Q1 Study Group Information

0 Points

Students can optionally form study groups of *no more than 3 students* to complete lab activities.

Study groups are not allowed to collaborate to complete any other assignments in the course besides written lab activities.

Please enter the names/unityIDs (for example: Jason King, jtking) of the students in your study group:

Vishnu Challa, vchalla2
Srujan Ponnur, sponnur
Varun Kumar Veginati, vvegina

Q2 Stacktrace Information Disclosure

30 Points

Attack Goal: Find some action or submit a request (somewhere other than through the `ftp` access point) in the web application that causes an error message with a full stack trace.

Q2.1 Steps

10 Points

List your steps, including the exact input fields used and exact inputs used:

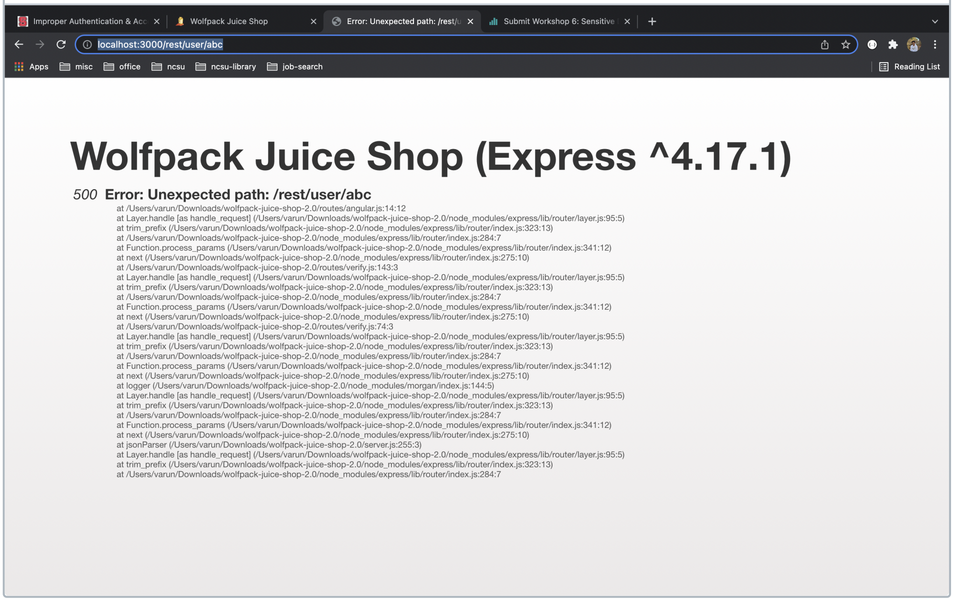
1. From the workshop training we got to know that there is an endpoint "whoami" to display the user information. http://localhost:3000/rest/user/whoami.
2. We just edited the URL to see if we can get any stack trace. Updated whoami to ABC in the URL.
3. URL used is: http://localhost:3000/rest/user/abc
4. When the above URL is opened in a new tab there is a 500 error with a stack trace.

Q2.2 Attack

10 Points

Upload an image/screenshot of your successful attack:

▾ 2.2.1.png Download


Improper Authentication & Acc
Wolfpack Juice Shop
Error: Unexpected path: /rest/u
Submit Workshop 6: Sensitive
localhost:3000/rest/user/abc
Apps
misc
office
ncsu
ncsu-library
job-search
Reading List

