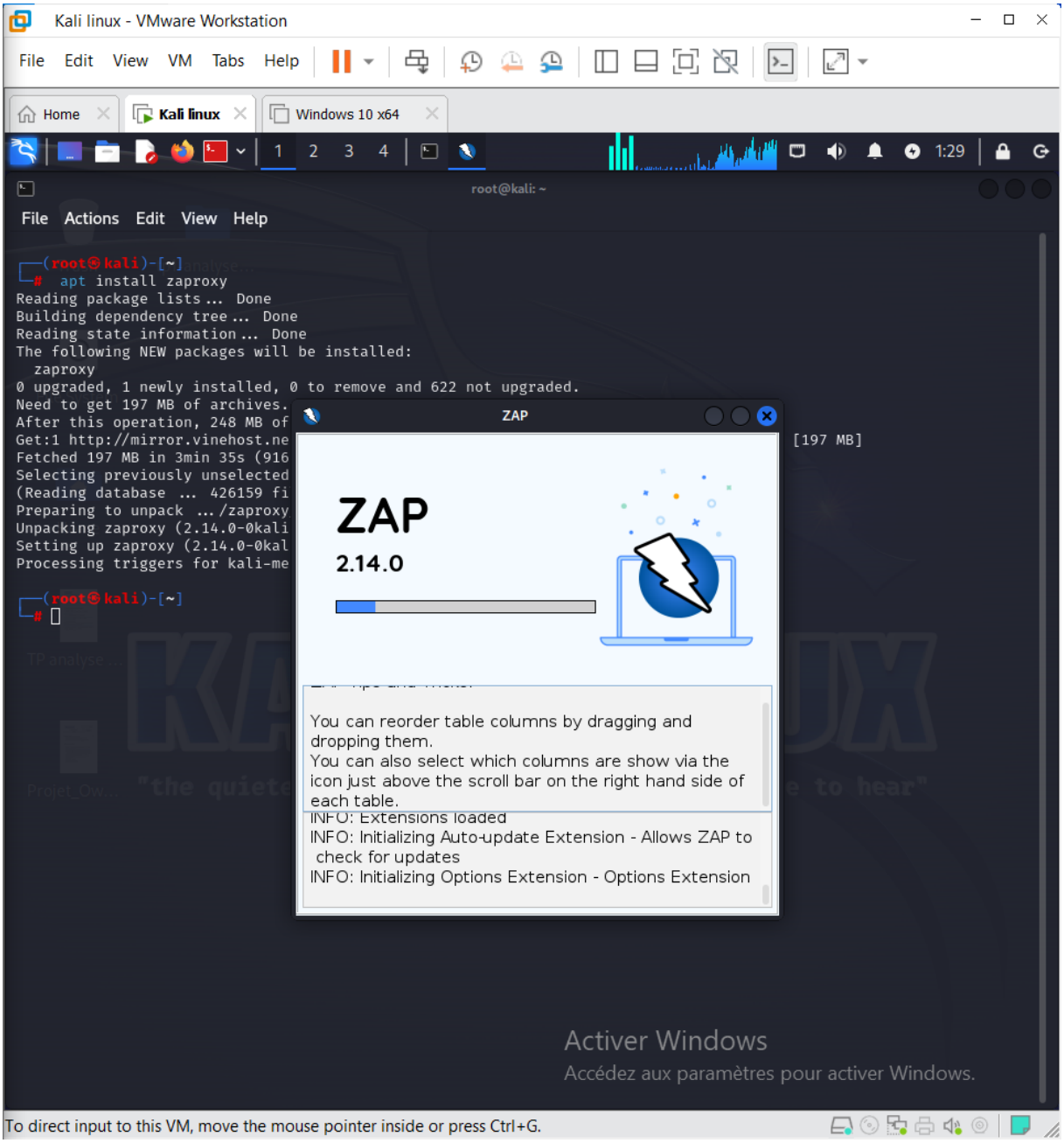
3.Tests dynamiques de la sécurité des applications (DAST)

3.1Analyse du code de l'application « ghost » de la machine vulnérable « OWASP_Broken_Web_Apps_VM_1.2 » à l'aide de l'outil « Zaproxy »

