Etap 1

Wstęp

Po odpaleniu serwera i wejściu na wypisany w konsoli adres http, powinnaś/powinieneś zobaczyć formularz logowania. Spróbuj wpisać do niego jakieś wartości, co widzisz?

Wykorzystanie exploitu

Formularz jest skonstruowany w taki sposób, że zawiera krytyczną podatność, mianowicie rodzielony jest błąd nazwy użytkownika oraz hasła.

Co to oznacza?

W dobrze działającej aplikacji mamy jeden komunikat w stylu: "Nieprawidłowa nazwa użytkownika lub hasło", natomiast tutaj widzimy sytuację wprost przeciwną. Podawany jest błąd "Podany użytkownik nie istnieje". Dzięki temu, jesteśmy w stanie użyć hydry do zgadnięcia nazwy użytkownika, ponieważ jesteśmy w stanie stwierdzić, który użytkownik istnieje w bazie danych, a który nie. Następnym krokiem jest złamanie hasła dla naszego odgadniętego użytkownika.

Użycie THC Hydra

Przykładowe polecenie w programie:

```
hydra -t 1 -l nazwa_uzytkownika -P zbior_hasel.txt -s 5000
[ip_serwera_lokalnego] http-post-form
"/login:username=^USER^&password=^PASS^:Blad uzytkownika lub hasla"
```

Ważniejsze paramtery:

- -t -> Wskazujemy na ilu taskach hydra ma pracować (najlepiej wprowadzić tutaj górną wartość, czyli 64. Znacznie przyspiesza proces)
- -l lub -L -> nazwa lub zbiór nazw użytkownika do wprowadzania przez program
- -p lub -P -> hasło lub zbiór haseł do wprowadzania przez program

Zadanie

Twoim zadaniem jest poprawne zalogowanie się bazując na przykładowym poleceniu. Użyj plików common_usernames.txt oraz common_passwords.txt.