Cours:
TEST DE PENETRATION

Atelier 4:
Test de Pénétration Web application

29/4/2022

Loi n° 07-03
complétant le code pénal
en ce qui concerne les infractions relatives
aux systèmes de traitement automatisé des données

Article unique

Le titre I du livre III du code pénal est complété par le chapitre X ainsi qu'il suit :

« LIVRE III

« Titre premier

« *Chapitre X*

« De l'atteinte aux systèmes
« de traitement automatisé des données

« *Article 607-3.* – Le fait d'accéder, frauduleusement, dans « tout ou partie d'un système de traitement automatisé de données « est puni d'un mois à trois mois d'emprisonnement et de 2.000 à « 10.000 dirhams d'amende ou de l'une de ces deux peines « seulement.

« Est passible de la même peine toute personne qui « se maintient dans tout ou partie d'un système de traitement « automatisé de données auquel elle a accédé par erreur et alors « qu'elle n'en a pas le droit.

Pr: BELMEKKI ELMOSTAFA

UNIVERSITE MOHAMMED 6 POLYTECHNIQUE - BENGUERIR -

Sommaire

Lab 2: OWASP TOP 10

I. Scénario

Vous avez été engagé pour effectuer une pénétration de la sécurité des applications web sur certaines de vos applications interne et externe de vos client. votre objectif est d'identifier les failles dans l'application en effectuant des exploits basés sur le Top Ten OWASP.

II. Exercise 1- injection flaws - SQL injection (OWASP WebGoat .net site)

a. objectifs

Apprenez à accéder à une application Web en exploitant une faille d'injection SQL

b. Ressources

OWASP Broken Web Apps VM

Linux Attack VM

c. Steps:

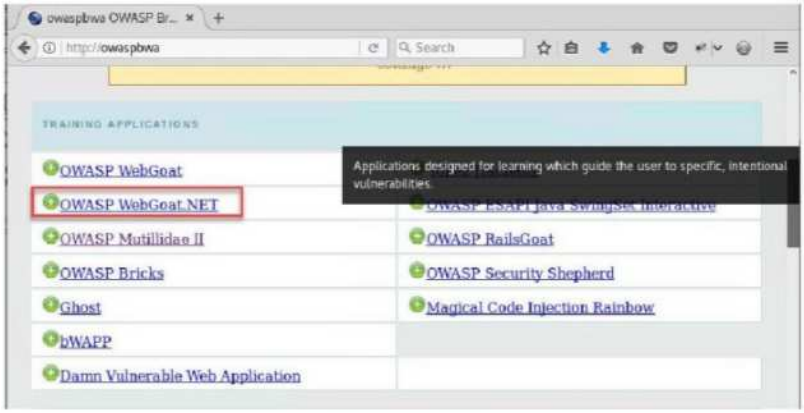
Injection flaws:

Des failles d'injection, telles que l'injection SQL, OS et LDAP, se produisent lorsque des données non fiables sont envoyées à un interpréteur dans le cadre d'une commande ou d'une requête. les données hostiles de l'attaquant peuvent inciter l'interprète à exécuter des commandes involontaires ou à accéder aux données sans autorisation appropriée.

1. Démarrez votre machine d'attaque linux
2. Démarrez firefox assurez-vous que votre firefox n'utilise aucun proxy
3. En utilisant firefox, allez sur le site OWASP webGOat.net

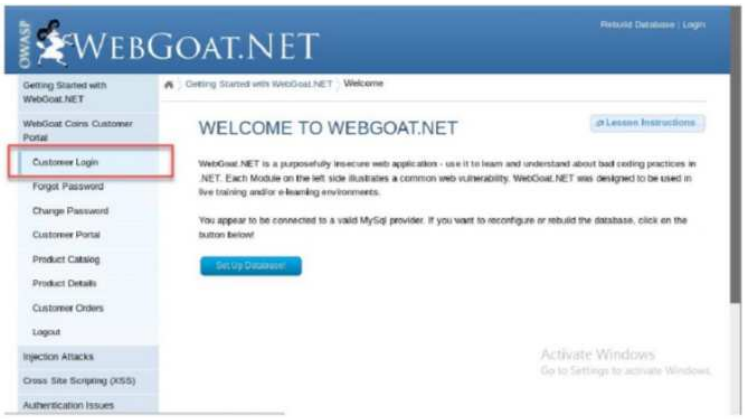
- http: // OWASPBWA /

4. Faites défiler vers le bas et cliquez sur le lien "OWASP WebGOat.Net"

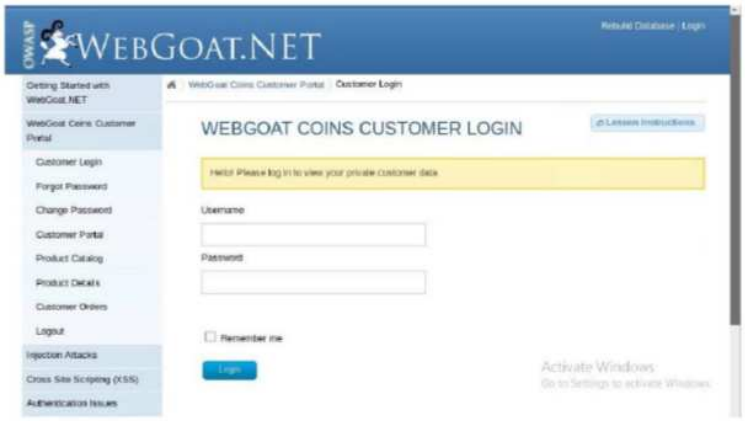


5. Sur l'écran principal d'OWASPGoat.net, cliquez sur le "WEBGoat Coins Customer Portal"

6. Sur l'écran suivant, cliquez sur le lien"Customer Login" link



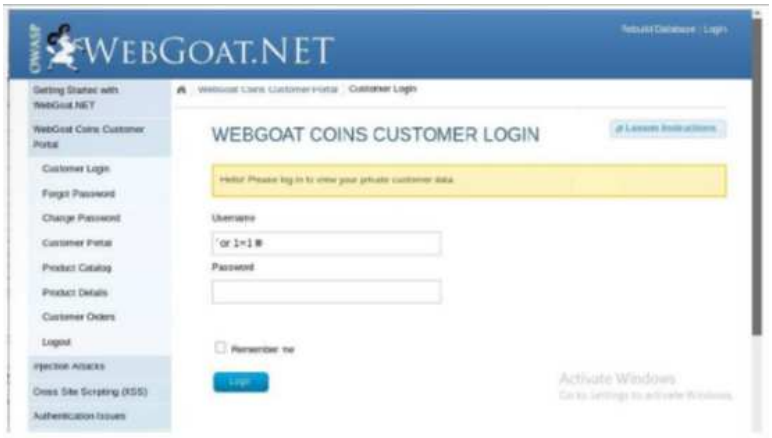
7. Vous obtiendrez un écran similaire au suivant:



8. Nous ne nous connecterons pas sans connaître un nom d'utilisateur et un mot de passe valides, entrez simplement

Username = 'or 1=1 #

9. Appuyez sur le bouton "login" (le mot de passe est laissé vide)



10. Vous avez désormais accès à l'application en exploitant une faille d'injection SQL

11. Vous pouvez maintenant tout fermer

III. Exercice 2 injection Flaws - String SQL injection (OWASP Broken Apps WebGoat).

a. Objectives

Accéder à l'application Web webgoat et exploiter une attaque par injection SQL à l'aide de Webscarab

b. Ressources

OWASP Broken Web Apps VM

Kali linux VM

c. Steps:

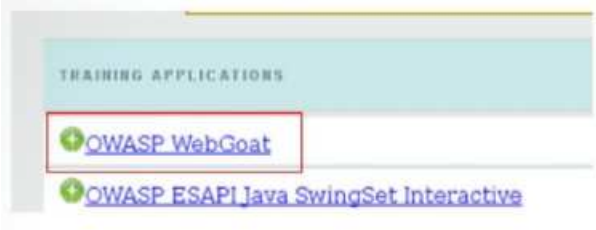
Injection flaws:

cette application est un peu mieux protégée que la précédente, donc si nous essayons l'attaque précédente sur cette page, cela ne fonctionnera pas, mais pour prouver qu'elle est toujours vulnérable, nous utiliserons l'application proxy WebScarab pour effectuer l'injection SQL.

1. Démarrez votre machine kali linux

2. Démarrer WebScarab
3. Démarrer Firefox: assurez-vous que votre Firefox envoie du trafic via le webscarab
4. En utilisant firefox, accédez à l'application de vulnérabilité OWASP en tapant l'URL "http: // owaspbwa".

