Sri Lanka Institute of Information Technology

Path traversal

WD - Wednesday Group Submission

IE2062 – Web Security.

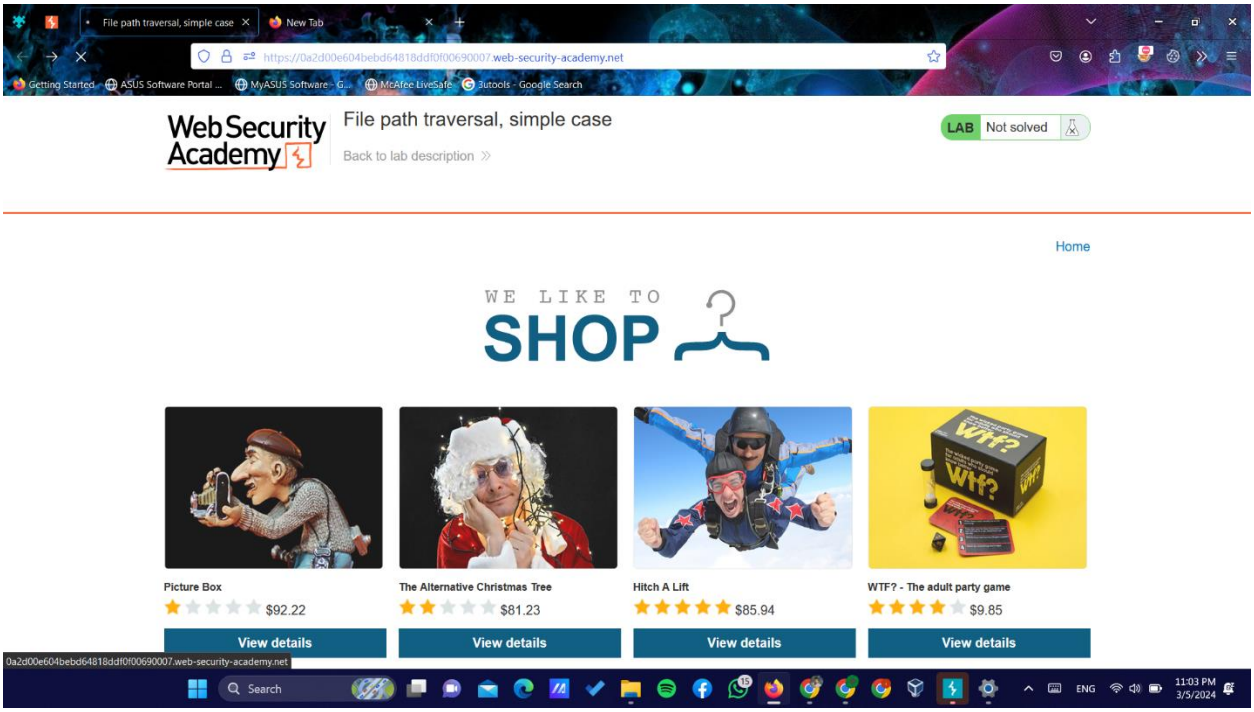
Submitted by:

