OWASP

Open Web Application Security Project

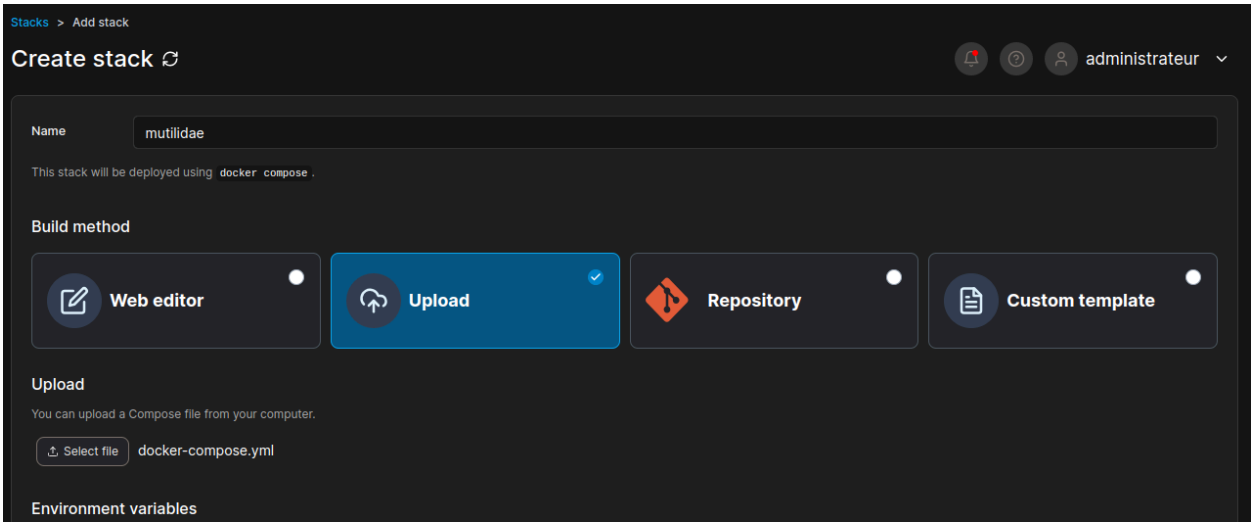
01/10/24

Hafaidh
Mohamed
BTS-SIO2

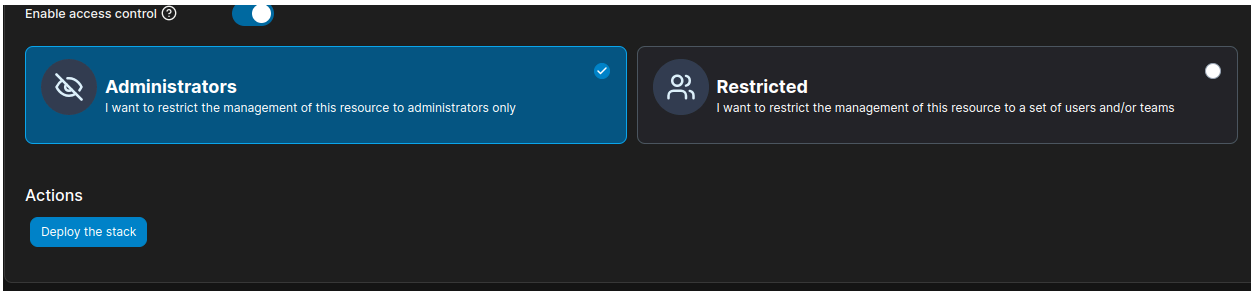
SOMMAIRE

PORTAINER DOCKER

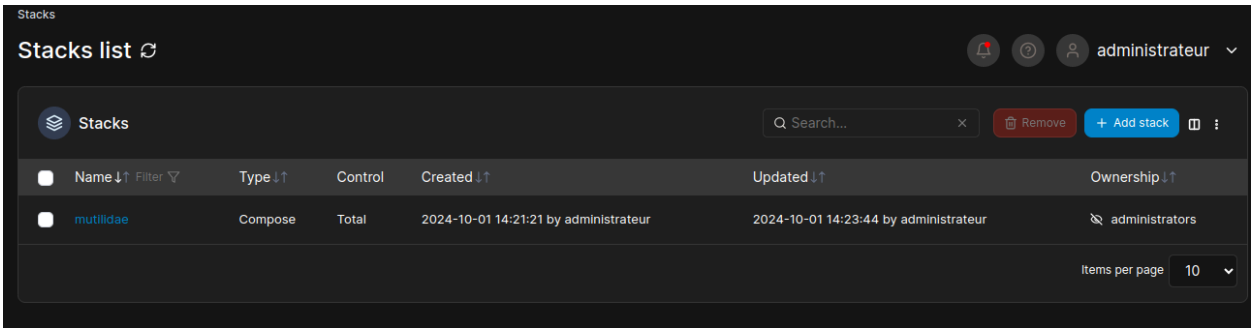
Tout d'abord nous devons créer un stack comme c'est expliqué dans l'activité, avec le nom mutilidae une fois cela fait nous devons installer le fichier mutillidae-dockerhub sur github. Dans le dossier nous allons retrouver un fichier au nom de docker-compose.yml qu'on doit ajouter dans le stack.

