XSS-Game

Hint and Solution to XSS Game on Appspot

Level 1

Hint

The textbox will include any html in page including tags.

Solution

Type `<script>alert("GG")</script>` and it will give you the popup.

Level 2

Hint

If you read the hints of the level, then you should already know what to do

Solution

Use the `<img />` tag and its `onerror` attribute. `<img src="forbidden" onerror="alert('GG')" />`

Level 3

Hint

Go on and click on the tabs and notice how the URL changes. Not only the URL changes but the page also generates an HTTP GET request. Enter something like `#11` at the end of url instead of `#1` (Why 11? Well, 11 is my birth date. The more you know! :P). So this time no image loads. That's fine but we need a little bit more information.
Let's look at the source. Open up `index.html` given in Target Code. The sweet stuff we need is at line `17`.

```
html += "<img src='/static/level3/cloud" + num + ".jpg' />";
```

Hmmm, `onerror`? ;)

Solution

Changing the line to something like this, we can use `onerror` again!

```
html += "<img src='/static/level3/cloud" + "11.jpg' onerror='alert("GG")' alt='" +
".jpg' />";
```

So use `#11.jpg' onerror='alert("GG")' alt='` in URL.

Level 4

Hint

Directly inserting JS in the textbox won't work. But there's still a way to do this. See `timer.html` line `21`

Solution

`10');alert('GG` gives us what we need. Line `21` converts to

```
<img src="/static/loading.gif" onload="startTimer('10');alert('GG');" />`
```

Level 5

Hint

Read Hints on the level and then this if you are clueless. And now read the source! ... Still nothing? Uh, ok ... Look at `welcome.html` line `13` and `signup.html` line `15`. See if you can use those parameters.

Solution

The URL `signup?next=javascript:alert('GG')` is what you need.

Level 6

Hint

Line `26` of `index.html` contains all the hints we need. We can't load a script that contains `http://` or `https://` in the beginning. Is there any other way?

Solution

So how do we tackle this? Well, simple just omit the `http:` or `https:` part. This way the request decides for itself which protocol is the best. Upload a js file containing `alert("GG")` anywhere and copy the url except the `http:/https:` part after the `#` in URL.

And we're done!

Here's the cake: