# TASK 5

1. Using A Firewall to Stop Attacks
   1. Search for any third-party firewall software on the Internet.
   2. Install and run the firewall into a lab virtual Windows 7 machine. Make sure the Windows firewall is off.
   3. Run back the **THREE (3)** exploits from your previous task (Task 4A lab assignment 2). Make sure the attacks are still successful.
   4. Now run the third-party firewall and set it up to make sure that the attacks earlier can be stopped by the firewall.
   5. Show inside the firewall logs or its screening area that it has stopped the attacks successfully.

***Provide a step-by-step screen snapshot with an explanation.***

# TASK 6

1. Capture Wireless Access Data Transmission
   1. Create and set a Wi-Fi hotspot network environment with a wireless connection using your computer. Connect your phone to the hotspot.
2. Open Settings

A screenshot of a computer

Description automatically generated

1. Open Menu tab Network & Internet

A screenshot of a computer

Description automatically generated

1. click menu Mobile Hotspot.

A screenshot of a computer

Description automatically generated

1. (Optional) Select Properties, and configure your mobile Hotspot. Configure your Name, password (must 7 characters, and Band (5 Ghz, 2.4 Ghz, or any available)

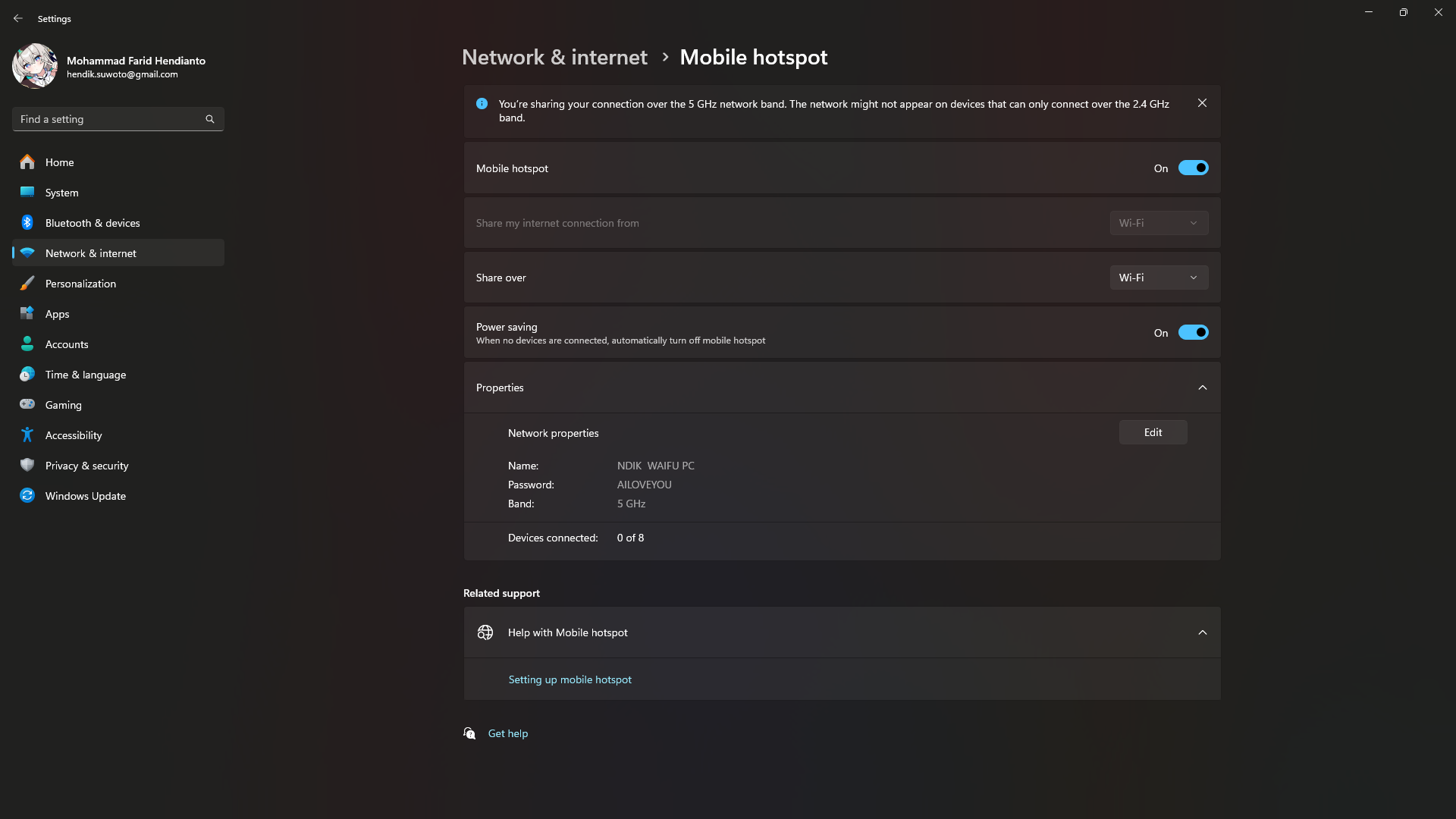
A screenshot of a computer

Description automatically generated

A screenshot of a computer

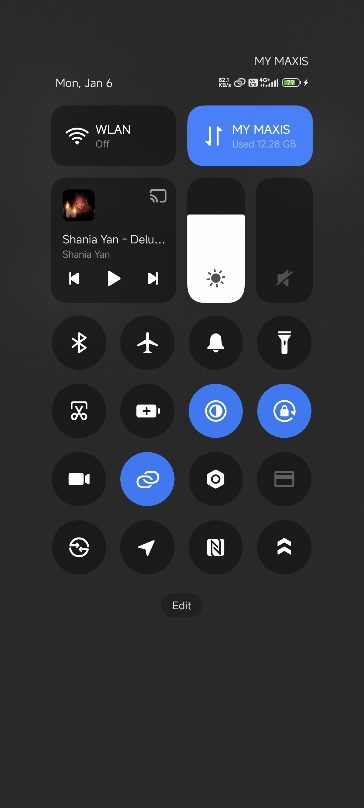
Description automatically generated

1. Click switch Mobile Data to ON



* 1. Show how you set the network and connected your mobile phone to your Wi-Fi hotspot network. Show a step-by-step screen snapshot of how you configure it until the phone can fully connect to the wireless and get an Internet connection. Report on the wireless security configuration.

1. Make sure the Mobile Hotspot from the computer is on’
2. Open quick settings Android on top bar, and click WLAN button



