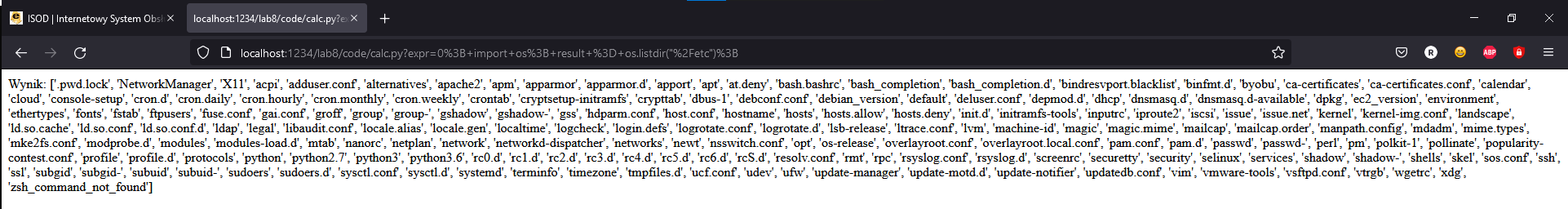
Code Injection:

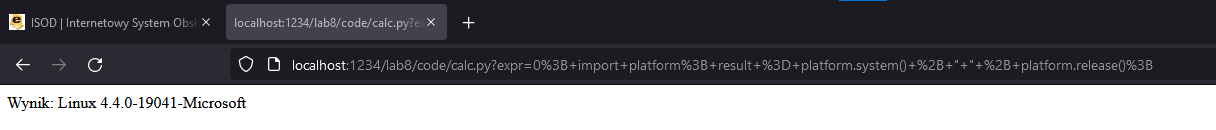
-wyświetlenie zawartości katalogu /etc/ na serwerze,

„0; import os; result = os.listdir("/etc");”



- rozpoznanie nazwy i wersji systemu operacyjnego serwera,

„0; import platform; result = platform.system() + " " + platform.release();”



- ściągnięcie z sieci dowolnego pliku i uruchomienie go.

//

2. Zablokowanie ataku (walidacja danych)

…

v = re.search('[a-zA-Z]', expr)

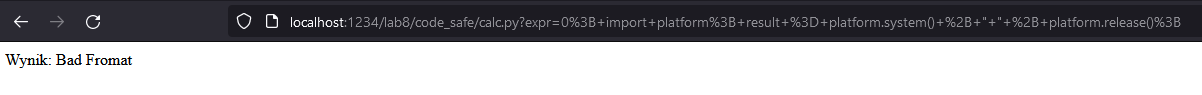
if(v == None):

exec "result=%s" % expr

else:

result = "Bad Fromat";

…



Obraz zawierający tekst

Opis wygenerowany automatycznie

SQL Injection:

1. Uruchom aplikację sql\_secrets.py, a następnie zademonstruj w jaki sposób można wykraść wszystkie sekrety.

Polecenie: ' UNION SELECT \* FROM secrets '

Obraz zawierający tekst

Opis wygenerowany automatycznie  
2. W jaki sposób atakujący może poznać wszystkie pola key?

Polecenie: ' UNION Select "s", key FROM secrets '

Obraz zawierający tekst

Opis wygenerowany automatycznie

3. Zaproponuj modyfikację programu blokującą omawiany atak.

…  
key = key.replace("'", "");

…  
Test:

