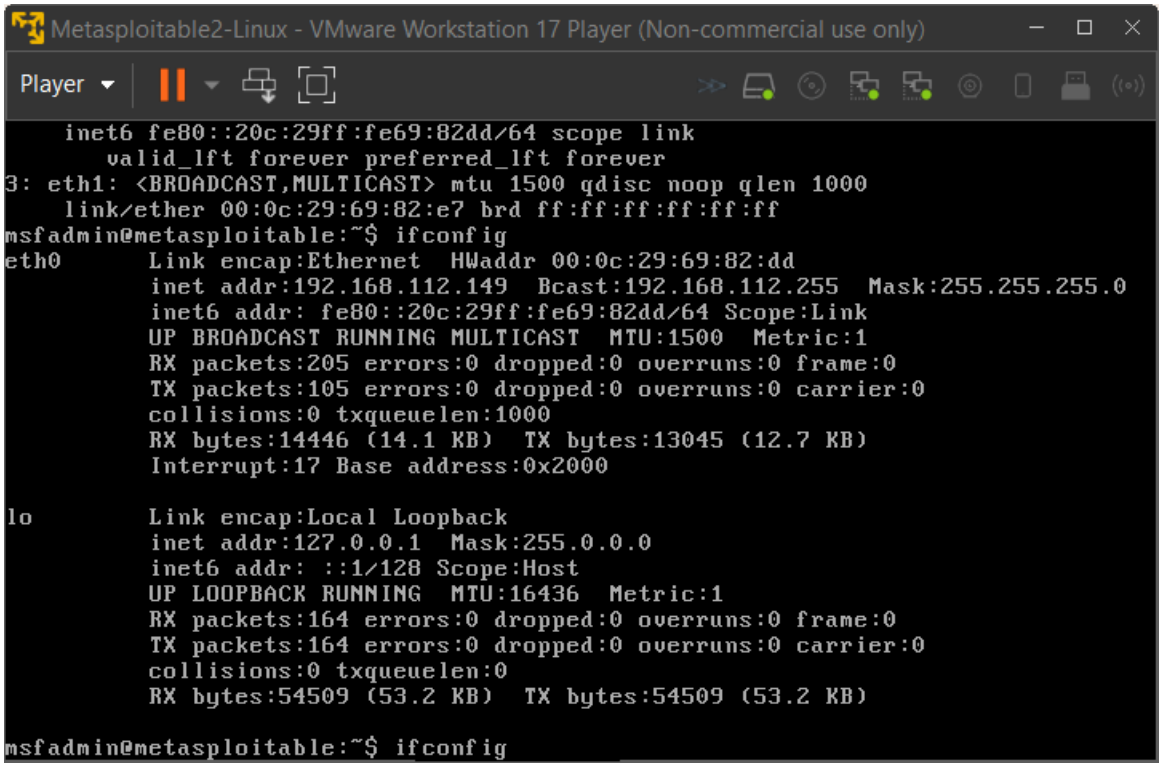
TP:PENTENTING D'UNE APPLICATION WEB AVEC KALI LUNIX

OBJECTIFS:

Apprendre à utiliser Kali Lunix et metasploit pour effectuer un test d'intrusion sur une application web vulnérable en explorant des vulnérabilités courantes commz les injections SQL,XSS et les failles de gestion de session