5. Allez à l'application WebGoat (vous devrez peut-être faire défiler vers le bas pour trouver l'option appropriée)



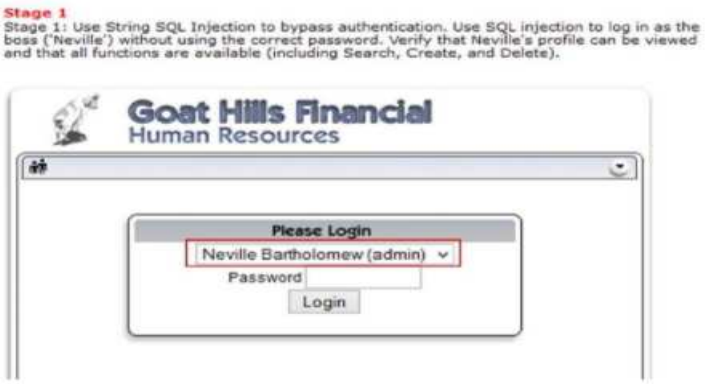
6. Se connecter en utilisant guest / guest
7. Cliquez sur démarrer "démarrer WebGoat"

8. Cliquez sur "1.injection Flaws" et cliquez sur 2.stage 1: String SQL injection

9. WebGoat Stage 1- String SQL Injection

   Description de l'étape "1: Use String SQL injection" pour contourner l'authentification. utilisez l'injection SQL pour vous connecter en tant que patron ('Neville') sans utiliser le mot de passe correct. Vérifiez que le profil de Neville peut être consulté et que toutes les fonctions sont disponibles (y compris la recherche, la création et la suppression).

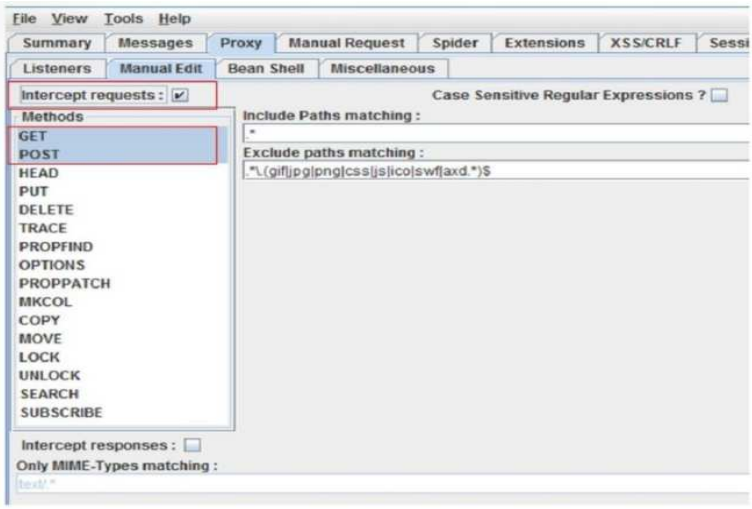
Sélectionnez Neville Bartholomew dans la liste déroulante:



10. Vérifiez que l'application webscarab est en cours d'exécution et sélectionnez l'option Intercepter les réponses, assurez-vous également que les méthodes GET et POST sont mises en évidences.

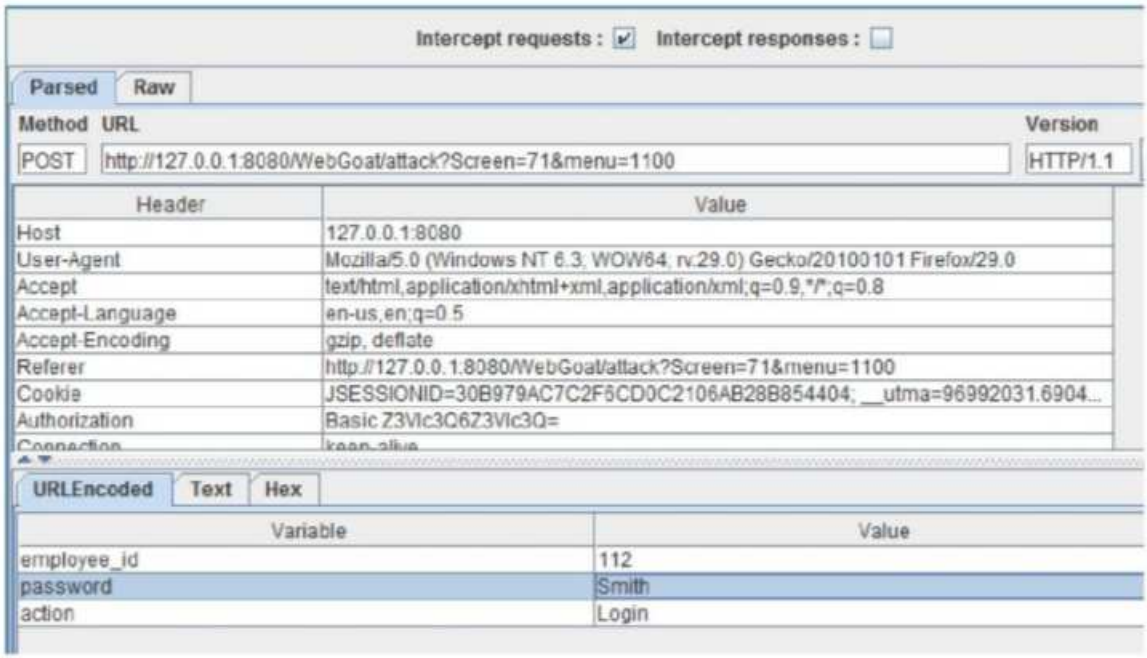
    - Trouvez la fenêtre webscarab et sélectionnez l'onglet "proxy", puis l'onglet "édition manuelle" et activez la case à cocher "intercept requests" (en cliquant dessus si besoin) et assurez-vous que les méthodes "GET" et "POST" sont actives comme montré sur la capture d'écran suivante. si les méthodes GET et