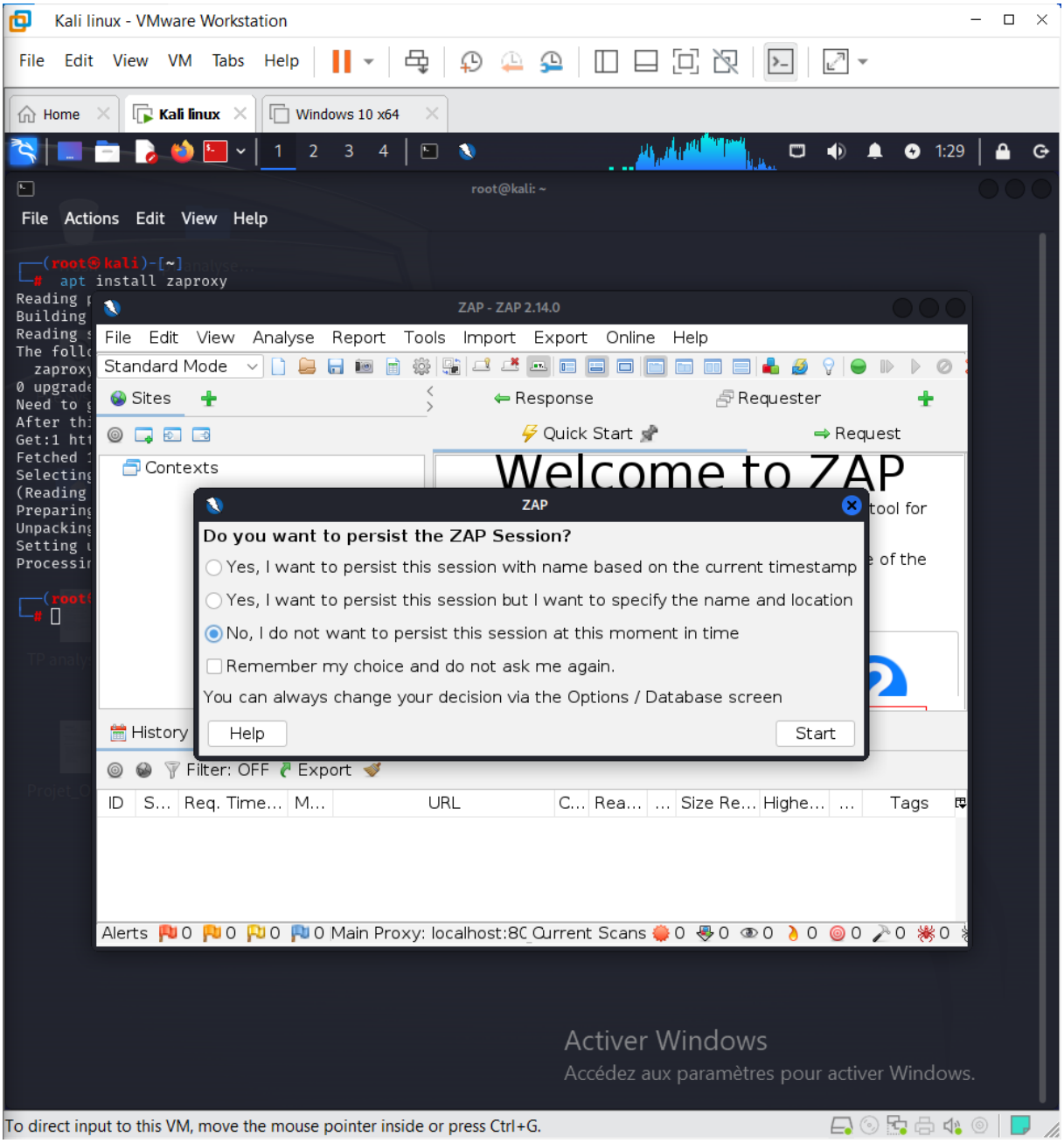
1.installer zaproxy



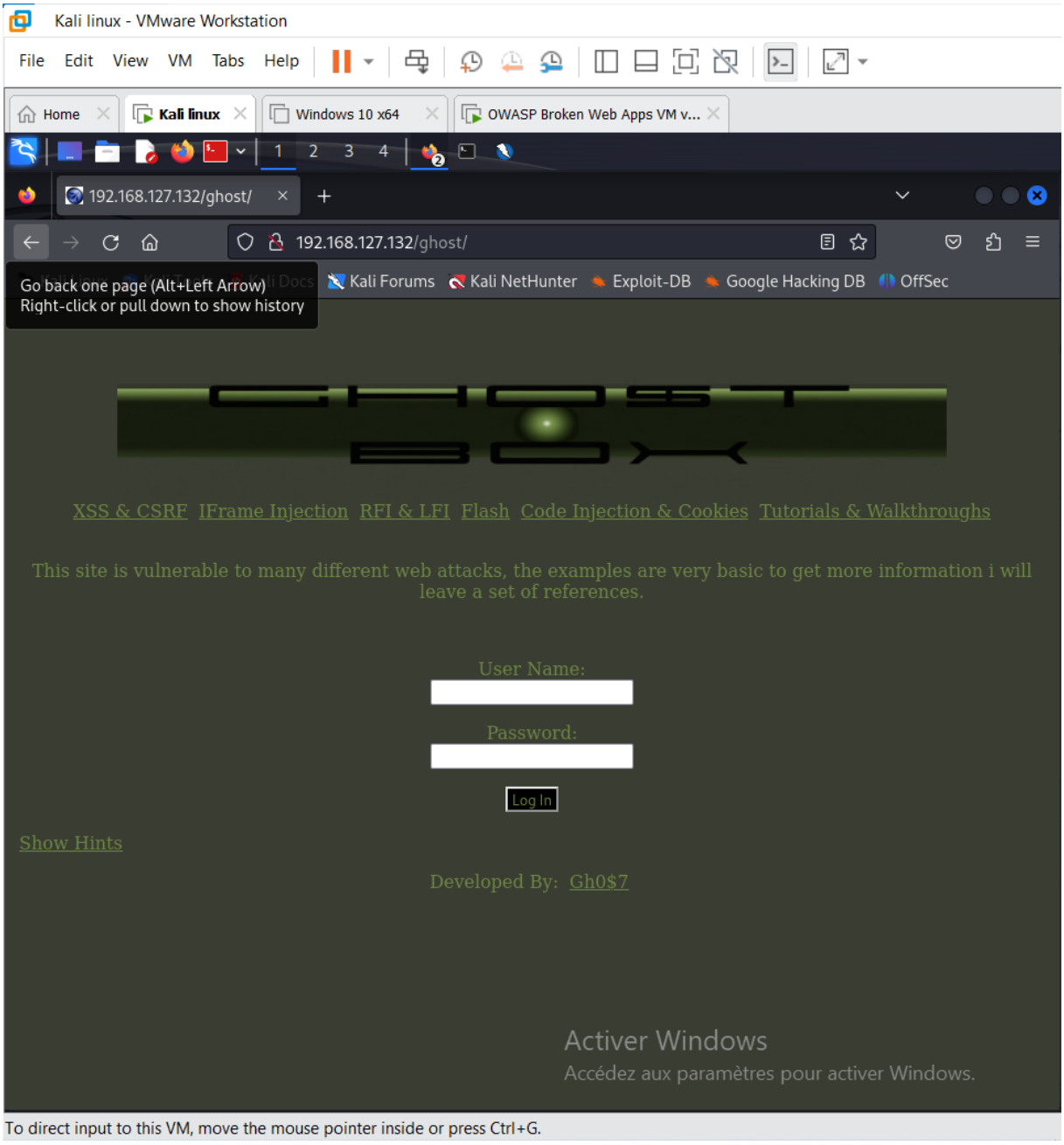
2.lancer zaproxy



3. choisir l'option

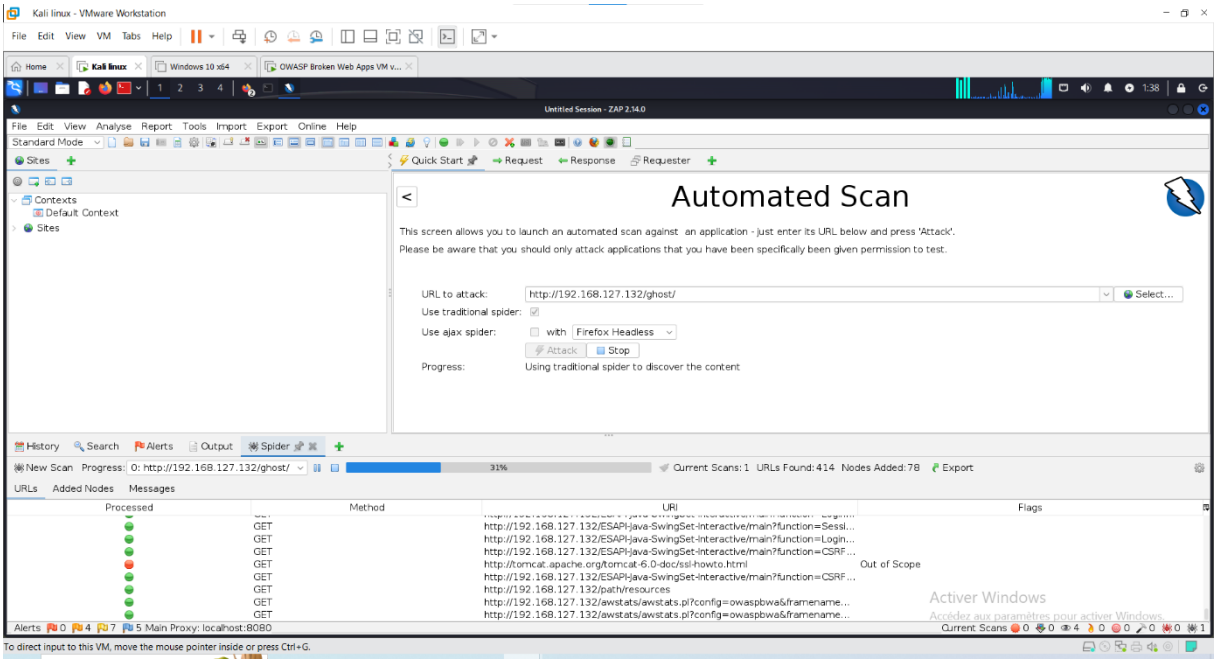


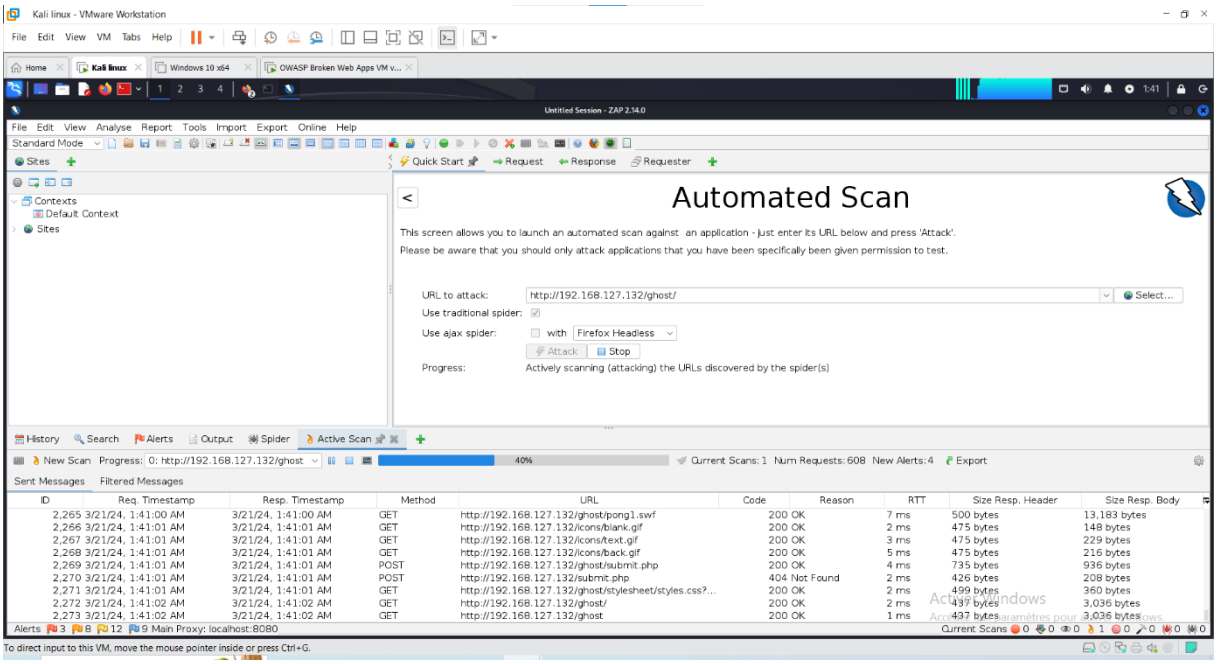
4- Lancer un test automatique sur l'application "ghost" de la machine vulnérable « OWASP_Broken_Web_Apps_VM_1.2 »