1. Click, “More Settings”

A screenshot of a phone

Description automatically generated

1. Click WIFI with SSID “NDIK WAIFU PC”

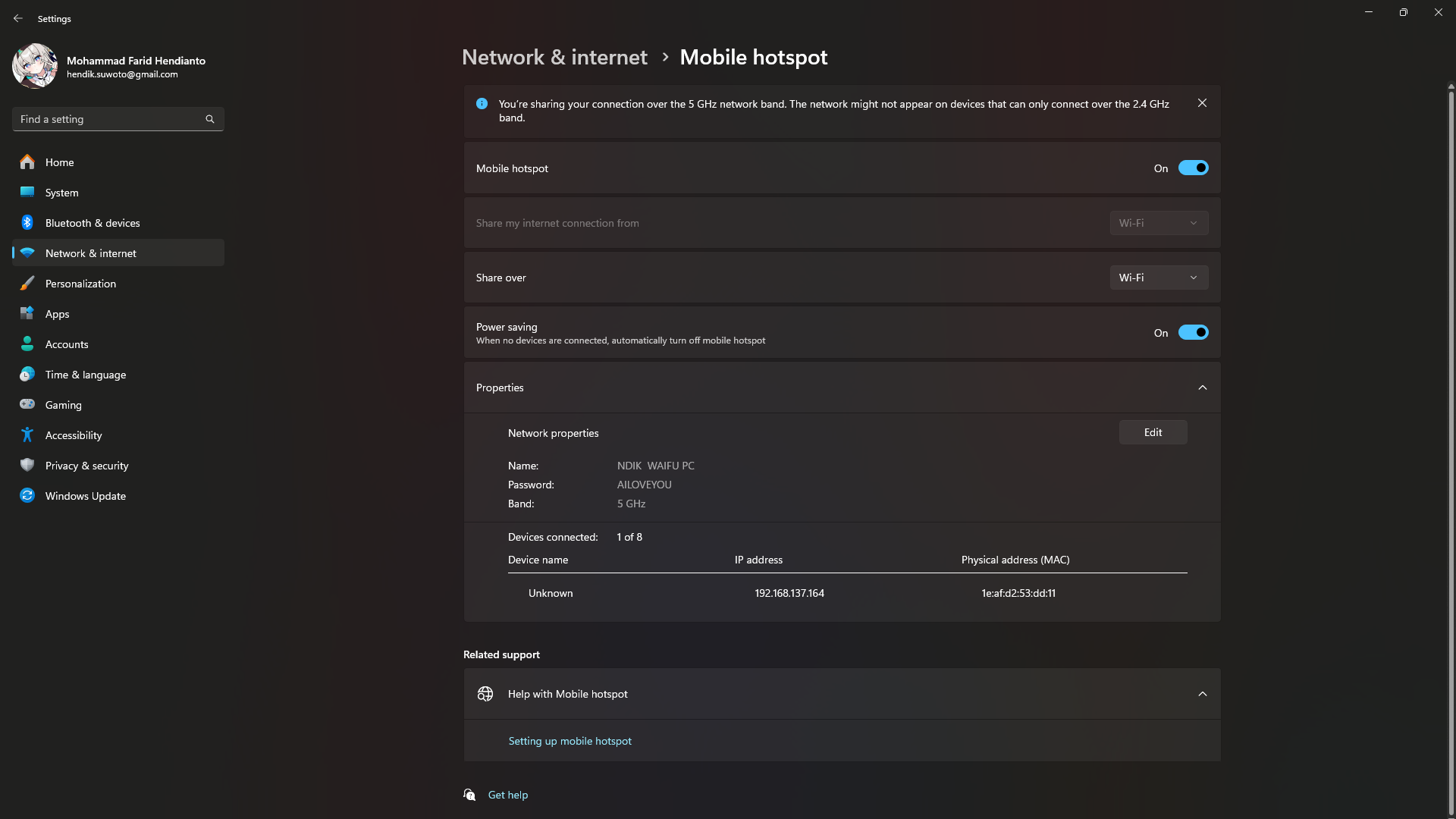
A screenshot of a phone

