Lab: OS command injection, simple case

Zapytanie idzie jako POST, w body są parametry, dopisujemy do domyślnej wartości w tym parametrze komendę |whoami, co skutkuje wypisaniem na stronie wyniku tej komendy

Lab: Blind OS command injection with time delays

Podatny jest parameter w body (email), dopisujemy do niego ||ping+-c+10+127.0.0.1||

Pałki rozpoczynają i kończą komendę, tutaj jest to istotne ponieważ po tym parametrze idą następne parametry.

Lab: Blind OS command injection with output redirection

Dostajemy informację, że jest folder możliwy do edycji, więc wykorzystujemy podatny parametr email do zapisania do niego pliku. Dodajemy do parametru email w elemencie feedback komendę ||whoami>/var/www/images/output.txt|| która dodaje nam plik outputu do danego folderu. Następnie lokalizuję funkcjonalnosc strony, gdzie występuje zaciąganie plików z tego folderu. Zmieniamy tam nazwę zaciąganego pliku obrazka na nazwę pliku który właśnie dodaliśmy za pomocą podatnego parametru. W efekcie, gdy przenalizujemy odpowiedź zapytania, widzimy wynik komendy.