POST ne sont pas sélectionnées, cliquez dessus pour les sélectionner

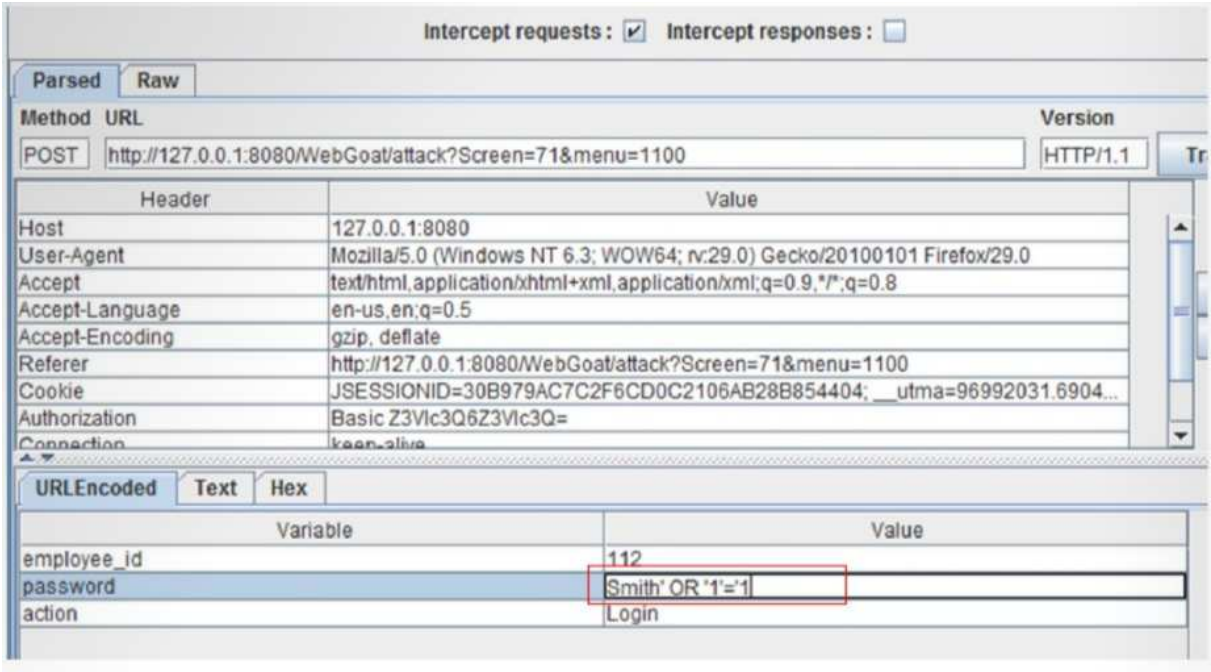


11. Passer à Firefox et Smith comme mot de passe et cliquer sur le bouton "Login" button

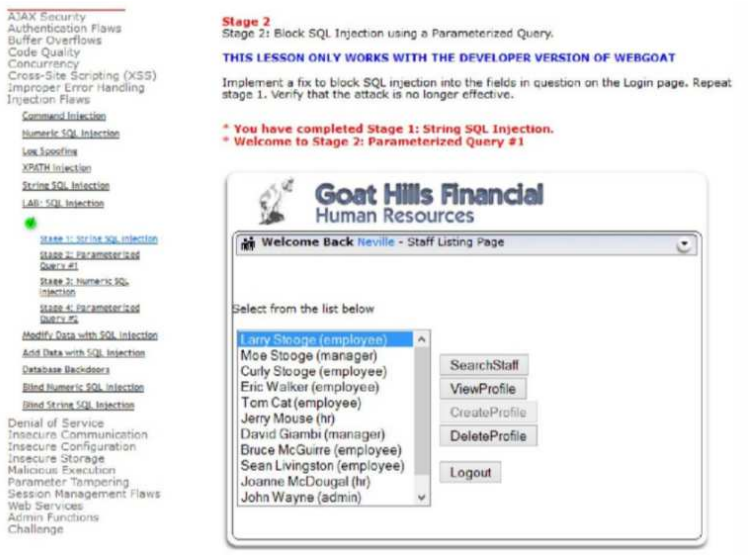
12. Webscarab a intercepté le nom d'utilisateur entré sur l'écran de connexion et maintenant vous pourrez insérer une injection SQL pour forcer une connexion.



13. Double-cliquez sur la cellule " value " de la variable " password " et changez son contenu en smith 'OR' 1 '=' 1 et cliquez sur le bouton "accepter les modifications"



14. CONGRATULATION! Votre injection SQL vous a permis de vous connecter en tant que Neville sans authentifier le mot de passe.



IV. Exercise 3- Injection Flaws - command injection

a. Objectives

learning how a command injection flaw can be used to execute arbitrary commands

b. Resources

OWASP Broken Web Apps VM

Kali Linux VM

c. Steps

Injection Flaws

cette application exécute une commande et renvoie le résultat à l'écran, donc nous supposons que nous pouvons en exécuter une autre en la concaténant avec le caractère 1.

1. Démarrez ton kali
2. Démarrez votre OWASP Broken Apps Maching
3. Démarrez Firefox et ouvrez l'URL "http: // owaspbwa"

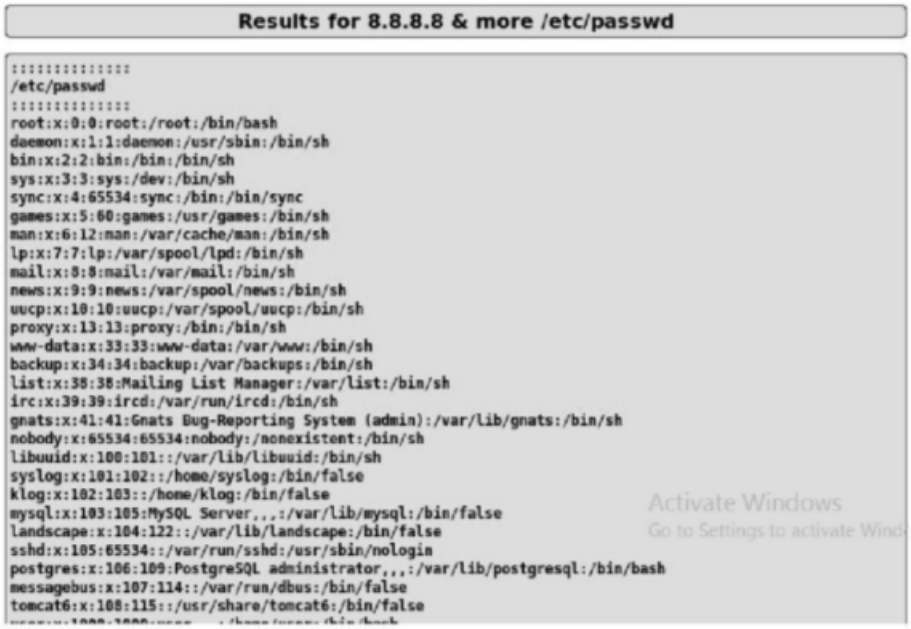
4. Allez à "Mutillidae II"

5. Puis allez à "OWASP 2017 / A1- injection(Other)" /command injcetion /DNS Lookup

6. Cette page est utilisée pour fournir une fonctionnalité "ping". pour l'essayer, entrez une IP dans la zone de texte (comme 8.8.8.8) et appuyez sur le bouton "Lookup DNS"

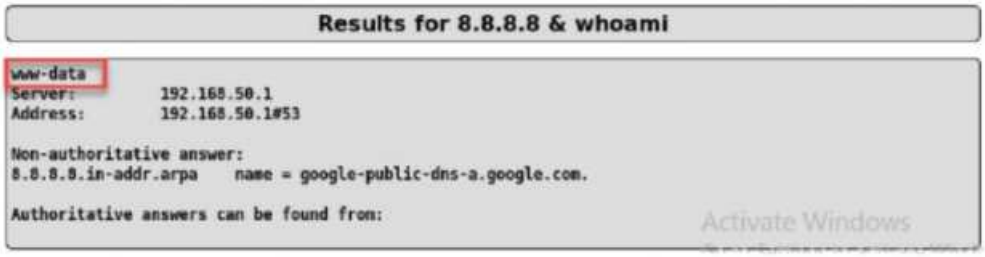
7. Vous obtiendrez un résultat similaire à

8. En analysant la sortie, vous pourriez commencer à penser que nous pourrions essayer d'exécuter autre chose, donc, dans cette même page, insérons le texte "8.8.8.8 & more /etc/passwd



9. Cela indique qu'il est vraiment vulnérable à l'injection de commande.

10. Nous pourrions essayer de savoir s'il fonctionne avec root ou un autre utilisateur pour découvrir l'étendue de notre piratage. Tapons "8.8.8.8 & whoami" dans la zone de texte et exécutons-le.



11. Le cadre rouge montre qu'il fonctionne avec l'utilisateur "www-data" donc même si cela est vulnérable à l'injection de commande, nous devons encore trouver un moyen d'augmenter nos autorisations.
12. Fin d'exercice.

V. Exercise 4- broken Authentification - Brute force a login

a. Objectives

apprendre pourquoi vous devriez avoir une technique d'authentification qui n'autorise pas les tentatives infinies de connexion

b. Resources

owasp Broken Web Apps VM

kali linus VM

c. Steps

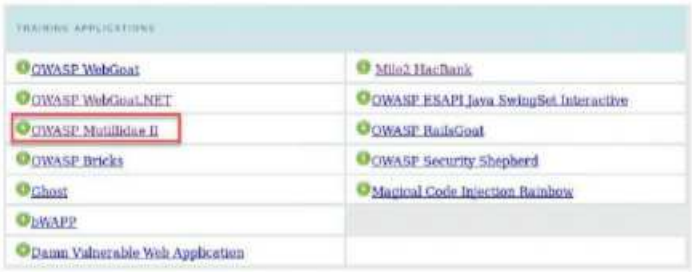
Brute force / Dictionary Attack

- Cette application est toujours mieux protégée que la précédente, nous ne pourrons donc pas y injecter de code pour y accéder, mais avec un peu d'effort, nous pourrons essayer un grand nombre de noms d'utilisateur et de mots de passe afin de trouver un code valide.
- Nous effectuerons une attaque par dictionnaire au lieu d'une force brute réelle. la différence entre les deux est que l'attaque par dictionnaire essaiera beaucoup de vrais mots (mots qui pourraient

être trouvés dans un dictionnaire) tandis que la force brute essaiera n'importe quelle combinaison de caractères réels (comme "a", "ab", "abc "," abde "et ainsi de suite).