Ils’agit de decouvrir tous les repertoires , tous les fichier , tous les scripts et tout ce qui touve a l’interieur de site web

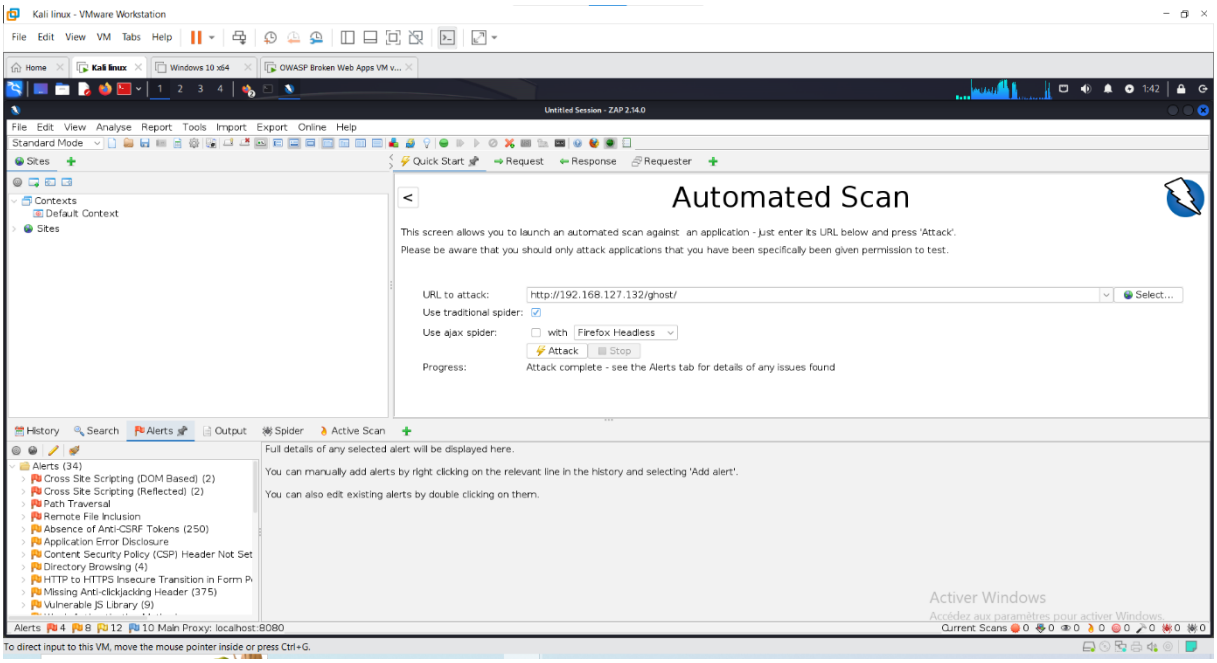
Afin qu’une fois que vous avez la liste de tous ces differents repertoires , noous saura exactement ou se touvent les formulaires d’entree ,ou se trouve les zones possibles sur lesquelles nous pouvons executer nos charges utiles ou notre injection





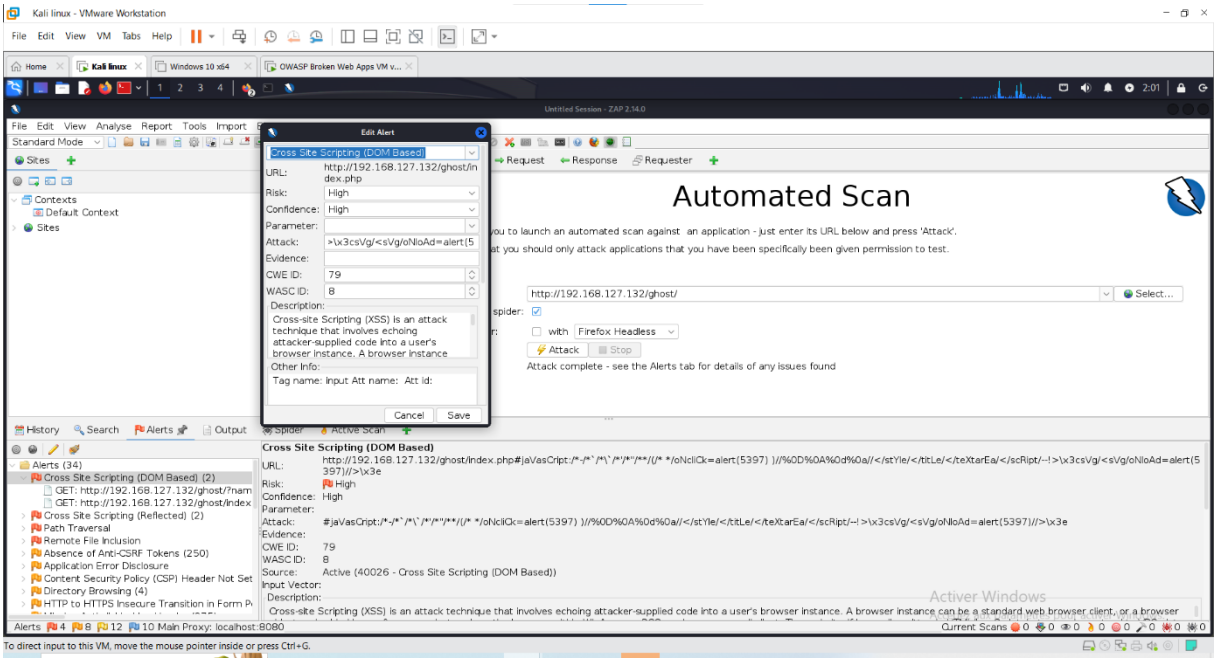
5- Retourner les résultats du test

Il existes 34 alertes

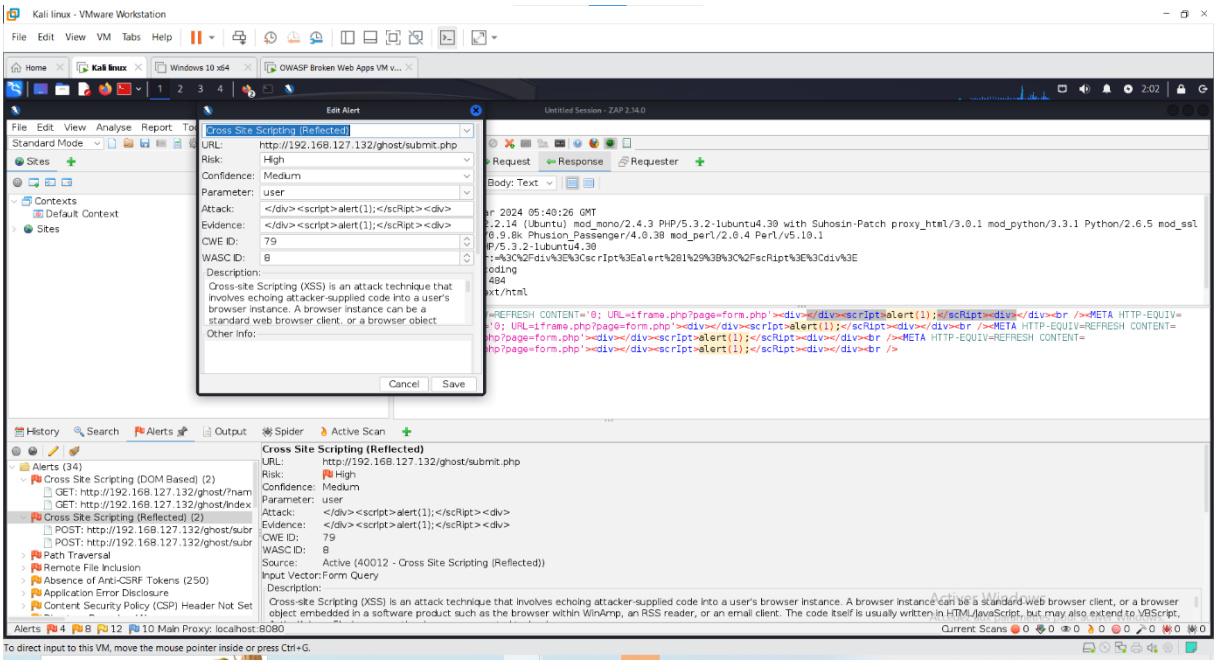


Citons l'exemples de ses trois alertes :