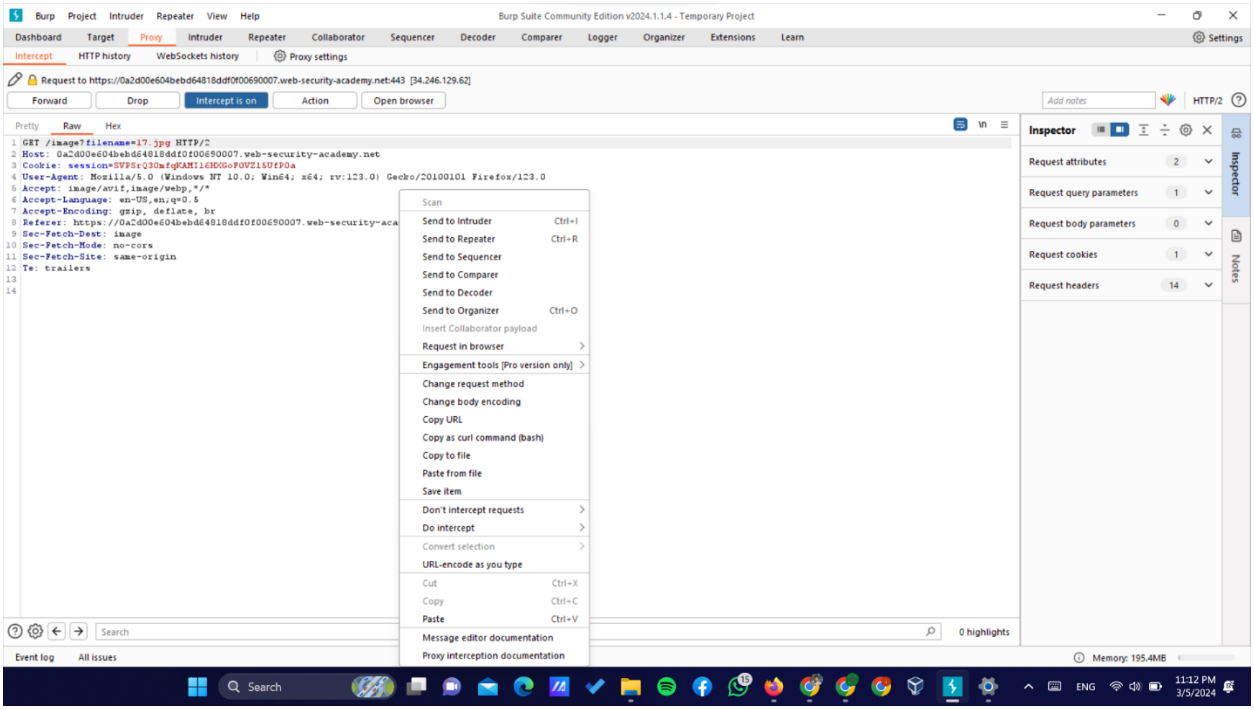
IT22199508 – Athapaththu A.M.M.I.P

Date of submission

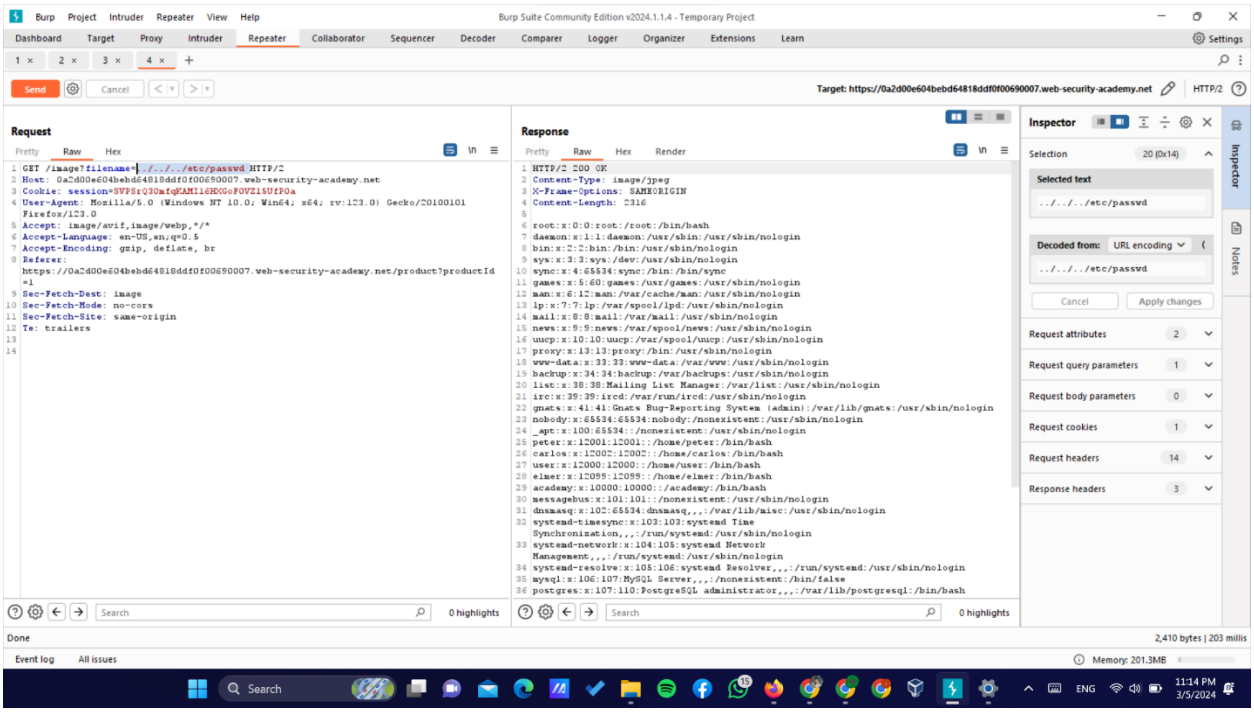
2024.03.06

1. File path traversal, simple case

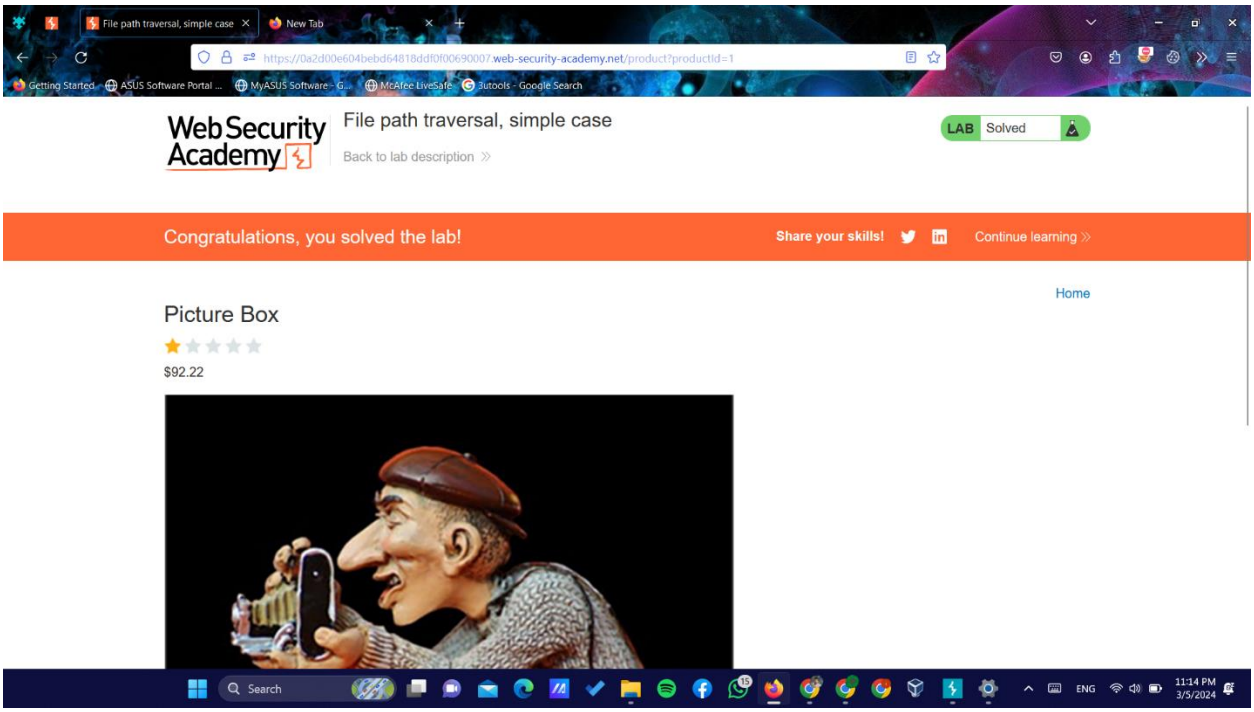




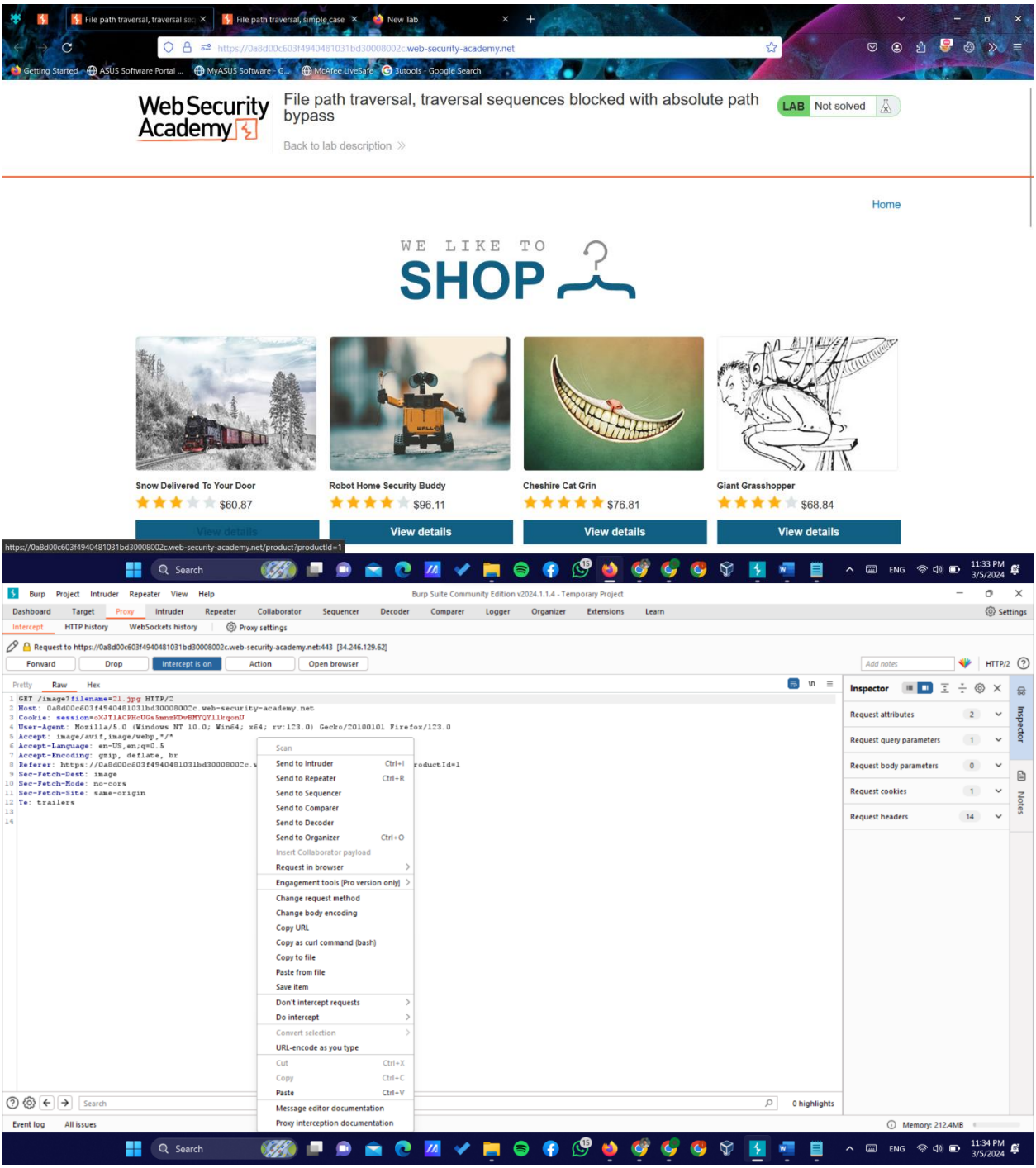
- This lab contains a path traversal vulnerability in the display of product images.