Description automatically generated

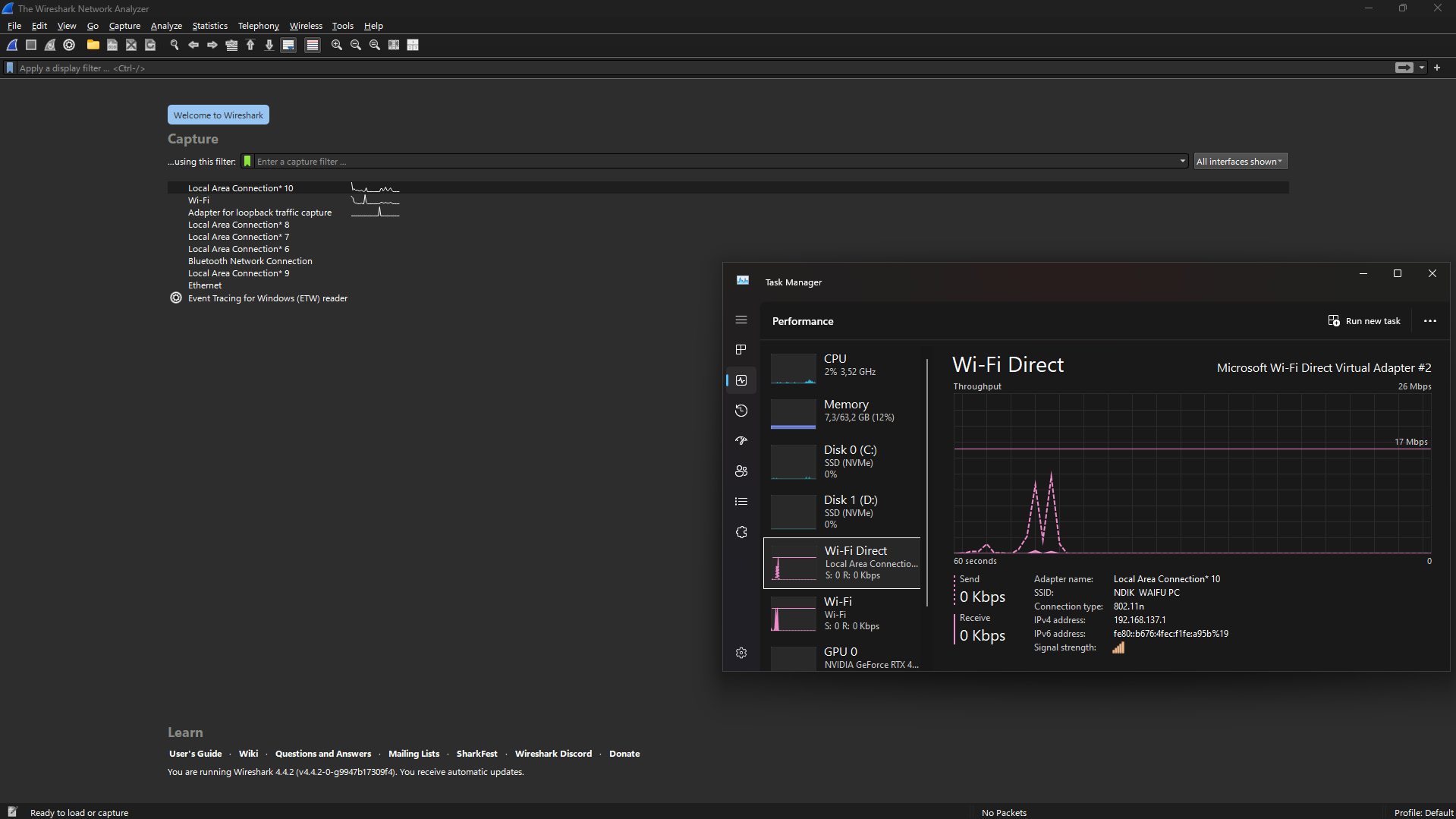
1. Input the password “AILOVEYOU”. Now your WIFI is connected to “NDIK WAIFU PC”. Device show connected on PC.

