Web Form 2 Instructions

Step 1:

First open up any web-browser, and go to webpuzzle.pythonanywhere.com.

Step 2:

Click in the Register link in the top right of the main website, or if you have an account already click the Log In option next to Register.

To register for an account all you need is to create your user name, give a valid e-mail, and create a password to use.

If you had to register then check your email and click on the link in an email to activate the account, return to webpuzzle.pythonanywhere.com and log in.

Step 3:

After you have logged in, you can tell because of the change in the links at the top right of the web page, if you haven't gone back to the main web page then return there.

Step 4:

When on the main web page look the right with all of the level menus available, and click on Level 2 in the Web Form Challenges section.

Step 5 (Fuzzing):

Now when the web form comes up it will be randomly chosen from several. What your objective here is is to find all of the problems in the form, and what may trigger unexpected behavior server side:

None: There are no seen weaknesses for this input field.

Having no maximum length: The input field has not maximum length and when submitting the form the website still accepts it. Not having a length can cause a lot of problems server side if it goes unchecked. This can lead to a system crash for the server, or even something like SQL truncation and give an attacker administration level privileges.

Not checking Formatting: The program that checks the information in the background when submitting doesn't make sure that the format of the information given matches theirs. This can cause parsing errors, or even allow code injection which also may lead to some unexpected behavior for the web server taking this form.

Not validating any information: This is when the program in the background doesn't correctly check the information given leading to some logical errors. As far as logical errors not really seeming like a big deal when it comes to your birthday, it can vastly effect a bank transaction on-line by allowing negative values for the transfer. That would allow you to just take money from whatever other account your transaction is involved with.

Or some combination of the last three vulnerabilities. To test for these vulnerabilities in any input field:

For max length, try to give it some huge number of characters for the form to use.

For Formatting, try to give the form input doesn't expect, like special symbols (<>! #) or input it doesn't expect, like letters instead of numbers.

For Validating, try to see if there is some logical errors you can create like it taking a birthday that hasn't even happened (9/13/2019), or possibly it doesn't even check if the emails or passwords given match the confirming versions.

Step 6 (All vulnerabilities are found):

After you have found all the vulnerabilities are found, then click on the button on the bottom to expose a submission sheet for you to put the answers in. After all of your answers are on the sheet, then hit the submit button to receive your grade.

Cheat sheet for form vulnerability puzzle

Answer options:

0: None

1: It does not have a maximum length

2: It does not validate the information given

3: It does not check the formatting of the information

Random _number

0:

UserName = ["None"];

Email = ["It does not have a maximum length", "It does not validate the information given"];

Confirm Email = ["It does not validate the information given"];

Password = ["None"];

Confirm Password = ["It does not have a maximum length"];

First Name = ["It does not have a maximum length"];

LastName = ["It does not check the formatting of the information"];

Middle Initial = ["It does not have a maximum length"];

Phone Number = ["It does not check the formatting of the information"];

BrithDay = ["None"];

1:

UserName = ["None"];

Email = ["It does not validate the information given"];

Confirm Email = ["It does not validate the information given"];

Password = ["It does not have a maximum length", "It does not check the formatting of the information"];

Confirm Password = ["It does not check the formatting of the information"];

First Name = ["It does not check the formatting of the information", "It does not have a maximum length"];

LastName = ["None"];

Middle Initial = ["It does not check the formatting of the information", "It does not have a maximum length"];

Phone Number = ["None"];

BrithDay = ["It does not validate the information given"];

2:

UserName = ["It does not check the formatting of the information"];

Email = ["It does not have a maximum length"];

Confirm Email = ["None"];

Password = ["It does not have a maximum length", "It does not validate the information given"];

Confirm Password = ["It does not validate the information given"];

First Name = ["None"];

LastName = ["None"];

Middle Initial = ["It does not check the formatting of the information"];

Phone Number = ["It does not check the formatting of the information", "It does not have a maximum length"];