D'abor nous allons mettre en place nos deux machines virtuels

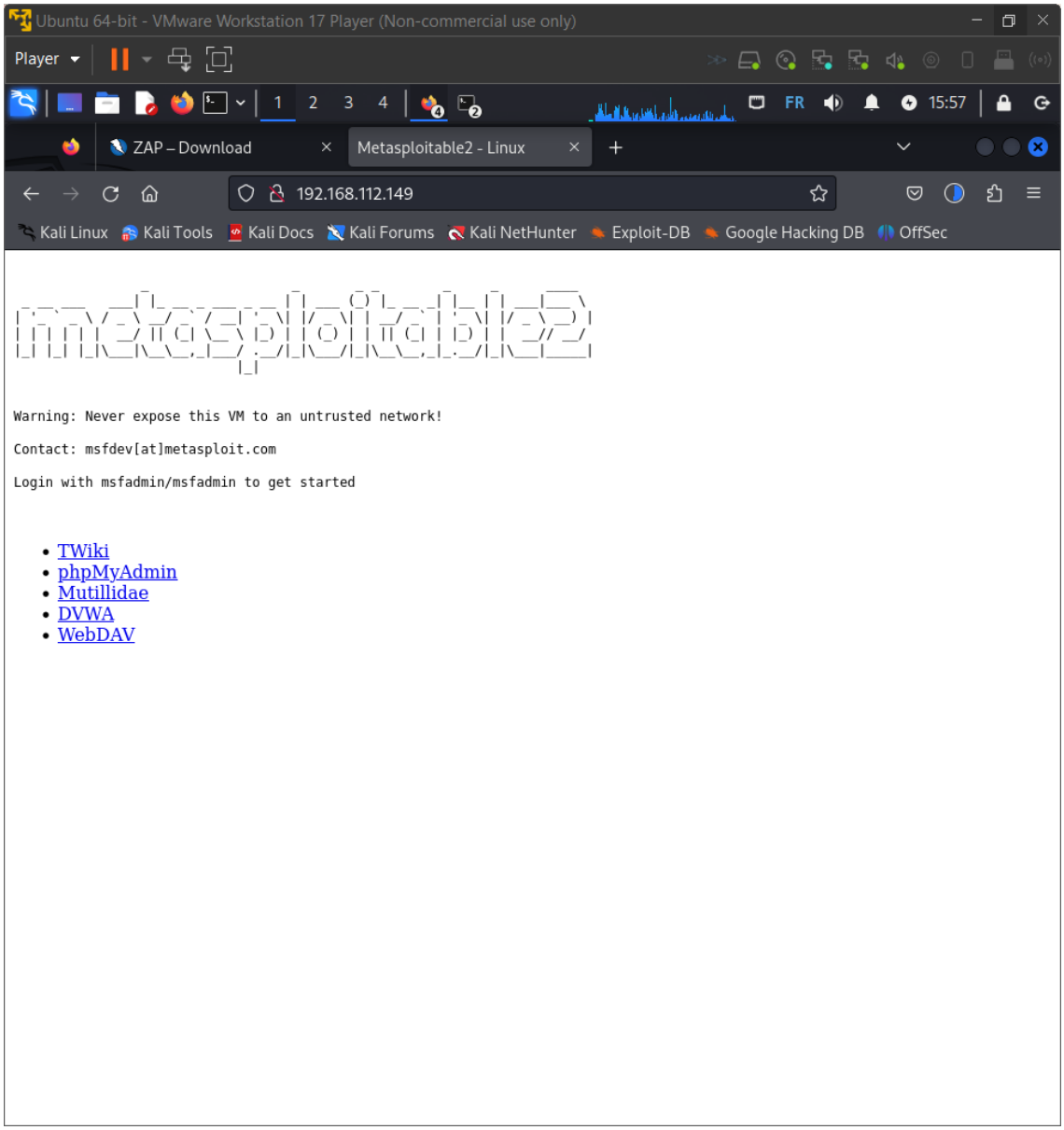
1. METASPLOITABLE



2.

Nous verifions ici les addresses ip pour pouvoir acceder au site Web dans KALI LUNIX

3. **SITE WEB METASPLOIT**

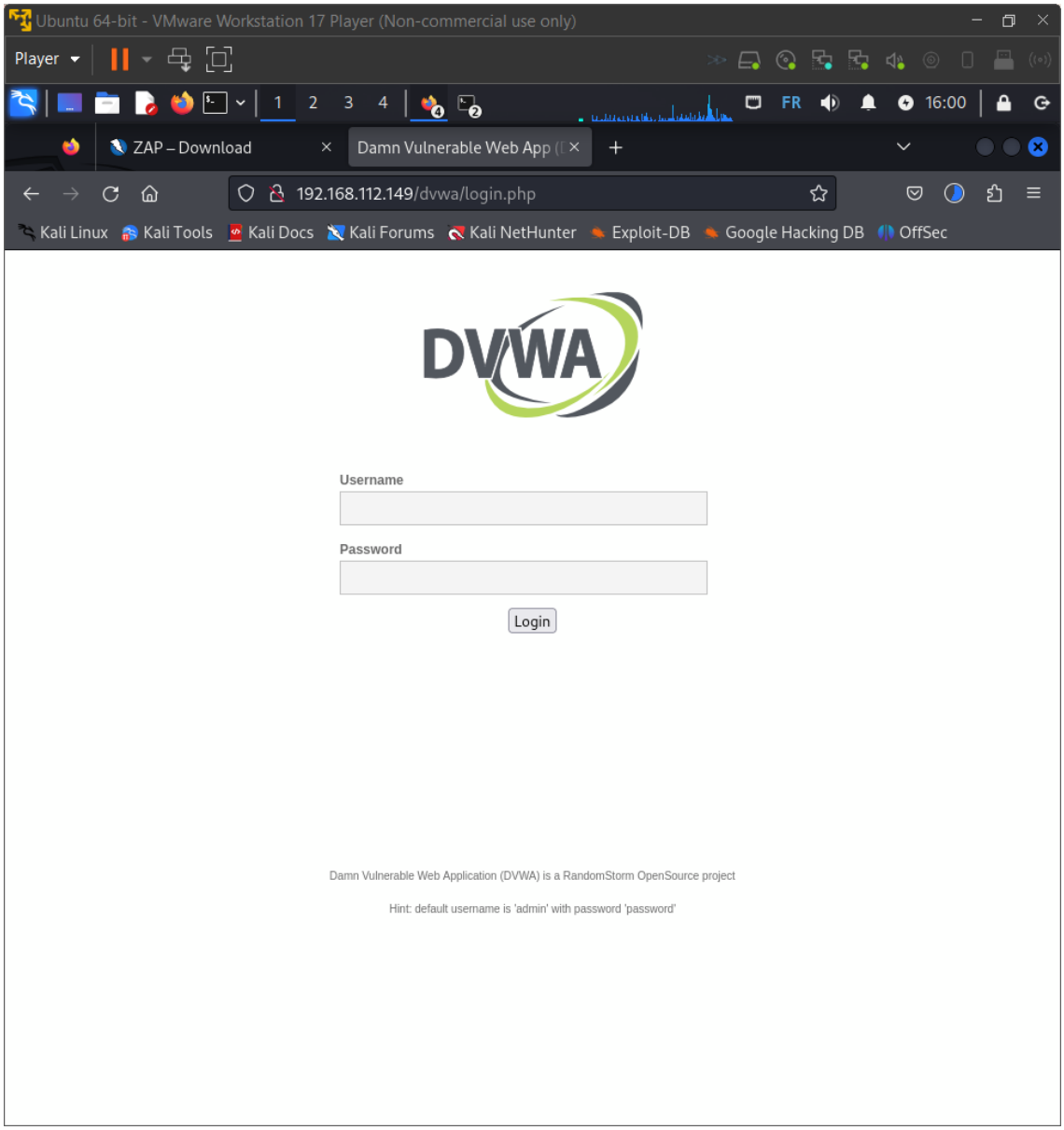


Etape 1: Préparation de l'environnement

D'abord faut que les deux machines soit sur le même réseau avant toute chose après cette étape nous allons procéder à l'activation de DVWA

