



WHAT IS THE VULNERABILITY SHOWN IN THIS CODE?

```
<!DOCTYPE html>
 2
     <html lang="en">
 3
     <head>
 4
         <meta charset="UTF-8">
 5
         <meta http-equiv="X-UA-Compatible" content="IE=edge">
         <meta name="viewport" content="width=device-width, initial-scale=1.0">
 6
 7
         <title>I'm Secureeeeeeeee</title>
 8
     </head>
 9
     <body>
         <h1>Very Secure Website</h1>
10
         <form method="GET" action="">
11
             <label for="input">Enter your name:</label>
12
             <input type="text" id="input" name="username">
13
             <button type="submit">Submit</button>
14
15
         </form>
16
         17
18
             Hello, <span id="name"></span>
         19
20
21
         <script>
22
             const urlParams = new URLSearchParams(window.location.search);
23
             const username = urlParams.get('username');
24
25
             if (username) {
                 document.getElementById('name').innerHTML = username;
26
27
28
         </script>
29
     </body>
30
     </html>
```





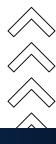
WHAT IS THE VULNERABILITY SHOWN IN THIS CODE?

```
<?php
 2
     $servername = "localhost";
 3
     $username = "root";
     $password = "";
 4
 5
     $dbname = "testdb";
 6
7
     $conn = new mysqli($servername, $username, $password, $dbname);
 8
9
     if ($conn->connect_error) {
10
         die("Connection failed: " . $conn->connect_error);
11
12
     if (isset($_GET['id'])) {
13
         $id = $_GET['id'];
14
15
16
         $sql = "SELECT * FROM users WHERE id = $id";
         $result = $conn->query($sql);
17
18
         if ($result->num_rows > 0) {
19
             while($row = $result->fetch_assoc()) {
20
                  echo "User: " . $row['username'] . "<br>";
21
22
         } else {
23
             echo "No user found.";
24
25
26
27
28
     $conn->close();
29
```





WHAT IS THE VULNERABILITY SHOWN IN THIS CODE?







IDENTIFY THE RED FLAGS IN THE FOLLOWING CODE:

```
from flask import Flask, request, redirect, session, render_template_string
     app = Flask(__name__)
     app.secret_key = 'supersecretkey'
4
  v users db = {
          'admin': 'password123',
         'user1': 'mypassword',
6
 7
         'user2': 'letmein'
8
9
     @app.route('/')
10 v def index():
         if 'username' in session:
11 \
12
             return f"Hello, {session['username']}! <a href='/logout'>Logout</a>"
13
         return "You are not logged in. <a href='/login'>Login here</a>"
14
     @app.route('/login', methods=['GET', 'POST'])
15 v def login():
         if request.method == 'POST':
16
             username = request.form.get('username')
17
             password = request.form.get('password')
18
19
20 V
             if username in users_db and users_db[username] == password:
                 session['username'] = username
21
22
                 return redirect('/')
23 V
             else:
                 return "Invalid credentials. Try again."
24
25
         return render template string('''
26 V
27
             <form method="POST">
                 Username: <input type="text" name="username"><br>
28
29
                 Password: <input type="password" name="password"><br>
                 <input type="submit" value="Login">
30
             </form>
31
          "")
32
     @app.route('/logout')
33
34 ∨ def logout():
35
         session.pop('username', None)
36
         return redirect('/')
```