Cybersecurity

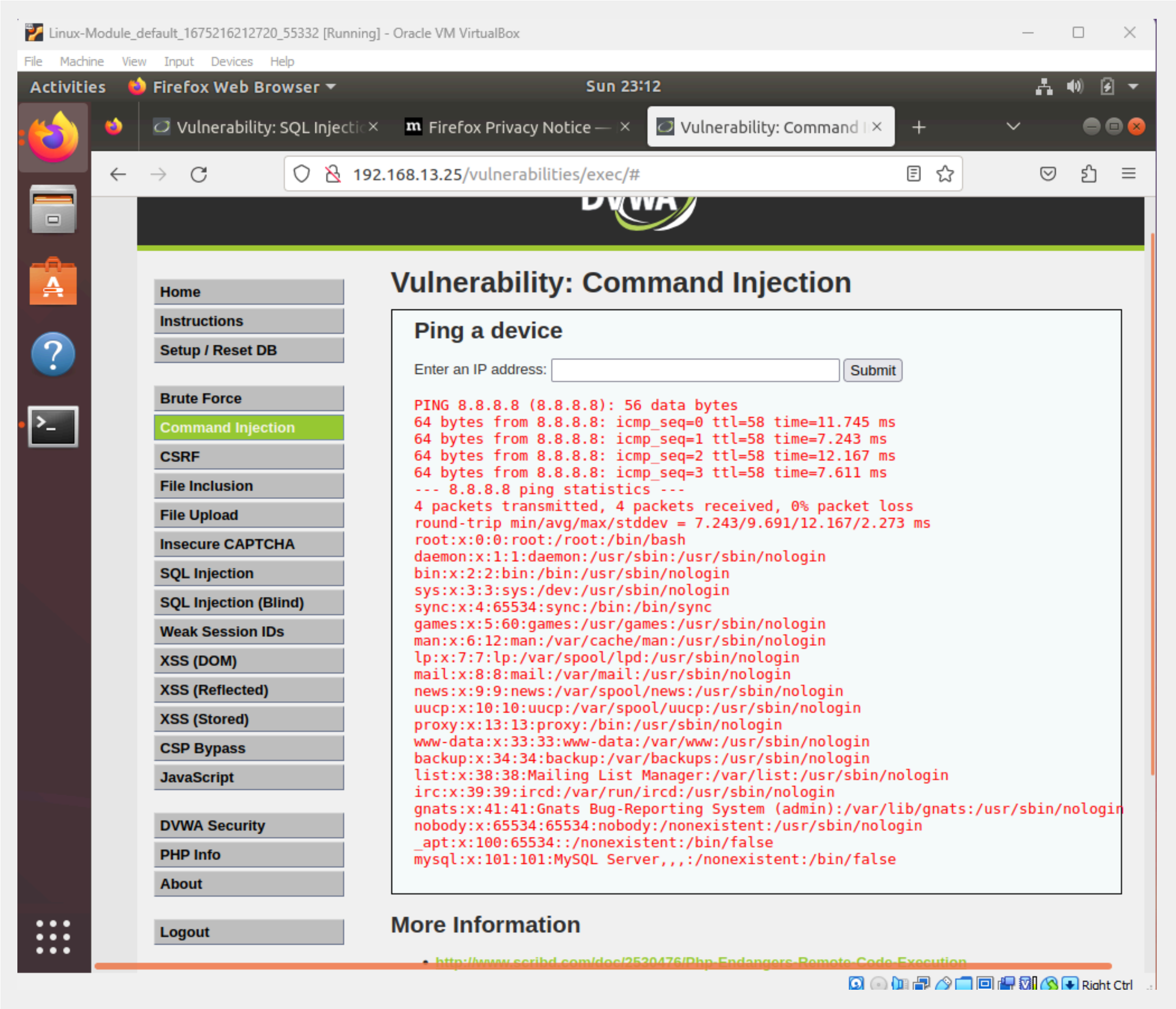
Module 15 Challenge Submission File

Testing Web Applications for Vulnerabilities

Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

Web Application 1: *Your Wish is My Command Injection*

Provide a screenshot confirming that you successfully completed this exploit:



