

CSC 515: Spring 2023 – Workshop 6: Sensitive Data Exposure

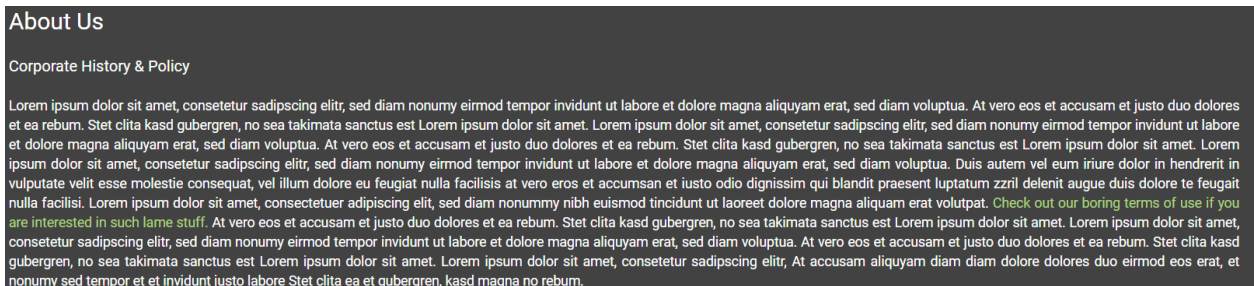
In this workshop, we will exploit a vulnerable web application by exposing sensitive information

For this workshop, you'll need to complete the following tasks and then answer questions in Gradescope.

#	Task	Description
1	Coupon codes	Access coupon codes in the web application
2	Easter Egg	Access an Easter egg
4	On Your Own	Perform additional attacks and report on your progress

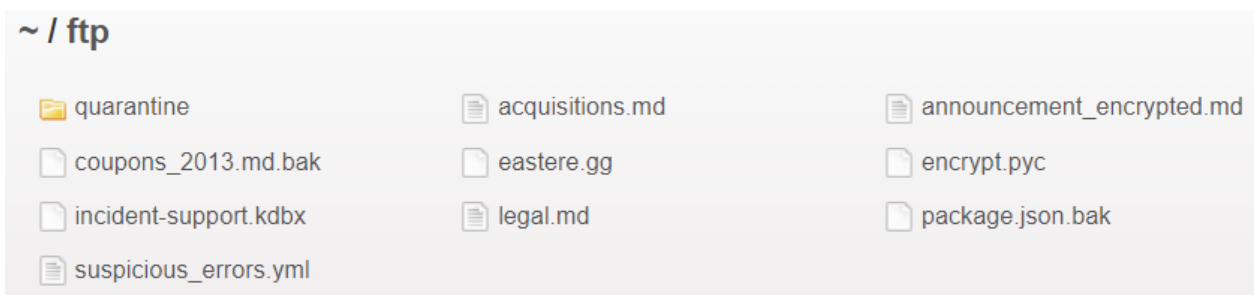
Access Coupon Codes

1. Open the OWASP Juice Shop application. Login as any user (e.g., demo/demo) Make sure your browser's developer tools are open and currently monitoring network requests.
2. Open the "About Us" page. Scroll down the page and click the link to "Check out our boring terms of use"



[Link to Terms of Use](#)

3. Notice the terms of use file is a markdown .md file stored in an ftp directory. Edit the URL address to try to browse to the ftp directory.



FTP Directory Listing

4. Open the coupons_2013.md.bak file. What happens?

OWASP Juice Shop (Express ^4.17.1)

403 Error: Only .md and .pdf files are allowed!

```
at verify (/app/build/routes/fileServer.js:32:18)
at /app/build/routes/fileServer.js:16:13
at Layer.handle [as handle_request] (/app/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/app/node_modules/express/lib/router/index.js:328:13)
at /app/node_modules/express/lib/router/index.js:286:9
at param (/app/node_modules/express/lib/router/index.js:365:14)
at param (/app/node_modules/express/lib/router/index.js:376:14)
at Function.process_params (/app/node_modules/express/lib/router/index.js:421:3)
at next (/app/node_modules/express/lib/router/index.js:280:10)
at /app/node_modules/serve-index/index.js:145:39
at callback (/app/node_modules/graceful-fs/polyfills.js:306:20)
at FSReqCallback.oncomplete (node:fs:212:5)
```

File Type Error

5. Copy the URL for the coupons_2013.md.bak file, paste the URL into the address bar, and add the following to the end of the url: %2500.md What does this do? This is a trick that uses a poison null byte to trick the file server into thinking the file is a .md file. For example, %00 is a common way to indicate a null byte or termination character. However, in a URL, the % sign, itself, must be encoded by using %25. Therefore, by appending %2500.md to the end of the file name in the URL, we can trick the web application's file server logic into thinking the file is actually a .md file, which allows us to access and download files with other extensions.

Easter Egg

1. Access the FTP directory of the Juice Shop application
2. Using the poison null byte trick, download the eastere.gg file
3. View the contents of the eastere.gg file with a text editing program

```
"Congratulations, you found the easter egg!"
```

```
- The incredibly funny developers
```

```
...
...
...
```

Oh' wait, this isn't an easter egg at all! It's just a boring text file! The real easter egg can be found here:

```
L2d1ci9xcmlmL25lci9mYi9zaGFhC9ndXJsL3V2cS9uYS9ybmZncmUvcnR0L2p2Z3V2YS9ndXlvcn5mZ3JlL3J0dA==
```

Good luck, egg hunter!

eastere.gg File Contents







4. If you notice the L2... line, this looks like data that's been base-64 encoded. The characters present and the trailing "==" indicate. Find a base-64 decoder online

The resulting decoding looks like –

```
/gur/qrif/ner/fb/shaal/gurl/uvq/na/rnfgre/rtt/jvguva/gur/rnfgre/rtt
```

Looks like another path. See if you can access it.

- Since it does look like a path, it is most likely not encrypted with a robust encryption algorithm such as AES (Advanced Encryption Standard). Also notice that characters repeat within the string such as “rtt”.
- Find online Caesar-Cipher decrypter and plug the string into that.

Results      

Brute-Force mode: the 25 shifts (for the alphabet ABCDEFGHIJKLMNOPQRSTUVWXYZ) are tested and sorted from most probable to least probable.

↑↓	↑↓
→13 (←13)	/the/devs/are/so/funny/they/hid/an/easter/egg/within/the/easter/egg
→17 (←9)	/pda/zaro/wna/ok/bqjj/pdau/dez/wj/awopan/acc/sepdej/pda/awopan/acc
→2 (←24)	/esp/opgd/lcp/dz/qfyyj/espj/sto/ly/pldepc/prr

Possible Decryptions

- Now access the easter eggs with the path:
the/devs/are/so/funny/they/hid/an/easter/egg/within/the/easter/egg

On Your Own

In Moodle, answer the questions in the Workshop 6 activity by performing attacks in which the application does not appropriately hide sensitive data.