Wolfpack Juice Shop (Express ^4.17.1)

```
500 Error: Unexpected path: /rest/user/abc
    at /Users/varun/Downloads/wolfpack-juice-shop-2.0/routes/angular.js:14:12
    at Layer.handle [as handle_request] (/Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/layer.js:95:5)
    at trim_prefix (/Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/index.js:323:13)
    at /Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/index.js:284:7
    at Function.process_params (/Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/index.js:341:12)
    at next (/Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/index.js:275:10)
    at /Users/varun/Downloads/wolfpack-juice-shop-2.0/routes/verify.js:143:3
    at Layer.handle [as handle_request] (/Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/layer.js:95:5)
    at trim_prefix (/Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/index.js:323:13)
    at /Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/index.js:284:7
    at Function.process_params (/Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/index.js:341:12)
    at next (/Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/index.js:275:10)
    at /Users/varun/Downloads/wolfpack-juice-shop-2.0/routes/verify.js:74:3
    at Layer.handle [as handle_request] (/Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/layer.js:95:5)
    at trim_prefix (/Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/index.js:323:13)
    at /Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/index.js:284:7
    at Function.process_params (/Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/index.js:341:12)
    at next (/Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/index.js:275:10)
    at logger (/Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/morgan/index.js:144:5)
    at Layer.handle [as handle_request] (/Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/layer.js:95:5)
    at trim_prefix (/Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/index.js:323:13)
    at /Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/index.js:284:7
    at Function.process_params (/Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/index.js:341:12)
    at next (/Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/index.js:275:10)
    at jsonParser (/Users/varun/Downloads/wolfpack-juice-shop-2.0/server.js:255:3)
    at Layer.handle [as handle_request] (/Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/layer.js:95:5)
    at trim_prefix (/Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/index.js:323:13)
    at /Users/varun/Downloads/wolfpack-juice-shop-2.0/node_modules/express/lib/router/index.js:284:7
```

Q2.3 Description

10 Points

In 1-2 sentences, briefly describe what data is exposed and how it could be used to threaten one or more of the security objectives.

It displays what files are available within the juice shop library including the routes of files. Also, it's that the juice shop library is built using javascript since many .js files and file paths are displayed in the stack trace.

Q3 Access Confidential Documents

30 Points

Attack Goal: Find a document that contains confidential information (*the document should include the text "Confidential" or "Do not redistribute").

Q3.1 Steps

15 Points

List your steps, including the exact input fields used and exact inputs used:

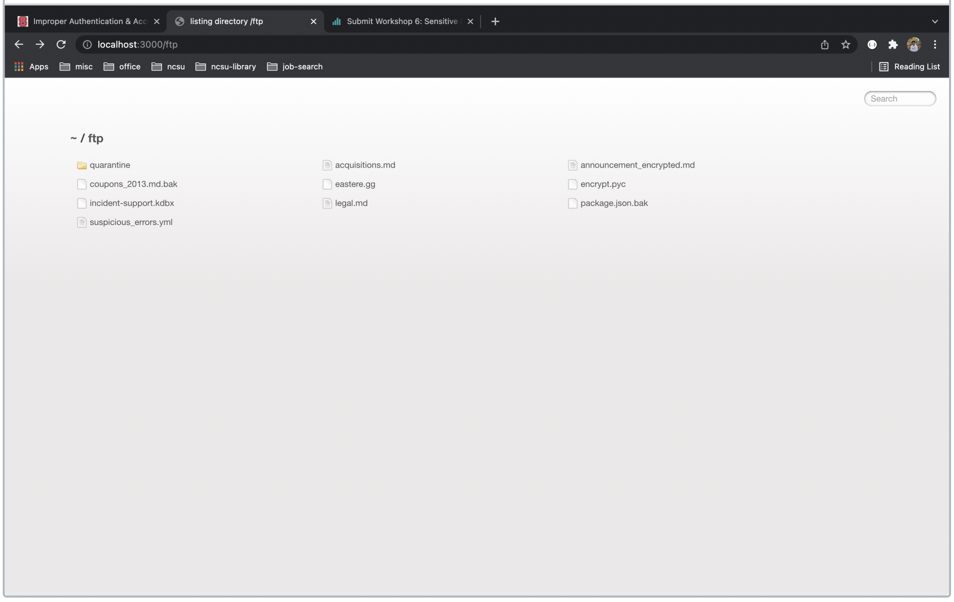
1. logged in as a user with username: demo and password: demo.
2. Went to the about us page.
3. Clicked on "Check out our boring terms of use if you are interested in such lame stuff." clickable link which took us to a page that included legal information. (http://localhost:3000/ftp/legal.md).
4. The URL of legal.md shows that it's saved in a directory.
5. Updated the URL to http://localhost:3000/ftp.
6. It took us to the ftp folder which included many files.
7. Tried opening all the files in ftp folder.
8. acquisitions.md file has the text "Confidential".
9. http://localhost:3000/ftp/acquisitions.md is the URL for the acquisitions file.

