1. **Explain the exercise**
2. **Show normal execution of the software**

```
GET /index.html HTTP/1.1
GET /frobnick/100.frob.txt HTTP/1.1
```

3. **Go to `orig_webserver_commented.c` and show the `get_header` function**
4. **Show where the function is used**
5. **Search `BUFSIZE` and show the vuln**
6. **Exploit the vuln, go into the `/bo-cvd/Exploit` folder and start the `payload-ims.sh` script**
7. **Show the content of the payload**
8. **Execute the `exploit.sh` script**
9. **Introduce the `RCE`**
10. **Start the code with `gdb`**
11. **Create this payload and send it**

```
python3 -c 'print("GET / HTTP/1.1\r\nIf-Modified-Since: " + "A"*1134 + "\r\n\r\n")' > payload
```

12. **Show the segmentation fault and show how the rip has been replaced with 414141...**
13. **Explain the structure of the malicious payload: `NOP + SHELLCODE + NOP + NEW RIP`**
14. **Cat the content of `rce.py` and explain the script**
15. **Start the webserver and perform the attack**
16. **Connect to the new shell with**

```
nc localhost 4444
```

17. **Perform some commands**
18. **Explain the patch**
19. **Copy the patch, rename the `webserver.c` file and apply the patch**

```
patch bug_webserver.c -i fix.patch -o webserver.c
```

20. **Conclusion**