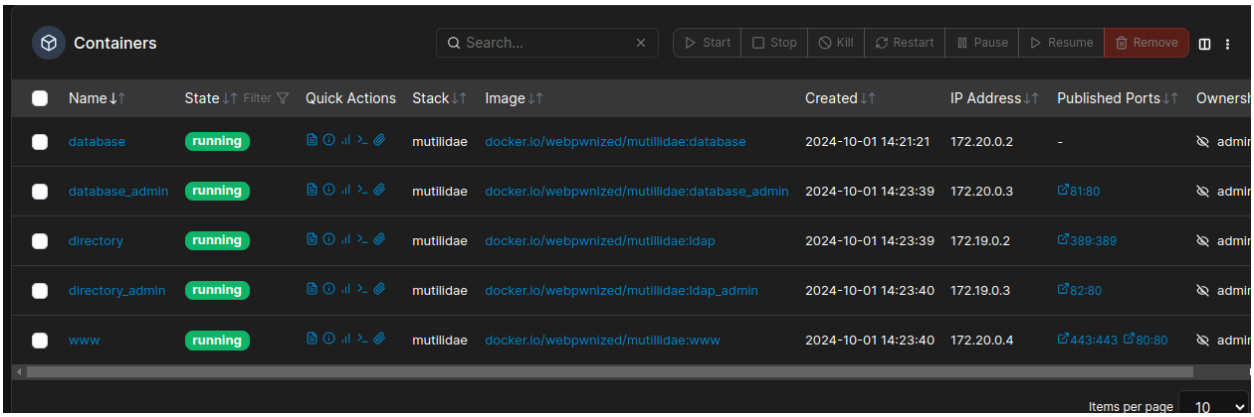


Une fois fini vous devez déployer le projet cela prendra du temps c'est normal.

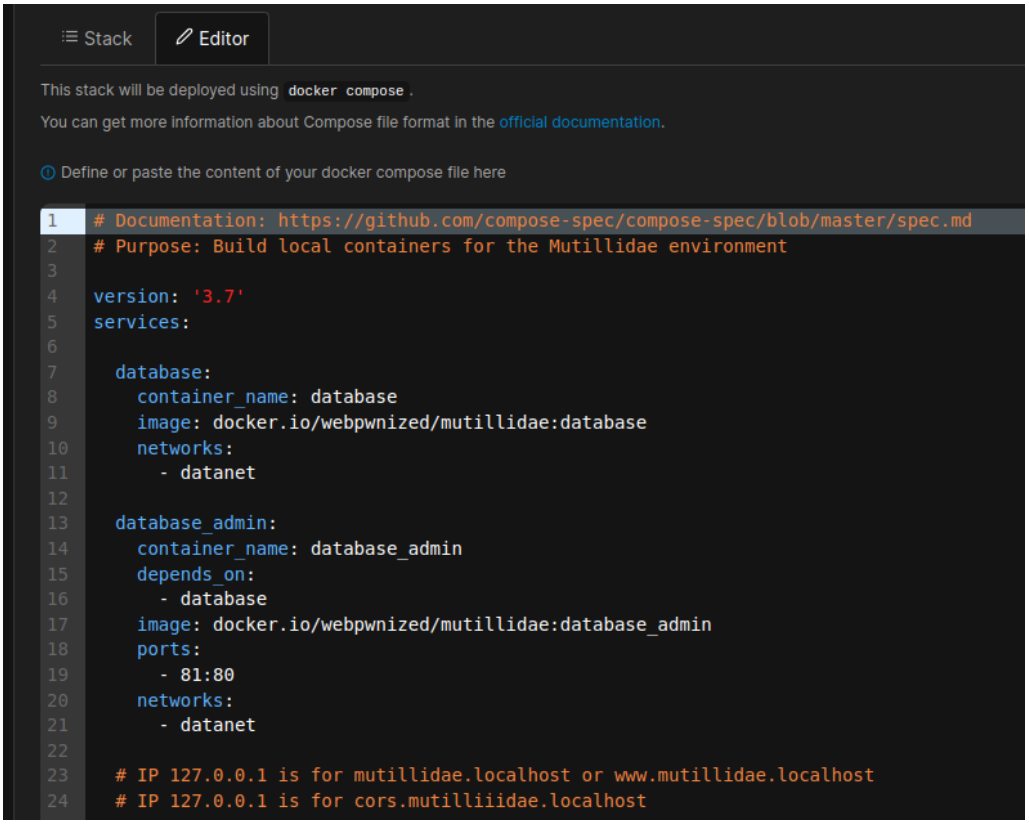


Le projet déployer vous devriez avoir cela :





N’oublier pas d’enlever les ip et laisser les port sur l’editor :



DATABASE SERVER

Maintenant vous devez taper votre ip du serveur sur le navigateur cela vous ramènera sur une page comme celle-ci :

The database server at database appears to be offline.

1. **Click here** to attempt to setup the database. Sometimes this works.
2. Be sure the username and password to MySQL is the same as configured in includes/database-config.inc
3. Be aware that MySQL disables password authentication for root user upon installation or update in some systems. This may happen even for a minor update. Please check the username and password to MySQL is the same as configured in includes/database-config.inc
4. A **video is available** to help reset MySQL root password
5. Check the error message below for more hints
6. If you think this message is a false-positive, you can opt-out of these warnings below

Database Diagnostics Information

Database Error message:

Database host: database
Database post: 3306
Database username: root
Database password: mutillidae
Database name: mutillidae