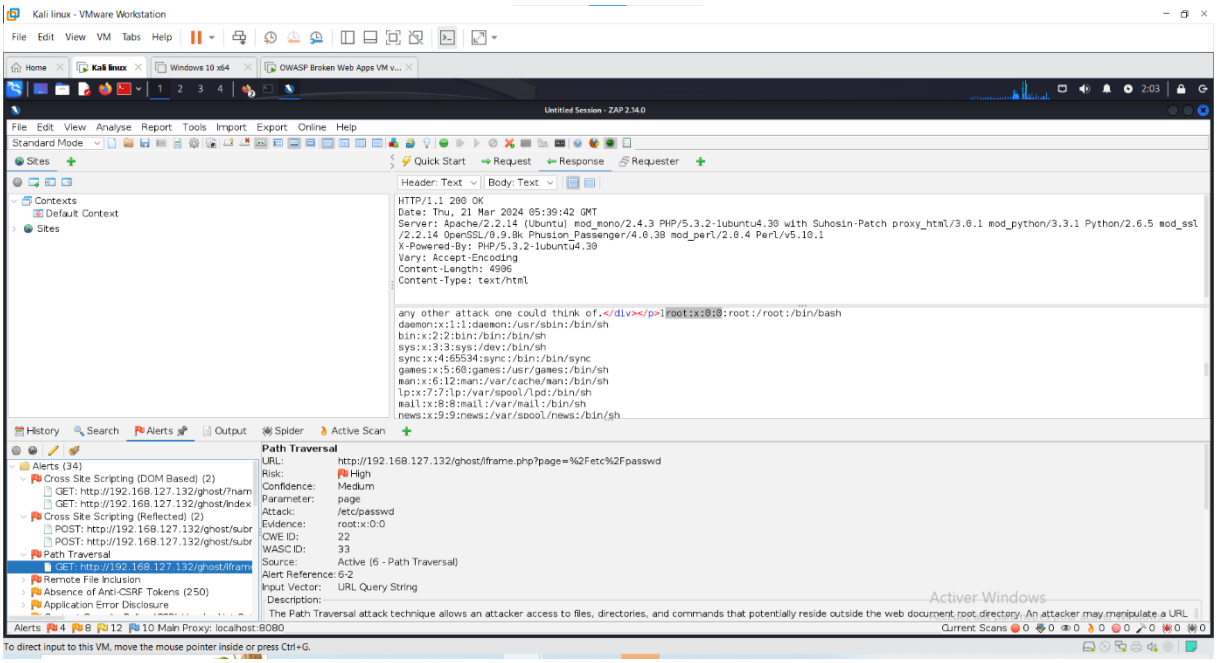
Cross site scripting :



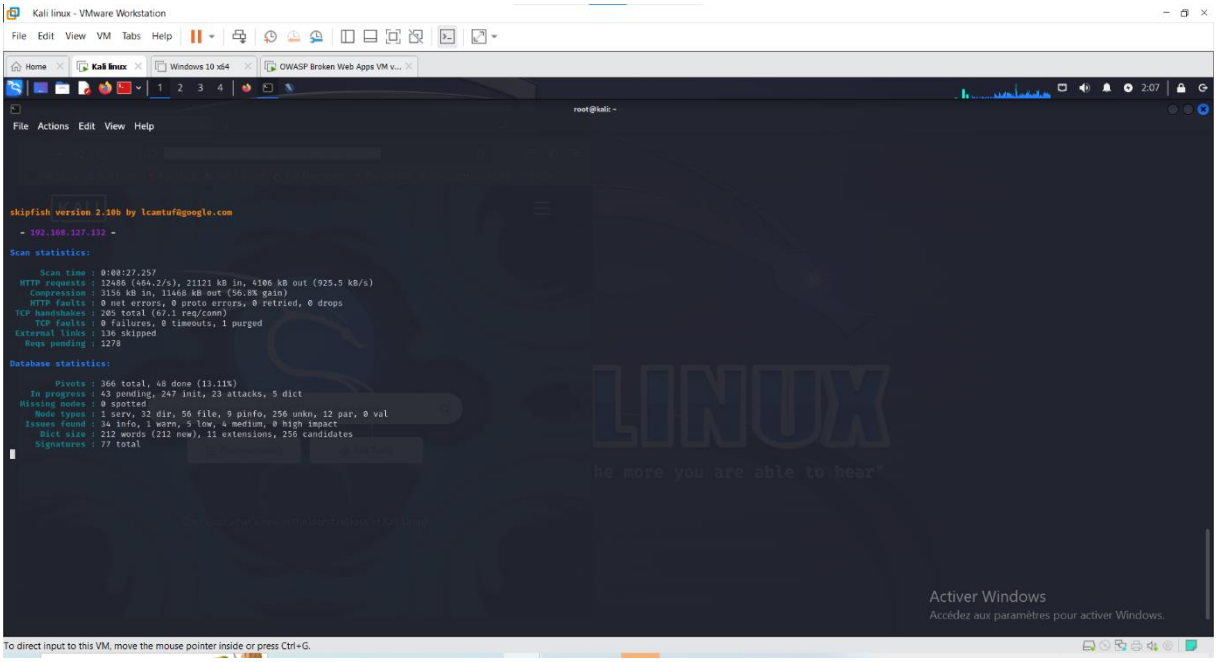
Cross site scripting (reflected)

