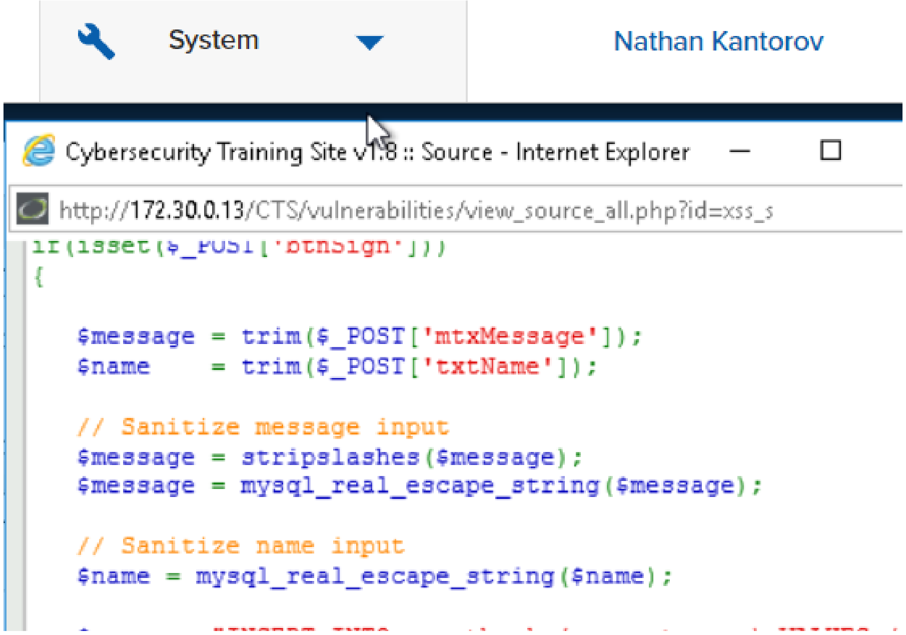
Unit 2.3.4
Goals:

- Collaborate with a cybersecurity team.
- Participate in a “training exercise” to recognize:
- An XSS Stored attack
- A Command Execution attack
- Perform a penetration test on a website and document it.
- Reflect on your cyber team experience.

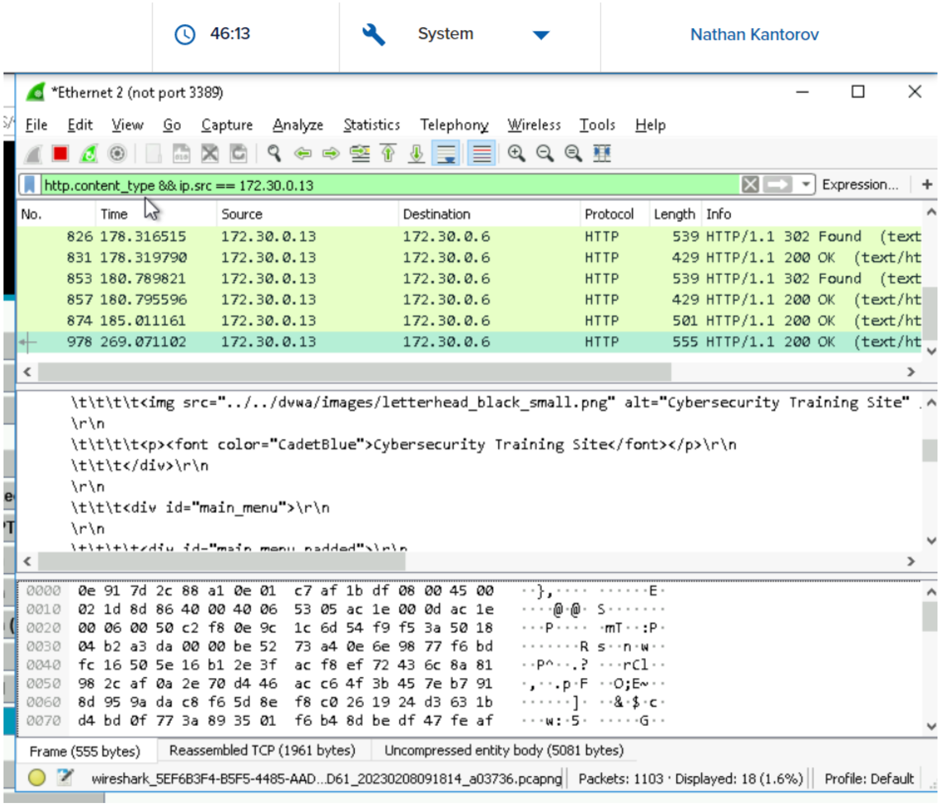
#2 - Notebook: Work with your team to brainstorm at least three positive collaboration practices that you consider important team norms. Be open minded to everyone’s ideas. Communication is key. Have a growth mindset.