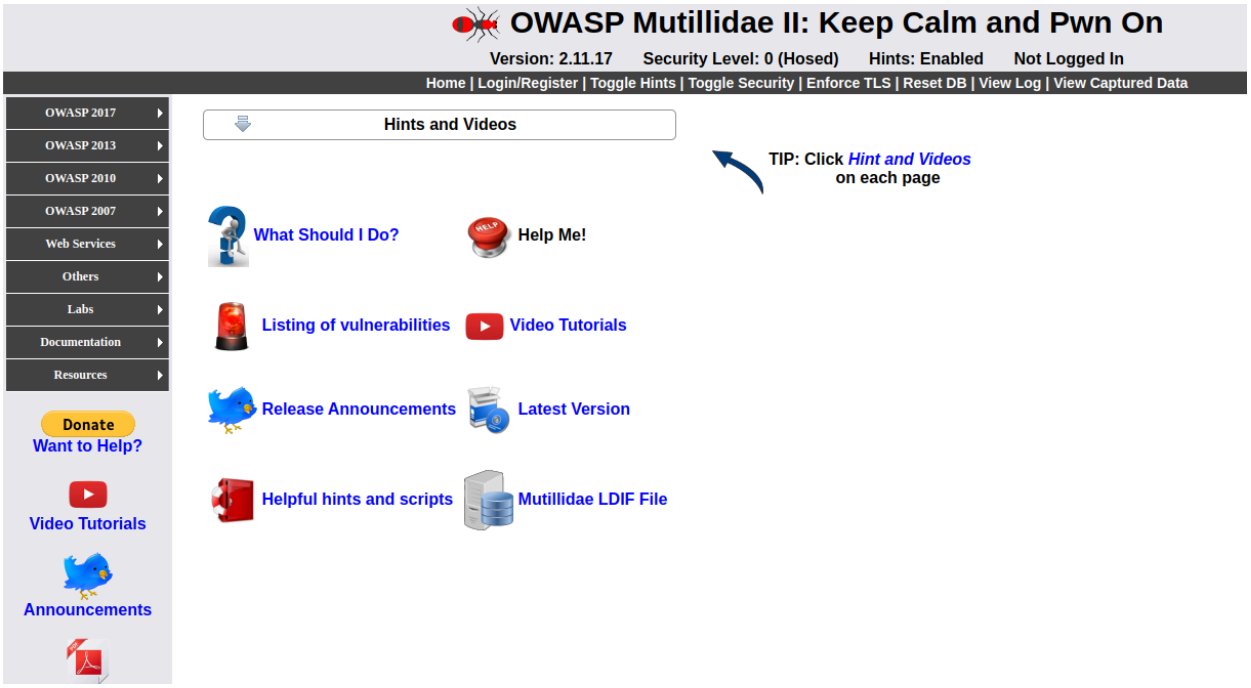
IP resolved from database hostname: 172.20.0.2

Ping database results:

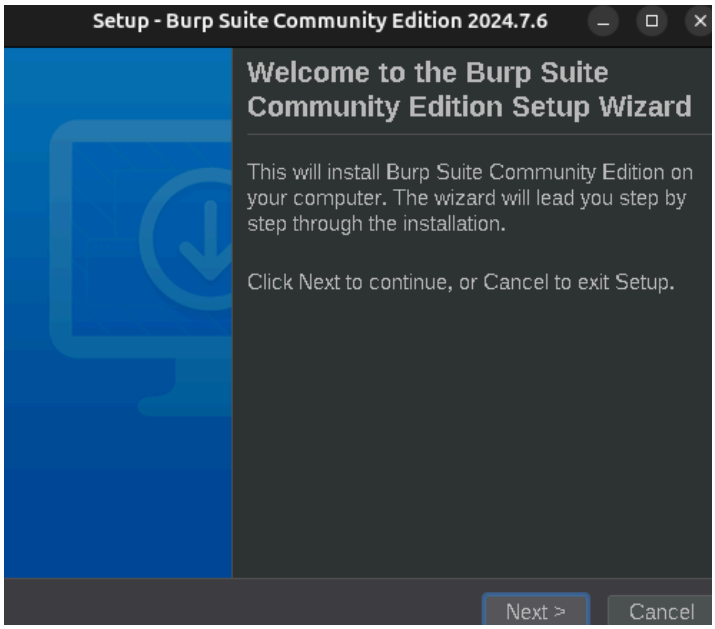
```
PING database (172.20.0.2) 56(84) bytes of data.
64 bytes from database.mutilidae_datanet (172.20.0.2): icmp_seq=1 ttl=64 time=0.218 ms

--- database ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.218/0.218/0.218/0.000 ms
```

Traceroute database results:

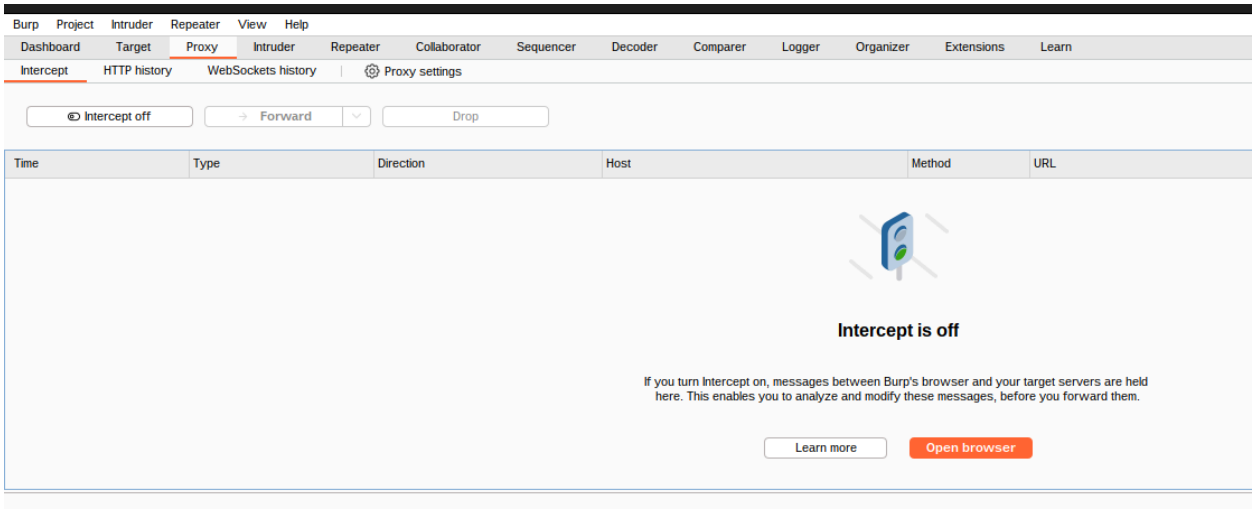
Vous devriez cliquer sur Click Here pour accéder au site web OWASP Mutillidae II.



Maintenant vous allez installer BurpSuite :



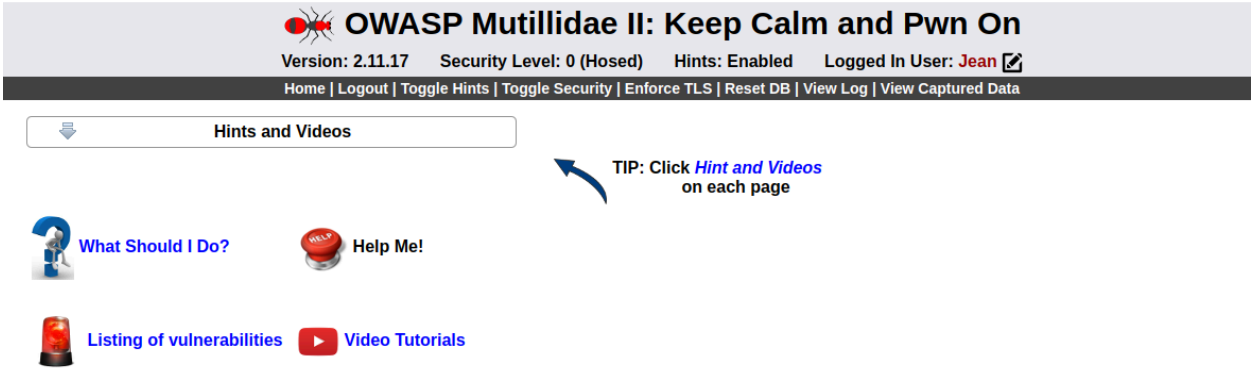
Une fois installer vous tomber sur une page comme celle-ci :



Activité 1

Travail à faire 1 :

Q1. Créer un compte permettant de vous authentifier sur la plate-forme.



Q2. Utiliser une méthode de votre choix afin de découvrir les noms des champs login et mot de passe du formulaire d'authentification.

Ouvrez BurpSuite et créez un projet temporaire.

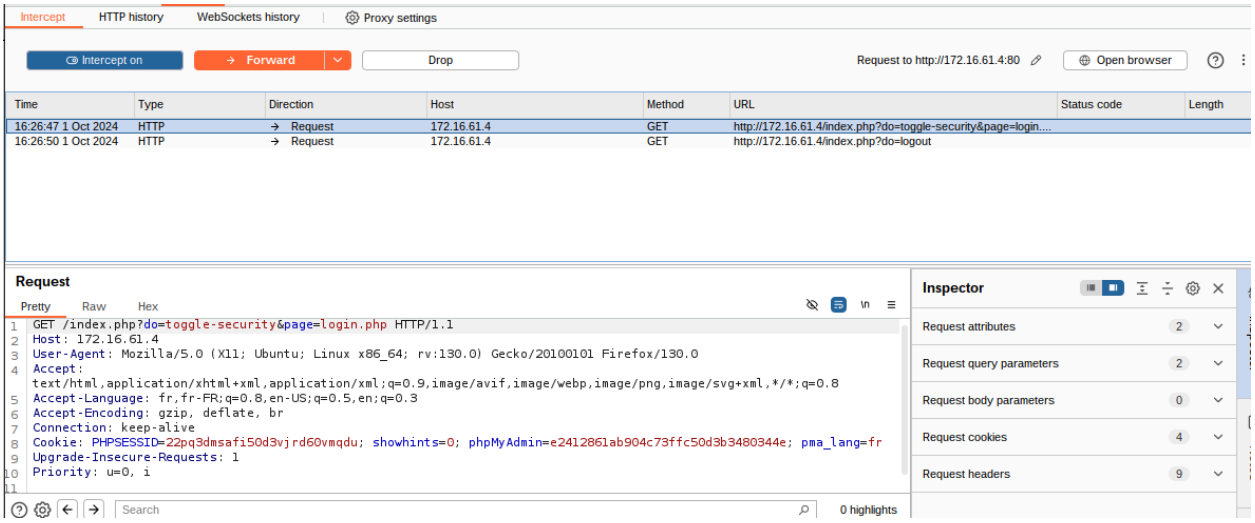
Dans l'onglet **Proxy**, assurez-vous que l'interception est désactivée (Intercept is off).

n'oubliez pas d'activer votre proxy dans les paramètre de votre navigateur ou dans les paramètres de linux.