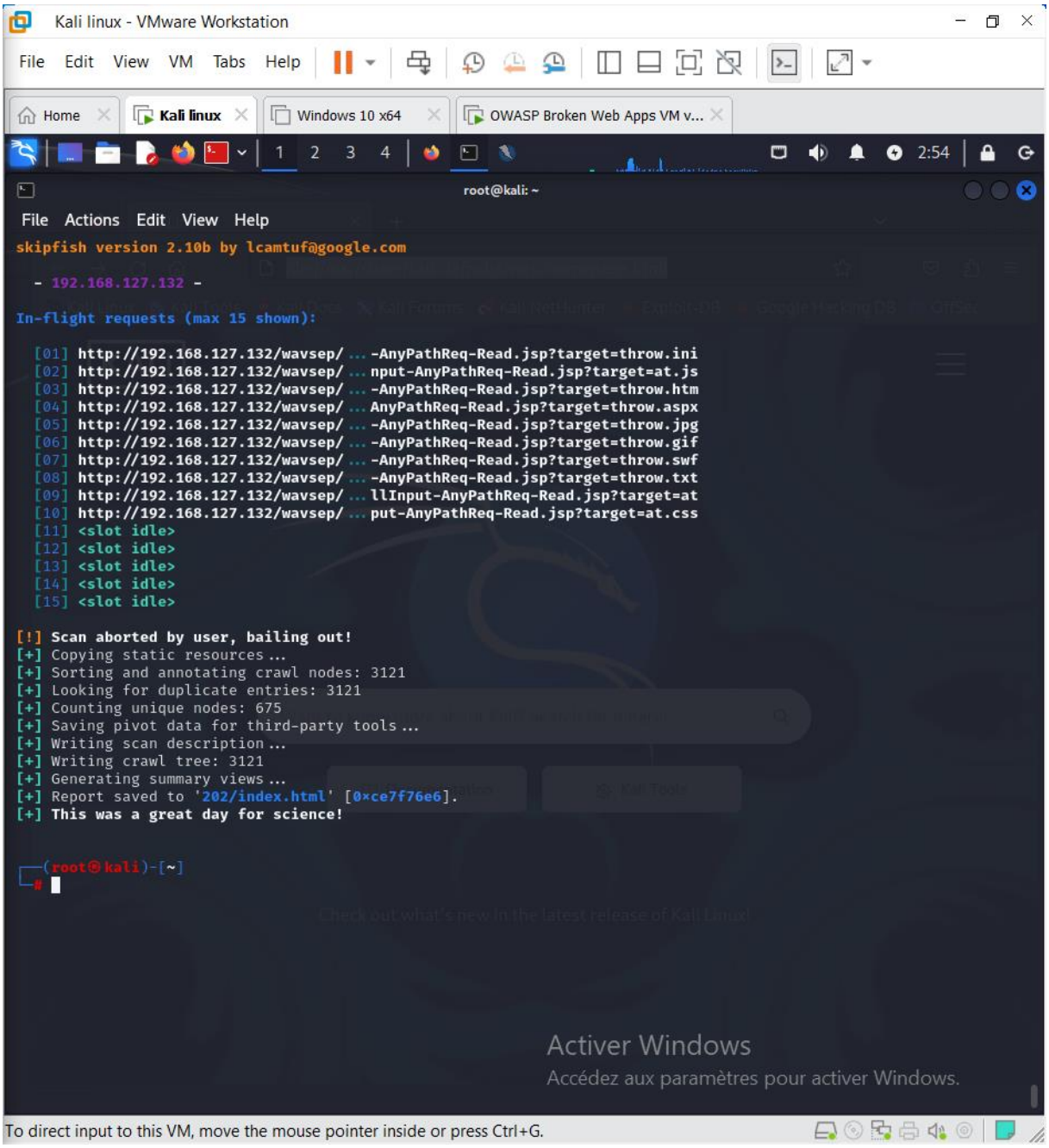


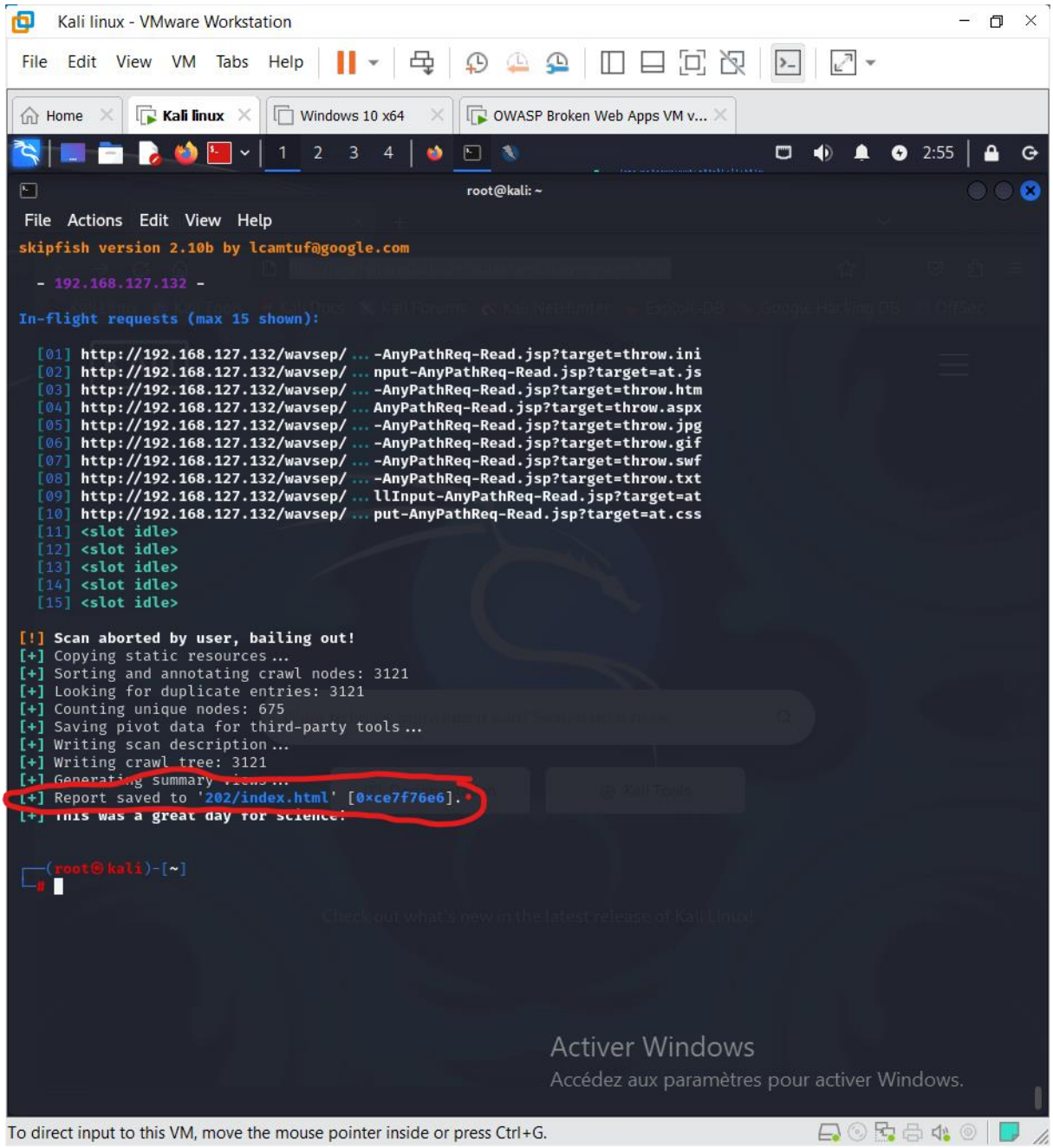
Path travelsal

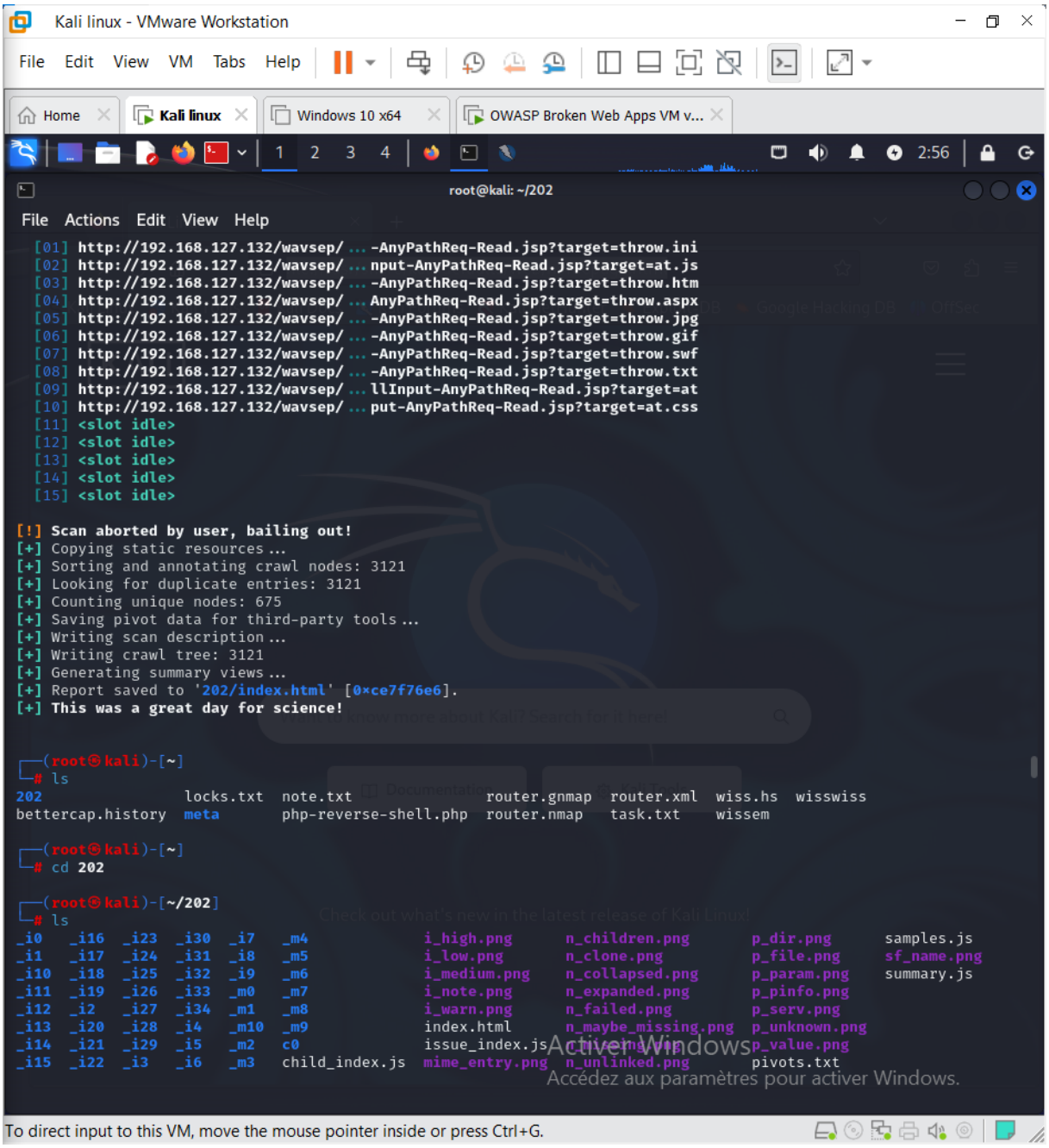


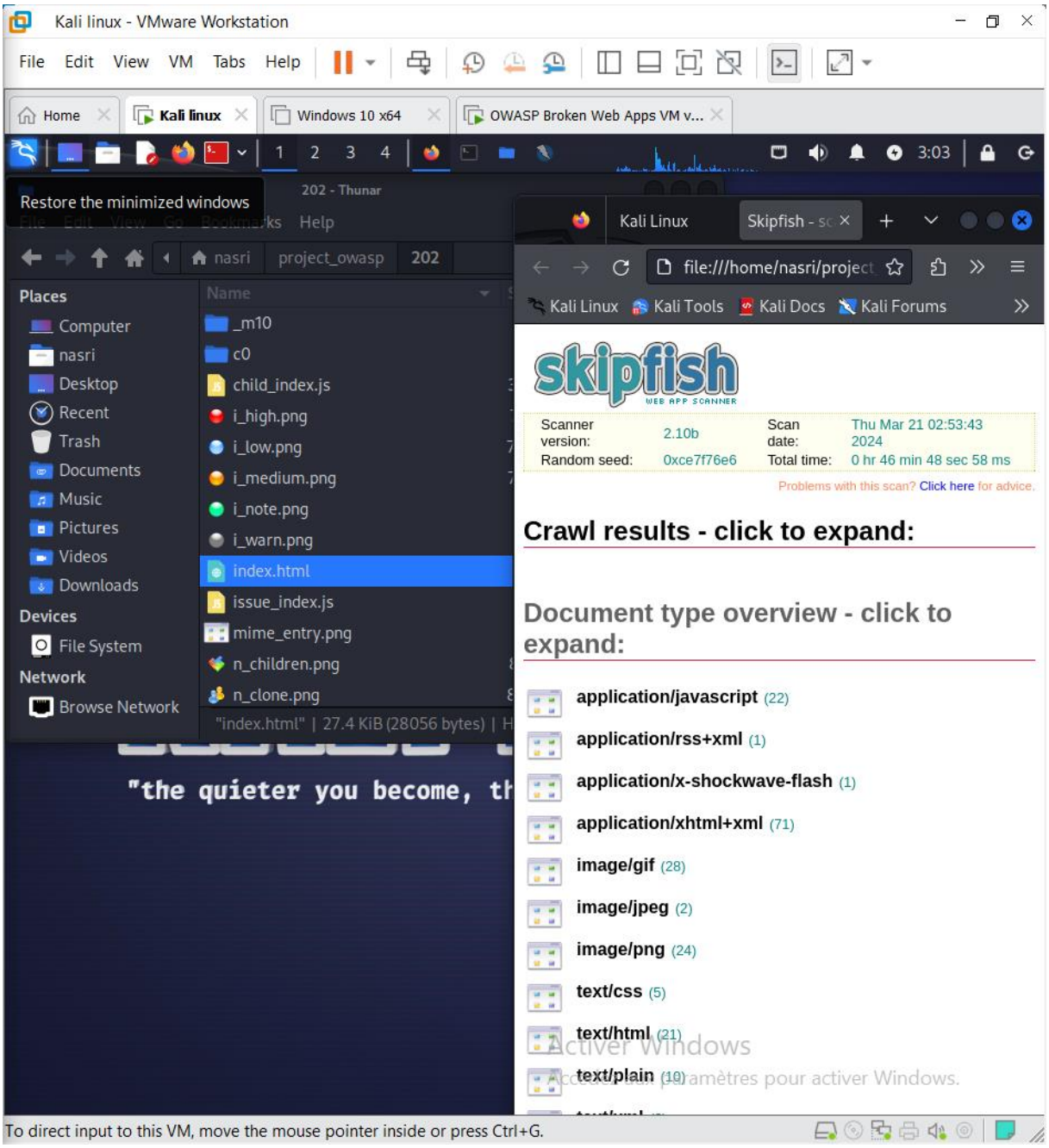
Exercice2

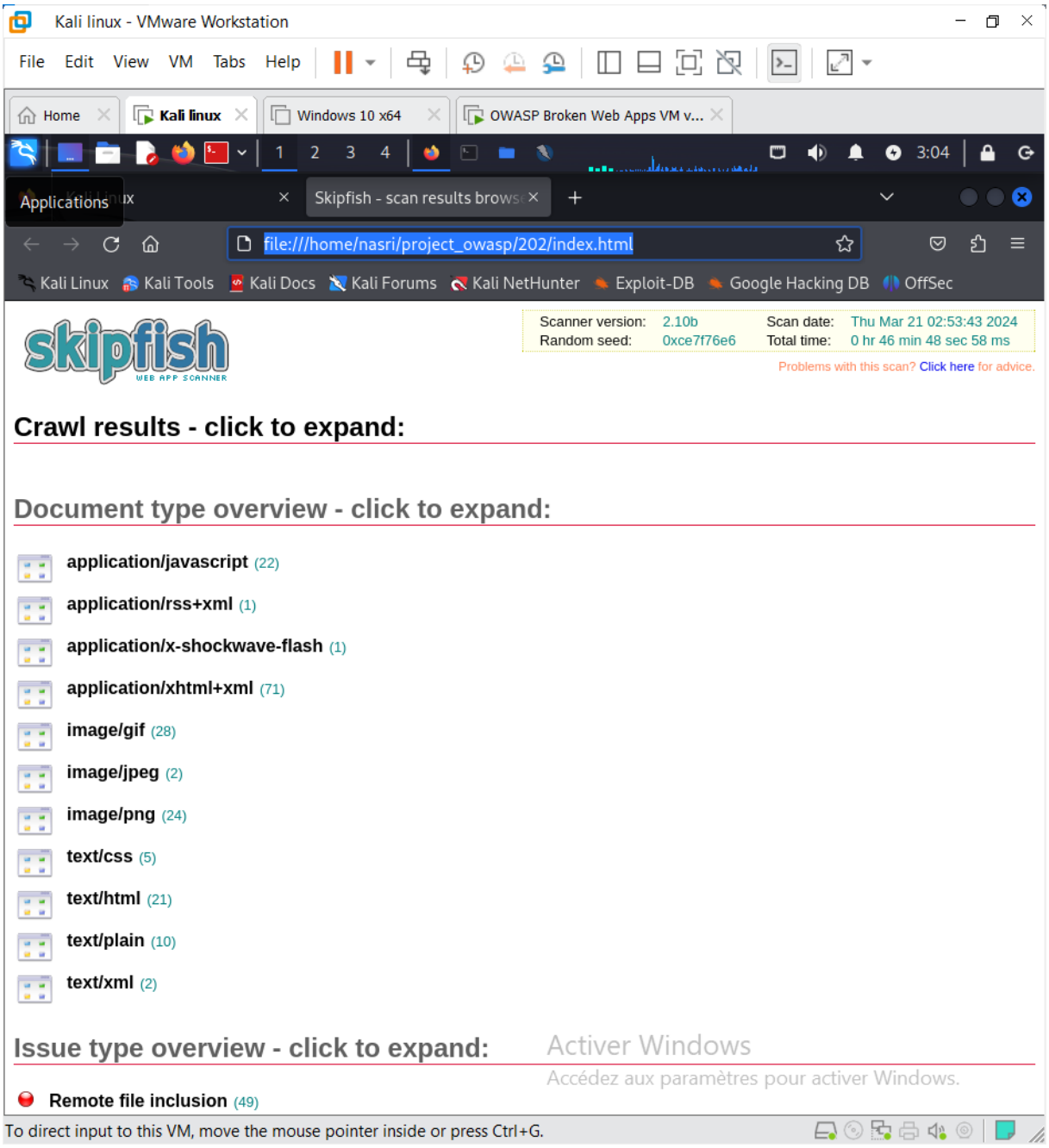

Kali linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
Windows 10 x64
OWASP Broken Web Apps VM v...
root@kali: ~
File Actions Edit View Help
skipfish version 2.10b by lcamtuf@google.com
- 192.168.127.132 -
Scan statistics:
Scan time : 0:00:27.257
HTTP requests : 12486 (464.2/s), 21121 kB in, 4106 kB out (925.5 kB/s)
Compression : 3156 kB in, 11468 kB out (56.8% gain)
HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
TCP handshakes : 205 total (67.1 req/conn)
TCP faults : 0 failures, 0 timeouts, 1 purged
External links : 136 skipped
Reqs pending : 1278
Database statistics:
Pivots : 366 total, 48 done (13.11%)
In progress : 43 pending, 247 init, 23 attacks, 5 dict
Missing nodes : 0 spotted
Node types : 1 serv, 32 dir, 56 file, 9 pinfo, 256 unkn, 12 par, 0 val
Issues found : 34 info, 1 warn, 5 low, 4 medium, 0 high impact
Dict size : 212 words (212 new), 11 extensions, 256 candidates
Signatures : 77 total
Activer Windows
Accédez aux paramètres pour activer Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