Etape 2: ACTIVER DVWA

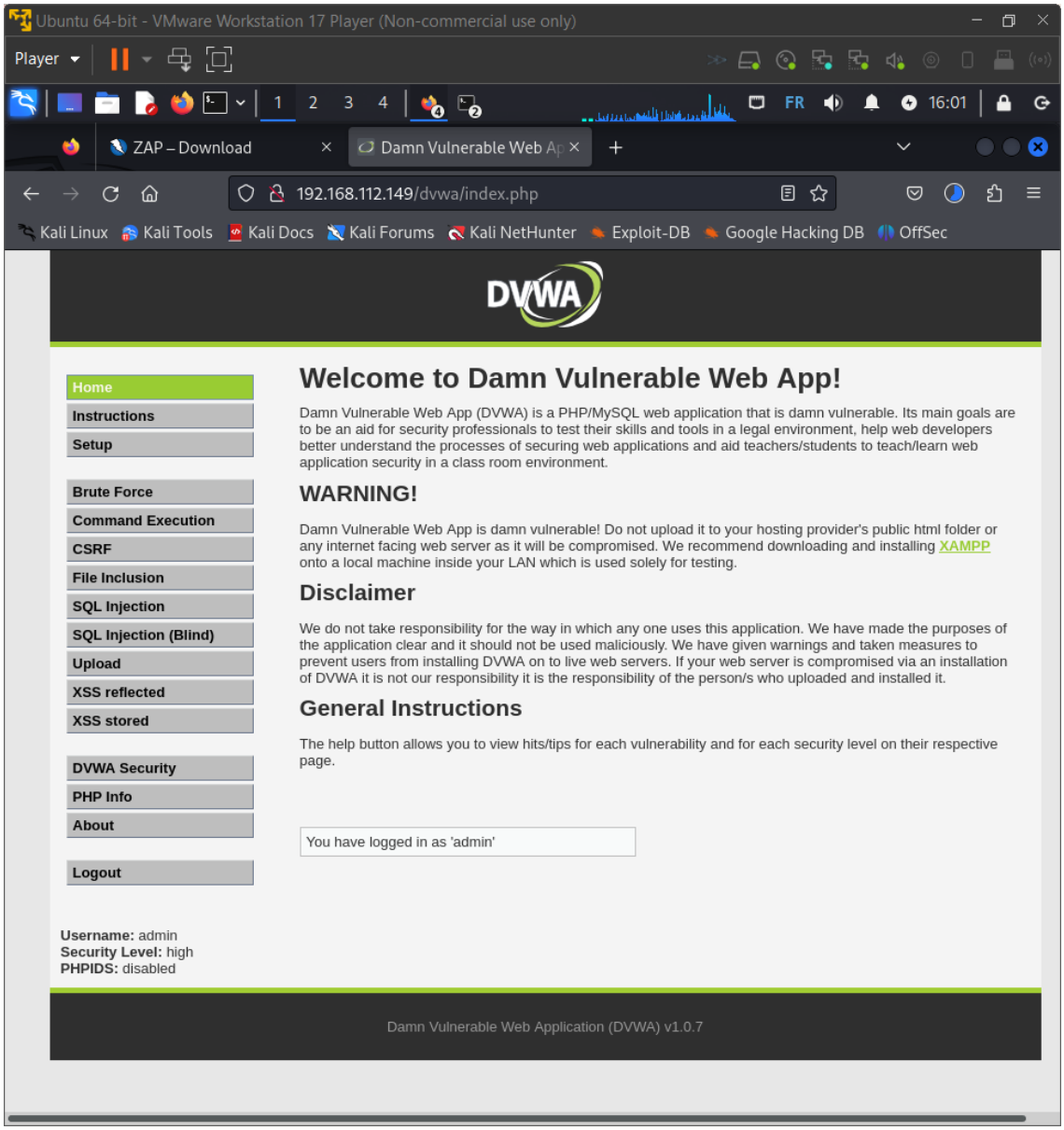
Pour activer cette derniere faut que les interfaces de DVWA soit conecté et précise



