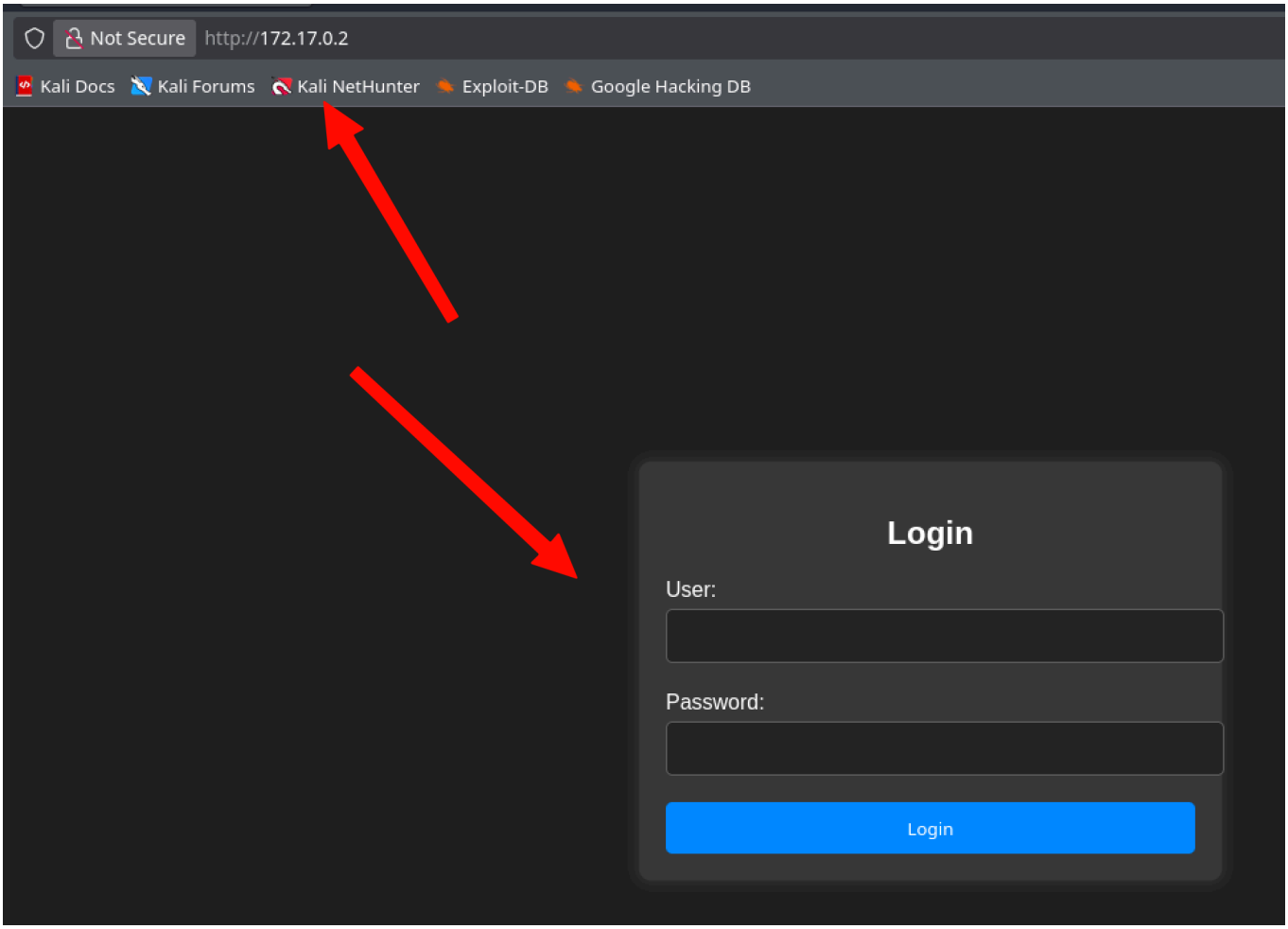
CTF Writeup — SQL Injection en formulario de login

1. Formulario vulnerable

Tenemos un formulario de login:



2. Payload de inyección SQL

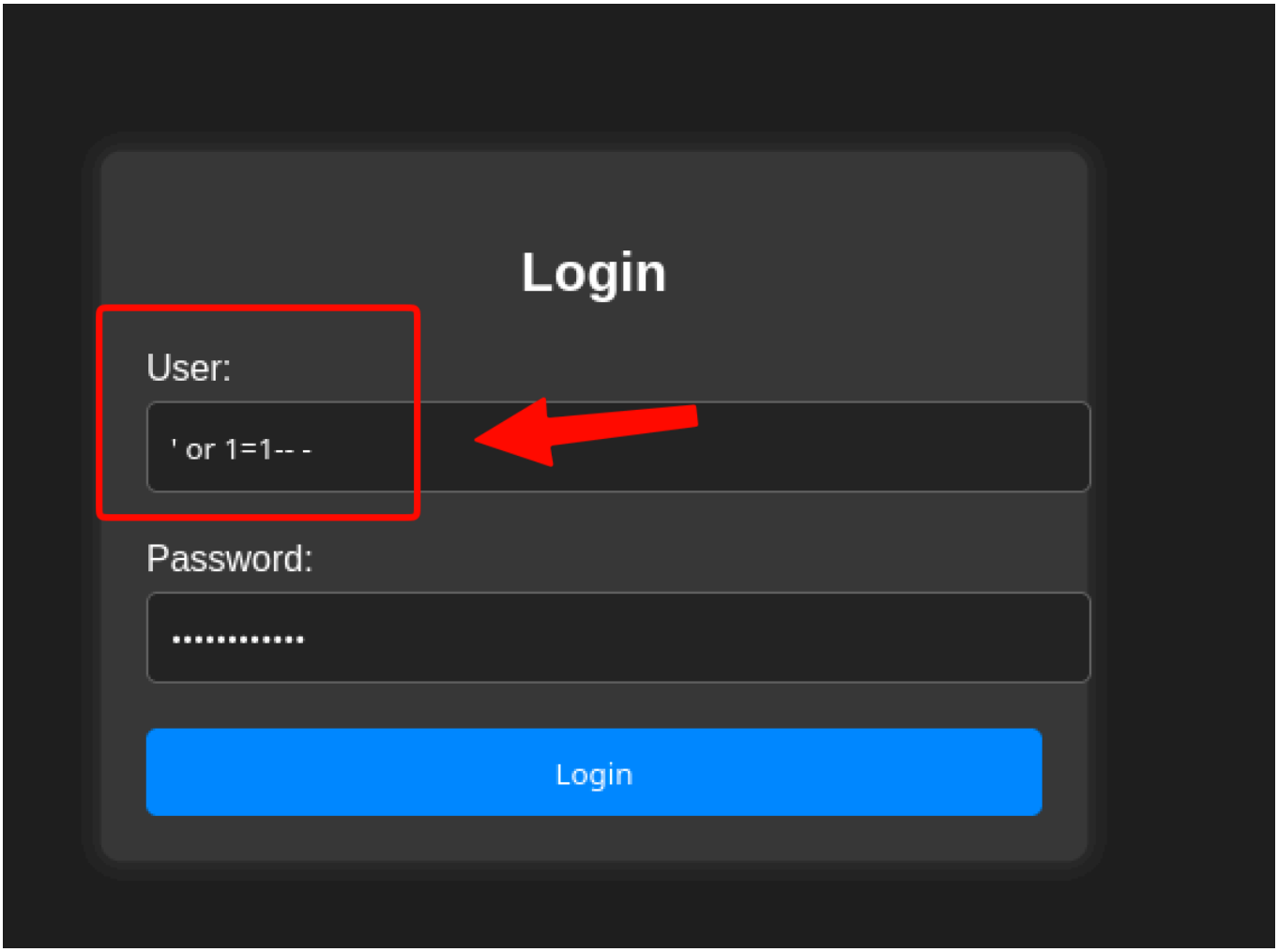
El formulario es vulnerable a un payload de SQLi. Usamos el siguiente payload en el campo correspondiente (por ejemplo, en el campo de usuario o contraseña):

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

Este payload funciona de la siguiente manera:

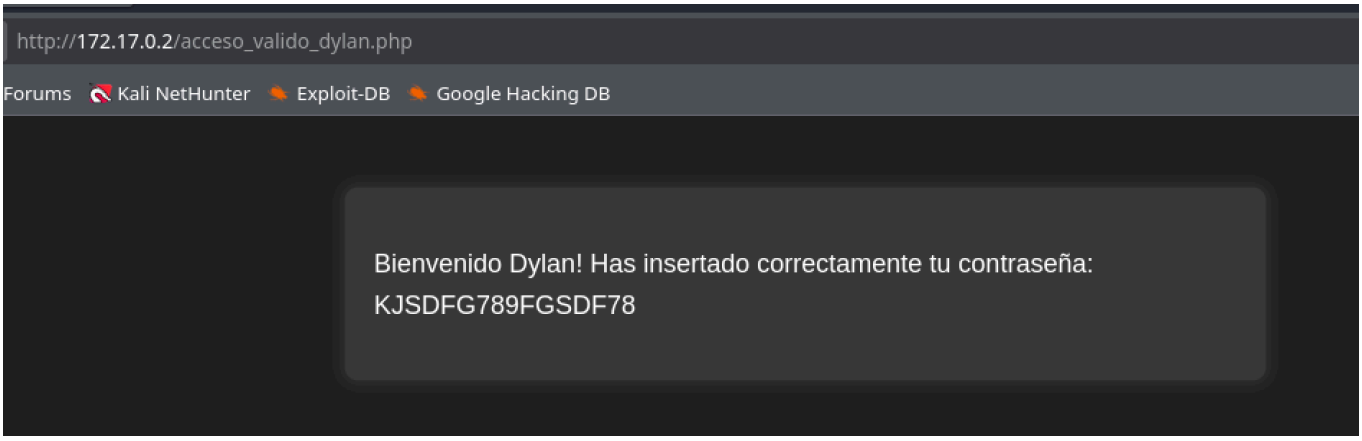
- La comilla simple `'` cierra la cadena de texto de la consulta SQL original.
- `or 1=1` añade una condición que siempre es verdadera.
- `-- -` comenta el resto de la consulta original, evitando errores de sintaxis.

Así se ve el payload aplicado en el formulario:



3. Resultado del ataque

Comprobamos si el ataque ha funcionado:



✅ El ataque ha funcionado correctamente, logrando eludir la autenticación del formulario.

Notas

- Este tipo de vulnerabilidad se debe a la falta de sanitización/parametrización de las consultas SQL.
- Como mitigación, se recomienda usar **prepared statements** (consultas parametrizadas) en lugar de concatenar directamente la entrada del usuario en la query SQL.