Maintenant vous allez sur le site web OWASP et vous allez mettre vos identifiant rentre au par avant attention il ne faut pas se login :

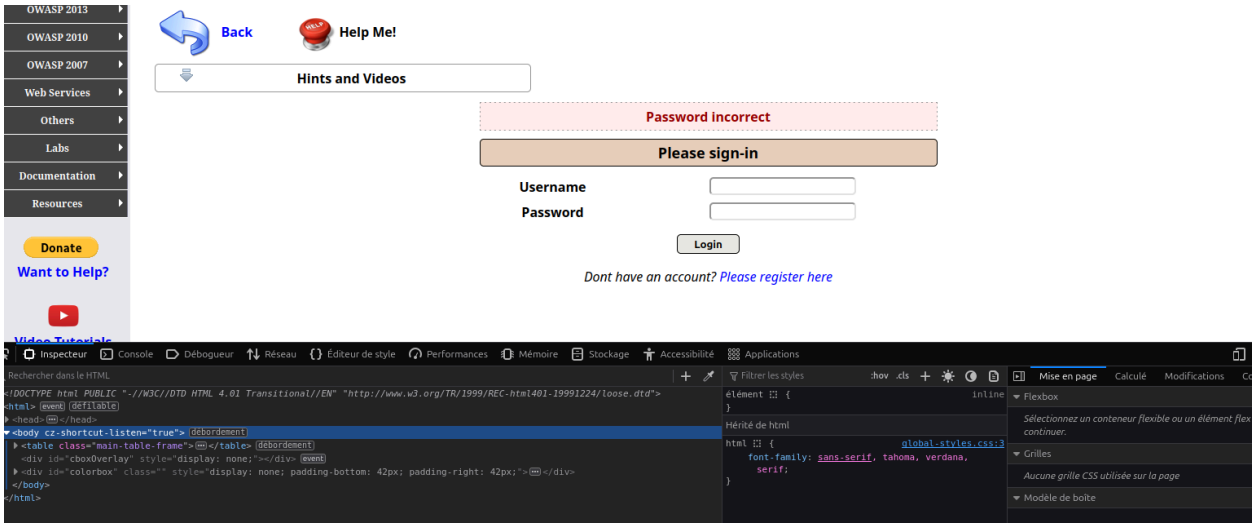
Maintenant vous activez Intercept is on pour recevoir les requêtes. puis vous faites login.

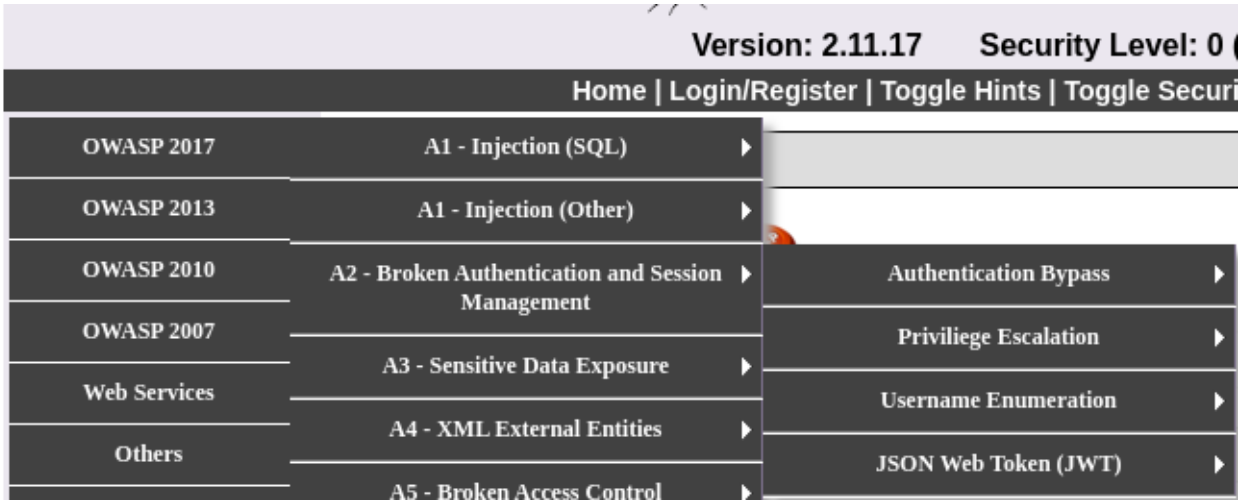
Q3. Positionner le niveau de sécurité du code à 0 (Hosed) :



Comme on le voit, le niveau de sécurité a été modifié.

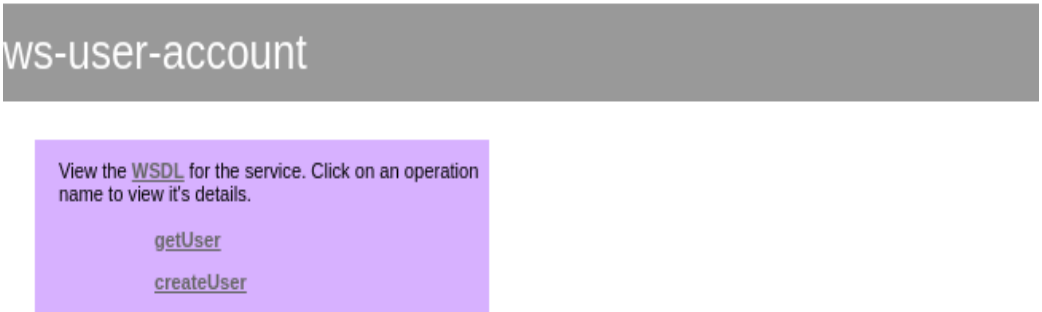
Allez dans les paramètres de sécurité et changez le niveau de sécurité à **un niveau supérieur** (par exemple, **niveau 1 ou 2**). Ce niveau active des mesures de protection contre les attaques SQLi.