#7 - Screenshot:


System
Nathan Kantorov
Cybersecurity Training Site v1.8 :: Source - Internet Explorer
http://172.30.0.13/CTS/vulnerabilities/view_source_all.php?id=xss_s

```
if(isset($_POST['btnSign']))
{

   $message = trim($_POST['mtxMessage']);
   $name    = trim($_POST['txtName']);

   // Sanitize message input
   $message = stripslashes($message);
   $message = mysql_real_escape_string($message);

   // Sanitize name input
   $name = mysql_real_escape_string($name);
```

#8 - Screenshot:


46:13
System
Nathan Kantorov
*Ethernet 2 (not port 3389)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

http.content_type && ip.src == 172.30.0.13

```
No.     Time        Source          Destination     Protocol  Length  Info
    826 178.316515  172.30.0.13     172.30.0.6      HTTP         539 HTTP/1.1 302 Found  (text
    831 178.319790  172.30.0.13     172.30.0.6      HTTP         429 HTTP/1.1 200 OK  (text/ht
    853 180.789821  172.30.0.13     172.30.0.6      HTTP         539 HTTP/1.1 302 Found  (text
    857 180.795596  172.30.0.13     172.30.0.6      HTTP         429 HTTP/1.1 200 OK  (text/ht
    874 185.011161  172.30.0.13     172.30.0.6      HTTP         501 HTTP/1.1 200 OK  (text/ht
    978 269.071102  172.30.0.13     172.30.0.6      HTTP         555 HTTP/1.1 200 OK  (text/ht
```

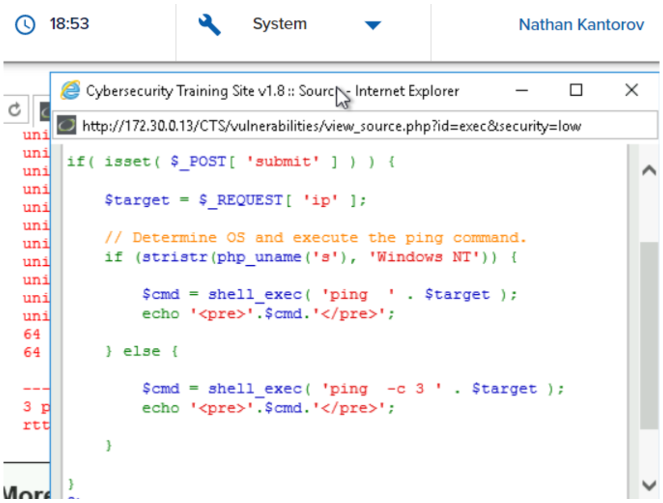
```
\t\t\t\t<img src="../../dvwa/images/letterhead_black_small.png" alt="Cybersecurity Training Site"
\r\n
\t\t\t\t<p><font color="CadetBlue">Cybersecurity Training Site</font></p>\r\n
\t\t\t</div>\r\n
\r\n
\t\t\t<div id="main_menu">\r\n
\r\n
\t\t\t\t<div id="main_menu_padded">\r\n
```

```
0000  0e 91 7d 2c 88 a1 0e 01  c7 af 1b df 08 00 45 00   ··},····  ······E·
0010  02 1d 8d 86 40 00 40 06  53 05 ac 1e 00 0d ac 1e   ····@·@·  S·······
0020  00 06 00 50 c2 f8 0e 9c  1c 6d 54 f9 f5 3a 50 18   ···P····  ·mT··:P·
0030  04 b2 a3 da 00 00 be 52  73 a4 0e 6e 98 77 f6 bd   ·······R  s··n·w··
0040  fc 16 50 5e 16 b1 2e 3f  ac f8 ef 72 43 6c 8a 81   ··P^··.?  ···rCl··
0050  98 2c af 0a 2e 70 d4 46  ac c6 4f 3b 45 7e b7 91   ·,··.p·F  ··O;E~··
0060  8d 95 9a da c8 f6 5d 8e  f8 c0 26 19 24 d3 63 1b   ······]·  ··&·$·c·
0070  d4 bd 0f 77 3a 89 35 01  f6 b4 8d be df 47 fe af   ···w:·5·  ·····G··
```