- Open the burp suit and turn on the intercept on and access the lab, when you get the RAW code send it to the repeater.



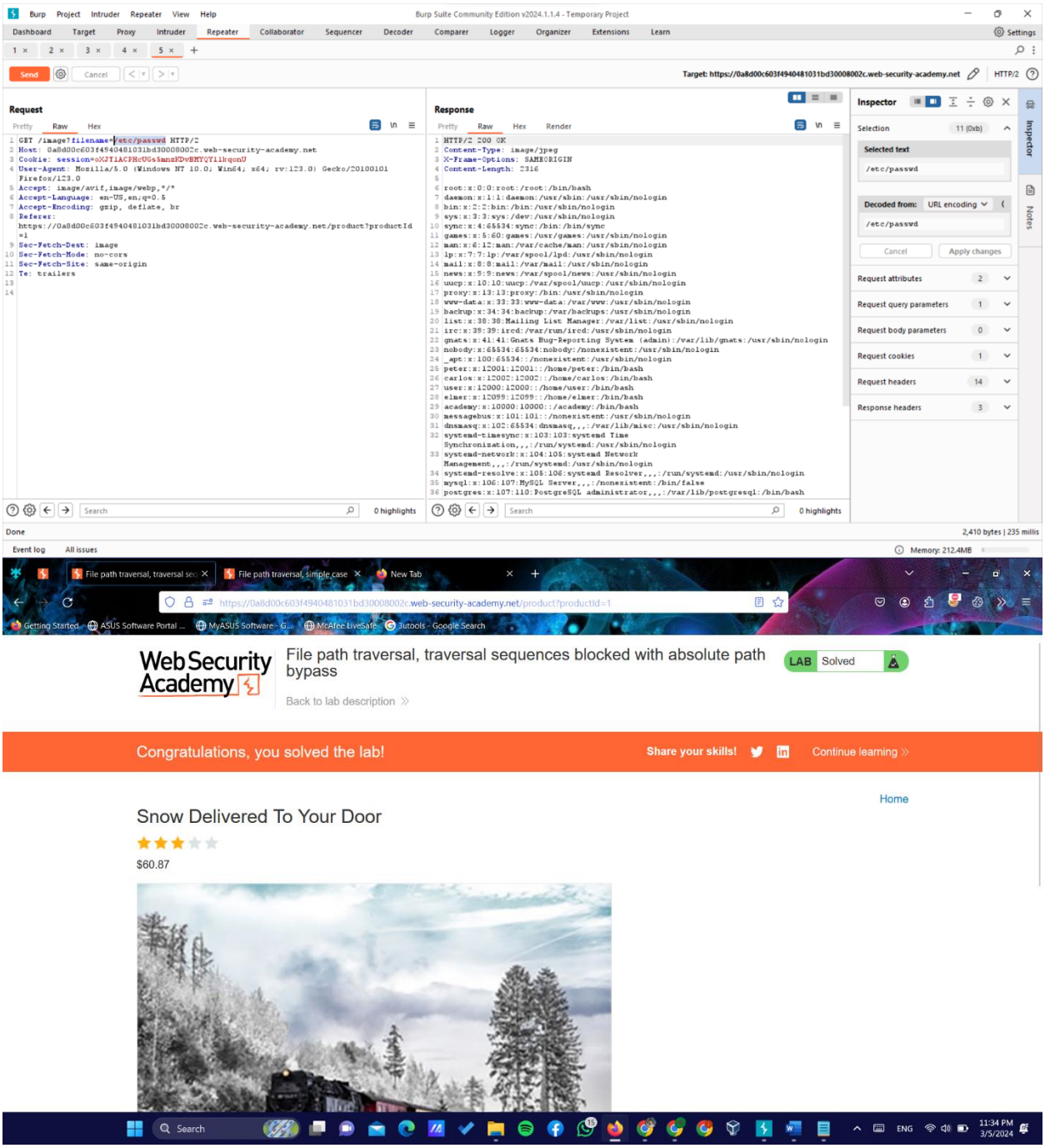
- To solve the lab, retrieve the contents of the /etc/passwd file. Edit it as **'../../../etc/passwd'** and send it, now refresh the lab page and you can see solved lab massage.