VOICI le site DVWA mais pour y acceeder faut entre le login et la mot de passe

Login: admin

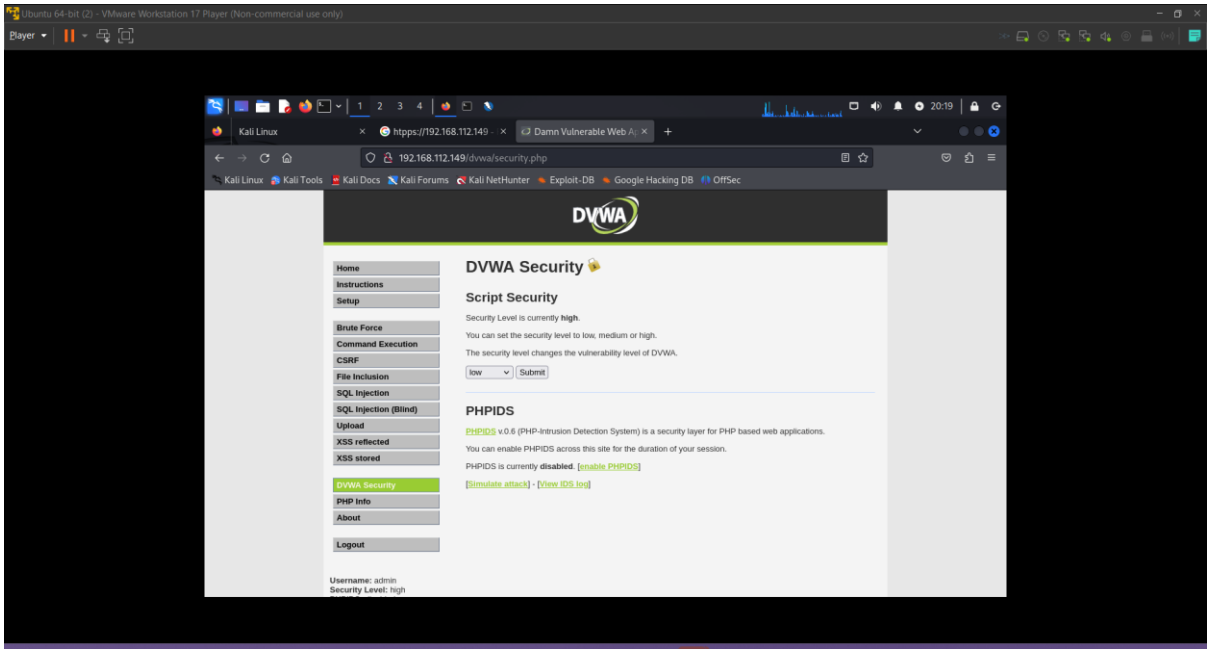
Password: password



Une fois cela fait fait nous allons accéder entrer dans DVWA et maintenat le travail peut commencer

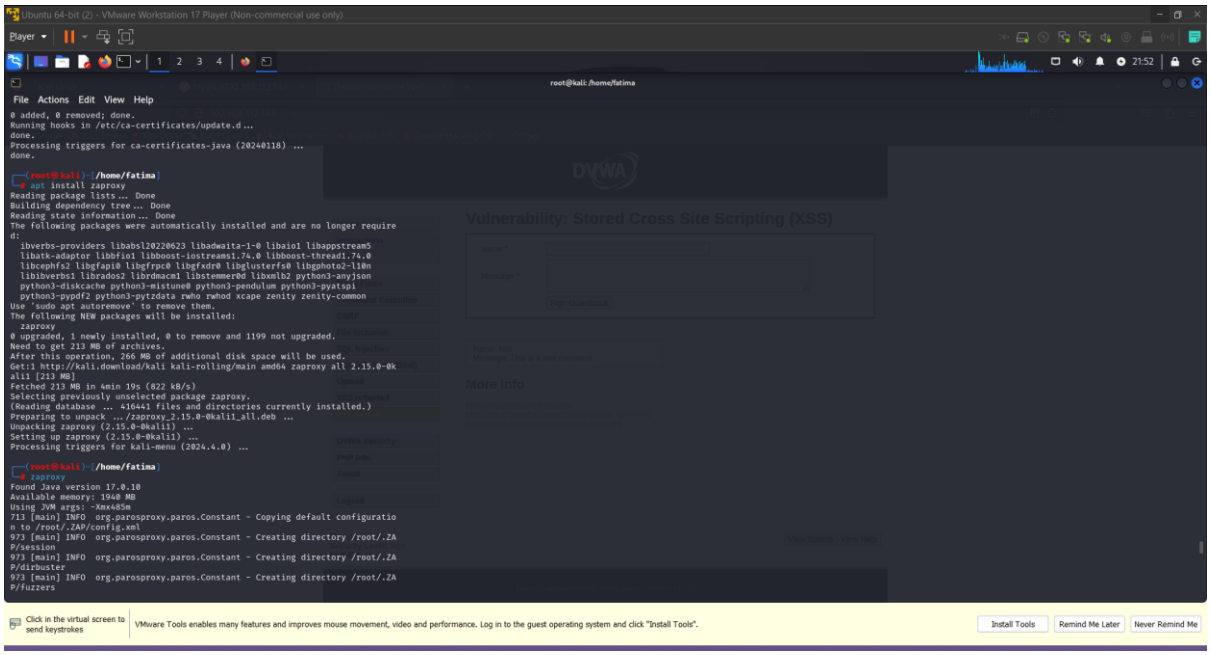
Etape 3: Configuration du niveau de securité sur “LOW”

Cette configuration nous permet de garder notre notre site en securité mais aussi le refus de quelconque cookies mais aussi de nous signalé s’il y’a une personne qui veut attaquer ou quand la sécurité semble être faible il est donc essentiel de prendre des mesures adaptées



Etape 4 : SCANNE DES VULNÉRABILITÉS

Ensuite nous allons installer owasp zap depuis kali pour faire le scanne de vulnérabilité