Frame (555 bytes) | Reassembled TCP (1961 bytes) | Uncompressed entity body (5081 bytes)

wireshark_5EF6B3F4-B5F5-4485-AAD...D61_20230208091814_a03736.pcapng | Packets: 1103 · Displayed: 18 (1.6%) | Profile: Default

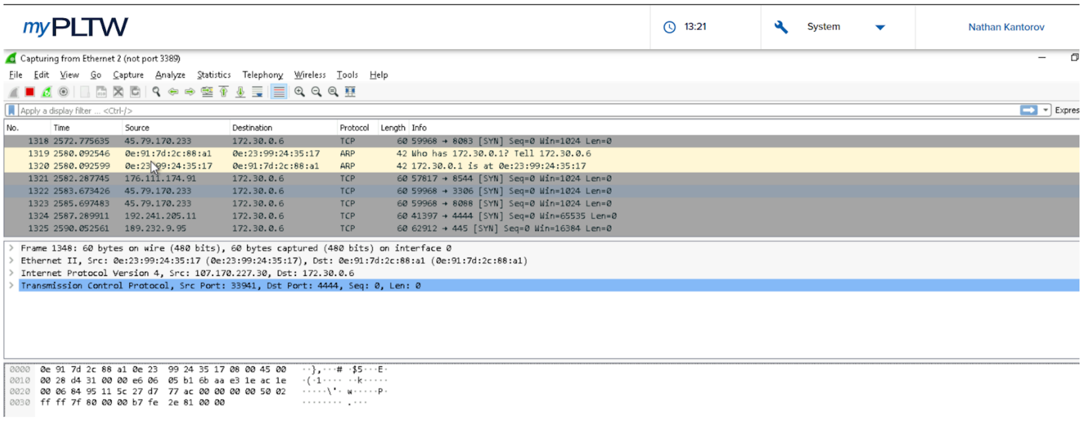
#10 - Screenshot:


18:53
System
Nathan Kantorov
Cybersecurity Training Site v1.8 :: Source - Internet Explorer

http://172.30.0.13/CTS/vulnerabilities/view_source.php?id=exec&security=low

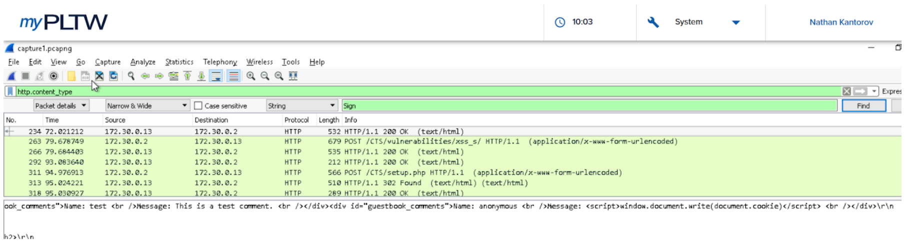
```
if( isset( $_POST[ 'submit' ] ) ) {

    $target = $_REQUEST[ 'ip' ];

    // Determine OS and execute the ping command.
    if (stristr(php_uname('s'), 'Windows NT')) {

        $cmd = shell_exec( 'ping  ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    } else {

        $cmd = shell_exec( 'ping  -c 3 ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    }

}
```