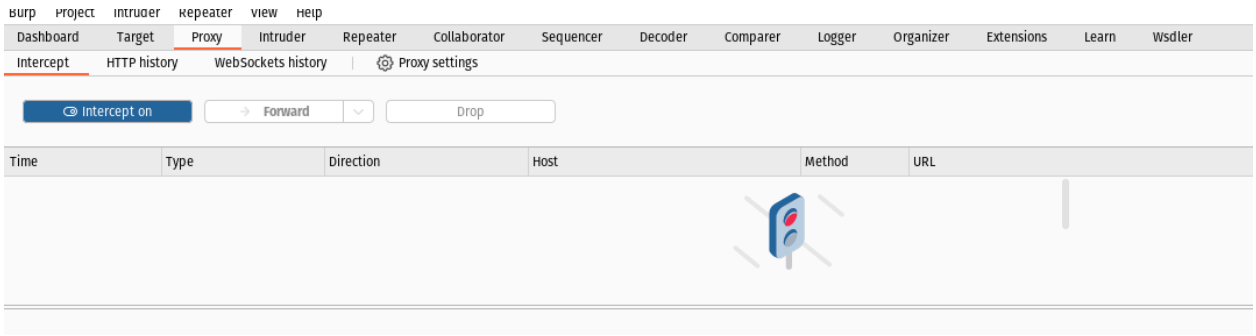


Vous devez vous dériger vers **OWASP 2017** pour accéder **A2-Broken Auth….** Puis **Username Enumeration** puis **LookUp user.**

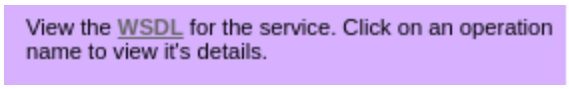
Cela fait vous tombez sur une page comme celle-ci :



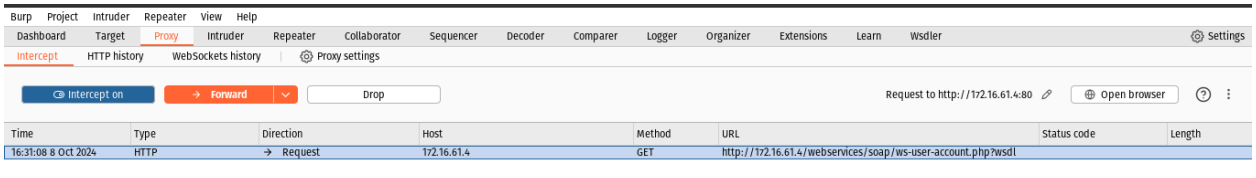
Maintenant vous allez sur Burp Suite pour activer Intercept off en on. Comme ce screen :

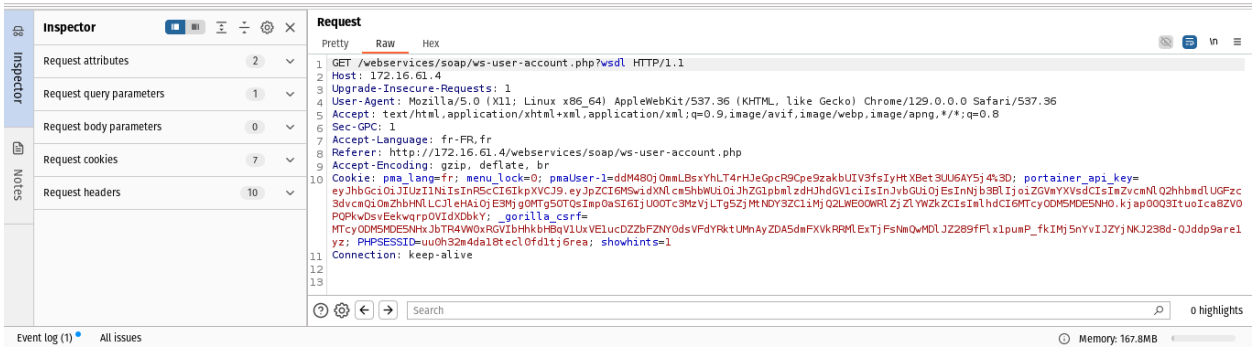


Une fois que le Intercept est en on vous devez cliquer sur L'URL "WSDL" de la page précédente attention vous devez avoir votre proxy bien activé si cela ne fonctionnera pas :



Très bien, maintenant vous allez sur Burp Suite :



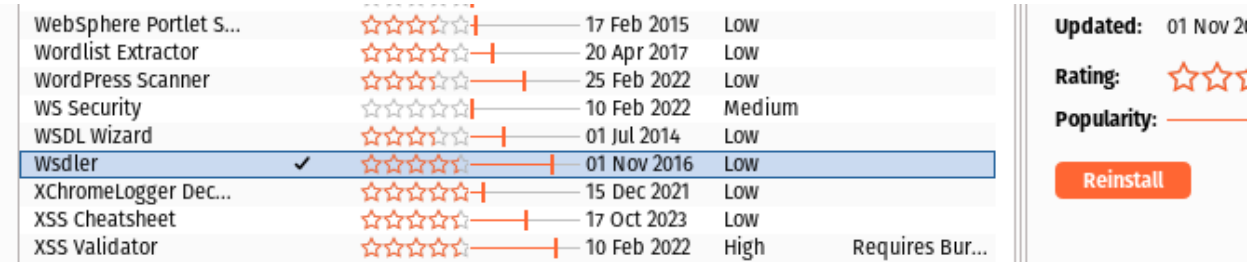


Si la manipulation a bien fonctionné normalement vous devez tomber sur la même interface du screen au-dessus.