A screenshot of a phone

Description automatically generated A screenshot of a phone

Description automatically generated 

* 1. Run the Wireshark program on your computer and capture traffic from the Wi-Fi hotspot network. Try to log in and access the e-banking system, UMPSA’s Kalam website and <http://testphp.vulnweb.com/login.php> website using your phone. Stop the Wireshark capture traffic.



Setup:

Download wireshark on Windows, then open Wireshark. Capture Local Area Connection 10 (adjust based your Wi-Fi Virtual driver on your Windows. Then double click on it.

**e-banking system (BRIMO)**

1. Open BRIMO application. If you haven’t already downloaded it, search BRIMO from Google Play Store
2. Click Login button

A screenshot of a mobile app

Description automatically generated

1. Input username and password, then click Login

A screenshot of a video game

Description automatically generated

1. Now you have in dashboard BRIMO

A screenshot of a phone

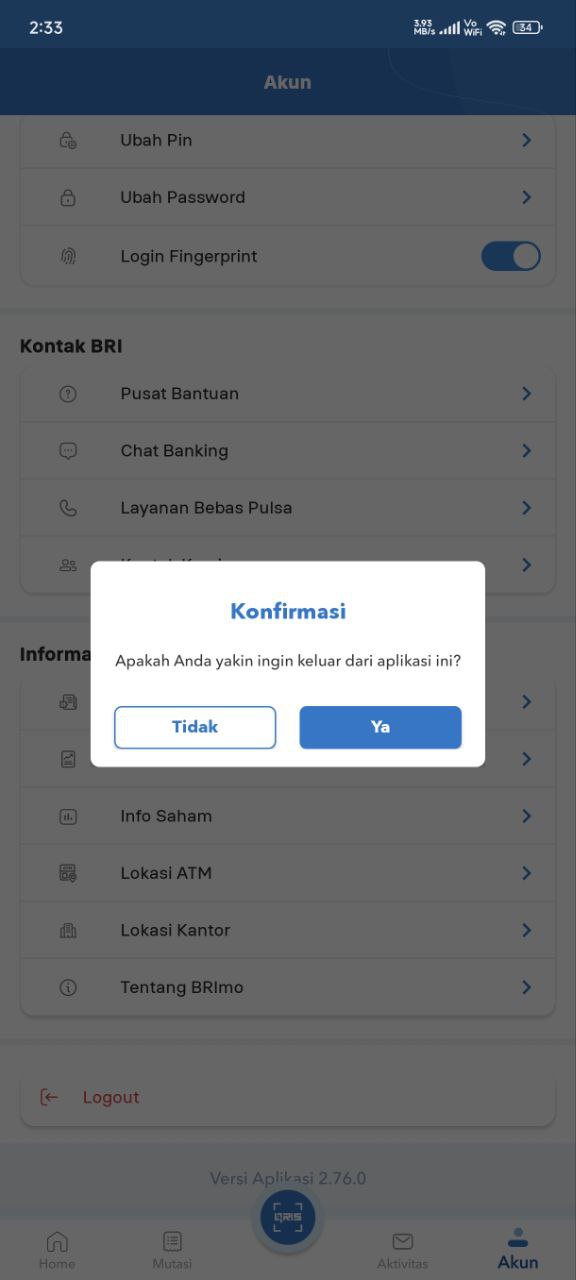
Description automatically generated

1. Click “Akun”, then click Logout button

A screenshot of a phone

Description automatically generated

1. Confirmation dialog Logout, click “Ya”.



**UMPSA’s Kalam website**

1. Access link <https://kalam.ump.edu.my/> from your Android browser

A screenshot of a phone

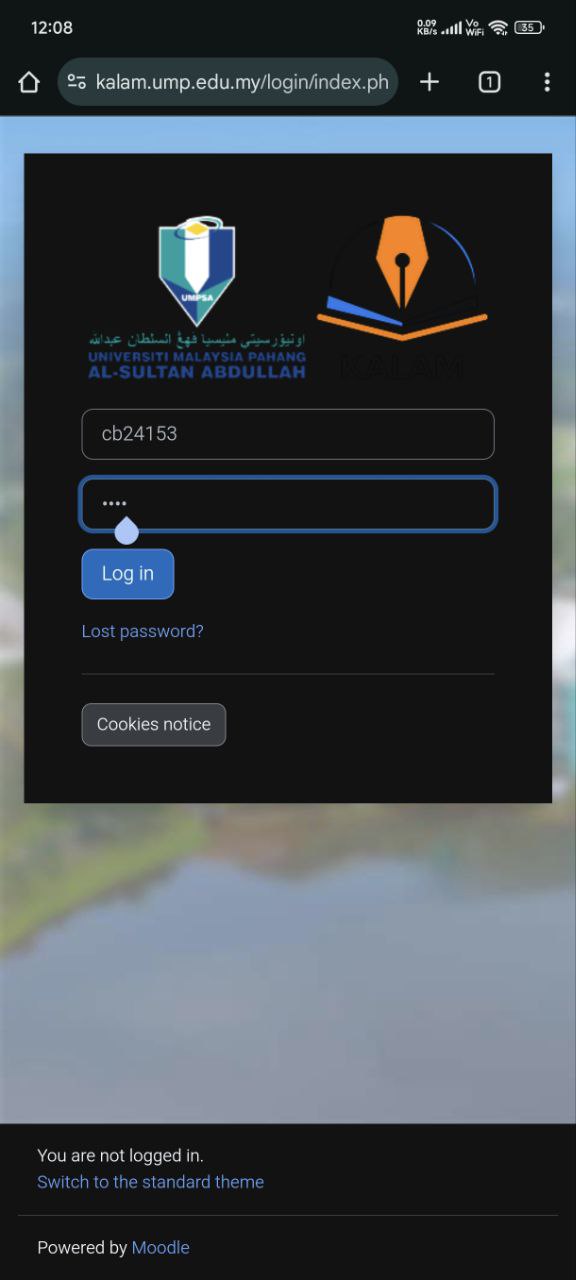
Description automatically generated

1. Click Login button on top right

A screenshot of a cell phone

Description automatically generated