Vulnerability: Command Injection

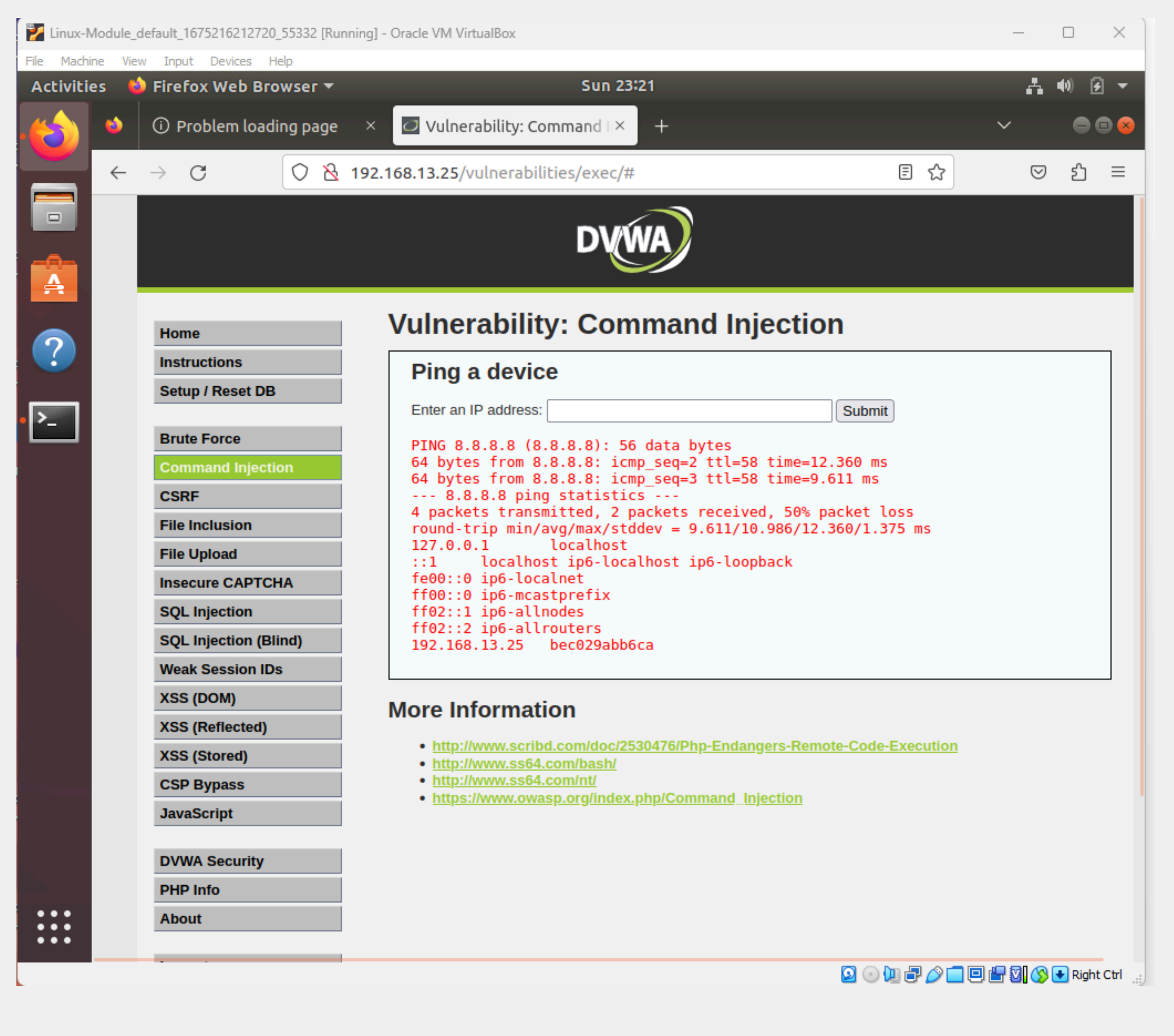
Ping a device

Enter an IP address: [ ] Submit

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=58 time=11.745 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=58 time=7.243 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=12.167 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=58 time=7.611 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 7.243/9.691/12.167/2.273 ms
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
_apt:x:100:65534::/nonexistent:/bin/false
mysql:x:101:101:MySQL Server,,,:/nonexistent:/bin/false
```

More Information

- http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution



Vulnerability: Command Injection

Ping a device

Enter an IP address: Submit

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=12.360 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=58 time=9.611 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 2 packets received, 50% packet loss
round-trip min/avg/max/stddev = 9.611/10.986/12.360/1.375 ms
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
192.168.13.25   bec029abb6ca
```