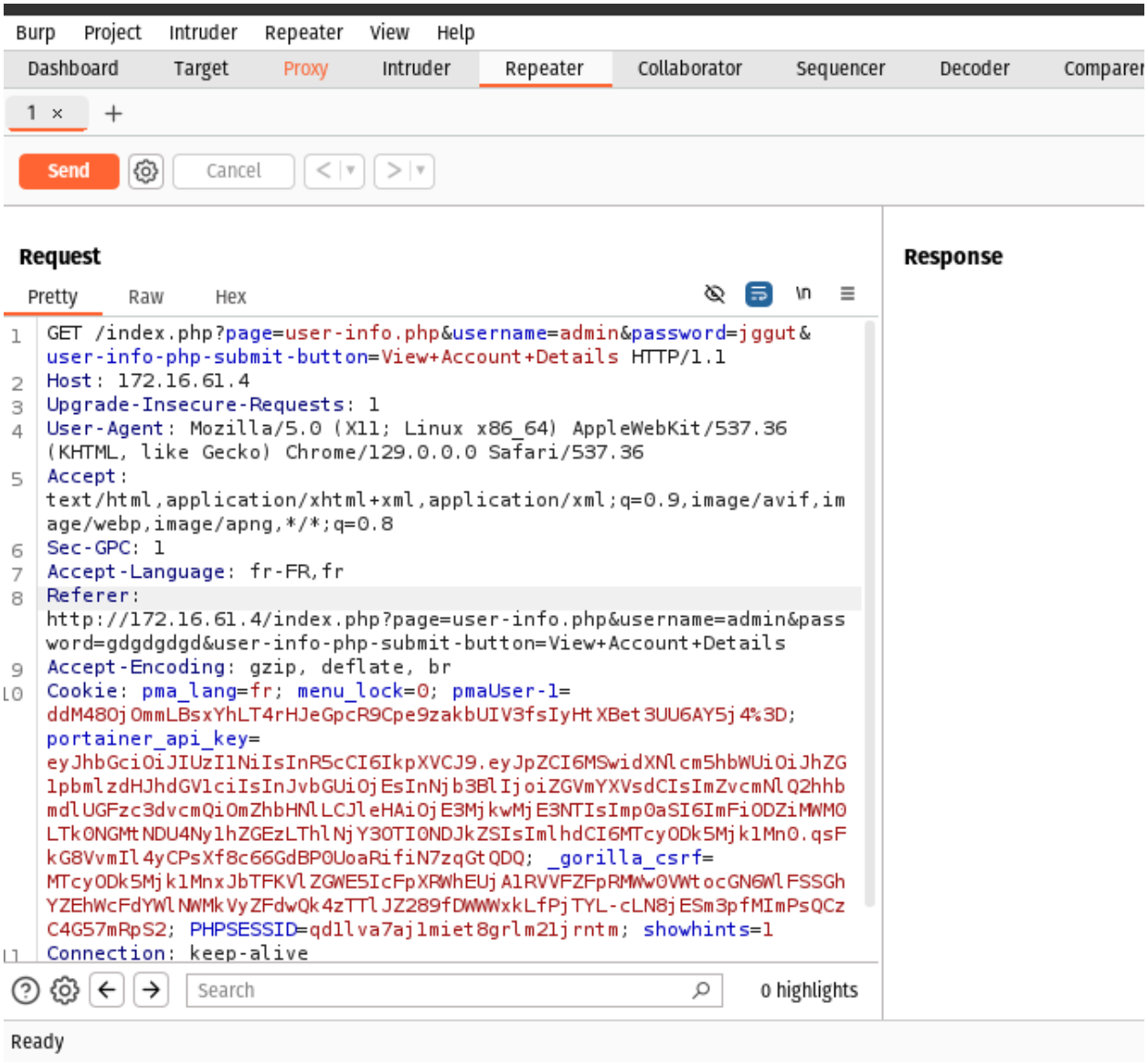
ACTIVITÉ 2

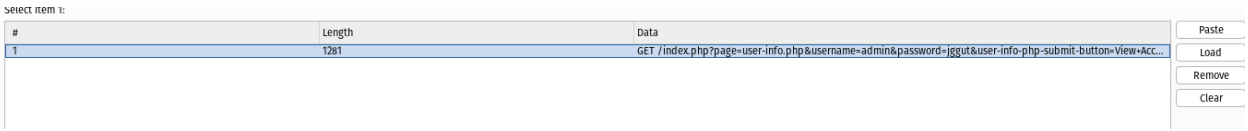
Travail à faire 1

Q1. Commencer par installer l'extension Wsdler en réalisant les manipulations décrites dans l'étape n°1. Puis, positionner le niveau de sécurité à 0.