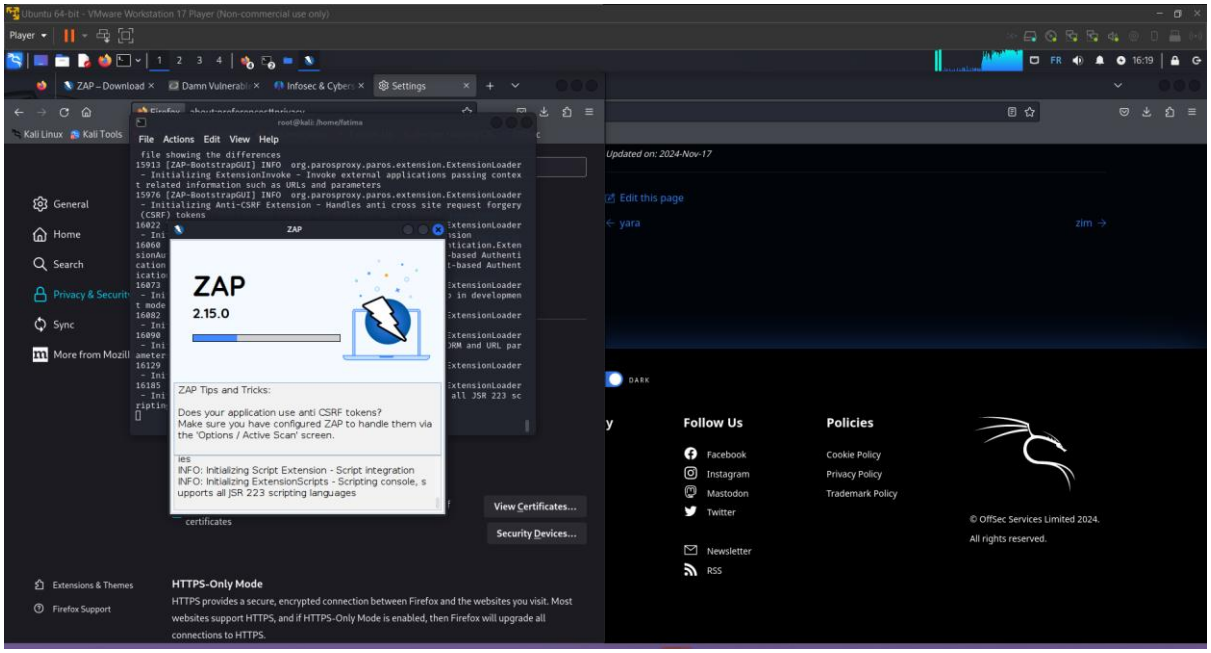


On a laissé les commande suivant

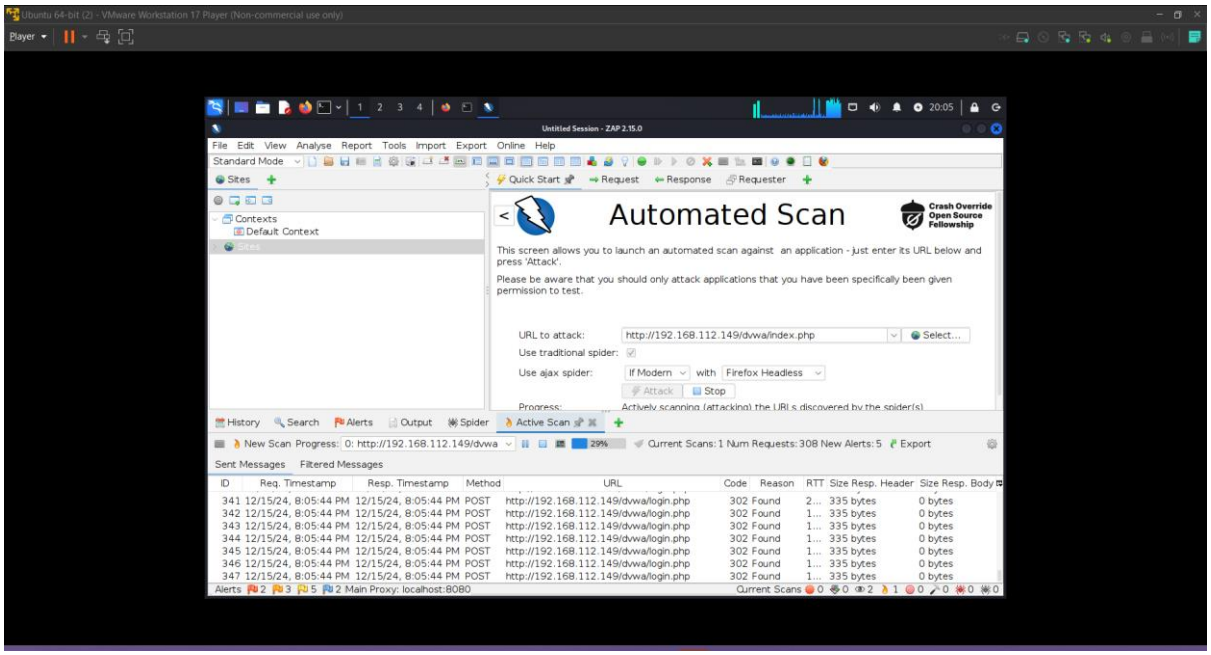
SUDO APT INSTALL ZAPROXY

ZAPROXY

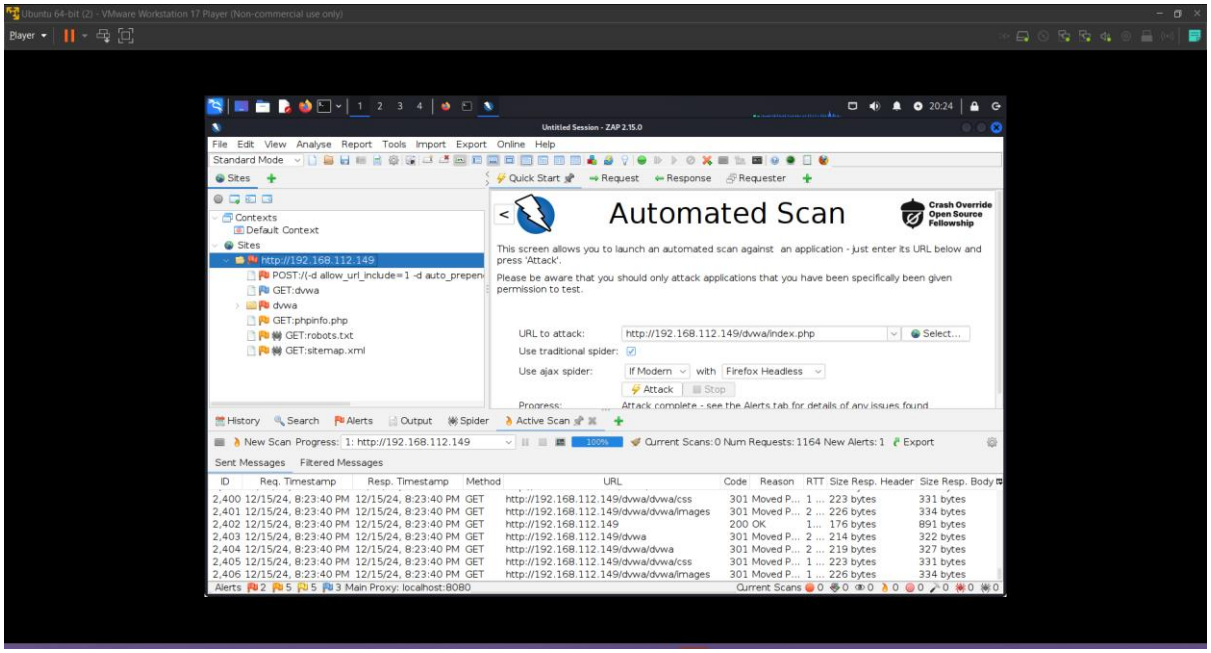
La deuxieme commande nous permet d'acceder à l'appli