#11 - Screenshot:


myPLTW
13:21
System
Nathan Kantorov
Capturing from Ethernet 2 (not port 3389)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expres

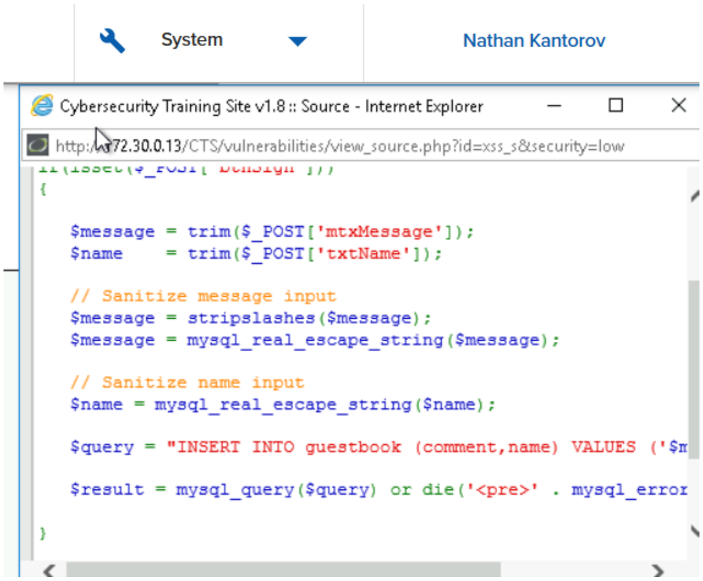
```
No.   Time         Source             Destination        Protocol Length Info
 1318 2572.775635  45.79.170.233      172.30.0.6         TCP      60 59968 → 8083 [SYN] Seq=0 Win=1024 Len=0
 1319 2580.092546  0e:91:7d:2c:88:a1  0e:23:99:24:35:17  ARP      42 Who has 172.30.0.1? Tell 172.30.0.6
 1320 2580.092599  0e:23:99:24:35:17  0e:91:7d:2c:88:a1  ARP      42 172.30.0.1 is at 0e:23:99:24:35:17
 1321 2582.287745  176.111.174.91     172.30.0.6         TCP      60 57817 → 8544 [SYN] Seq=0 Win=1024 Len=0
 1322 2583.673426  45.79.170.233      172.30.0.6         TCP      60 59968 → 3306 [SYN] Seq=0 Win=1024 Len=0
 1323 2585.697483  45.79.170.233      172.30.0.6         TCP      60 59968 → 8088 [SYN] Seq=0 Win=1024 Len=0
 1324 2587.289911  192.241.205.11     172.30.0.6         TCP      60 41397 → 4444 [SYN] Seq=0 Win=65535 Len=0
 1325 2590.052561  189.232.9.95       172.30.0.6         TCP      60 62912 → 445 [SYN] Seq=0 Win=16384 Len=0

> Frame 1348: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: 0e:23:99:24:35:17 (0e:23:99:24:35:17), Dst: 0e:91:7d:2c:88:a1 (0e:91:7d:2c:88:a1)
> Internet Protocol Version 4, Src: 107.170.227.30, Dst: 172.30.0.6
> Transmission Control Protocol, Src Port: 33941, Dst Port: 4444, Seq: 0, Len: 0

0000  0e 91 7d 2c 88 a1 0e 23  99 24 35 17 08 00 45 00   ··},···# ·$5···E·
0010  00 28 d4 31 00 00 e6 06  05 b1 6b aa e3 1e ac 1e   ·(·1···· ··k·····
0020  00 06 84 95 11 5c 27 d7  77 ac 00 00 00 00 50 02   ·····\'· w·····P·
0030  ff ff 7f 80 00 00 b7 fe  2e 81 00 00               ········ .···
```

#16 - Notebook & Screenshot:

<table>
<tr><th colspan="2">Exploit 1</th></tr>
<tr><td>a. Suspicious packet</td><td>


http.content_type

Sign

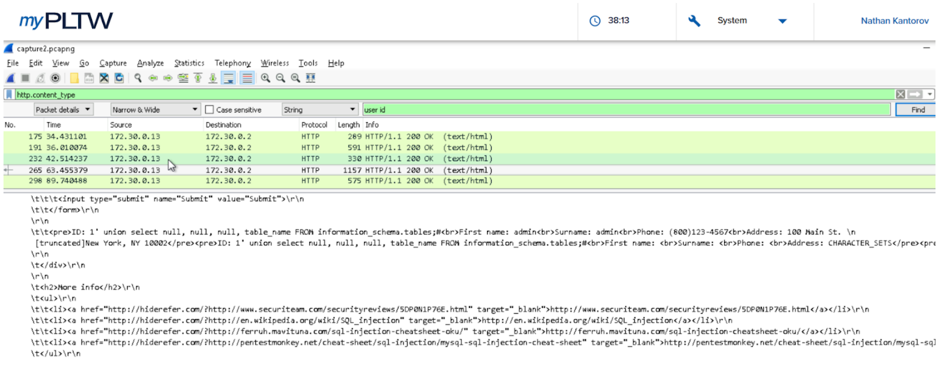
```
No.  Time       Source       Destination  Protocol Length Info
 234 72.021212  172.30.0.13  172.30.0.2   HTTP     532 HTTP/1.1 200 OK  (text/html)
 263 79.678749  172.30.0.2   172.30.0.13  HTTP     679 POST /CTS/vulnerabilities/xss_s/ HTTP/1.1  (application/x-www-form-urlencoded)
 266 79.684403  172.30.0.13  172.30.0.2   HTTP     535 HTTP/1.1 200 OK  (text/html)
 292 93.083640  172.30.0.13  172.30.0.2   HTTP     212 HTTP/1.1 200 OK  (text/html)
 311 94.976913  172.30.0.2   172.30.0.13  HTTP     566 POST /CTS/setup.php HTTP/1.1  (application/x-www-form-urlencoded)
 313 95.024221  172.30.0.13  172.30.0.2   HTTP     510 HTTP/1.1 302 Found  (text/html) (text/html)
 318 95.030927  172.30.0.13  172.30.0.2   HTTP     289 HTTP/1.1 200 OK  (text/html)

ook_comments">Name: test <br />Message: This is a test comment. <br /></div><div id="guestbook_comments">Name: anonymous <br />Message: <script>window.document.write(document.cookie)</script> <br /></div>\r\n

h2>\r\n
```
</td></tr>
<tr><td>b. Code</td><td>

System
Nathan Kantorov
Cybersecurity Training Site v1.8 :: Source - Internet Explorer

http://172.30.0.13/CTS/vulnerabilities/view_source.php?id=xss_s&security=low

```
if(isset($_POST['btnSign']))
{

   $message = trim($_POST['mtxMessage']);
   $name    = trim($_POST['txtName']);

   // Sanitize message input
   $message = stripslashes($message);
   $message = mysql_real_escape_string($message);

   // Sanitize name input
   $name = mysql_real_escape_string($name);

   $query = "INSERT INTO guestbook (comment,name) VALUES ('$m

   $result = mysql_query($query) or die('<pre>' . mysql_error

}
```
</td></tr>
<tr><td>c. What I did</td><td>After opening the capture, I filtered the packets with the http.content_type filter. Then I used the search bar to find packets that had strings from the website, and then looked at the content to see if there was anything suspicious. The information that might have compromised would be anything stored in cookies, so passwords, usernames, and so on.</td></tr>
</table>

Exploit 2

a. Suspicious packet


myPLTW
38:13
System
Nathan Kantorov
capture2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Find

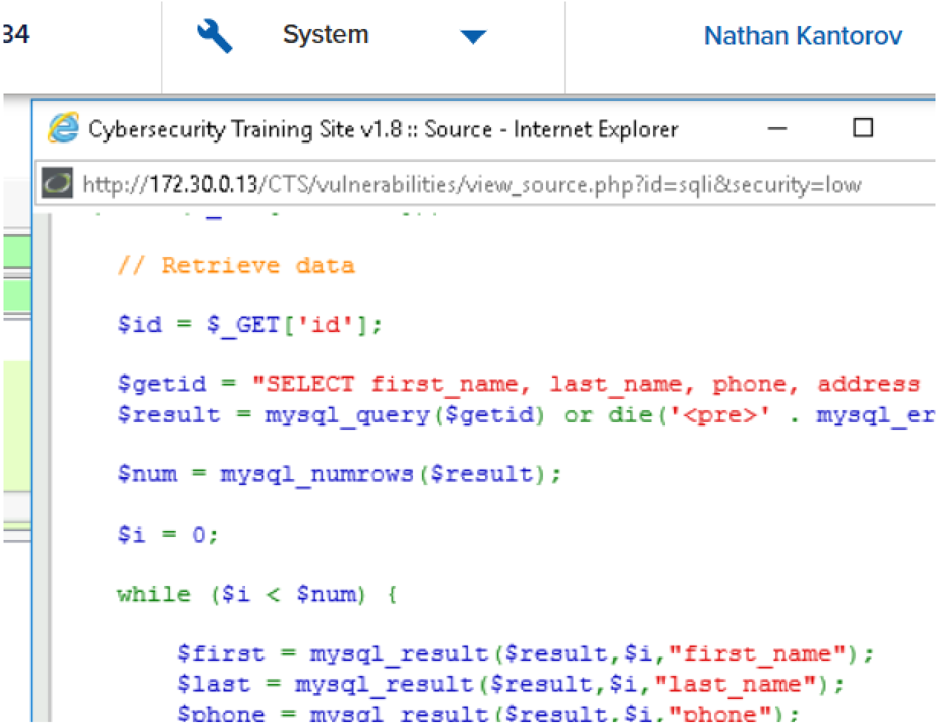
http.content_type

Packet details | Narrow & Wide | ☐ Case sensitive | String | user id

```
No.   Time        Source        Destination   Protocol  Length  Info
  175 34.431101   172.30.0.13   172.30.0.2    HTTP       289 HTTP/1.1 200 OK  (text/html)
  191 36.010074   172.30.0.13   172.30.0.2    HTTP       591 HTTP/1.1 200 OK  (text/html)
  232 42.514237   172.30.0.13   172.30.0.2    HTTP       330 HTTP/1.1 200 OK  (text/html)
  265 63.455379   172.30.0.13   172.30.0.2    HTTP      1157 HTTP/1.1 200 OK  (text/html)
  298 89.740488   172.30.0.13   172.30.0.2    HTTP       575 HTTP/1.1 200 OK  (text/html)
```

```
\t\t\t<input type="submit" name="Submit" value="Submit">\r\n
\t\t</form>\r\n
\r\n
\t\t<pre>ID: 1' union select null, null, null, table_name FROM information_schema.tables;#<br>First name: admin<br>Surname: admin<br>Phone: (800)123-4567<br>Address: 100 Main St. \n
 [truncated]New York, NY 10002</pre><pre>ID: 1' union select null, null, null, table_name FROM information_schema.tables;#<br>First name: <br>Surname: <br>Phone: <br>Address: CHARACTER_SETS</pre><pre
\r\n
\t</div>\r\n
\r\n
\t<h2>More info</h2>\r\n
\t<ul>\r\n
\t\t<li><a href="http://hiderefer.com/?http://www.securiteam.com/securityreviews/5DP0N1P76E.html" target="_blank">http://www.securiteam.com/securityreviews/5DP0N1P76E.html</a></li>\r\n
\t\t<li><a href="http://hiderefer.com/?http://en.wikipedia.org/wiki/SQL_injection" target="_blank">http://en.wikipedia.org/wiki/SQL_injection</a></li>\r\n
\t\t<li><a href="http://hiderefer.com/?http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/" target="_blank">http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/</a></li>\r\n
\t\t<li><a href="http://hiderefer.com/?http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet" target="_blank">http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql
\t</ul>\r\n
```