Q3.2 Attack

15 Points

Upload an image/screenshot of your successful attack:

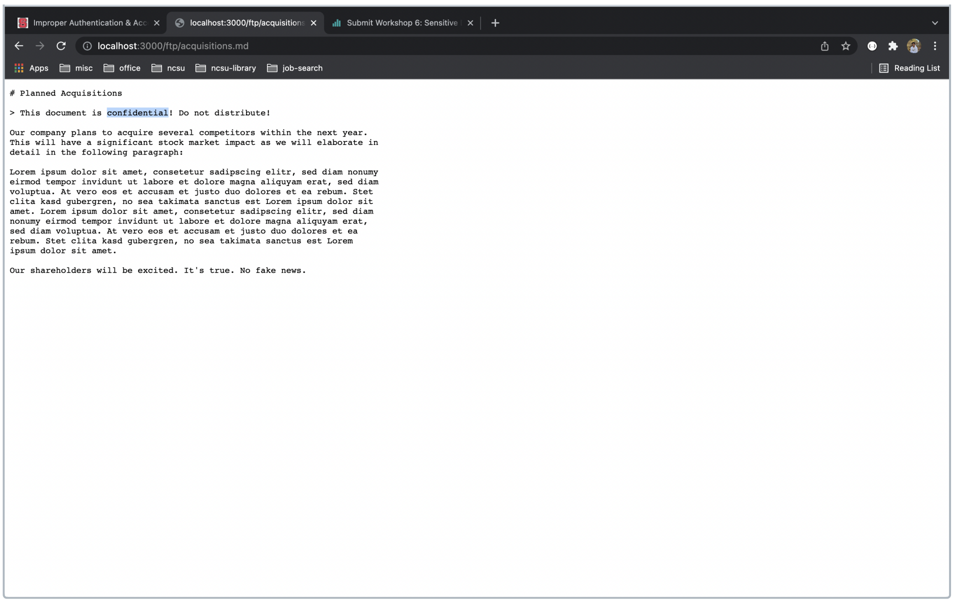
▾ 3.2.1.png Download



~ / ftp

```
quarantine                acquisitions.md          announcement_encrypted.md
coupons_2013.md.bak       eastere.gg               encrypt.pyc
incident-support.kdbx     legal.md                 package.json.bak
suspicious_errors.yml
```

▾ 3.2.2.png Download


Improper Authentication & Acc
localhost:3000/ftp/acquisitions
Submit Workshop 6: Sensitive
localhost:3000/ftp/acquisitions.md
Apps
misc
office
ncsu
ncsu-library
job-search
Reading List

```
# Planned Acquisitions

> This document is confidential! Do not distribute!

Our company plans to acquire several competitors within the next year.
This will have a significant stock market impact as we will elaborate in
detail in the following paragraph:

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy
eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam
voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet
clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit
amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam
nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat,
sed diam voluptua. At vero eos et accusam et justo duo dolores et ea
rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem
ipsum dolor sit amet.

Our shareholders will be excited. It's true. No fake news.
```

Q4 Data Exposure in Response

30 Points

Attack Goal: Find an endpoint other than `rest/user/whoami` that exposes sensitive information when an authentication header is not included as part of the request.