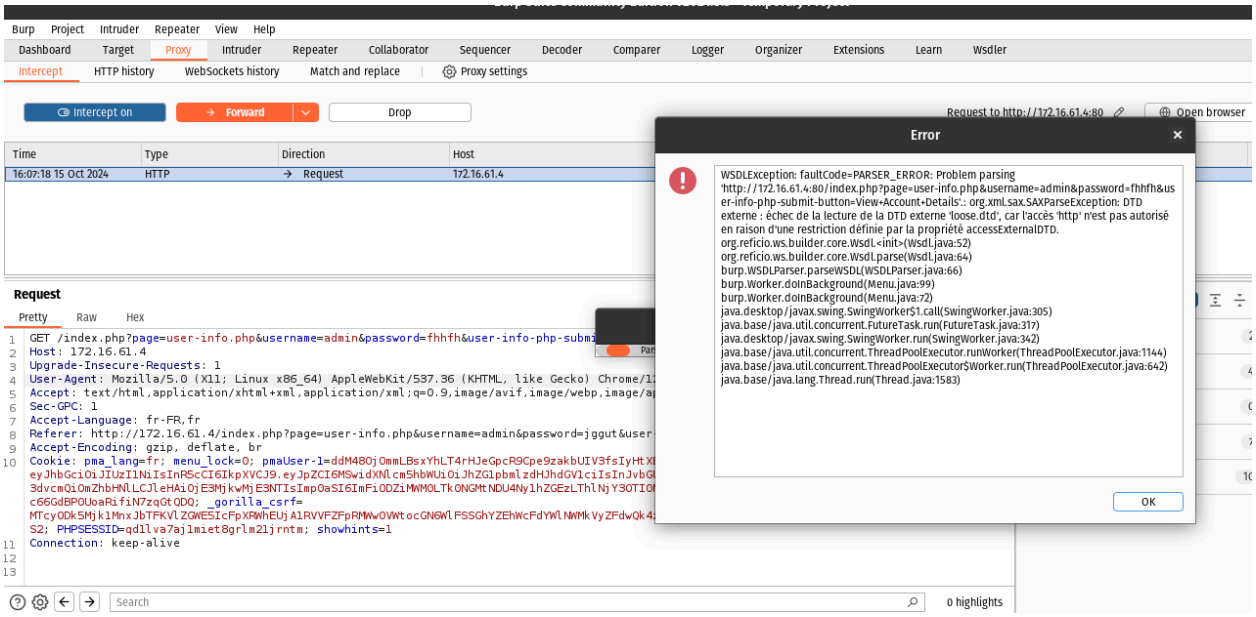


Tester un exemple de requête et de réponse à l'aide d'un login non valide en réalisant les manipulations décrites dans l'étape n°2 (parse de la page wsdl, envoi au répéteur, génération de la réponse et envoi au comparateur).





Cela me fait une erreur quand j'essaye de l'envoyer à WSDLER


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Wsdler
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://172.16.61.4:80
Open browser
Time Type Direction Host
16:07:18 15 Oct 2024 HTTP Request 172.16.61.4
Request
Pretty Raw Hex
GET /index.php?page=user-info.php&username=admin&password=fhhfh&user-info-php-subm
Host: 172.16.61.4
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
Sec-GPC: 1
Accept-Language: fr-FR,fr
Referer: http://172.16.61.4/index.php?page=user-info.php&username=admin&password=jggut&user
Accept-Encoding: gzip, deflate, br
Cookie: pma_lang=fr; menu_lock=0; pmaUser-1=ddM48OjOmmLBsxYhLT4rHJeGpcR9Cpe9zakbUIV3fsIyHtX
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwidXNlcm5hbWUiOiJhZG1pbmlzdHJhdGV1ciIsInJvbG
3dvcmQiOmZhbHNlLCJleHAiOjE3MjkwMjE3NTIsImp0aSI6ImFiODZiMWM0LTk0NGMtNDU4Ny1hZGEzLThlNjY3OTI0
c66GdBP0UoaRifiN7zqGtQDQ; _gorilla_csrf=
MTcyODk5Mjk1MnxJbTFKVlZGWE5IcFpXRWhEUjA1RVVFZFpRMWwOVWtocGN6WlFSSGhYZEhWcFdYWlNWMkVyZFdwQk4
S2; PHPSESSID=qdllva7ajlmiet8grlm21jrntm; showhints=1
Connection: keep-alive
Search
0 highlights
Error
WSDLException: faultCode=PARSER_ERROR: Problem parsing 'http://172.16.61.4:80/index.php?page=user-info.php&username=admin&password=fhhfh&user-info-php-submit-button=View+Account+Details'.: org.xml.sax.SAXParseException: DTD externe : échec de la lecture de la DTD externe 'loose.dtd', car l'accès 'http' n'est pas autorisé en raison d'une restriction définie par la propriété accessExternalDTD.
org.reficio.ws.builder.core.WsdL.<init>(WsdL.java:52)
org.reficio.ws.builder.core.WsdL.parse(WsdL.java:64)
burp.WSDLParser.parseWSDL(WSDLParser.java:66)
burp.Worker.doInBackground(Menu.java:99)
burp.Worker.doInBackground(Menu.java:72)
java.desktop/javax.swing.SwingWorker$1.call(SwingWorker.java:305)
java.base/java.util.concurrent.FutureTask.run(FutureTask.java:317)
java.desktop/javax.swing.SwingWorker.run(SwingWorker.java:342)
java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1144)
java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:642)
java.base/java.lang.Thread.run(Thread.java:1583)
OK