



checking password

*name=Alice&pwd=pass4alice*



*/signin/*





## Login

Username:

Password:

☐ Remember me

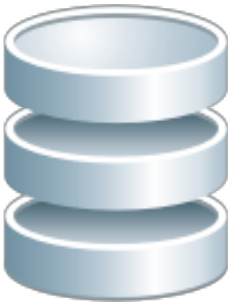
Login »

Access Granted!











# Checking password

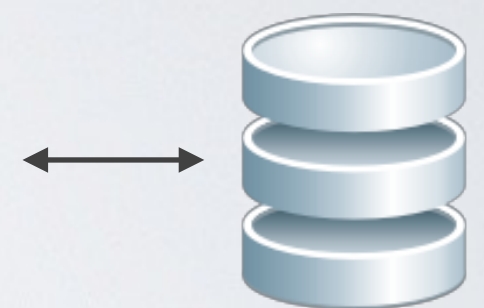
signin.html



A screenshot of the WordPress login form. It features a blue background with the WordPress logo at the top. Below the logo, the word "Login" is displayed. There are two input fields: "Username:" and "Password:". Below the password field is a checkbox labeled "Remember me". At the bottom right, there is a button labeled "Login »".

*name=Alice&pwd=pass4alice*

/signin/



Access **Granted!**

# Bypassing password check

```
db.run("SELECT * FROM users  
WHERE USERNAME = ' " + username + " '  
      AND PASSWORD = ' " + password + " ' ")
```

```
username: alice  
password: pass4alice
```