1. Démarrez vos machines kali linux
2. Démarrez votre OWASP Broken Web Apps Machine
3. Revenez à votre machine kali linux et connectez-vous
4. Démarrer OWASP- ZAP
5. Démarrez firefox assurez-vous que votre firefox envoie du trafic via ZAP
6. A l'aide de Firefox, accédez aux OWASP Broken Web Apps en saisissant l'URL http: // owaspbwa

7. Cliquez sur le lien Mutillidae II.

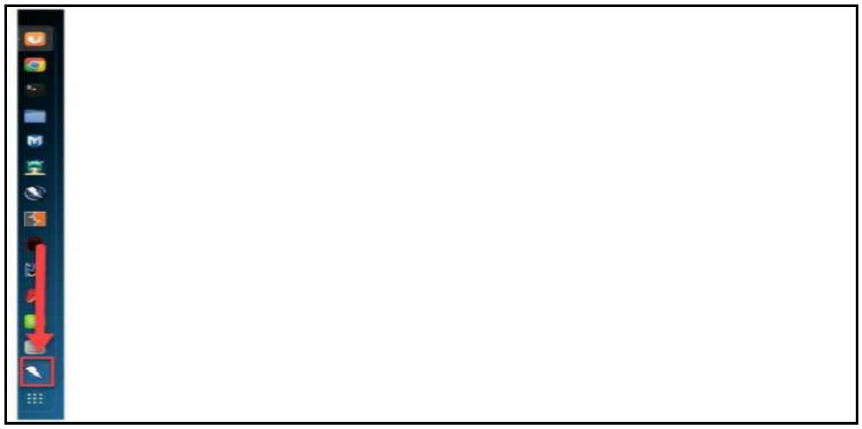


8. Accédez à OWASP 2017 / "A2-Broken Authentication and Session Management / Authentication Bypass / Via Brute Force / Login

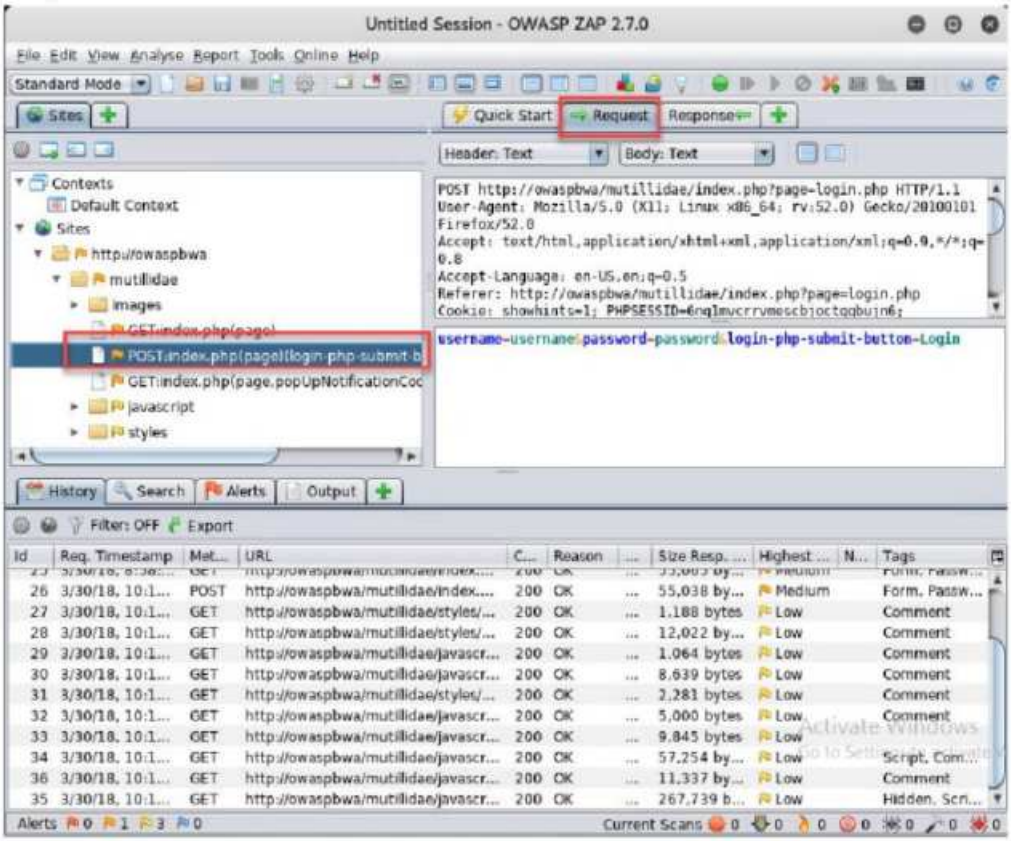
9. Tapez " username " comme nom d'utilisateur et " password " comme mot de passe et appuyez sur le bouton " login "

10. Nous devrions recevoir le message " Account does not exist " donc nous recevons l'appel dans le proxy et l'utiliser pour exploiter

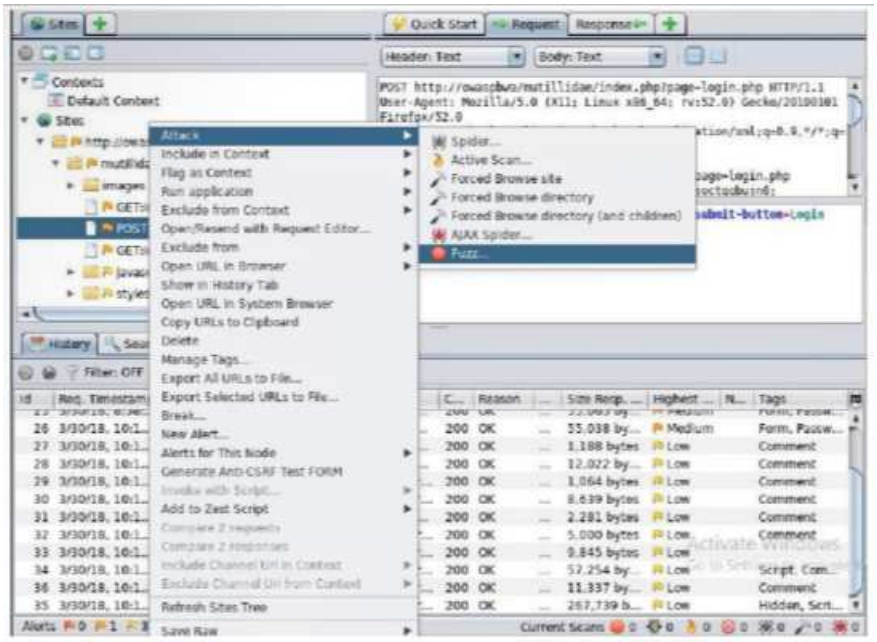
11. Allons chercher la bonne commande http dans le proxy ZAP. cliquez sur l'icône signalée par la flèche tout en bas de l'onglet gauche.



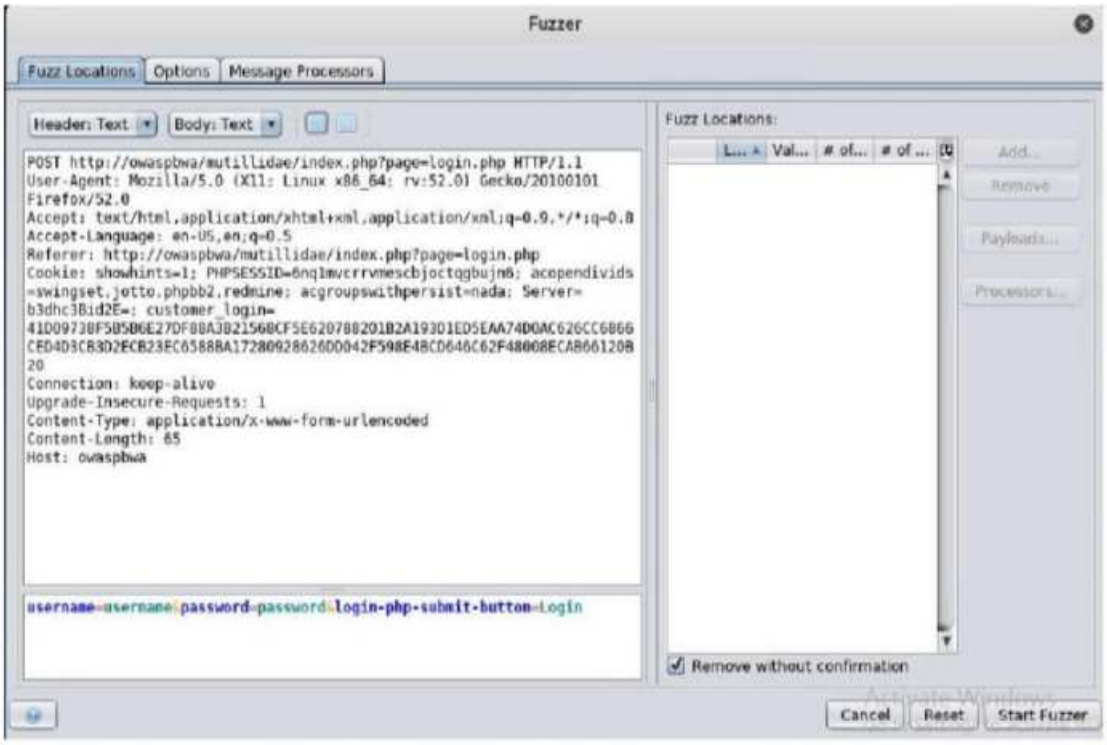
12. Une fois que nous avons la fenêtre ZAP, cliquez sur la commande "POST" pour l'écran index/login et cliquez sur l'onglet " Request " afin que nous puissions ouvrir les détails de l'appel. Remarquez comment les paramètres de publication incluent le " username " et le " password " "valeurs que nous venons d'insérer à l'écran avec tous les autres paramètres nécessaires pour effectuer une demande de connexion valide.