More Information

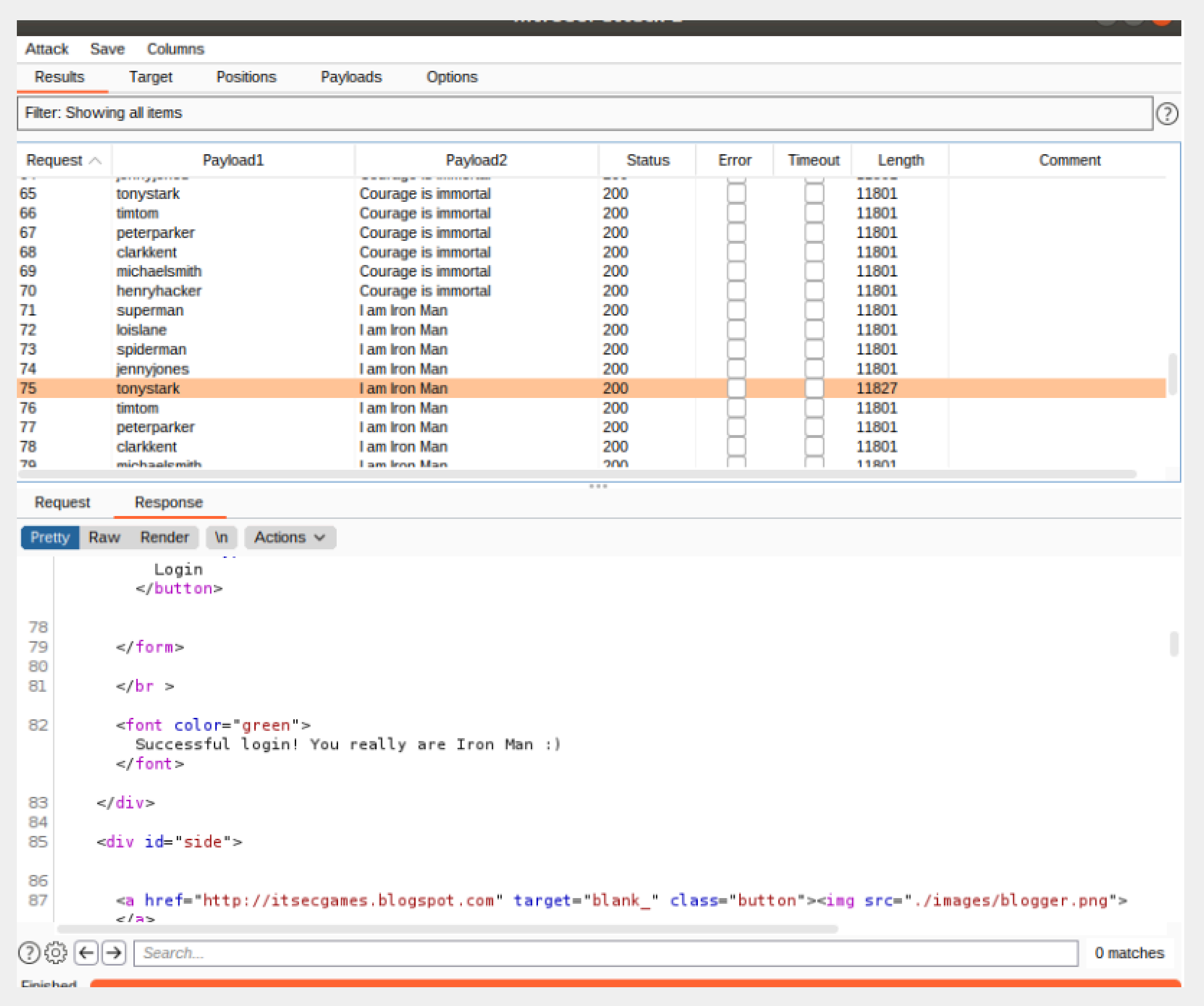
- http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://www.owasp.org/index.php/Command_Injection