BrithDay = ["It does not check the formatting of the information"];

3:

UserName = ["It does not have a maximum length"];

Email = ["It does not check the formatting of the information", "It does not validate the information given"];

Confirm Email = ["It does not check the formatting of the information", "It does not validate the information given"];

Password = ["It does not check the formatting of the information", "It does not validate the information given"];

Confirm Password = ["It does not check the formatting of the information", "It does not validate the information given", and "It does not have a maximum length"];
First Name = ["None"];
LastName = ["It does not check the formatting of the information"];
Middle Initial = ["None"];
Phone Number = ["It does not have a maximum length"];
BrithDay = ["None"];

4:
UserName = ["It does not have a maximum length", "It does not check the formatting of the information"];
Email = ["None"];
Confirm Email = ["It does not have a maximum length"];
Password = ["It does not validate the information given"];
Confirm Password = ["It does not validate the information given"];
First Name = ["It does not have a maximum length", "It does not check the formatting of the information"];
LastName = ["None"];
Middle Initial = ["None"];
Phone Number = ["None"];
BrithDay = ["It does not check the formatting of the information", "It does not have a maximum length"];

5:
UserName = ["None"];
Email = ["It does not validate the information given"];
Confirm Email = ["It does not validate the information given", "It does not check the formatting of the information"];
Password = ["It does not have a maximum length", "It does not check the formatting of the information", "It does not validate the information given"];
Confirm Password = ["It does not check the formatting of the information", "It does not validate the information given"];
First Name = ["It does not check the formatting of the information"];
LastName = ["None"];
Middle Initial = ["It does not have a maximum length"];
Phone Number = ["It does not have a maximum length"];
BrithDay = ["None"];

6:
UserName = ["It does not have a maximum length", "It does not check the formatting of the information"];
Email = ["None"];
Confirm Email = ["None"];
Password = ["It does not check the formatting of the information", "It does not validate the information given"];
Confirm Password = ["It does not check the formatting of the information", "It does not validate the information given"];
First Name = ["None"];
LastName = ["It does not have a maximum length"];
Middle Initial = ["It does not check the formatting of the information"];
Phone Number = ["It does not check the formatting of the information"];
BrithDay = ["It does not validate the information given"];

7:
UserName = ["It does not have a maximum length"];
Email = ["It does not have a maximum length", "It does not check the formatting of the information", "It does

not validate the information given"];

Confirm Email = ["It does not have a maximum length", "It does not check the formatting of the information", "It does not validate the information given"];

Password = ["None"];

Confirm Password = ["None"];

First Name = ["None"];

LastName = ["None"];

Middle Initial = ["It does not have a maximum length", "It does not check the formatting of the information"];

Phone Number = ["It does not have a maximum length", "It does not check the formatting of the information"];

BrithDay = ["None"];

8:

UserName = ["It does not check the formatting of the information"];

Email = ["None"];

Confirm Email = ["None"];

Password = ["It does not have a maximum length"];

Confirm Password = ["None"];

First Name = ["It does not have a maximum length"];

LastName = ["None"];

Middle Initial = ["It does not check the formatting of the information"];

Phone Number = ["It does not have a maximum length", "It does not check the formatting of the information"];

BrithDay = ["It does not have a maximum length", "It does not check the formatting of the information", "It does not validate the information given"];

9:

UserName = ["It does not have a maximum length"];

Email = ["It does not have a maximum length", "It does not check the formatting of the information", "It does not validate the information given"];

Confirm Email = ["It does not have a maximum length", "It does not check the formatting of the information", "It does not validate the information given"];

Password = ["None"];

Confirm Password = ["It does not have a maximum length"];

First Name = ["None"];

LastName = ["It does not have a maximum length", "It does not check the formatting of the information"];

Middle Initial = ["It does not have a maximum length"];

Phone Number = ["None"];

BrithDay = ["It does not check the formatting of the information"];