SQLi Basic 2

Description

The hint shows that it hates

- The password is hashed for database comparison
- System filters out some characters it hates like comments

Solution

```
'or 1=1 or ''='
```

Why is this the solution?

- The payload `'or 1=1 or ''='` is a classic example of a SQL injection payload that bypasses the authentication mechanism.
- The payload is designed to return all rows from the `users` table by making the condition `1=1` always evaluate to true.
- The payload uses the `OR` operator to combine multiple conditions, effectively bypassing the authentication mechanism.
- The payload also uses the `''='` condition to ensure that the injected SQL statement is syntactically correct.
- The payload does not contain any comments or other characters that might be filtered out by the system, making it a reliable and effective injection payload.
- When this payload is injected into a vulnerable SQL query, it effectively changes the query to `SELECT * FROM users WHERE username = ''or 1=1 or ''='' AND password = 'password'`. This query will return all rows from the `users` table, effectively bypassing the authentication mechanism.