b. Code


34
System
Nathan Kantorov
Cybersecurity Training Site v1.8 :: Source - Internet Explorer

http://172.30.0.13/CTS/vulnerabilities/view_source.php?id=sqli&security=low

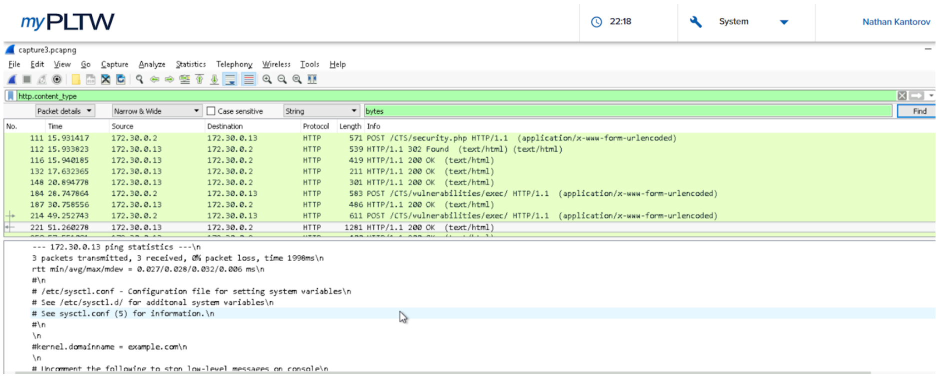
```
    // Retrieve data

    $id = $_GET['id'];

    $getid = "SELECT first_name, last_name, phone, address
    $result = mysql_query($getid) or die('<pre>' . mysql_er

    $num = mysql_numrows($result);

    $i = 0;

    while ($i < $num) {

        $first = mysql_result($result,$i,"first_name");
        $last = mysql_result($result,$i,"last_name");
        $phone = mysql_result($result,$i,"phone");
```

c. What I did

After opening the capture I used the http.content_type filter. I then looked through some of the packets to find where the breach accrued, then I looked up key phrases from that page in the packets. I then saw the suspicious packets with results including usernames and passwords, accessed through SQL injection.