1. Input username with Matrix ID and password. First try with wrong password

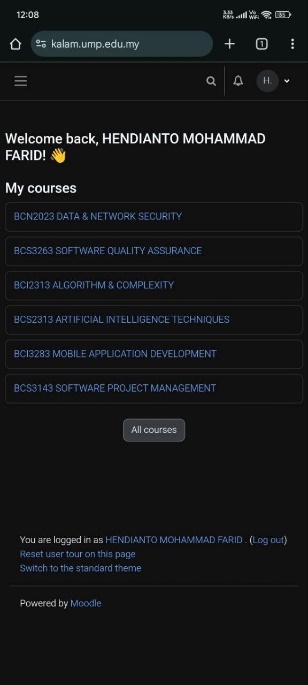


1. Input username and password with correct password

A screenshot of a login form

Description automatically generated

1. Now you have navigated it into the dashboard page.

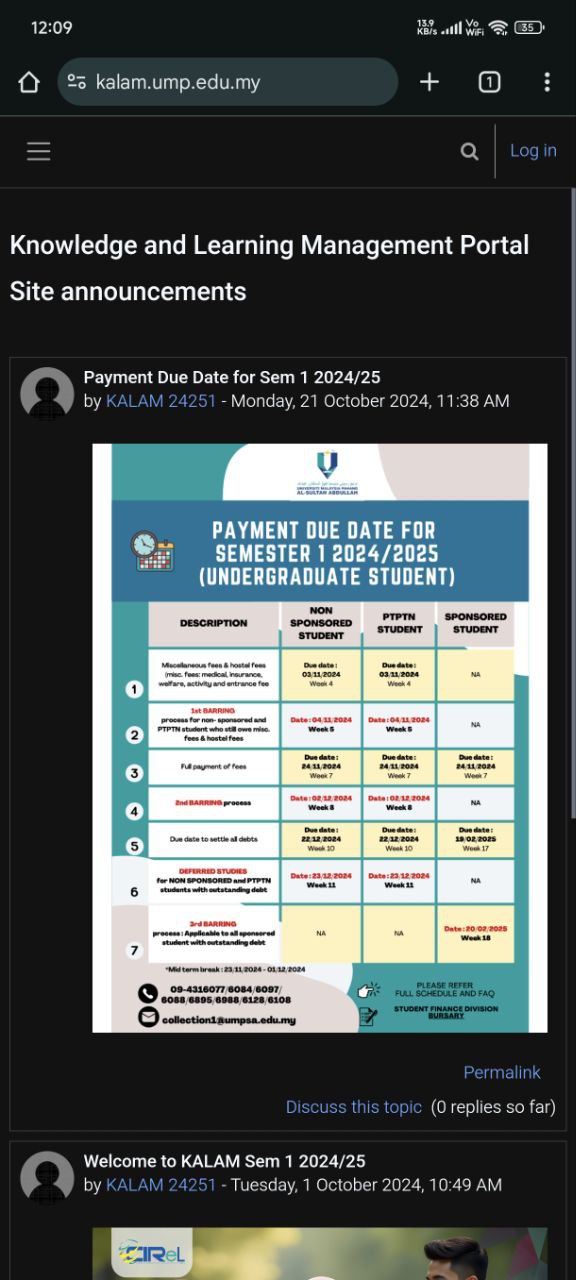


1. Click photo profile on top right side, then click logout

A screenshot of a computer

Description automatically generated

1. Now you have successfully logout the account.

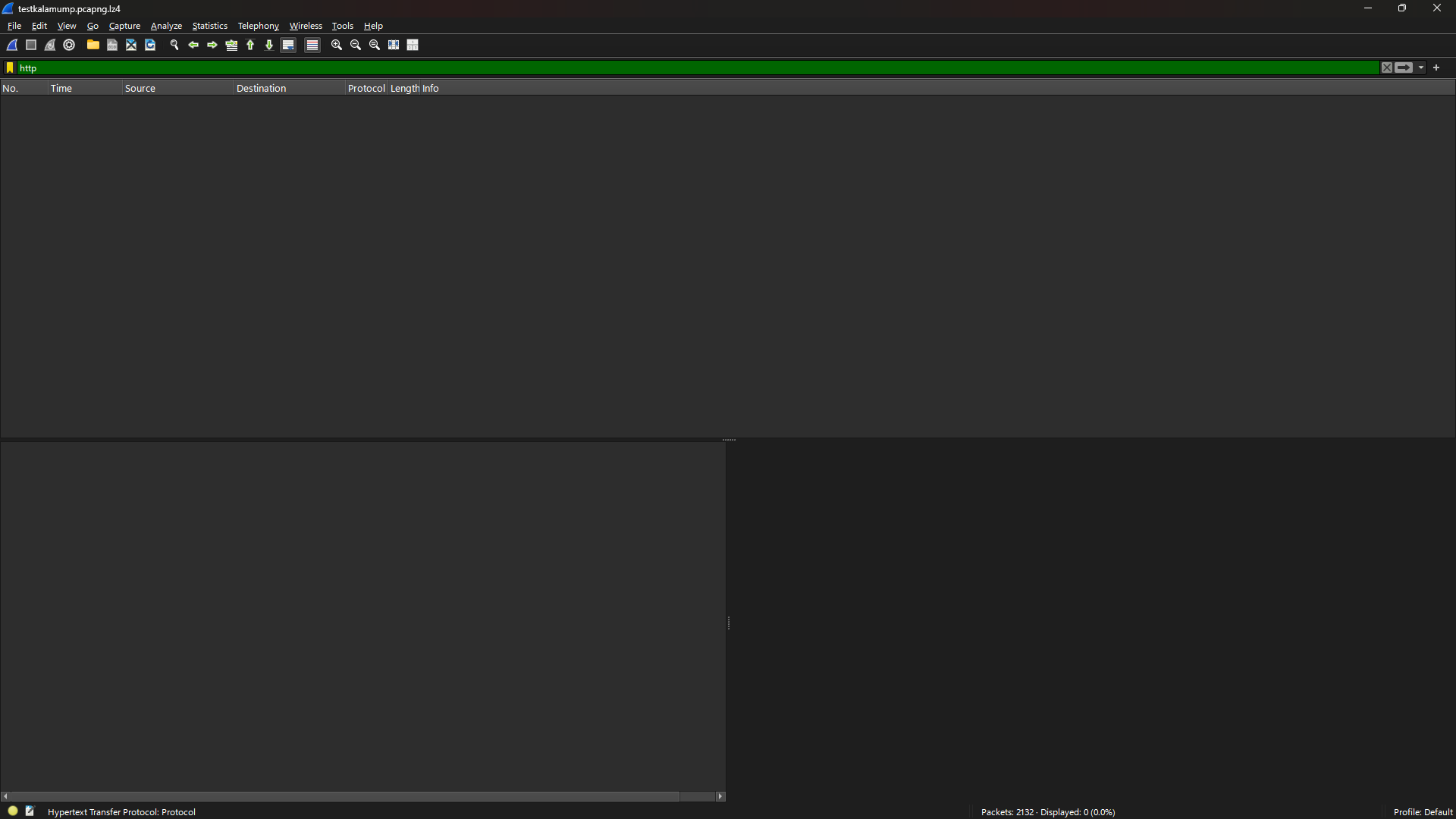


Because kalam UMPSA is encrypted, we must search

tls.handshake.type eq 1

A screenshot of a computer

Description automatically generated



A screenshot of a computer

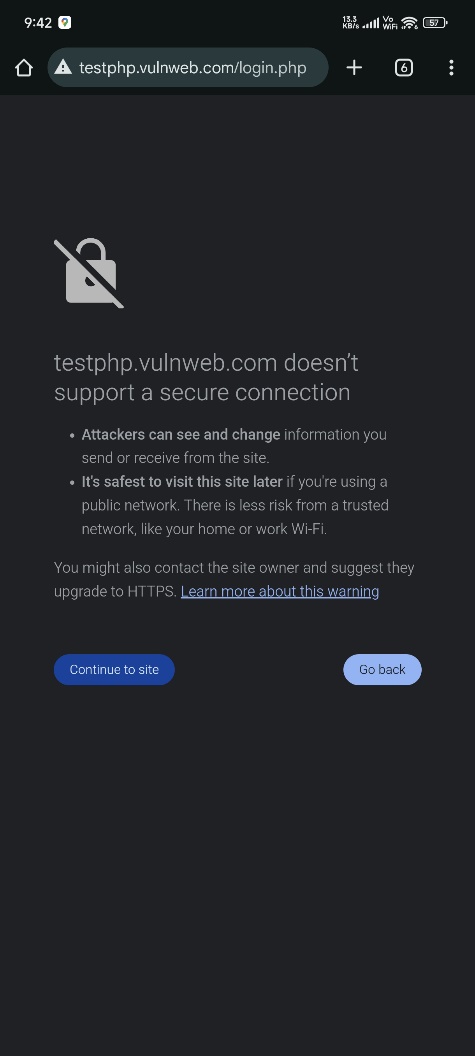