Etape 5 :SCANNE DE L'APPLICATION



Pour scanner l'application nou allons utiliser "ACTIVE SCANN"pour decouvrir les vulnérabilités comme SQL INJECTION XSS



es scans de vulnérabilité sont des outils ou des processus utilisés pour analyser un système informatique, un réseau ou une application afin d'identifier des failles de sécurité potentielles. Ces scans permettent de détecter des vulnérabilités qui pourraient être exploitées par des attaquants pour compromettre la confidentialité, l'intégrité ou la disponibilité des données.

Voici à quoi servent les scans de vulnérabilité :

Identification des failles de sécurité : Ils détectent des vulnérabilités spécifiques, telles que des configurations incorrectes, des logiciels obsolètes, des ports ouverts non sécurisés, des erreurs de codage dans des applications, etc.

Prévention des attaques : En identifiant ces failles avant qu'elles ne soient exploitées, les scans permettent de prendre des mesures pour les corriger, réduisant ainsi le risque d'attaque.

Mise à jour des systèmes : Les scans peuvent signaler des logiciels non mis à jour ou des patchs de sécurité manquants, ce qui permet aux responsables de la sécurité de s'assurer que tous les systèmes sont à jour avec les dernières protections.

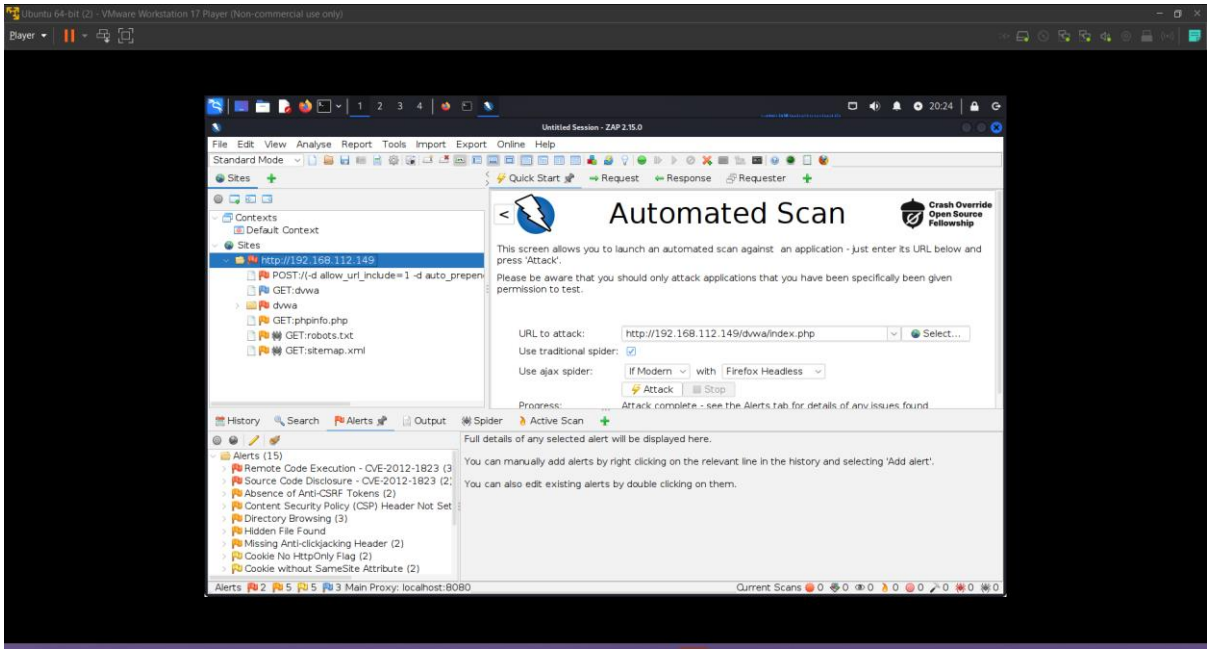
Audit de sécurité : Ils servent également à effectuer des audits réguliers pour vérifier la conformité aux bonnes pratiques de sécurité et aux normes de sécurité telles que le PCI-DSS, HIPAA, ISO 27001, etc.

Gestion des risques : En identifiant et en évaluant les vulnérabilités, les scans de sécurité aident à prioriser les risques en fonction de leur gravité et de leur potentiel d'impact, permettant une gestion proactive de la sécurité.

