**Project 4:**

**Web Security Report Entry**

*Fall 2020*

## **Task 1 – Warm Up Exercises**

**Activity 1 - The Inspector & Console tabs**

1. What is the value of the ‘CanYouSeeMe’ input? *Do not include quotes in your answer.*

TheCakeIsALie

1. The page references a single JavaScript file in a script tag. Name this file including the file extension. *Do not include the path, just the file and extension. Ex: “ajavascriptfile.js”.*

/js/cs6035.js

1. The script file has a JavaScript function named ‘runme’. Use the console to execute this function. What is the output that shows up in the console?

I’m a teapot

**Activity 2 - Network Tab**

1. What request method (http verb) was used in the request to the server?

POST

1. What status code did the server return? *Include both the code and description. Ex: “200 Ok”*

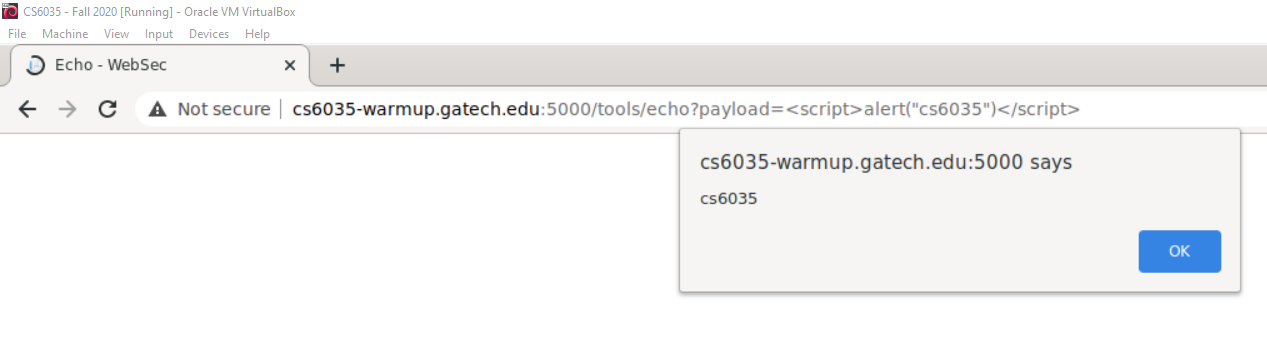
418 I’m a teapot

1. The server returned a cookie named ‘coffee’ for the browser to store. What is the value of this cookie? *Do not include quotes in your answer.*

With\_Cream

**Activity 3 - Built-in browser protections**

1. You can do more than just echo back text. Construct a URL such that a JavaScript alert dialog appears with the text cs6035 on the screen. Upload **activity3.html** and paste in a screenshot of the page with the dialog as your answer below. Be sure to include the URL of the browser in your screenshot.



**Activity 4 - Submitting forms**

1. Copy and paste below the entire output message you see and submit that as your answer to this activity. Upload **activity4.html** which is the form that you constructed.

**Activity 5 - Accessing the DOM with JavaScript**

1. Upload **activity5.html** which is the form that you constructed. No other answers are required for this activity.

## **Task 5 – Epilogue Questions**

**Target 1 Epilogue**

1. List the PHP page and lines that should be changed to fix the vulnerability.
2. Describe in detail why the code listed in the line numbers above are vulnerable. You’re free to use generalized concepts to help show your understanding but we also need to know details that pertain to this target and assignment. A definition of XSRF is not what we’re looking for.
3. Explanation of how to fix the code. Feel free to include snippets and examples. Be detailed!

**Target 2 Epilogue**

1. List the PHP page and lines that should be changed to fix the vulnerability.
2. Describe in detail why the code listed in the line numbers above are vulnerable. You’re free to use generalized concepts to help show your understanding but we also need to know details that pertain to this target and assignment. A definition of XSS is not what we’re looking for.
3. Explanation of how to fix the code. Feel free to include snippets and examples. Be detailed!
   1. Be careful with your explanation here. There are wrong ways to fix this vulnerability. Hint: Never write your own crypto algorithms. This concept extends to XSS sanitization.
   2. Warning: Removing site functionality will not be accepted here.

**Target 3 Epilogue**

1. List the PHP page and lines that should be changed to fix the vulnerability.
2. Describe in detail why the code listed in the line numbers above are vulnerable. You’re free to use generalized concepts to help show your understanding but we also need to know details that pertain to this target and assignment. A definition of SQL Injection is not what we’re looking for.
3. Explanation of how to fix the code. Feel free to include snippets and examples. Be detailed!
   1. Be careful with your explanation here. There are wrong ways to fix this vulnerability. Hint: Never write your own crypto algorithms. This concept extends to SQL sanitization.

**Additional Targets**

1. Describe any two additional issues (they need not be code issues) that create security holes in the site.
2. Provide an explanation of how to safely fix the identified issues. Feel free to include snippets and examples. Be detailed!

**Works Cited**

**You are required to include works cited**

**When complete, please save this form as a PDF and submit with your HTML files as “report.pdf”. Do not zip up anything!**