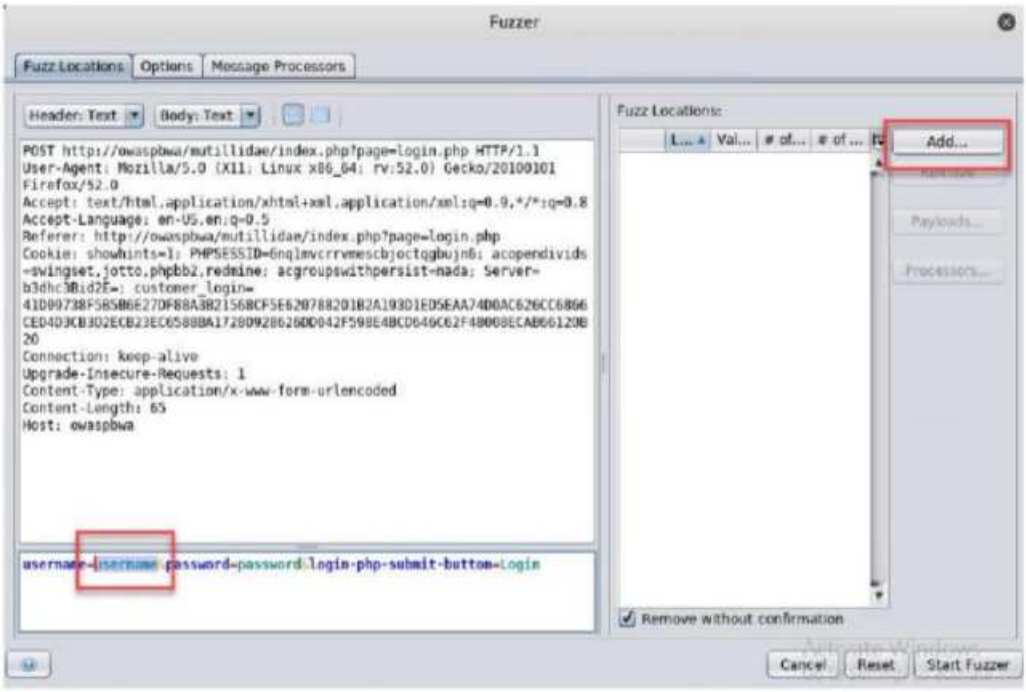
13. Maintenant, faisons un clic droit sur la commande "POST" à gauche et sélectionnez "Attaque/Fuzz"



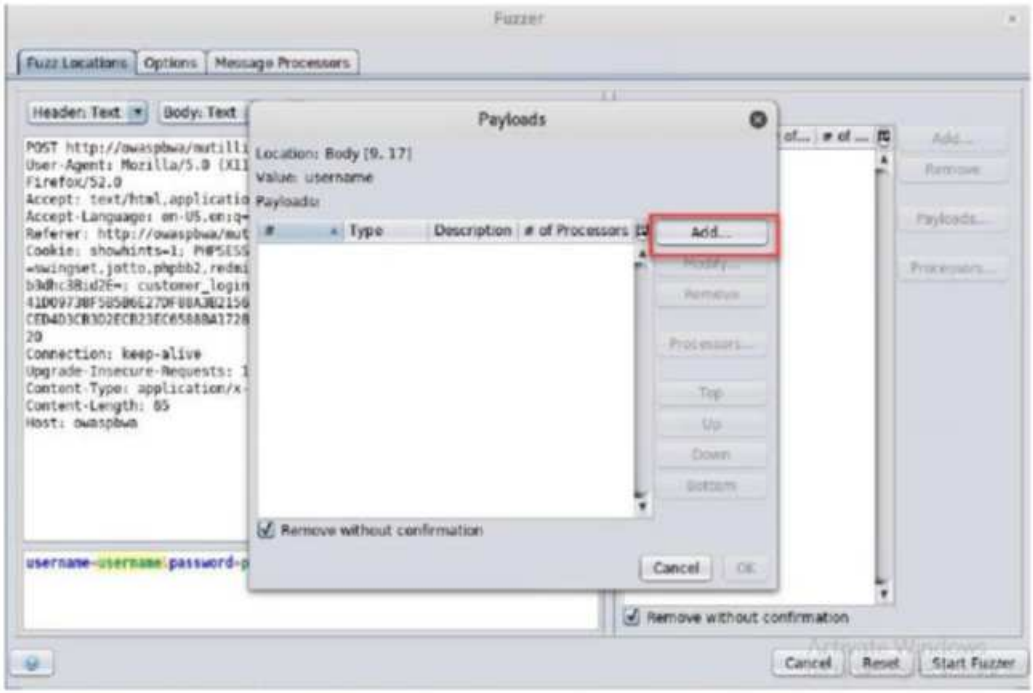
14. Vous obtiendrez l'écran suivant



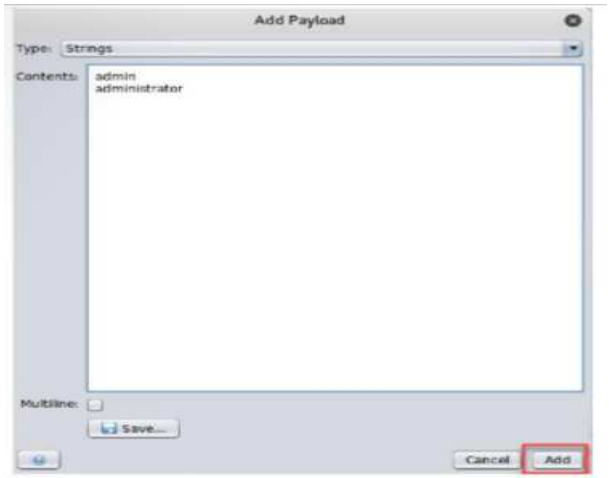
15. Pour cet exercice, nous supposerons que nous savons déjà le nom d'utilisateur est "admin" ou "administrator", mais nous devons trouver le mot de passe. la première chose que nous devons faire est de créer deux variables. pour les créer, sélectionnez username du texte comme indiqué dans la capture d'écran suivante et cliquez sur le bouton "ajouter"



16. Nous devons maintenant ajouter la " payload " ou les "values" que les variables vont prendre. cliquez sur le bouton "add"

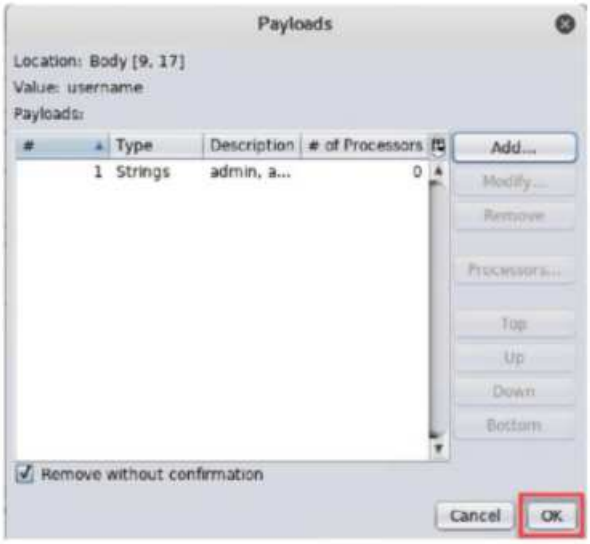


17. Ajoutez les différents noms d'utilisateur que vous souhaitez essayer dans la zone de texte. Un nom d'utilisateur par ligne

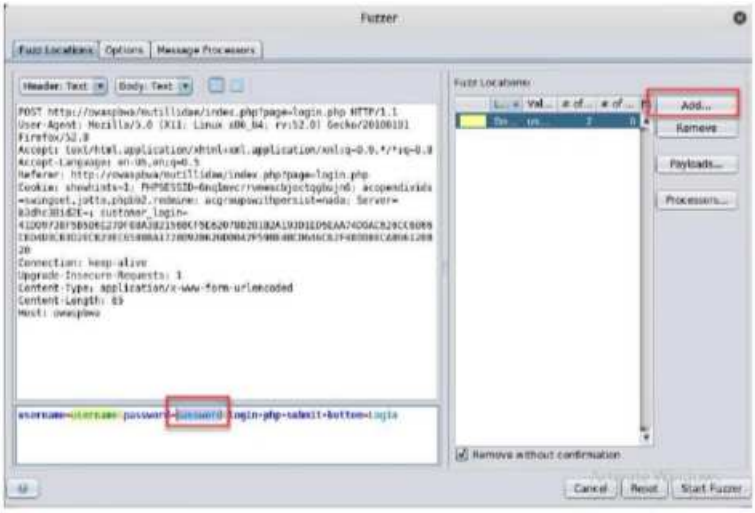


18. Cliquez sur le bouton "add".

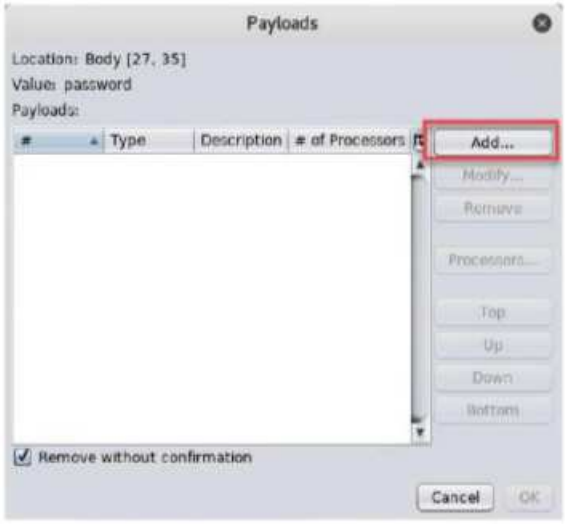
19. Maintenant que nous avons tous les noms d'utilisateurs que nous voulons essayer, ajoutons la liste des mots de passe. cliquez sur le bouton "OK"



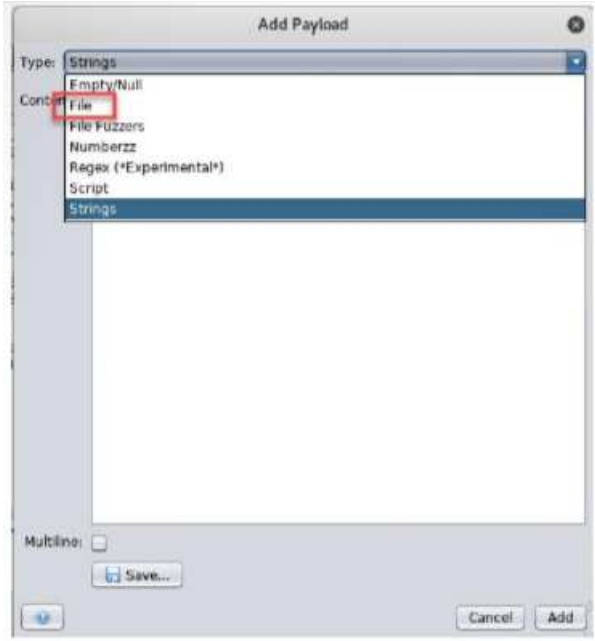
20. Sélectionnez maintenant le text "password" et cliquez sur le bouton "add"



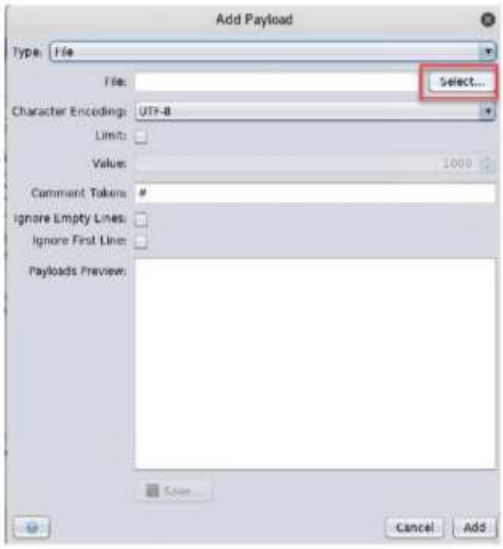
21. Cliquez sur le bouton ajouter "add".



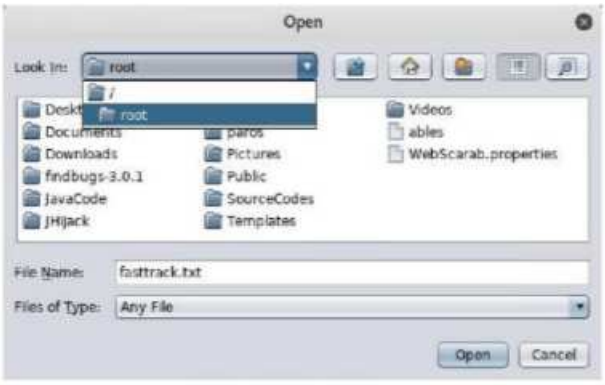
22. Dans la zone de liste déroulante, sélectionnez l'option "Fichier".

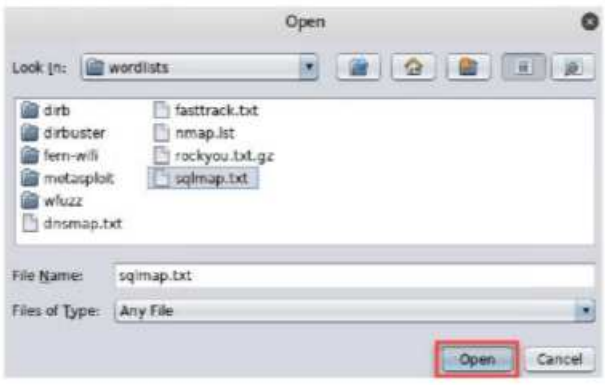


23. Cliquez maintenant sur le bouton "select"



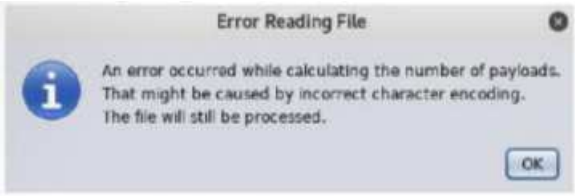
24. Sélectionnons le fichier "/usr/share/wordlist/sqlmap.txt" et cliquez sur "Open"



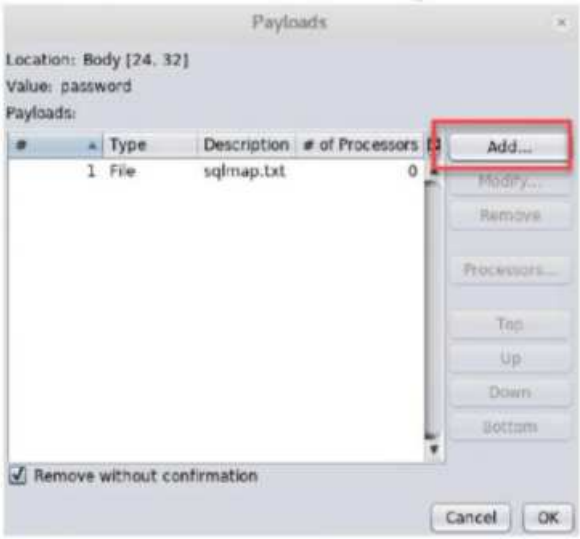


25. Une fois la liste chargée, cliquez sur "add"

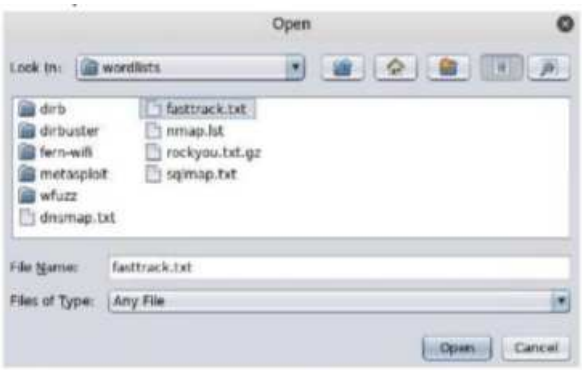
26. Si vous obtenez une erreur comme celle-ci, ignorez-la et cliquez sur "ok".



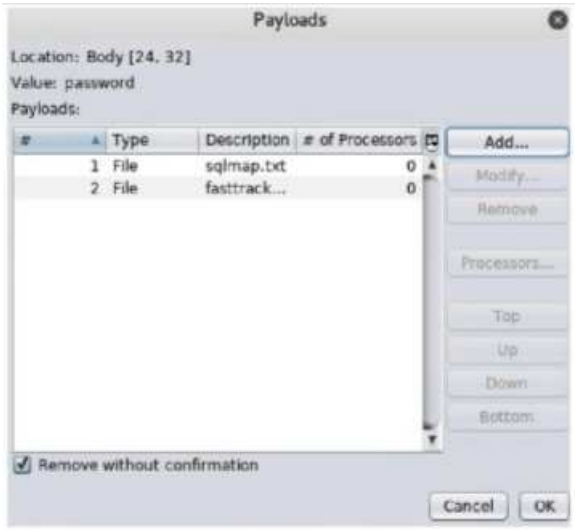
27. Ajoutons plus de mots de passe à la liste. cliquez à nouveau sur "add".



