



WHAT IS THE VULNERABILITY SHOWN IN THIS CODE?

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



WHAT IS THE VULNERABILITY SHOWN IN THIS CODE?

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



WHAT IS THE VULNERABILITY
SHOWN IN THIS CODE?

```
1  <?php
2  if (isset($_GET['ip'])) {
3      $ip = $_GET['ip'];
4
5      $output = shell_exec("ping -c 4 " . $ip);
6
7      echo "<pre>$output</pre>";
8  }
9  ?>
```





IDENTIFY THE RED FLAGS IN THE FOLLOWING CODE:

```
1  from flask import Flask, request, redirect, session, render_template_string
2  app = Flask(__name__)
3  app.secret_key = 'supersecretkey'
4  users_db = {
5      'admin': 'password123',
6      'user1': 'mypassword',
7      'user2': 'letmein'
8  }
9  @app.route('/')
10 def index():
11     if 'username' in session:
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 def login():
16     if request.method == 'POST':
17         username = request.form.get('username')
18         password = request.form.get('password')
19
20         if username in users_db and users_db[username] == password:
21             session['username'] = username
22             return redirect('/')
23         else:
24             return "Invalid credentials. Try again."
25
26     return render_template_string('''
27         <form method="POST">
28             Username: <input type="text" name="username"><br>
29             Password: <input type="password" name="password"><br>
30             <input type="submit" value="Login">
31         </form>
32     ''')
33 @app.route('/logout')
34 def logout():
35     session.pop('username', None)
36     return redirect('/')
```