Q4.1 Steps

15 Points

List your steps, including the exact input fields used and exact inputs used:

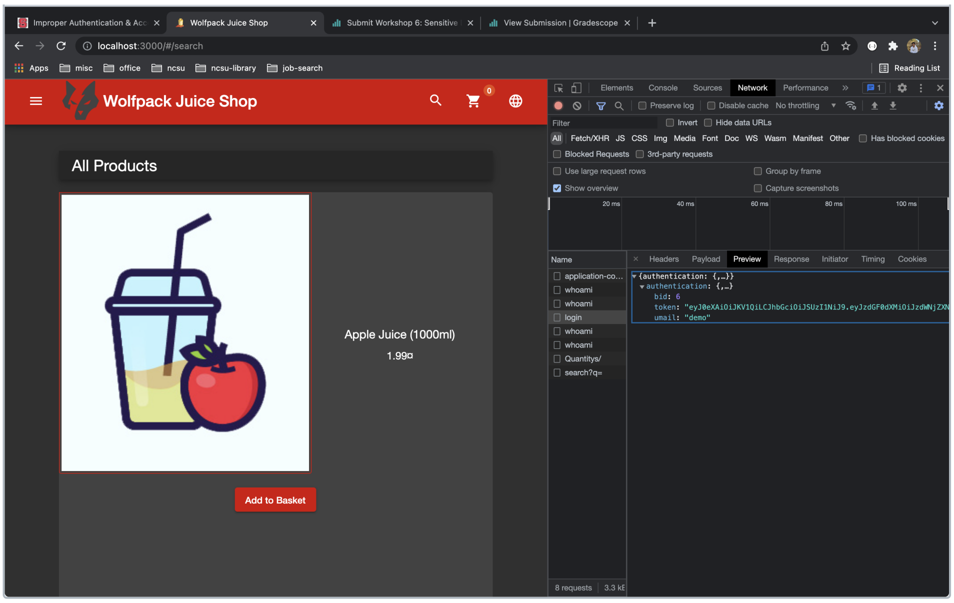
1. login endpoint contains the user token.
2. Network tab in Browser's developer tools is opened.
3. Logged in as a user with Username: demo and Password: demo.
4. Network tab contains a POST endpoint called login.
5. The response of the POST endpoint contains the user token, bid id, and mail id of the user which is sensitive.

Q4.2 Attack

15 Points

Upload an image/screenshot of your successful attack:

▾ 4.2.1.png Download



```
▼{authentication: {,…}}
  ▼authentication: {,…}
     bid: 6
     token: "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXN
     umail: "demo"
```

Q5 Mitigation Techniques

10 Points

Q5.1 ftp Mitigation Techniques

5 Points

In 2-3 sentences, briefly describe how you would address/mitigate the threats associated with the `ftp` functionality.

1. No sensitive information should be stored in the web directory. If stored in memory, it should be stored securely by using a standard encryption technique like AES-GCM mode and in a location that's not accessible to the users.
2. Web directory paths should not be accessible by the users. We have to use a default denylist so that users cannot access folders or files within the web directory.

Q5.2 whoami Endpoint Mitigation Strategy

5 Points

In 2-3 sentences, briefly describe how you would address/mitigate the threats associated with the `whoami` functionality.

1. APIs that contain sensitive information should not be accessed without a user token.
2. The sensitive information (which is email in this case) should

not be viewed directly in the response. It should be masked so that the email will not be exposed.

Workshop 6: Sensitive Data Exposure

● GRADED

GROUP

Vishnu Challa
Srujan Ponnur
Varun Kumar Veginati

View or edit group

TOTAL POINTS

96 / 100 pts

QUESTION 1

	Study Group Information	**0** / 0 pts

QUESTION 2

	Stacktrace Information Disclosure	**30** / 30 pts
2.1	Steps	**10** / 10 pts
2.2	Attack	**10** / 10 pts
2.3	Description	**10** / 10 pts

QUESTION 3

	Access Confidential Documents	**30** / 30 pts
3.1	Steps	**15** / 15 pts
3.2	Attack	**15** / 15 pts

QUESTION 4

	Data Exposure in Response	**26** / 30 pts
4.1	Steps	**11** / 15 pts
4.2	Attack	**15** / 15 pts

QUESTION 5

	Mitigation Techniques	**10** / 10 pts
5.1	ftp Mitigation Techniques	**5** / 5 pts

5.2 whoami Endpoint Mitigation Strategy

5 / 5 pts