Exploit 3

a. Suspicious packet



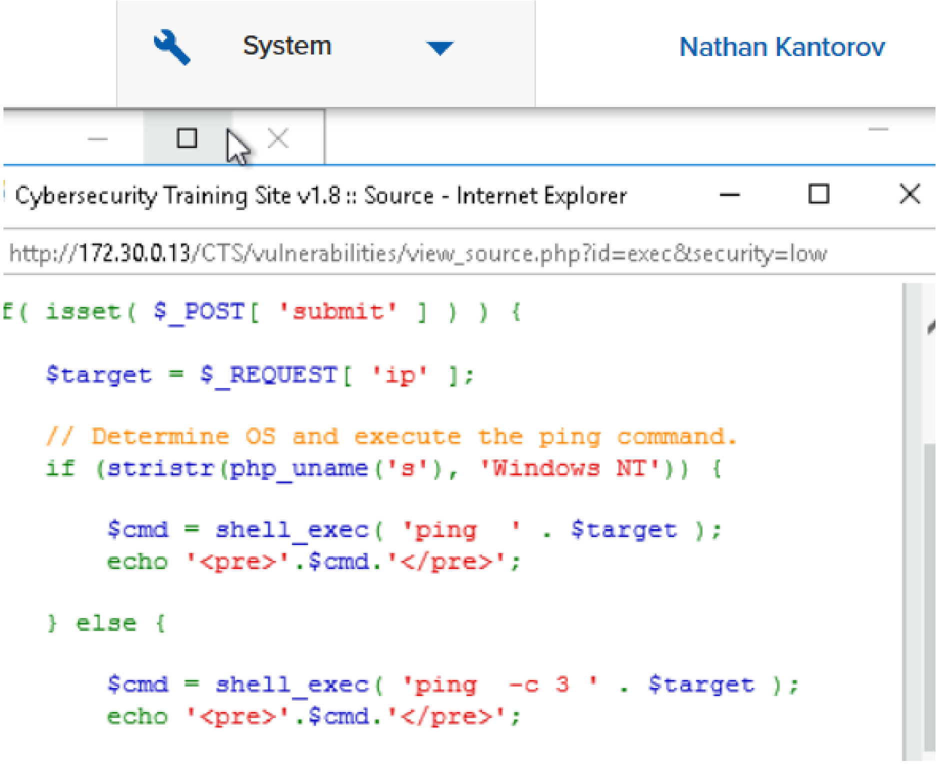
http.content_type

bytes

```
No.  Time       Source       Destination  Protocol Length Info
111 15.931417   172.30.0.2   172.30.0.13  HTTP      571 POST /CTS/security.php HTTP/1.1  (application/x-www-form-urlencoded)
112 15.933823   172.30.0.13  172.30.0.2   HTTP      539 HTTP/1.1 302 Found  (text/html) (text/html)
116 15.940185   172.30.0.13  172.30.0.2   HTTP      419 HTTP/1.1 200 OK  (text/html)
132 17.632365   172.30.0.13  172.30.0.2   HTTP      211 HTTP/1.1 200 OK  (text/html)
148 20.894778   172.30.0.13  172.30.0.2   HTTP      301 HTTP/1.1 200 OK  (text/html)
184 28.747864   172.30.0.2   172.30.0.13  HTTP      583 POST /CTS/vulnerabilities/exec/ HTTP/1.1  (application/x-www-form-urlencoded)
187 30.758556   172.30.0.13  172.30.0.2   HTTP      486 HTTP/1.1 200 OK  (text/html)
214 49.252743   172.30.0.2   172.30.0.13  HTTP      611 POST /CTS/vulnerabilities/exec/ HTTP/1.1  (application/x-www-form-urlencoded)
221 51.260278   172.30.0.13  172.30.0.2   HTTP     1281 HTTP/1.1 200 OK  (text/html)
```

```
--- 172.30.0.13 ping statistics ---\n
3 packets transmitted, 3 received, 0% packet loss, time 1998ms\n
rtt min/avg/max/mdev = 0.027/0.028/0.032/0.006 ms\n
#\n
# /etc/sysctl.conf - Configuration file for setting system variables\n
# See /etc/sysctl.d/ for additonal system variables\n
# See sysctl.conf (5) for information.\n
#\n
\n
#kernel.domainname = example.com\n
\n
# Uncomment the following to stop low-level messages on console\n
```

b. Code



System
Nathan Kantorov
Cybersecurity Training Site v1.8 :: Source - Internet Explorer
http://172.30.0.13/CTS/vulnerabilities/view_source.php?id=exec&security=low

```
f( isset( $_POST[ 'submit' ] ) ) {

   $target = $_REQUEST[ 'ip' ];

   // Determine OS and execute the ping command.
   if (stristr(php_uname('s'), 'Windows NT')) {

       $cmd = shell_exec( 'ping  ' . $target );
       echo '<pre>'.$cmd.'</pre>';

   } else {

       $cmd = shell_exec( 'ping  -c 3 ' . $target );
       echo '<pre>'.$cmd.'</pre>';
```

c. What I did

I used the http.content_type filter to find all the webpage related packets, then I looked for keywords in the PING command results, looking to see if there was anything suspicious after the ping command output. It appears that the computer can now be spoofed as well as enabled to allow packet forwarding, meaning the computer is now vulnerable to sent files containing malware.

#17 - Notebook: Why were some tasks not performed? Some tasks from the Cybersecurity lifecycle were not performed because they did not apply to the current situation. For example, there was now way that we could recover anything, so that was not possible to do. We could, however, identify what happened and why, then prevent that from happening again in the future.

#18 - Notebook: Describe what each team member contributed. We helped each other look through the packets, as there were times where it was hard to tell whether or not we had the correct packet.

Describe one moment during teamwork when your team: Worked well together. Could improve on collaboration. We had good communication, however we could have probably worked a bit on making sure everyone was on the same page.

Conclusion

1. How do you think the people responsible for the web server, web pages, and scripts could have prevented these vulnerabilities? The people responsible for the web server, web pages, and scripts could have prevented these vulnerabilities by making sure that all the inputs are sanitized completely and correctly before being used to find any information/data.
2. Why is this series of pen testing an ethical use of hacking skills?
   This is an ethical use of hacking skills because it helps build knowledge on how to better improve site security, with everyone having full knowledge of what is going on and what can and cannot be done.