Description automatically generated

A screenshot of a computer

Description automatically generated

**Testphp.vulnweb**

1. Access link <http://testphp.vulnweb.com/login.php> from your Android browser.
2. If there warning, click “Continue to site” because the web still HTTP.



1. Input textbox Username with “UMPSA” and Password with “CB24153”. This for checking error handling.

A screenshot of a computer

Description automatically generated

1. Input textbox Username and Password with “test”

A screenshot of a computer

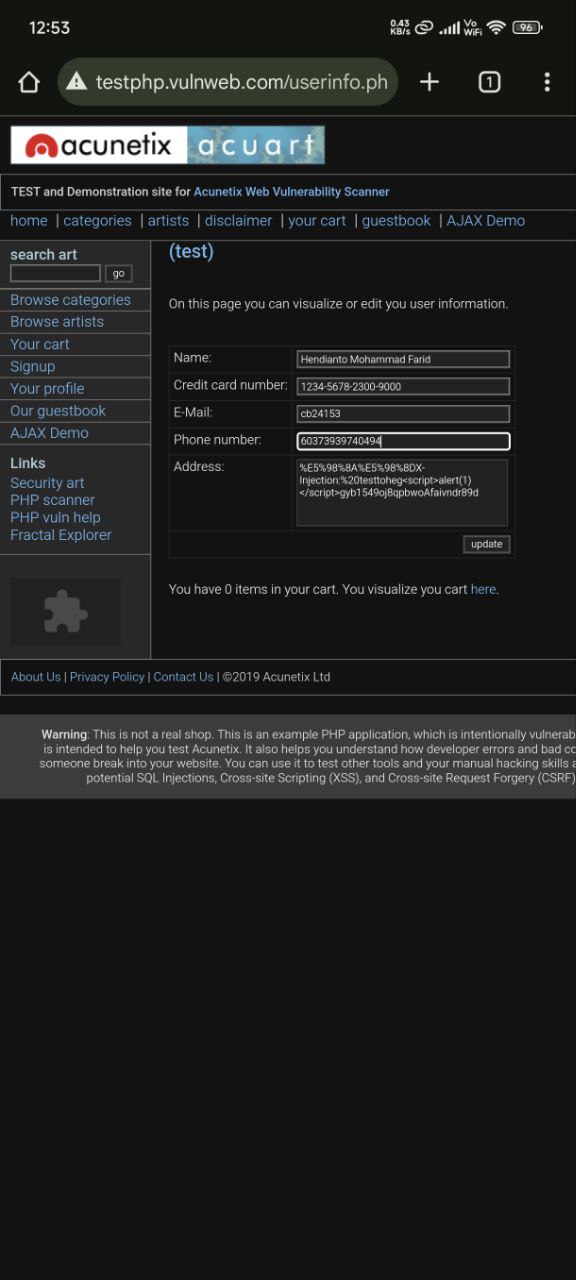
Description automatically generated

1. After login successfully, click OK from the warning “Change your password” because the password found in a data breach and written in the website.