28. En utilisant la même technique, ajoutez le fichier " /usr/share/wordlist/fasttrack.txt"

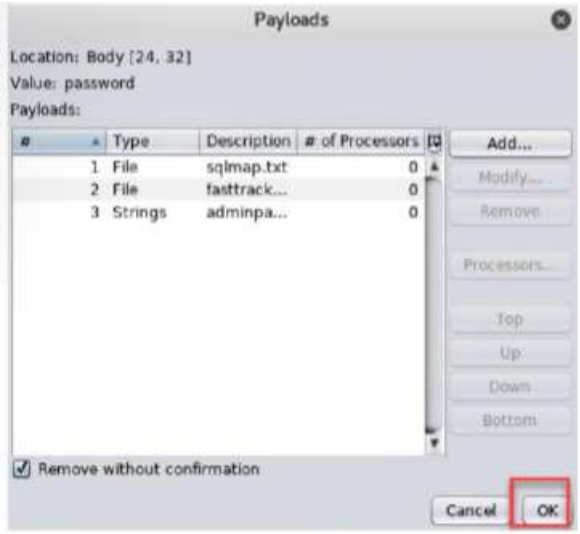


29. Vous avez maintenant deux dictionnaires que vous allez essayer. juste pour faire bonne mesure, ajoutons quelques mots de passe manuels qui, à notre avis, méritent d'être essayés. cliquez à nouveau sur "add".

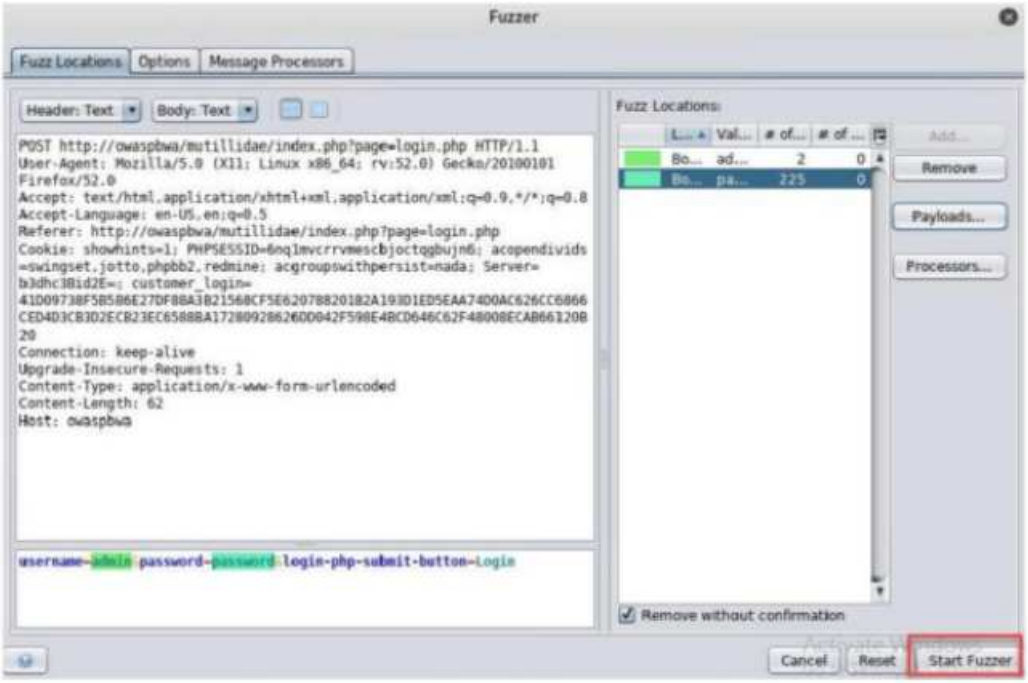


30. Tapez les mêmes mots de passe comme "adminpass", "adminadmin" et cliquez sur "add".

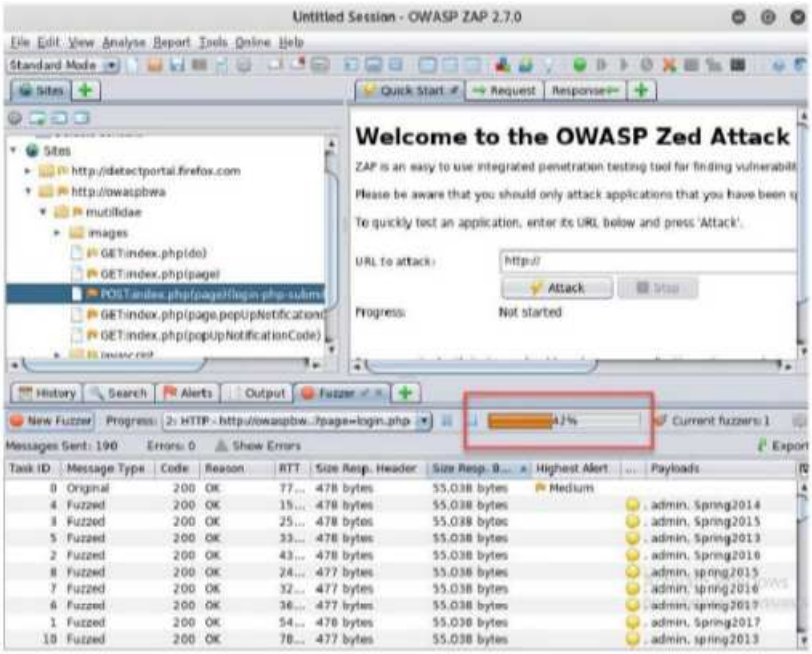
31. Continuons en cliquant sur "ok ".



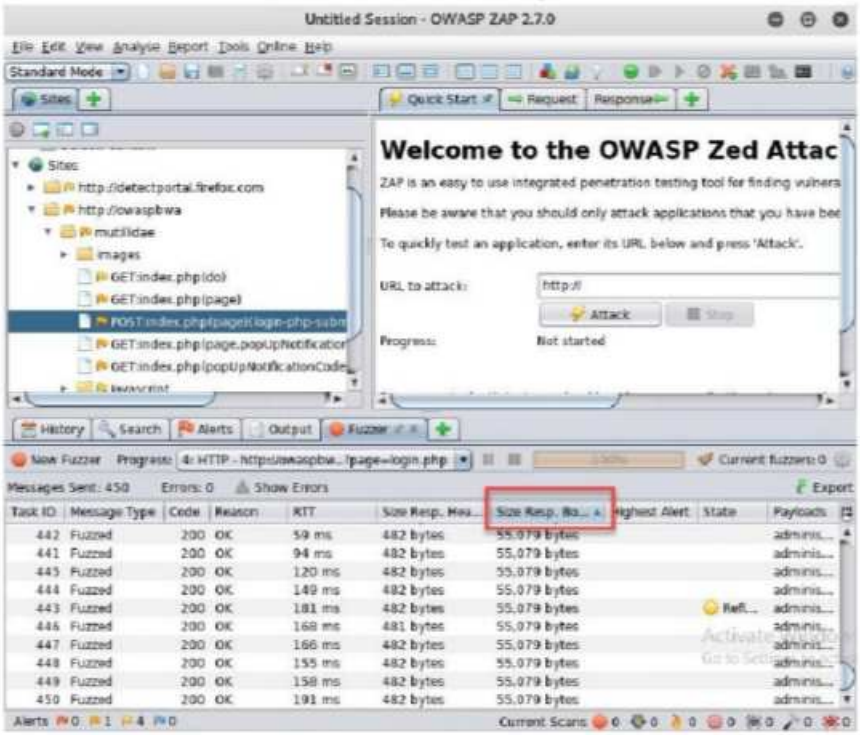
32. Nous sommes prêts à lancer l'attaque. cliquez sur "start Fuzzer"



