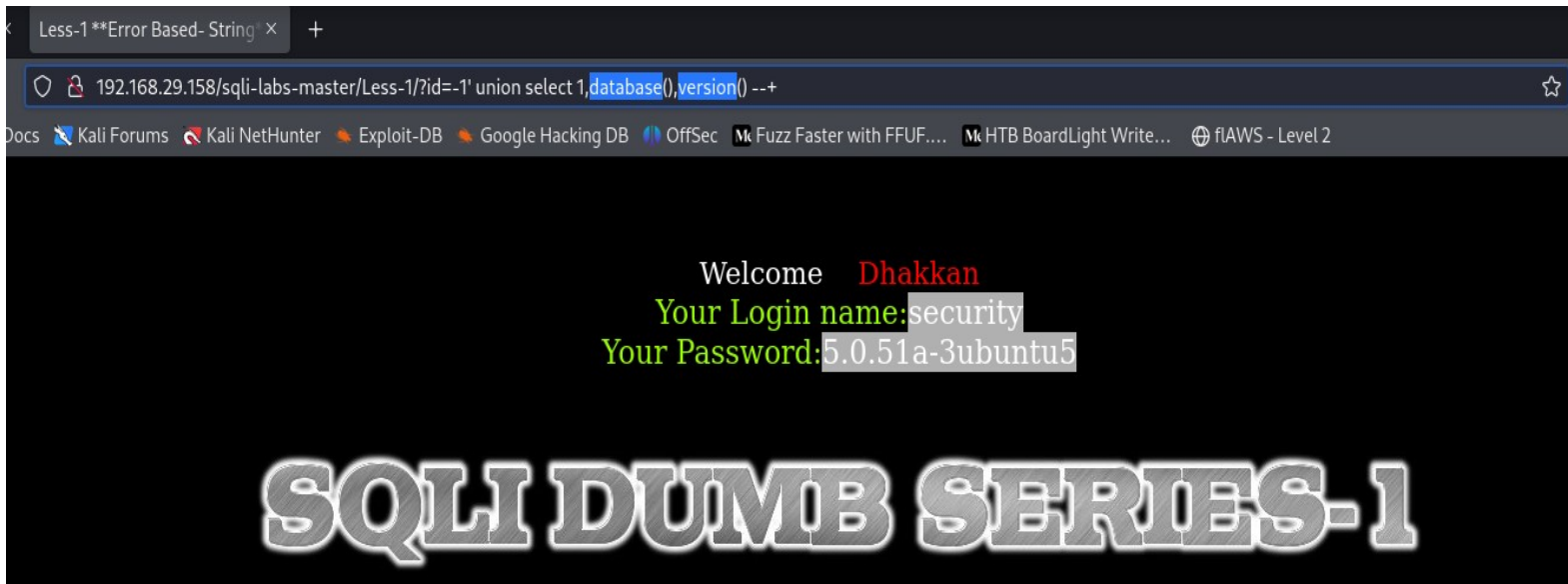# SQLi-Labs
Lesson 1: GET - Error Based - Single quotes - String

Balancing = Apostrophe (')
Type of Injection = get union based – Single quotes
No of Columns = 3
Database name = security
Database version = 5.0.51a-3ubuntu5
Union based conditions are accepting by website, which states SQL injection is possible.

Lesson 2 - GET-Error Based – integer based

Balancing = Space ( )
Type of Injection = Error Based – integer based
Condition = or 1=1
Integer based conditions are accepting by website, which states SQL injection is possible.

Lesson 3 – GET Error based – Single quotes with twist – string

Balancing = Apostrophe Closed parenthesis (‘))
Type of Injection = Error Based - Single quotes
Condition = ‘) or ‘1’=(‘1 ’)
Integer based conditions are accepting by website, which states SQL injection is possible.
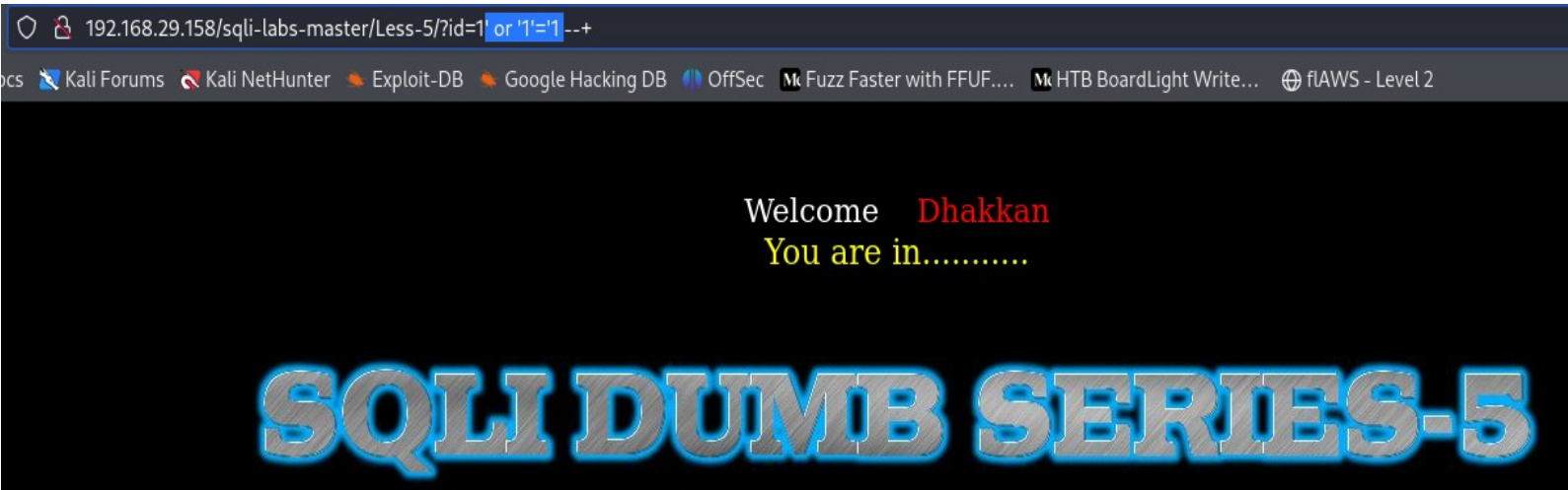
Lesson 4- Error Based-Double quotes – string

Balancing = Apostrophe Closed parenthesis (“))
Type of Injection = Error Based - Double quotes
Condition = ") or ("1")=("1
Integer based conditions are accepting by website, which states SQL injection is possible.

Lesson-5 Double Query – Single Quotes – String

Balancing = Apostrophe Closed parenthesis (')
Type of Injection = Error Based – single quote
Condition = ' or '1'='1
Integer based conditions are accepting by website, which states SQL injection is possible.

Lesson-6 Double Query-Double quotes – String

Balancing = Apostrophe Closed parenthesis (')
Type of Injection = Error Based – double quotes
Condition = " or "1""=”1
Integer based conditions are accepting by website, which states SQL injection is possible.