

```
1: <?
2:     /**
3:      * xss.php
4:      *
5:      * Demonstrates cross-site scripting.
6:      *
7:      * David J. Malan
8:      * Dan Armendariz
9:      * Computer Science E-75
10:     * Harvard Summer School
11:     */
12:
13:     // enable sessions
14:     session_start();
15:
16:     // set a cookie
17:     setcookie("secret", "12345");
18: ?>
19:
20: <!DOCTYPE html PUBLIC
21:     "-//W3C//DTD XHTML 1.0 Transitional//EN"
22:     "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
23:
24: <html xmlns="http://www.w3.org/1999/xhtml">
25:     <head>
26:         <title></title>
27:     </head>
28:     <body>
29:         <form action="xss2.php" method="get">
30:             <input name="name" type="text" />
31:             <input type="submit" value="Say My Name" />
32:         </form>
33:     </body>
34: </html>
```

```
1: <?
2:     /**
3:      * xss2.php
4:      *
5:      * Demonstrates cross-site scripting.
6:      *
7:      * David J. Malan
8:      * Dan Armendariz
9:      * Computer Science E-75
10:     * Harvard Summer School
11:     */
12: ?>
13:
14: <!DOCTYPE html PUBLIC
15:     "-//W3C//DTD XHTML 1.0 Transitional//EN"
16:     "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
17:
18: <html xmlns="http://www.w3.org/1999/xhtml">
19:     <head>
20:         <title></title>
21:     </head>
22:     <body>
23:         <h1>Hello, <? echo $_GET["name"]; ?></h1>
24:     </body>
25: </html>
```