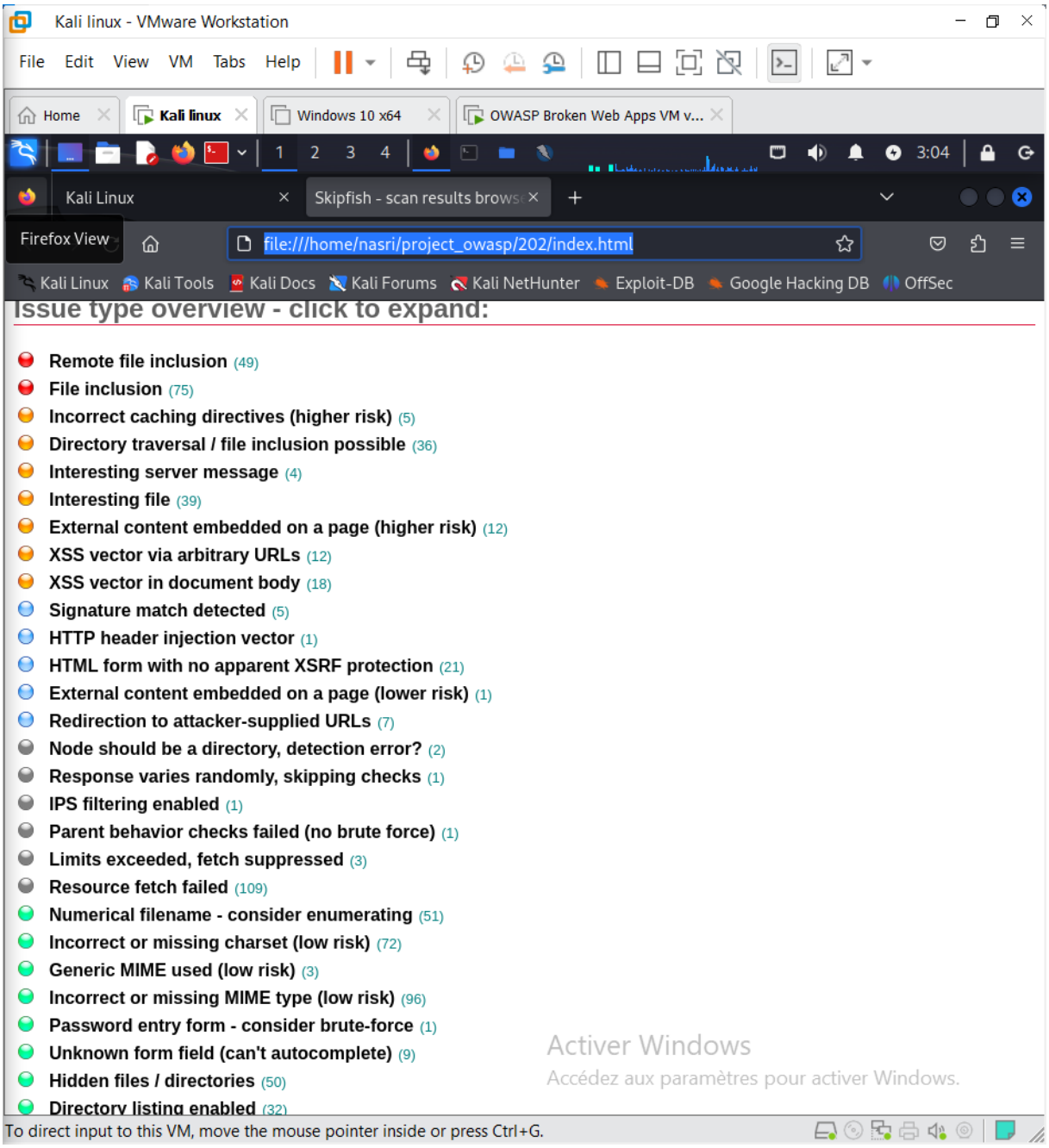

Kali linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
Windows 10 x64
OWASP Broken Web Apps VM v...
1 2 3 4
2:54
root@kali: ~
File Actions Edit View Help
skipfish version 2.10b by lcamtuf@google.com
- 192.168.127.132 -
In-flight requests (max 15 shown):
[01] http://192.168.127.132/wavsep/ ... -AnyPathReq-Read.jsp?target=throw.ini
[02] http://192.168.127.132/wavsep/ ... nput-AnyPathReq-Read.jsp?target=at.js
[03] http://192.168.127.132/wavsep/ ... -AnyPathReq-Read.jsp?target=throw.htm
[04] http://192.168.127.132/wavsep/ ... AnyPathReq-Read.jsp?target=throw.aspx
[05] http://192.168.127.132/wavsep/ ... -AnyPathReq-Read.jsp?target=throw.jpg
[06] http://192.168.127.132/wavsep/ ... -AnyPathReq-Read.jsp?target=throw.gif
[07] http://192.168.127.132/wavsep/ ... -AnyPathReq-Read.jsp?target=throw.swf
[08] http://192.168.127.132/wavsep/ ... -AnyPathReq-Read.jsp?target=throw.txt
[09] http://192.168.127.132/wavsep/ ... llInput-AnyPathReq-Read.jsp?target=at
[10] http://192.168.127.132/wavsep/ ... put-AnyPathReq-Read.jsp?target=at.css
[11] <slot idle>
[12] <slot idle>
[13] <slot idle>
[14] <slot idle>
[15] <slot idle>
[!] Scan aborted by user, bailing out!
[+] Copying static resources ...
[+] Sorting and annotating crawl nodes: 3121
[+] Looking for duplicate entries: 3121
[+] Counting unique nodes: 675
[+] Saving pivot data for third-party tools ...
[+] Writing scan description ...
[+] Writing crawl tree: 3121
[+] Generating summary views ...
[+] Report saved to '202/index.html' [0xce7f76e6].
[+] This was a great day for science!
(root㉿kali)-[~]
#
Activer Windows
Accédez aux paramètres pour activer Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
Windows 10 x64
OWASP Broken Web Apps VM v...
root@kali: ~
File Actions Edit View Help
skipfish version 2.10b by lcamtuf@google.com
- 192.168.127.132 -
In-flight requests (max 15 shown):
[01] http://192.168.127.132/wavsep/ ...-AnyPathReq-Read.jsp?target=throw.ini
[02] http://192.168.127.132/wavsep/ ...nput-AnyPathReq-Read.jsp?target=at.js
[03] http://192.168.127.132/wavsep/ ...-AnyPathReq-Read.jsp?target=throw.htm
[04] http://192.168.127.132/wavsep/ ...AnyPathReq-Read.jsp?target=throw.aspx
[05] http://192.168.127.132/wavsep/ ...-AnyPathReq-Read.jsp?target=throw.jpg
[06] http://192.168.127.132/wavsep/ ...-AnyPathReq-Read.jsp?target=throw.gif
[07] http://192.168.127.132/wavsep/ ...-AnyPathReq-Read.jsp?target=throw.swf
[08] http://192.168.127.132/wavsep/ ...-AnyPathReq-Read.jsp?target=throw.txt
[09] http://192.168.127.132/wavsep/ ...llInput-AnyPathReq-Read.jsp?target=at
[10] http://192.168.127.132/wavsep/ ...put-AnyPathReq-Read.jsp?target=at.css
[11] <slot idle>
[12] <slot idle>
[13] <slot idle>
[14] <slot idle>
[15] <slot idle>
[!] Scan aborted by user, bailing out!
[+] Copying static resources ...
[+] Sorting and annotating crawl nodes: 3121
[+] Looking for duplicate entries: 3121
[+] Counting unique nodes: 675
[+] Saving pivot data for third-party tools ...
[+] Writing scan description ...
[+] Writing crawl tree: 3121
[+] Report saved to '202/index.html' [0xce7f76e6].
(root@kali)-[~]
Activer Windows
Accédez aux paramètres pour activer Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
Windows 10 x64
OWASP Broken Web Apps VM v...
root@kali: ~/202
File Actions Edit View Help
[01] http://192.168.127.132/wavsep/ ... -AnyPathReq-Read.jsp?target=throw.ini
[02] http://192.168.127.132/wavsep/ ... nput-AnyPathReq-Read.jsp?target=at.js
[03] http://192.168.127.132/wavsep/ ... -AnyPathReq-Read.jsp?target=throw.htm
[04] http://192.168.127.132/wavsep/ ... AnyPathReq-Read.jsp?target=throw.aspx
[05] http://192.168.127.132/wavsep/ ... -AnyPathReq-Read.jsp?target=throw.jpg
[06] http://192.168.127.132/wavsep/ ... -AnyPathReq-Read.jsp?target=throw.gif
[07] http://192.168.127.132/wavsep/ ... -AnyPathReq-Read.jsp?target=throw.swf
[08] http://192.168.127.132/wavsep/ ... -AnyPathReq-Read.jsp?target=throw.txt
[09] http://192.168.127.132/wavsep/ ... llInput-AnyPathReq-Read.jsp?target=at
[10] http://192.168.127.132/wavsep/ ... put-AnyPathReq-Read.jsp?target=at.css
[11] <slot idle>
[12] <slot idle>
[13] <slot idle>
[14] <slot idle>
[15] <slot idle>
[!] Scan aborted by user, bailing out!
[+] Copying static resources ...
[+] Sorting and annotating crawl nodes: 3121
[+] Looking for duplicate entries: 3121
[+] Counting unique nodes: 675
[+] Saving pivot data for third-party tools ...
[+] Writing scan description ...
[+] Writing crawl tree: 3121
[+] Generating summary views ...
[+] Report saved to '202/index.html' [0xce7f76e6].
[+] This was a great day for science!
(root㉿kali)-[~]
ls
202 locks.txt note.txt router.gnmap router.xml wiss.hs wisswiss
bettercap.history meta php-reverse-shell.php router.nmap task.txt wissem
(root㉿kali)-[~]
cd 202
(root㉿kali)-[~/202]
ls
_i0 _i16 _i23 _i30 _i7 _m4 i_high.png n_children.png p_dir.png samples.js
_i1 _i17 _i24 _i31 _i8 _m5 i_low.png n_clone.png p_file.png sf_name.png
_i10 _i18 _i25 _i32 _i9 _m6 i_medium.png n_collapsed.png p_param.png summary.js
_i11 _i19 _i26 _i33 _m0 _m7 i_note.png n_expanded.png p_pinfo.png
_i12 _i2 _i27 _i34 _m1 _m8 i_warn.png n_failed.png p_serv.png
_i13 _i20 _i28 _i4 _m10 _m9 index.html n_maybe_missing.png p_unknown.png
_i14 _i21 _i29 _i5 _m2 c0 issue_index.js n_normal.png p_value.png
_i15 _i22 _i3 _i6 _m3 child_index.js mime_entry.png n_unlinked.png pivots.txt
Activer Windows
Accédez aux paramètres pour activer Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
Windows 10 x64
OWASP Broken Web Apps VM v...
Restore the minimized windows
202 - Thunar
Places
Computer
nasri
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
_m10
c0
child_index.js
i_high.png
i_low.png
i_medium.png
i_note.png
i_warn.png
index.html
issue_index.js
mime_entry.png
n_children.png
n_clone.png
"the quieter you become, th
Kali Linux
Skipfish - sc
file:///home/nasri/project
Kali Linux
Kali Tools
Kali Docs
Kali Forums
skipfish
WEB APP SCANNER
Scanner version: 2.10b
Scan date: Thu Mar 21 02:53:43 2024
Random seed: 0xce7f76e6
Total time: 0 hr 46 min 48 sec 58 ms
Problems with this scan? Click here for advice.
Crawl results - click to expand:
Document type overview - click to expand:
application/javascript (22)
application/rss+xml (1)
application/x-shockwave-flash (1)
application/xhtml+xml (71)
image/gif (28)
image/jpeg (2)
image/png (24)
text/css (5)
text/html (21)
text/plain (10)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
Windows 10 x64
OWASP Broken Web Apps VM v...
Applications
Skipfish - scan results brows
file:///home/nasri/project_owasp/202/index.html
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
skipfish
WEB APP SCANNER
Scanner version: 2.10b
Random seed: 0xce7f76e6
Scan date: Thu Mar 21 02:53:43 2024
Total time: 0 hr 46 min 48 sec 58 ms
Problems with this scan? Click here for advice.
Crawl results - click to expand:
Document type overview - click to expand:
application/javascript (22)
application/rss+xml (1)
application/x-shockwave-flash (1)
application/xhtml+xml (71)
image/gif (28)
image/jpeg (2)
image/png (24)
text/css (5)
text/html (21)
text/plain (10)
text/xml (2)
Issue type overview - click to expand:
Activer Windows
Accédez aux paramètres pour activer Windows.
Remote file inclusion (49)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali linux - VMware Workstation
File Edit View VM Tabs Help
Home
Kali linux
Windows 10 x64
OWASP Broken Web Apps VM v...
1 2 3 4
3:04
Kali Linux
Skipfish - scan results brows
Firefox View
file:///home/nasri/project_owasp/202/index.html
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Issue type overview - click to expand:
Remote file inclusion (49)
File inclusion (75)
Incorrect caching directives (higher risk) (5)
Directory traversal / file inclusion possible (36)
Interesting server message (4)
Interesting file (39)
External content embedded on a page (higher risk) (12)
XSS vector via arbitrary URLs (12)
XSS vector in document body (18)
Signature match detected (5)
HTTP header injection vector (1)
HTML form with no apparent XSRF protection (21)
External content embedded on a page (lower risk) (1)
Redirection to attacker-supplied URLs (7)
Node should be a directory, detection error? (2)
Response varies randomly, skipping checks (1)
IPS filtering enabled (1)
Parent behavior checks failed (no brute force) (1)
Limits exceeded, fetch suppressed (3)
Resource fetch failed (109)
Numerical filename - consider enumerating (51)
Incorrect or missing charset (low risk) (72)
Generic MIME used (low risk) (3)
Incorrect or missing MIME type (low risk) (96)
Password entry form - consider brute-force (1)
Unknown form field (can't autocomplete) (9)
Hidden files / directories (50)
Directory listing enabled (32)
Activer Windows
Accédez aux paramètres pour activer Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

4.Analyses (SAST vs DAST)

Partie5 :

1- Déterminer les points forts des tests statiques de la sécurité des applications (SAST)

-Détection précoce des vulnérabilités : SAST analyse le code source ou le bytecode avant même son exécution, permettant ainsi d'identifier les failles de sécurité dès le stade de développement.

-Analyse approfondie du code : SAST examine le code ligne par ligne, ce qui permet de détecter les vulnérabilités potentielles même dans les parties du code rarement ou jamais exécutées

-Intégration dans le processus de développement : Les outils SAST peuvent être intégrés dans les environnements de développement intégrés (IDE) ou les systèmes de gestion de versions (VCS), offrant ainsi une intégration transparente dans le processus de développement logiciel.

2- Déterminer les points forts des tests dynamiques de la sécurité des applications (DAST)

-Évaluation de la sécurité en conditions réelles : Contrairement à SAST, DAST évalue les applications en cours d'exécution dans des conditions réelles, ce qui permet de détecter les vulnérabilités liées à la configuration du serveur, à la gestion des sessions, etc.

-Détection des vulnérabilités liées à l'infrastructure : DAST identifie les vulnérabilités potentielles résultant de la configuration des serveurs, des paramètres réseau, des interactions avec d'autres systèmes, etc.

-Facilité de déploiement : Les tests DAST peuvent être déployés facilement, car ils ne nécessitent pas l'accès au code source de l'application et peuvent être exécutés à partir de l'extérieur.

3- Comparer SAST et DAST

-Nature de l'analyse : SAST analyse le code source ou le bytecode, tandis que DAST teste l'application en cours d'exécution.

-Moment de détection des vulnérabilités : SAST détecte les vulnérabilités lors de la phase de développement, tandis que DAST identifie les failles lors de l'exécution de l'application.

-Profondeur de l'analyse : SAST offre une analyse plus approfondie du code, tandis que DAST se concentre sur les vulnérabilités exposées lors de l'exécution.

-Types de vulnérabilités détectées : SAST est efficace pour détecter les vulnérabilités liées au code, tandis que DAST est plus approprié pour identifier les vulnérabilités liées à l'infrastructure et aux interactions avec d'autres systèmes.

-Intégration dans le processus de développement : SAST peut être intégré dans les IDE ou les VCS, tandis que DAST est généralement utilisé en tant qu'outil externe.

-Complémentarité : Les deux approches sont souvent complémentaires, car elles détectent différents types de vulnérabilités à différents stades du cycle de vie du développement logiciel.

Ce table aussi montre une comparaison entre les deux :

	SAST	DAST
Quand l'utiliser	Pendant le développement du code	Après le déploiement de l'application
Couverture de test	Code source, byte code et binaires	Applications en cours d'exécution
Avantages	Détecte les vulnérabilités avant le déploiement, réduisant ainsi les coûts de réparation	Détecte les vulnérabilités qui ne sont visibles qu'une fois l'application déployée et en cours d'exécution
Inconvénients	Peut produire de nombreux faux positifs	Ne peut pas détecter certaines vulnérabilités qui n'apparaissent que lors de l'exécution de scénarios spécifiques
Idéal pour	Les phases de développement précoce et les projets avec un code base large	Les applications déjà en production et les situations nécessitant des tests en temps réel