Etape 6 : ALERTE ⚠

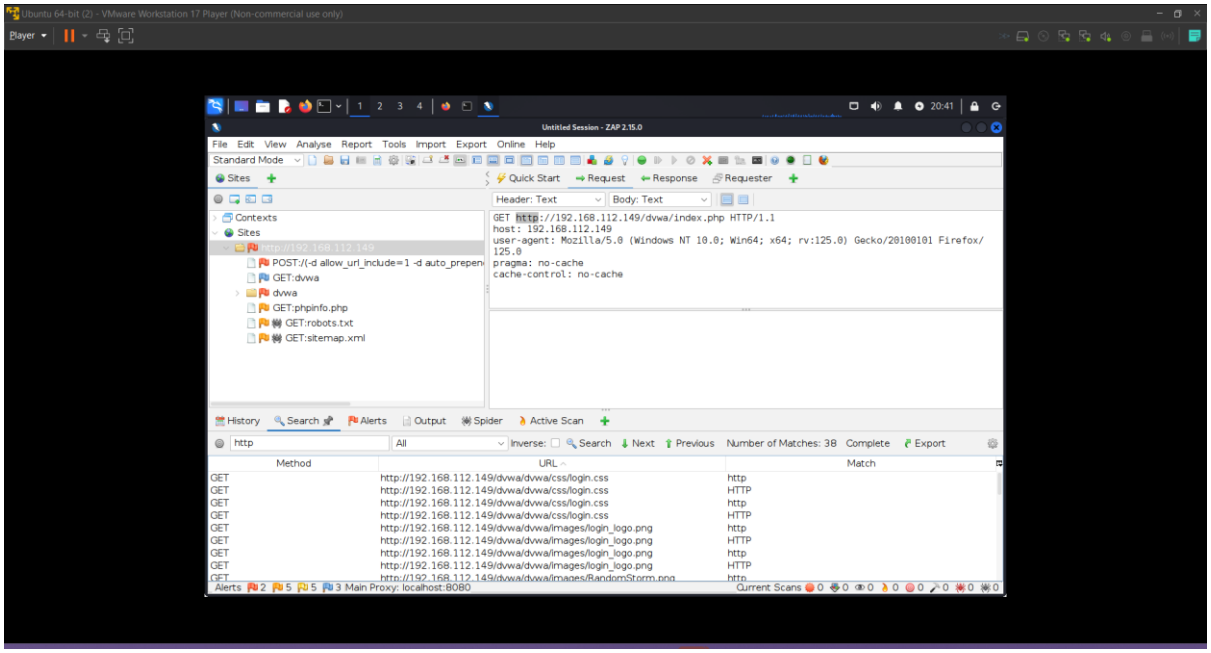
Nous avons eu la possibilité de voir les alerttes pour cette application mais à ce qui parait y'a pas d'alerte critique ou castastrophique