Write two or three sentences outlining mitigation strategies for this vulnerability:

1. Implement proper input validation techniques to prevent malicious input from being executed as commands. Sanitize user input to remove any potentially harmful characters or sequences.
2. Ensure that the user executing the command has the minimum necessary privileges required to carry out the task, reducing the potential impact of unauthorized access to sensitive files. Limit access rights to critical system files such as /etc/passwd and /etc/hosts to authorized users and processes only.

Web Application 2: *A Brute Force to Be Reckoned With*

Provide a screenshot confirming that you successfully completed this exploit:



Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
65	tonystark	Courage is immortal	200	☐	☐	11801	
66	timtom	Courage is immortal	200	☐	☐	11801	
67	peterparker	Courage is immortal	200	☐	☐	11801	
68	clarkkent	Courage is immortal	200	☐	☐	11801	
69	michaelsmith	Courage is immortal	200	☐	☐	11801	
70	henryhacker	Courage is immortal	200	☐	☐	11801	
71	superman	I am Iron Man	200	☐	☐	11801	
72	loislane	I am Iron Man	200	☐	☐	11801	
73	spiderman	I am Iron Man	200	☐	☐	11801	
74	jennyjones	I am Iron Man	200	☐	☐	11801	
75	tonystark	I am Iron Man	200	☐	☐	11827	
76	timtom	I am Iron Man	200	☐	☐	11801	
77	peterparker	I am Iron Man	200	☐	☐	11801	
78	clarkkent	I am Iron Man	200	☐	☐	11801	
79	michaelsmith	I am Iron Man	200	☐	☐	11801	

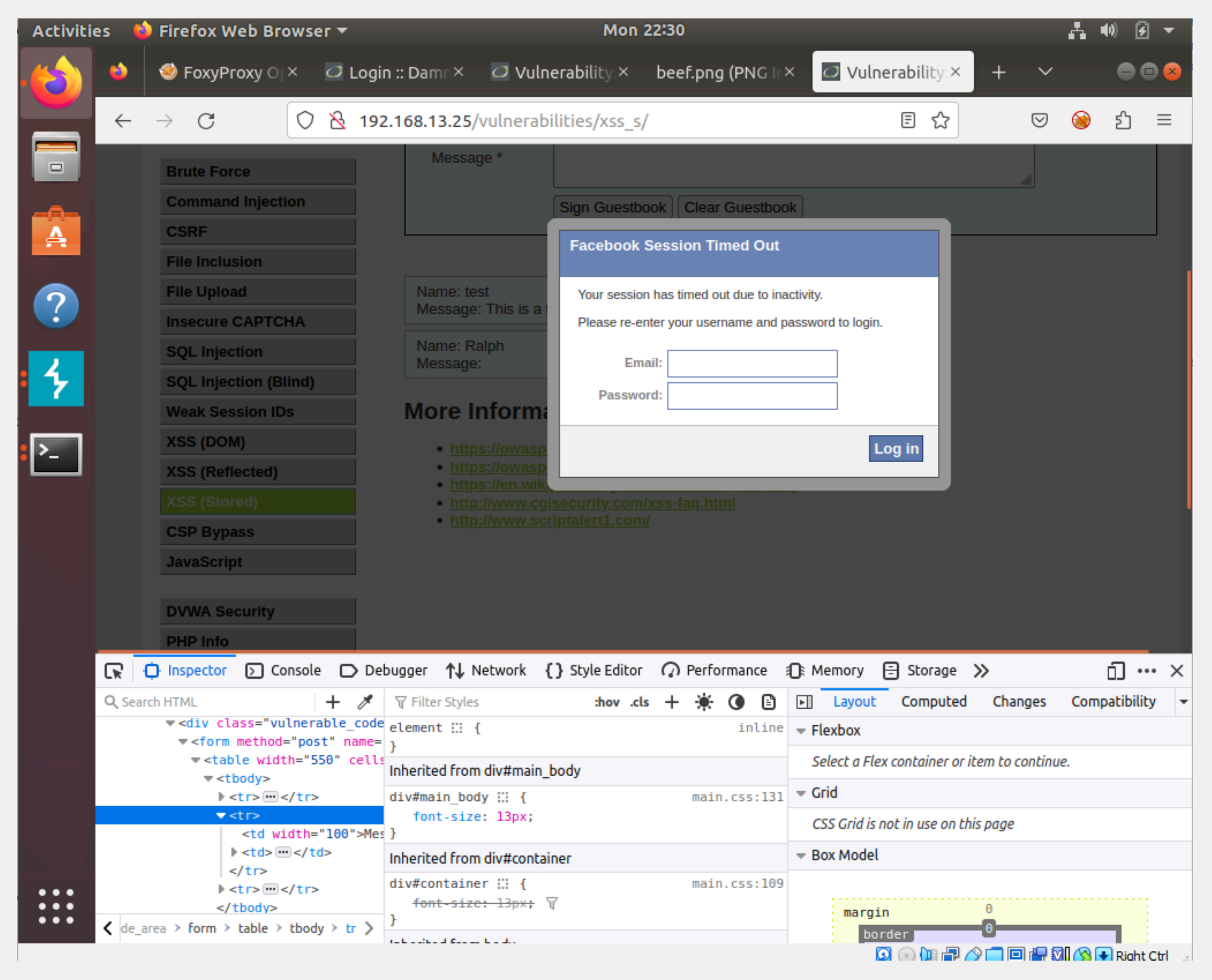
```
        Login
      </button>


    </form>

    </br >

    <font color="green">
      Successful login! You really are Iron Man :)
    </font>

  </div>

  <div id="side">

    <a href="http://itsecgames.blogspot.com" target="blank_" class="button"><img src="./images/blogger.png">
    </a>
```

