

HW6 (8 points)

Q1 (6 points) Given the php file and the css file (*HW6security.php*, *style.css*) with the form below, craft inputs to deface the webpage:

Original page:

Deface the webpage!

Enter here:

Try it!

- 1) (2 points) Craft an input to display a message on a new line: “Yes, I am a hacker.” after hitting the “Try it!” button:

Deface the webpage!

Enter here:

Yes, I am a hacker.

Try it!

Give your answer (input) here, and provide a screenshot of the defaced webpage:

">

Yes, I am a hacker.<?="

← ↻ ⓘ localhost/Assignment%206/H... A 🔍 ☆ ⋮

Deface the webpage!

Enter here:

Yes, I am a hacker. Try it!

- 2) (2 points) Craft an input to display an image of your own choice after hitting the “Try it!” button:

Deface the webpage!

Enter here:




Give your answer (input) here, and provide a screenshot of the defaced webpage:

">
<img
src=https://th.bing.com/th/id/OIP.PYipJ_hSncugM2SwnZitvgHaEK?w=296&h=180&c=7&r=0&o=5&dpr=1.5&pid=1.7

← ↻ ⓘ localhost/Assignment%206/H... 🔊 🔍 ☆ ⌵ 📱 👤 ⋮

Deface the webpage!

Enter here:



- 3) (2 points) Revise the code in the php file to avoid such HTML injections. Write the new part of code here (not the codes of the whole php file).

```
<input name="hacker" id="hacker" type="text" size="12pt" value="<?=htmlentities($myinput)?>"/>
```

Q2 (2 points) Given the *SkywardFlyers.php* and *ValidateUser.php* file in the *Flyer1.zip* (you can download from Canvas), with a part of the codes and screenshot below:

- Part of the codes in *ValidateUser.php*:

```
$Email=$_GET['email'];
$Password = $_GET['password'];

//connecting to the database with PDO
require_once("config.php");

$TableName = "frequent_flyers";

$sql = "SELECT * FROM $TableName
        WHERE email = '$Email'
        AND password = '$Password'";
$result = $pdo->query($sql);

if(!$row = $result->fetch())
    exit("You must enter a valid email address and password.");
else {
    $FlyerID = $row['flyerID'];}
```

- Part of screenshot of *SkywardFlyers.php*

Returning Flyers

E-mail Address	Password
<input type="text"/>	<input type="password"/>
<input type="button" value="log in"/>	

Suppose there is already a registered flyer (user account) with email as myemail@csusm.edu, craft two different password inputs to successfully log into the website without knowing its correct password.

Give your answer (crafted password input) here:

(1) Password 1:

anything' or 'x'='x

(2) Password 2:

hi' or 'l'='l

Late submissions: Late submissions are accepted up to 24 hours with 10% of penalty. No submission later than 24 hours.