2. File path traversal, traversal sequences blocked with absolute path bypass

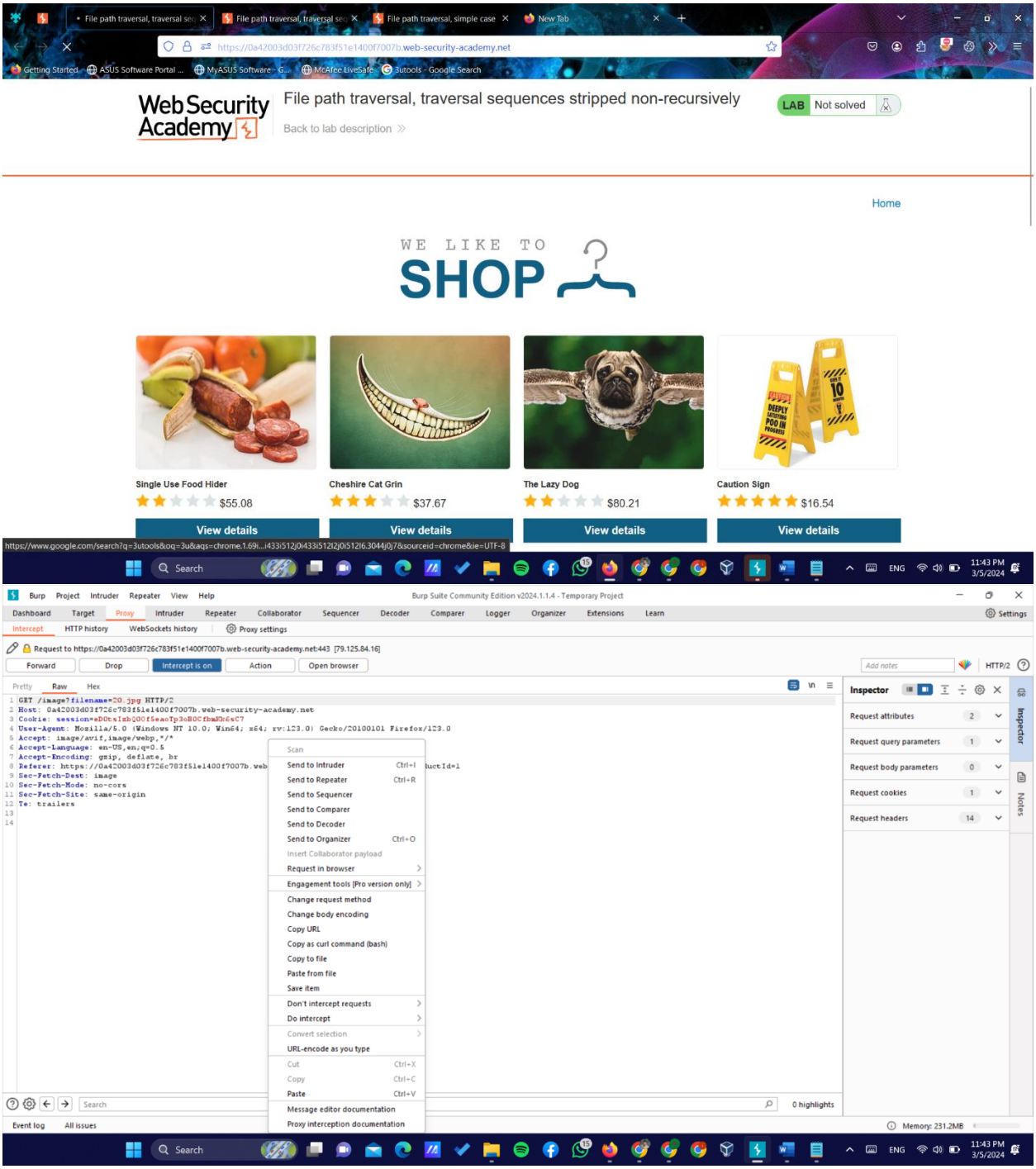


- This lab contains a path traversal vulnerability in the display of product images.
- Open the burp suit and turn on the intercept on and access the lab, when you get the RAW code send it to the repeater.