Mais on remarque que y'a peu de probable y'aucun risque

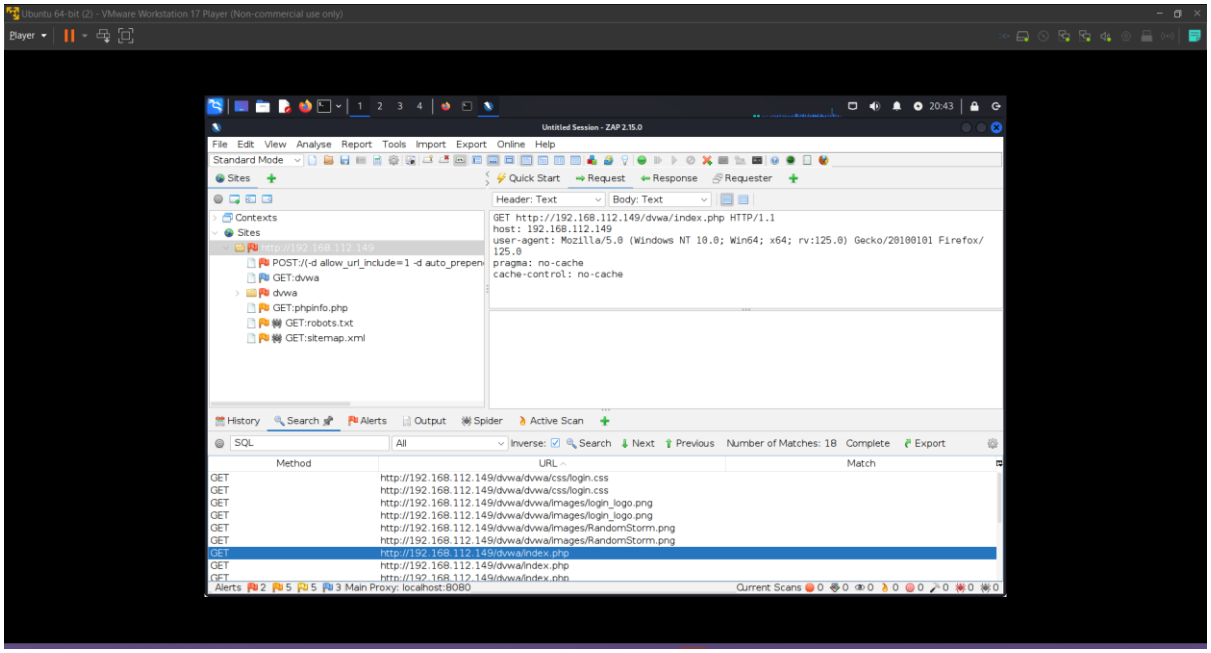


Etape 7: SEARCH SQL, HTTP POUR LE VULNERABILITES

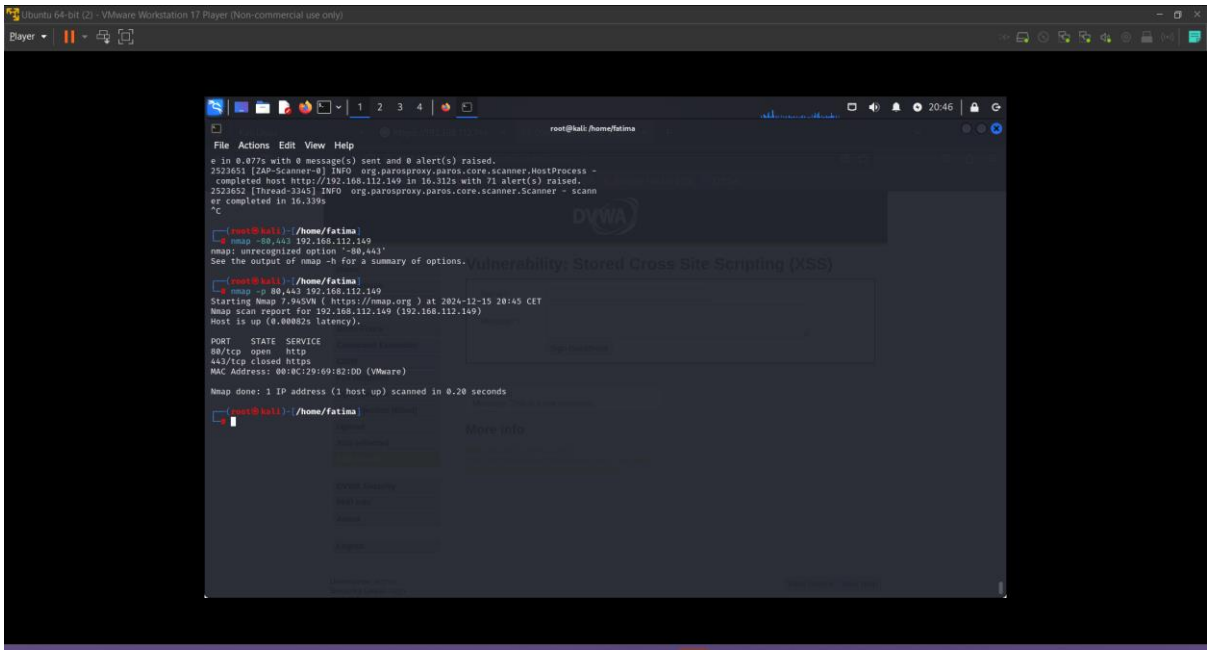
A) HTTP


Ubuntu 64-bit (2) - VMware Workstation 17 Player (Non-commercial use only)
Player
Untitled Session - ZAP 2.15.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
GET http://192.168.112.149/dvwa/index.php HTTP/1.1
host: 192.168.112.149
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101 Firefox/125.0
pragma: no-cache
cache-control: no-cache
Contexts
Sites
POST:/(-d allow_url_include=1 -d auto_prepen
GET:dvwa
dvwa
GET:phpinfo.php
GET:robots.txt
GET:sitemap.xml
History
Search
Alerts
Output
Spider
Active Scan
http
All
Inverse:
Search
Next
Previous
Number of Matches: 38
Complete
Export
Method
URL
Match
GET http://192.168.112.149/dvwa/dvwa/css/login.css http
GET http://192.168.112.149/dvwa/dvwa/css/login.css HTTP
GET http://192.168.112.149/dvwa/dvwa/css/login.css http
GET http://192.168.112.149/dvwa/dvwa/css/login.css HTTP
GET http://192.168.112.149/dvwa/dvwa/images/login_logo.png http
GET http://192.168.112.149/dvwa/dvwa/images/login_logo.png HTTP
GET http://192.168.112.149/dvwa/dvwa/images/login_logo.png http
GET http://192.168.112.149/dvwa/dvwa/images/login_logo.png HTTP
Alerts 2 5 5 3 Main Proxy: localhost:8080
Current Scans

B) SQL


Ubuntu 64-bit (2) - VMware Workstation 17 Player (Non-commercial use only)
Player
Untitled Session - ZAP 2.15.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
GET http://192.168.112.149/dvwa/index.php HTTP/1.1
host: 192.168.112.149
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101 Firefox/125.0
pragma: no-cache
cache-control: no-cache
Contexts
Sites
POST:/(-d allow_url_include=1 -d auto_prepen
GET:dvwa
dvwa
GET:phpinfo.php
GET:robots.txt
GET:sitemap.xml
History
Search
Alerts
Output
Spider
Active Scan
SQL
All
Inverse:
Search
Next
Previous
Number of Matches: 18
Complete
Export
Method
URL
Match
GET http://192.168.112.149/dvwa/dvwa/css/login.css
GET http://192.168.112.149/dvwa/dvwa/css/login.css
GET http://192.168.112.149/dvwa/dvwa/images/login_logo.png
GET http://192.168.112.149/dvwa/dvwa/images/login_logo.png
GET http://192.168.112.149/dvwa/dvwa/images/RandomStorm.png
GET http://192.168.112.149/dvwa/dvwa/images/RandomStorm.png
GET http://192.168.112.149/dvwa/index.php
GET http://192.168.112.149/dvwa/index.php
Alerts 2 5 5 3 Main Proxy: localhost:8080
Current Scans

Etape 8: IDENTIFICATION DES SERVICES OUVERTS (PORT 80?443 POUR LES WEB)



Enfin se TP nous permettre de commprendre la manupilation de ses logiciel mais aussi de comprendre comment fait un scann de vulnérabilité d’un site web ou application

Et l’utilisation de KALI LUNIX