Write two or three sentences outlining mitigation strategies for this vulnerability:

1. Require complex usernames and passwords to help increase the strength of authentication.
2. Implement a multi-factor authentication to add an additional layer of security.
3. Enable a lockout policy after a certain number of failed attempts.

Web Application 3: *Where's the BeEF?*

Provide a screenshot confirming that you successfully completed this exploit:



192.168.13.25/vulnerabilities/xss_s/

Facebook Session Timed Out

Your session has timed out due to inactivity.

Please re-enter your username and password to login.

Email:

Password:

Log in

Name: test
Message: This is a t

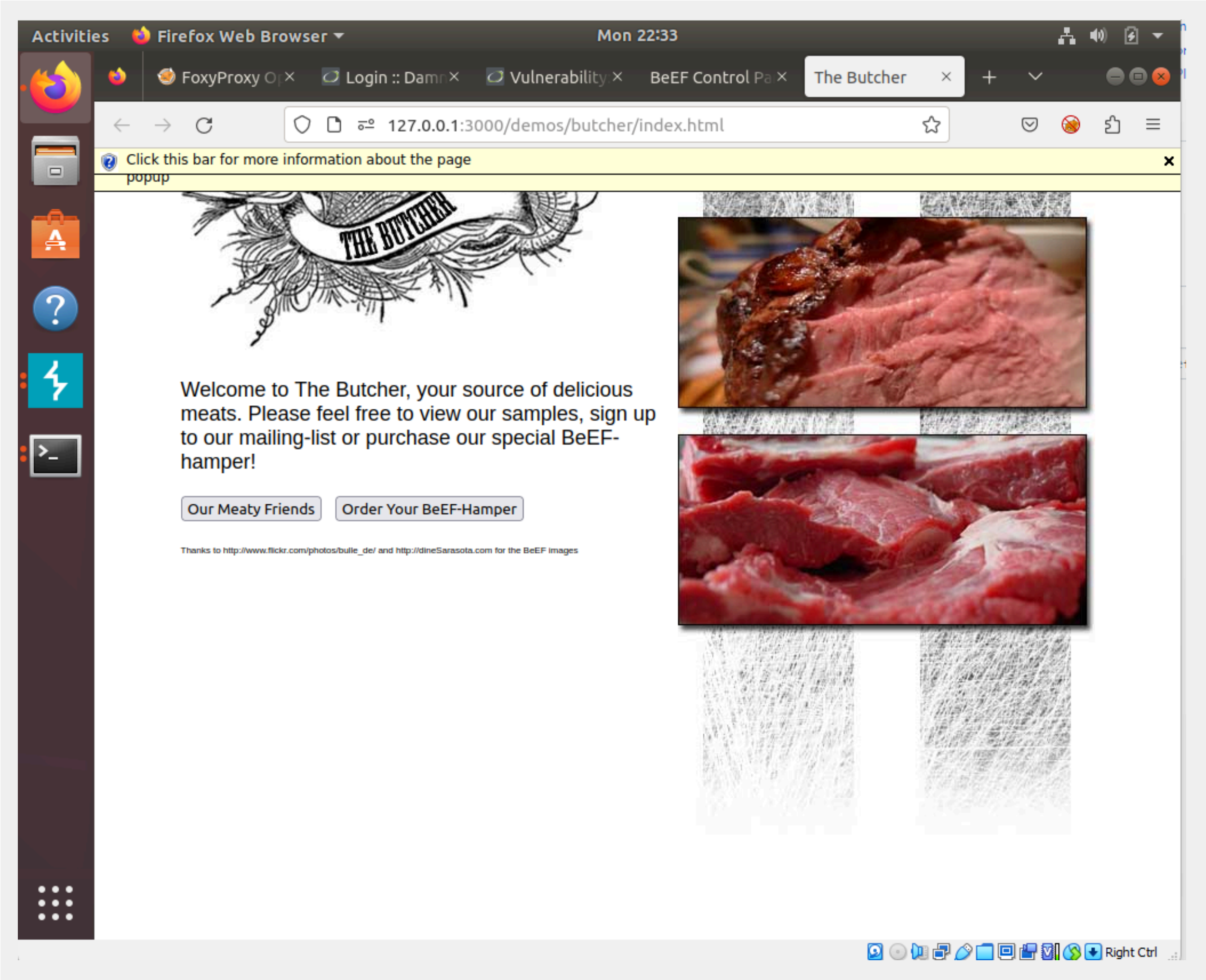
Name: Ralph
Message:

More Informa

- https://owasp
- https://owasp
- https://en.wik
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/

```
<div class="vulnerable_code
  <form method="post" name=
    <table width="550" cells
      <tbody>
        <tr>…</tr>
        <tr>
          <td width="100">Mes
          <td>…</td>
        </tr>
        <tr>…</tr>
      </tbody>
```

```
element {
}
Inherited from div#main_body
div#main_body {                     main.css:131
  font-size: 13px;
}
Inherited from div#container
div#container {                     main.css:109
  ~~font-size: 13px;~~
}
```