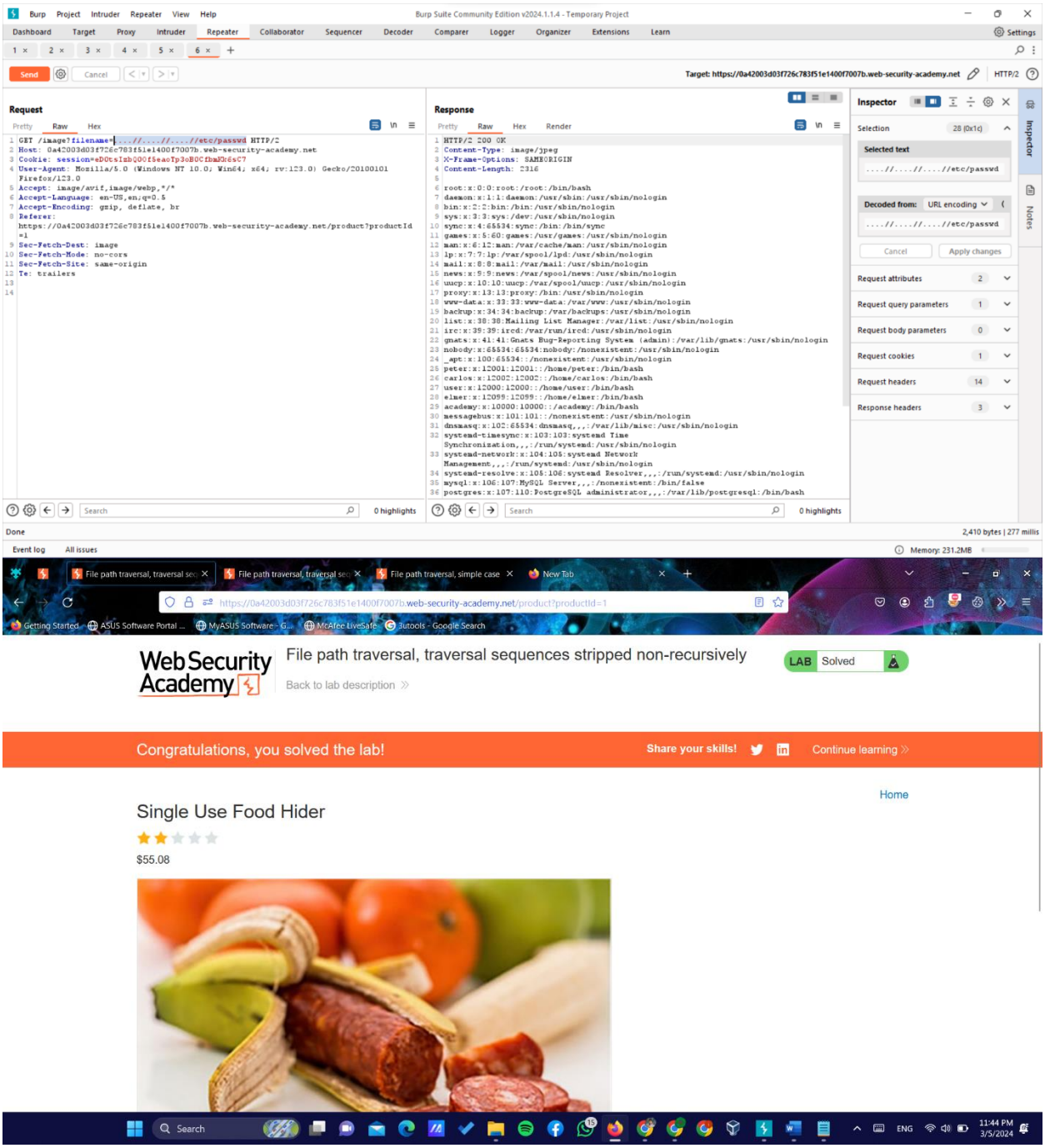


- To get the '/image?filename=' RAW code you have to forward the code
- To solve the lab, retrieve the contents of the /etc/passwd file. Edit it as **'/etc/passwd'** and send it, now refresh the lab page and you can see solved lab massage.

3. File path traversal, traversal sequences stripped non-recursively

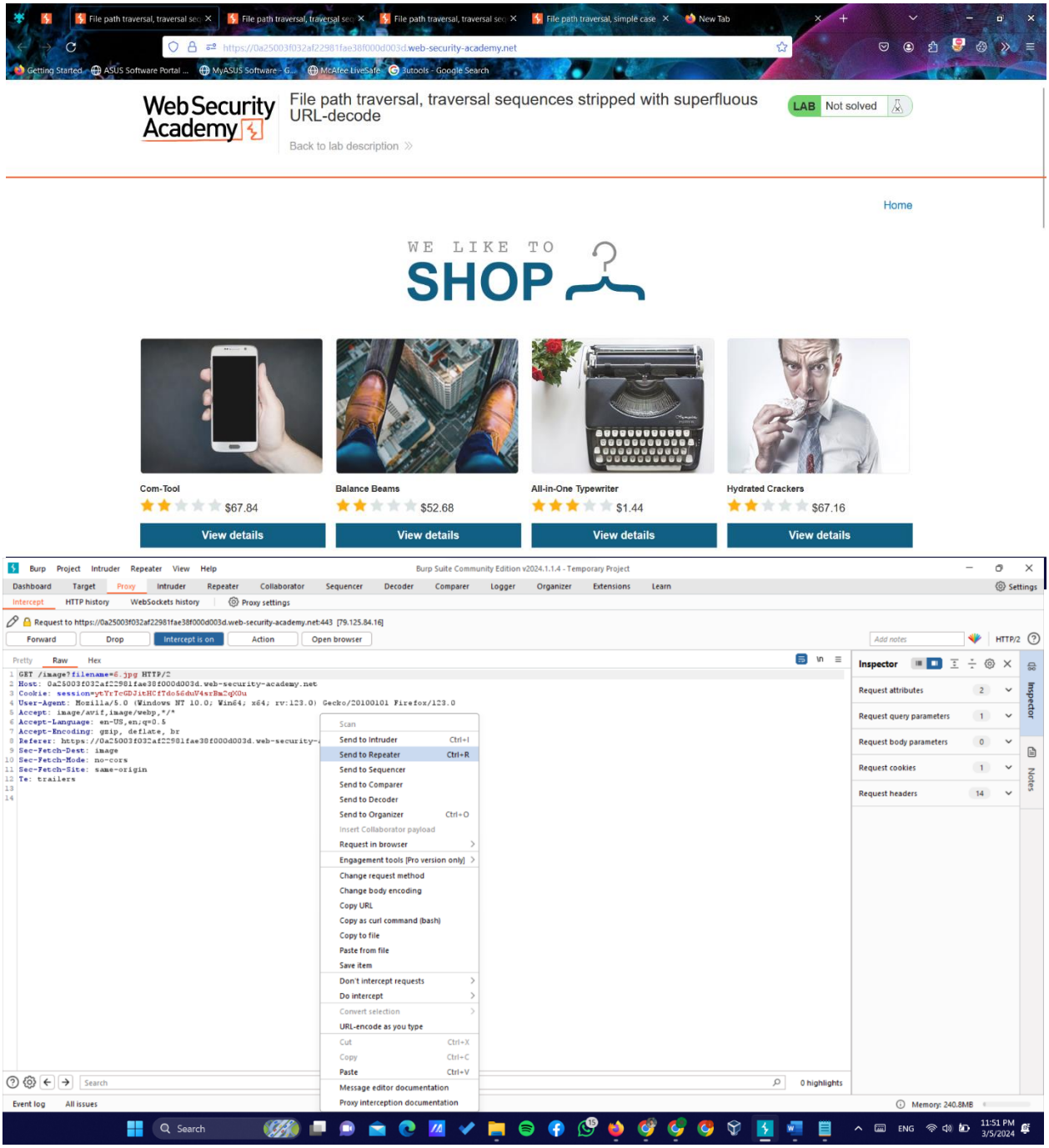


- This lab contains a path traversal vulnerability in the display of product images.
- Open the burp suit and turn on the intercept on and access the lab, when you get the RAW code send it to the repeater.