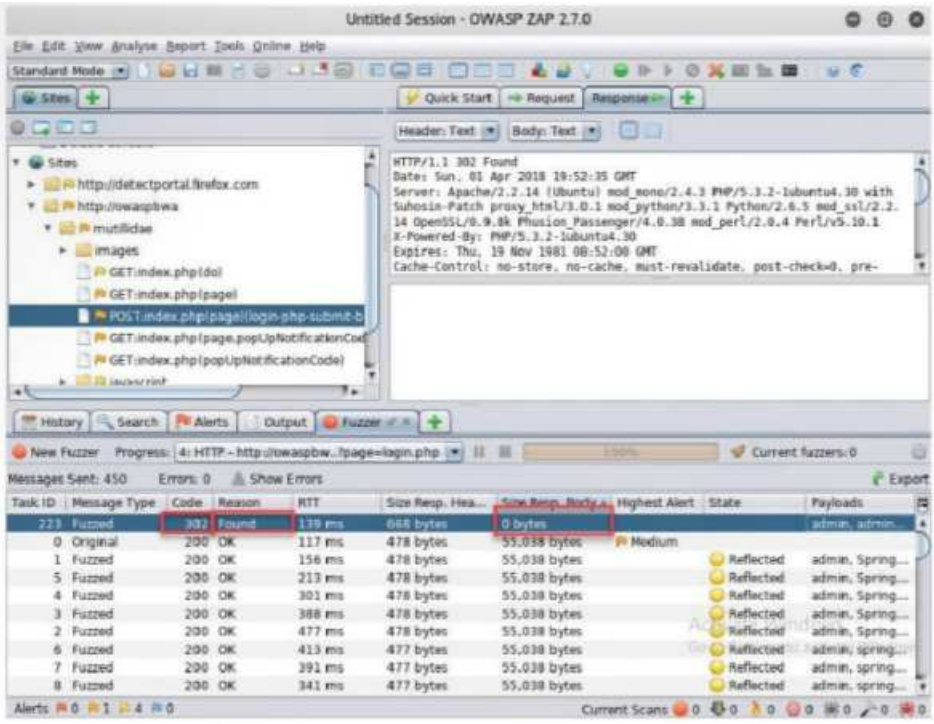
33. Attendez que la barre de progression atteint 100%..



34. Analysons maintenant le résultat. la première chose que nous allons examiner est la taille de la réponse. cliquez sur l'en-tête pour " size Response " et triez-les par taille.



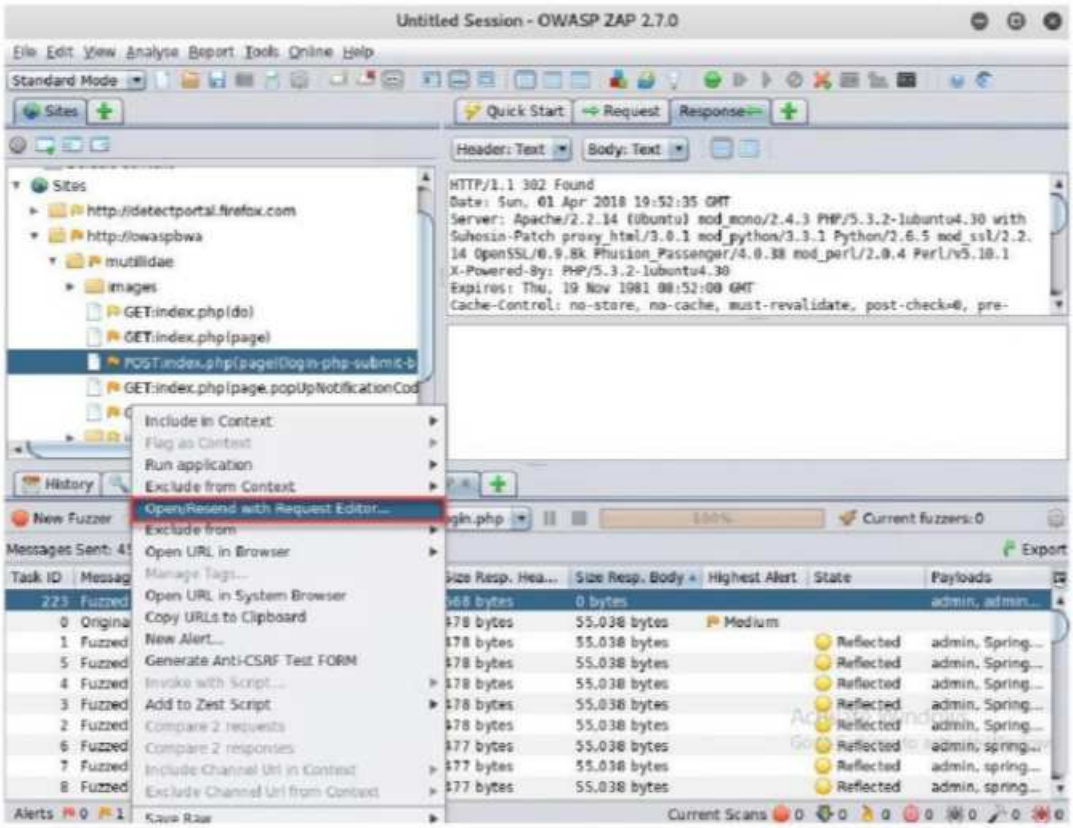
35. Une fois que nous avons terminé cela, nous devrions voir l'écran suivant.



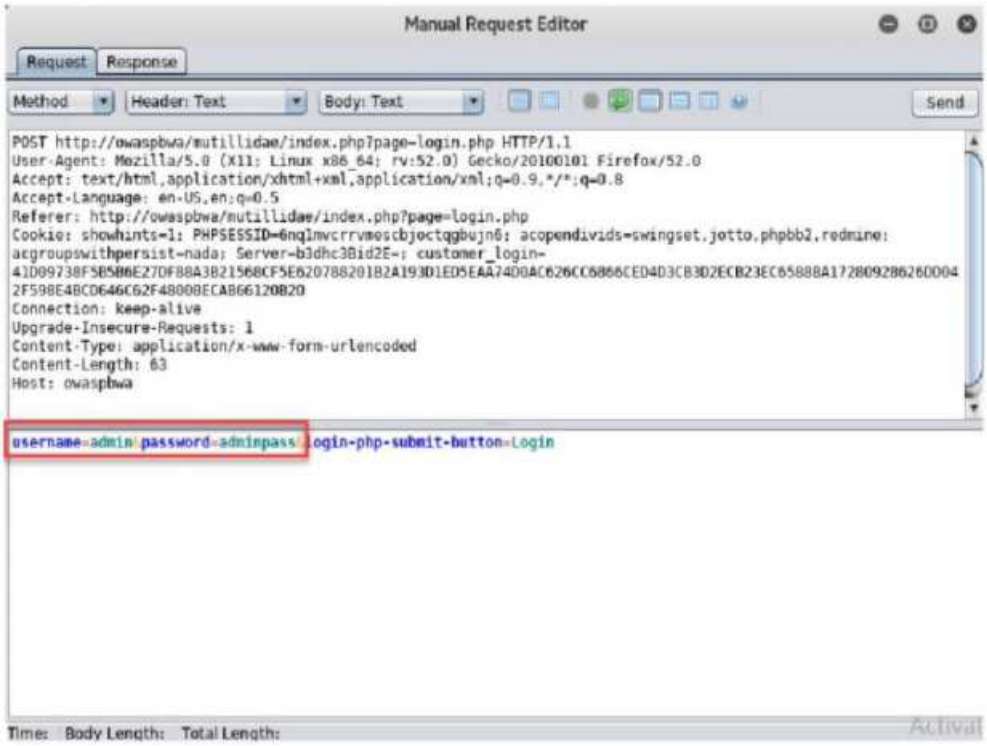
36. En plus de la taille différente de tout le reste, nous obtenons la " Reason " comme " Found " et le "Code" comme "302" qui signifie "REDIRECT", une manière très courante d'envoyer les utilisateurs vers une autre page où l'utilisateur est déjà connecté

37. Ayant trouvé le nom d'utilisateur et le mot de passe corrects, il nous suffit de voir de quelle paire il s'agit et de l'essayer dans le navigateur.

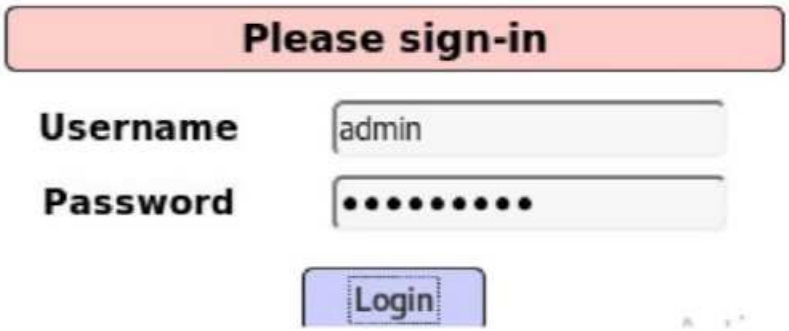
38. Faites un clic droit sur la ligne et cliquez sur " Open/Resend with Request Editor..."



39. L'écran montre que le nom d'utilisateur est "admin" et le mot de passe "adminpass"



40. Vous pouvez aller l'essayer sur l'écran réel.



41. Congratulations! vous êtes maintenant authentifié!

42. Cliquez sur le lien "Déconnexion" pour terminer l'exercice

43. Vous savez maintenant effectuer une attaque par dictionnaire.