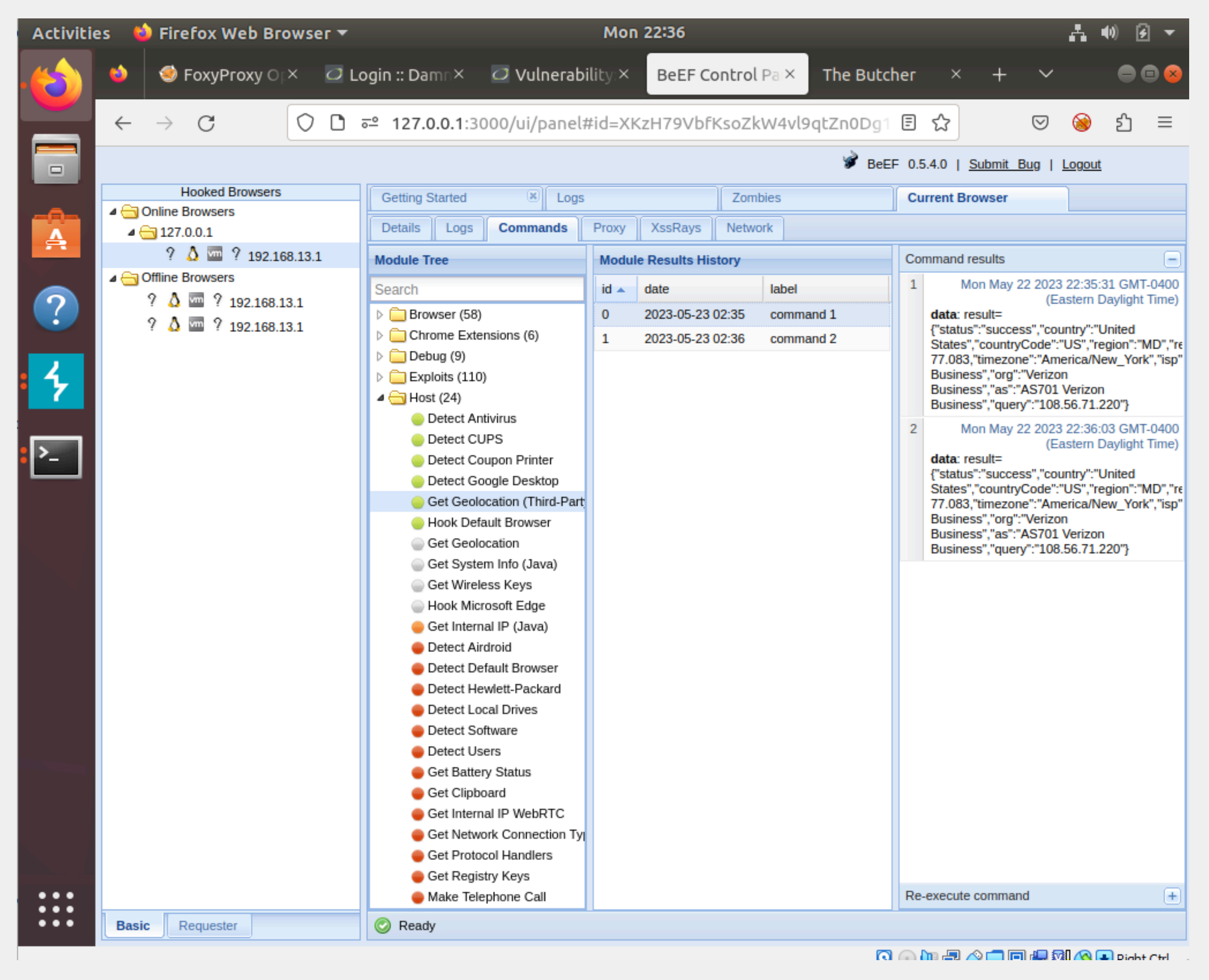


127.0.0.1:3000/demos/butcher/index.html

Click this bar for more information about the page popup

Welcome to The Butcher, your source of delicious meats. Please feel free to view our samples, sign up to our mailing-list or purchase our special BeEF-hamper!

Thanks to http://www.flickr.com/photos/bulle_de/ and http://dineSarasota.com for the BeEF images



id	date	label
0	2023-05-23 02:35	command 1
1	2023-05-23 02:36	command 2

```
1   Mon May 22 2023 22:35:31 GMT-0400
    (Eastern Daylight Time)
    data: result=
    {"status":"success","country":"United
    States","countryCode":"US","region":"MD","re
    77.083,"timezone":"America/New_York","isp"
    Business","org":"Verizon
    Business","as":"AS701 Verizon
    Business","query":"108.56.71.220"}
2   Mon May 22 2023 22:36:03 GMT-0400
    (Eastern Daylight Time)
    data: result=
    {"status":"success","country":"United
    States","countryCode":"US","region":"MD","re
    77.083,"timezone":"America/New_York","isp"
    Business","org":"Verizon
    Business","as":"AS701 Verizon
    Business","query":"108.56.71.220"}
```

Write two or three sentences outlining mitigation strategies for this vulnerability:

```
1. Implement strong input validation on both the client and server sides.
2. Properly encode and sanitize user-generated content before displaying
   in web pages.
3. Implement a content security policy on the web application.
```