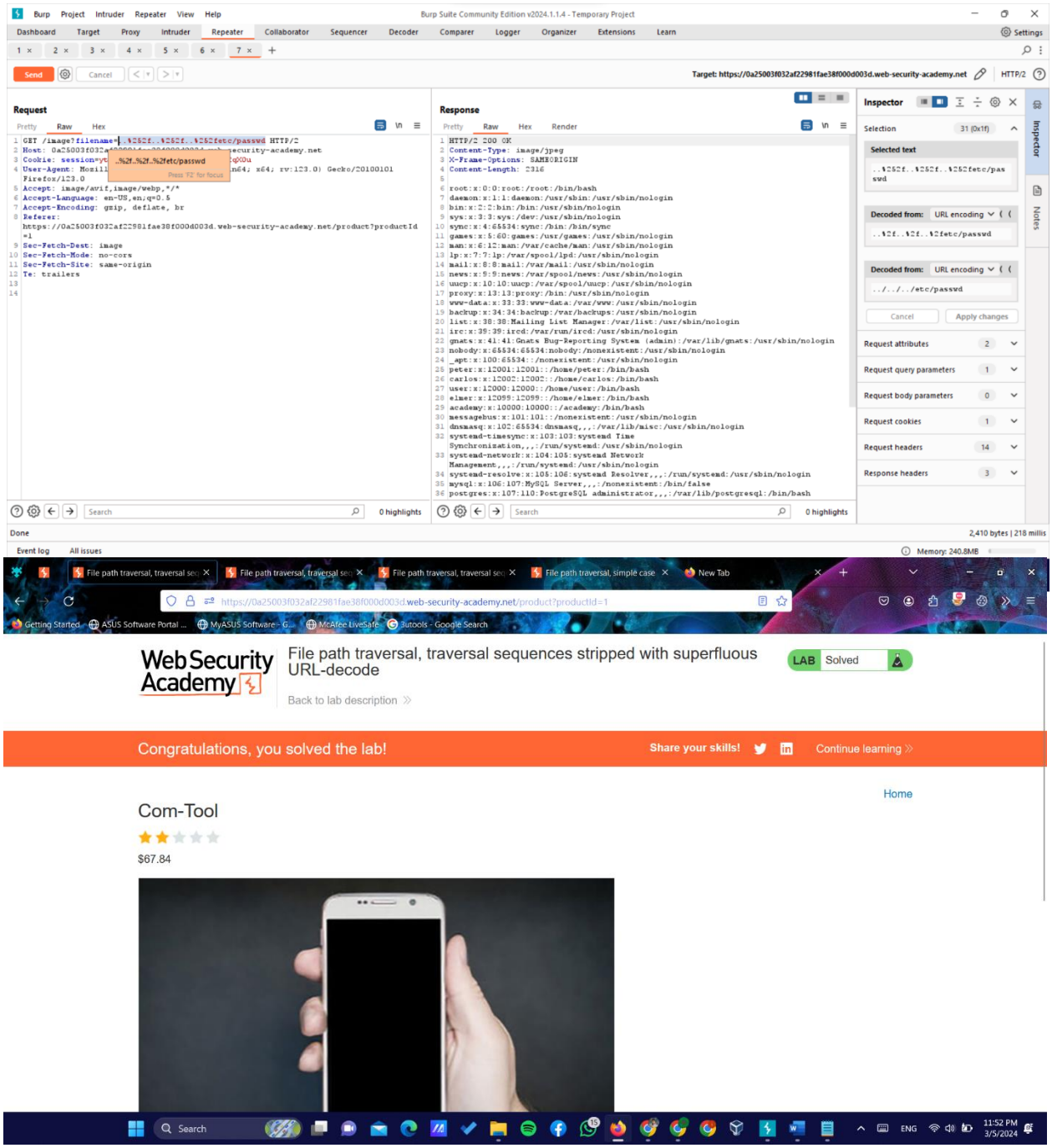


- To get the '/image?filename=' RAW code you have to forward the code
- To solve the lab, retrieve the contents of the /etc/passwd file. Edit it as **'….//….//….//….//etc/passwd'** and send it, now refresh the lab page and you can see solved lab massage.

4. File path traversal, traversal sequences stripped with superfluous URL-decode

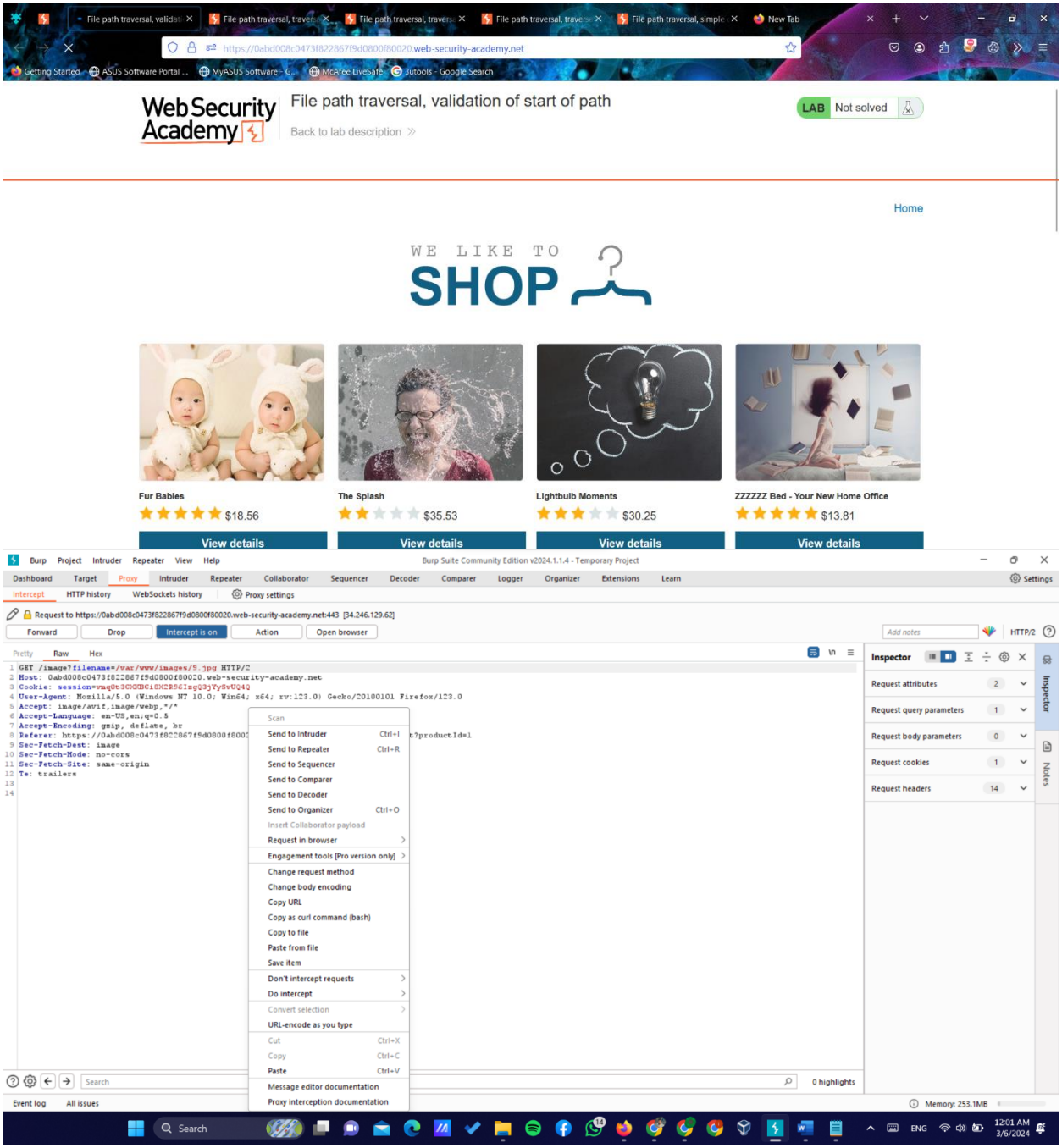


- This lab contains a path traversal vulnerability in the display of product images.
- Open the burp suit and turn on the intercept on and access the lab, when you get the RAW code send it to the repeater.

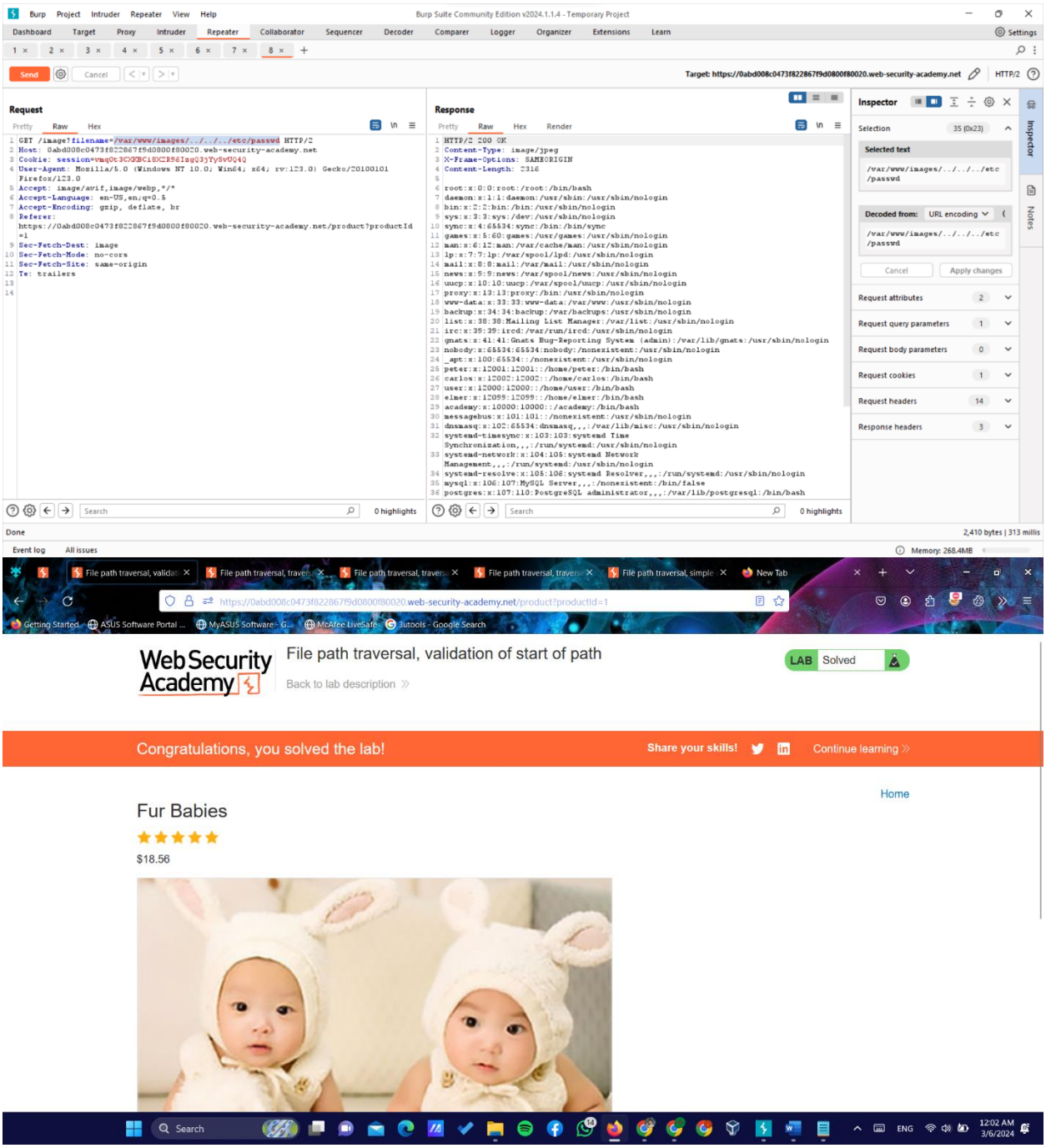


- To get the '/image?filename=' RAW code you have to forward the code
- To solve the lab, retrieve the contents of the /etc/passwd file. Edit it as **'..%252f..%252f..%252fetc/passwd'** and send it, now refresh the lab page and you can see solved lab massage.

5. File path traversal, validation of start of path

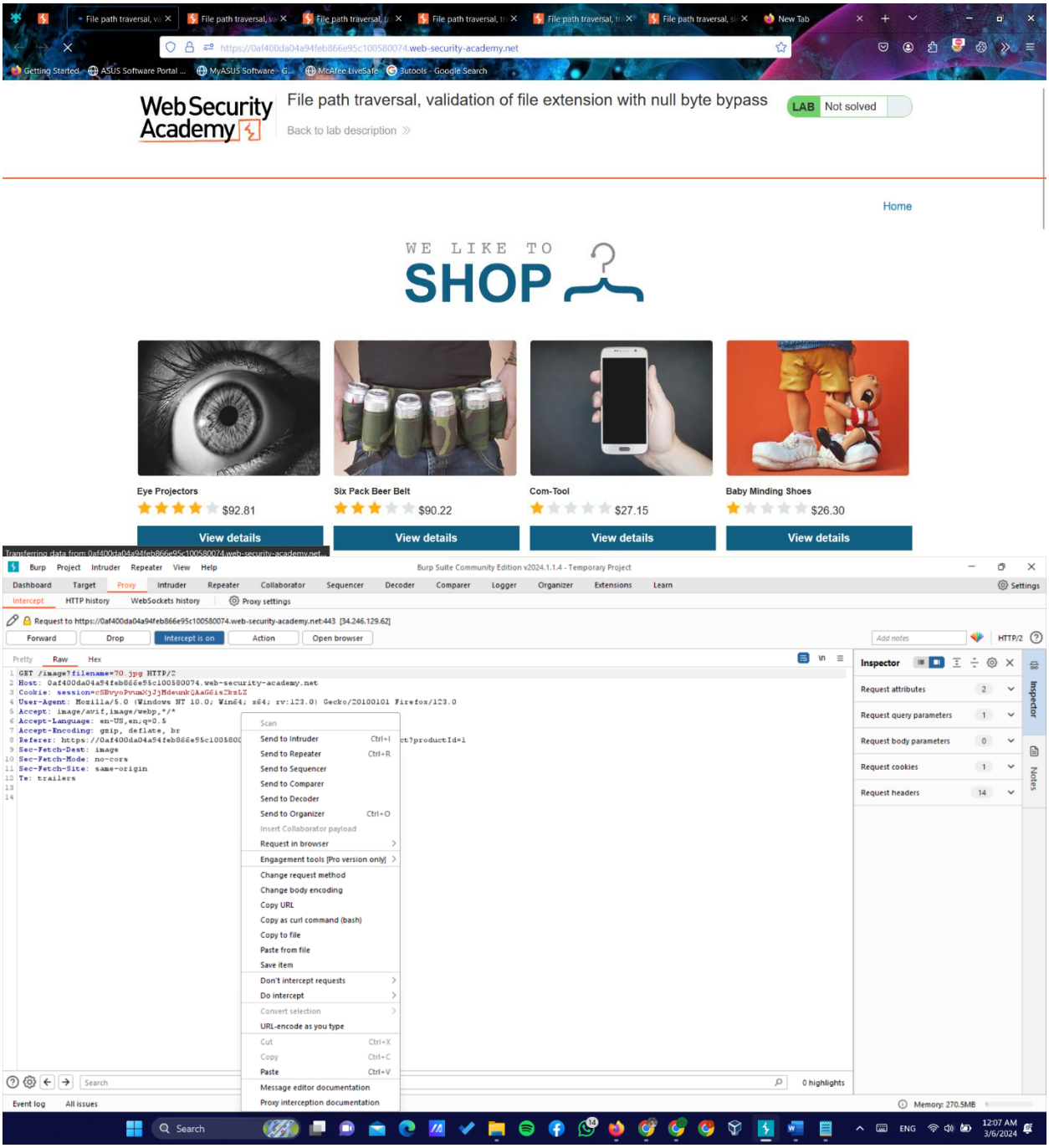


- This lab contains a path traversal vulnerability in the display of product images.
- Open the burp suit and turn on the intercept on and access the lab, when you get the RAW code send it to the repeater.

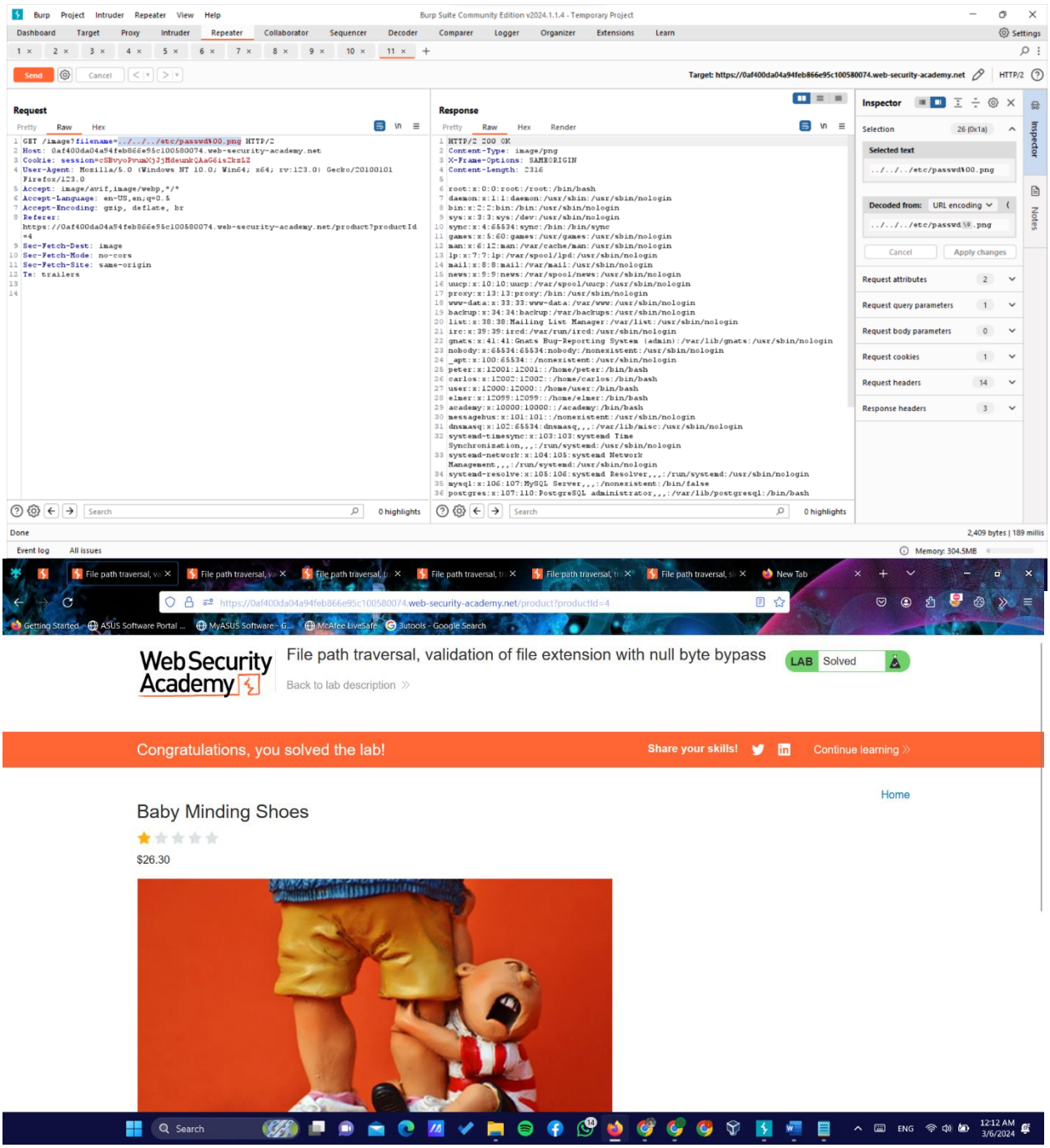


- To get the '/image?filename=' RAW code you have to forward the code
- To solve the lab, retrieve the contents of the /etc/passwd file. Edit it as '**/var/www/images/../../../etc/passwd'** and send it, now refresh the lab page and you can see solved lab massage.

6. File path traversal, validation of file extension with null byte bypass



- This lab contains a path traversal vulnerability in the display of product images.
- Open the burp suit and turn on the intercept on and access the lab, when you get the RAW code send it to the repeater.



- To get the '/image?filename=' RAW code you have to forward the code
- To solve the lab, retrieve the contents of the /etc/passwd file. Edit it as '`../../../etc/passwd%00.png`' and send it, now refresh the lab page and you can see solved lab massage.

❖ SUMMARY OF Path traversal