A screenshot of a computer

Description automatically generated

1. Edit the information about Name, Credit card number, E Mail, Phone number, and Address, then click Update.



1. After clicking update, name from **(test)** will update into **Hendianto Mohammad Farid (test)**

A screenshot of a computer

Description automatically generated

1. Click Logout on left side navigation tab.

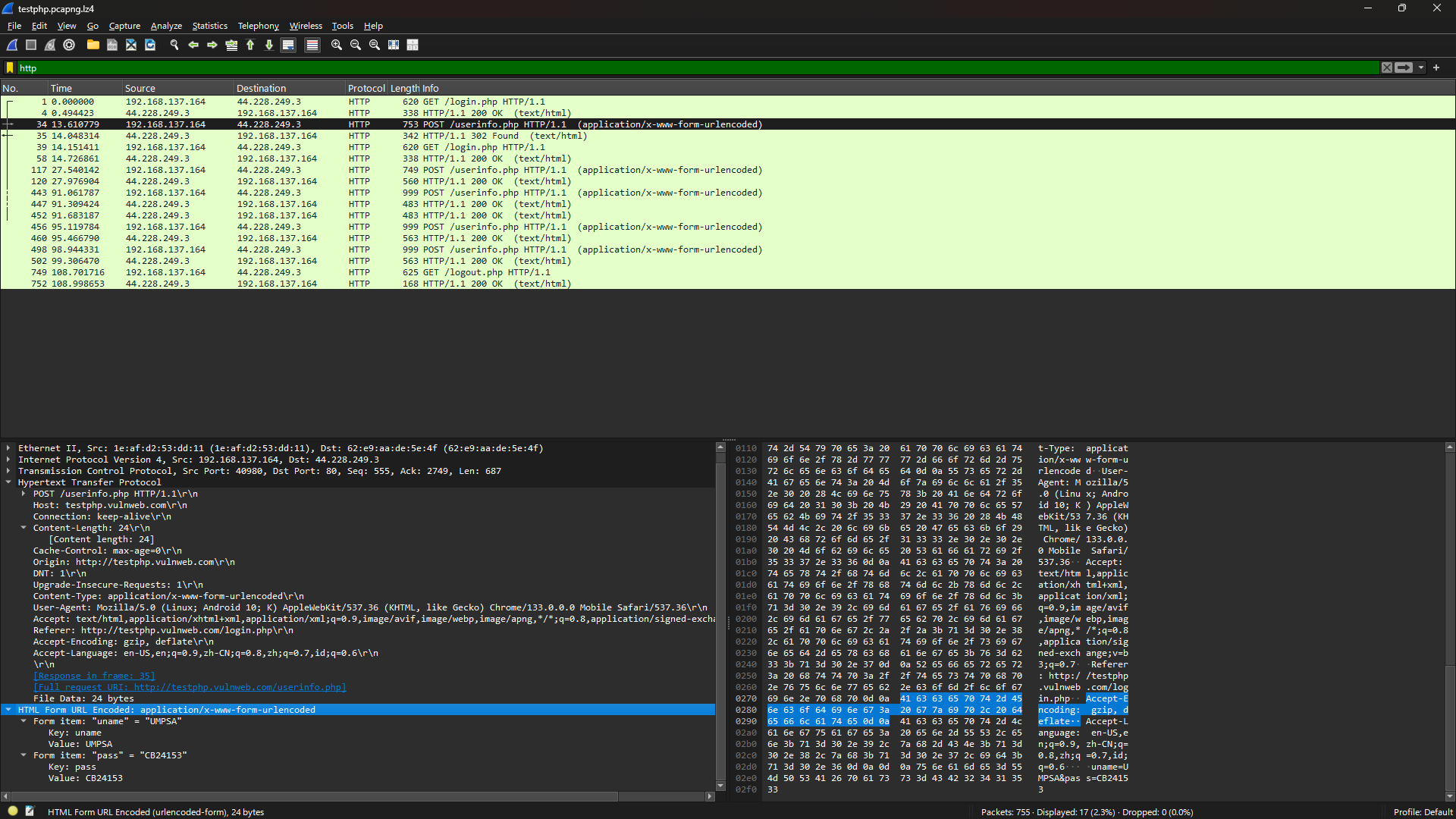
A screenshot of a computer

Description automatically generated

Search http

A screen shot of a computer

Description automatically generated



|  |
| --- |
| Frame 34: 753 bytes on wire (6024 bits), 753 bytes captured (6024 bits) on interface \Device\NPF\_{E419A63D-D7AE-4D5C-A6F5-9C9AE503FE7F}, id 0  Ethernet II, Src: 1e:af:d2:53:dd:11 (1e:af:d2:53:dd:11), Dst: 62:e9:aa:de:5e:4f (62:e9:aa:de:5e:4f)  Internet Protocol Version 4, Src: 192.168.137.164, Dst: 44.228.249.3  Transmission Control Protocol, Src Port: 40980, Dst Port: 80, Seq: 555, Ack: 2749, Len: 687  Hypertext Transfer Protocol  POST /userinfo.php HTTP/1.1\r\n  Host: testphp.vulnweb.com\r\n  Connection: keep-alive\r\n  Content-Length: 24\r\n  [Content length: 24]  Cache-Control: max-age=0\r\n  Origin: http://testphp.vulnweb.com\r\n  DNT: 1\r\n  Upgrade-Insecure-Requests: 1\r\n  Content-Type: application/x-www-form-urlencoded\r\n  User-Agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Mobile Safari/537.36\r\n  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n  Referer: http://testphp.vulnweb.com/login.php\r\n  Accept-Encoding: gzip, deflate\r\n  Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7,id;q=0.6\r\n  \r\n  [Response in frame: 35]  [Full request URI: http://testphp.vulnweb.com/userinfo.php]  File Data: 24 bytes  HTML Form URL Encoded: application/x-www-form-urlencoded  Form item: "uname" = "UMPSA"  Key: uname  Value: UMPSA  Form item: "pass" = "CB24153"  Key: pass  Value: CB24153 |

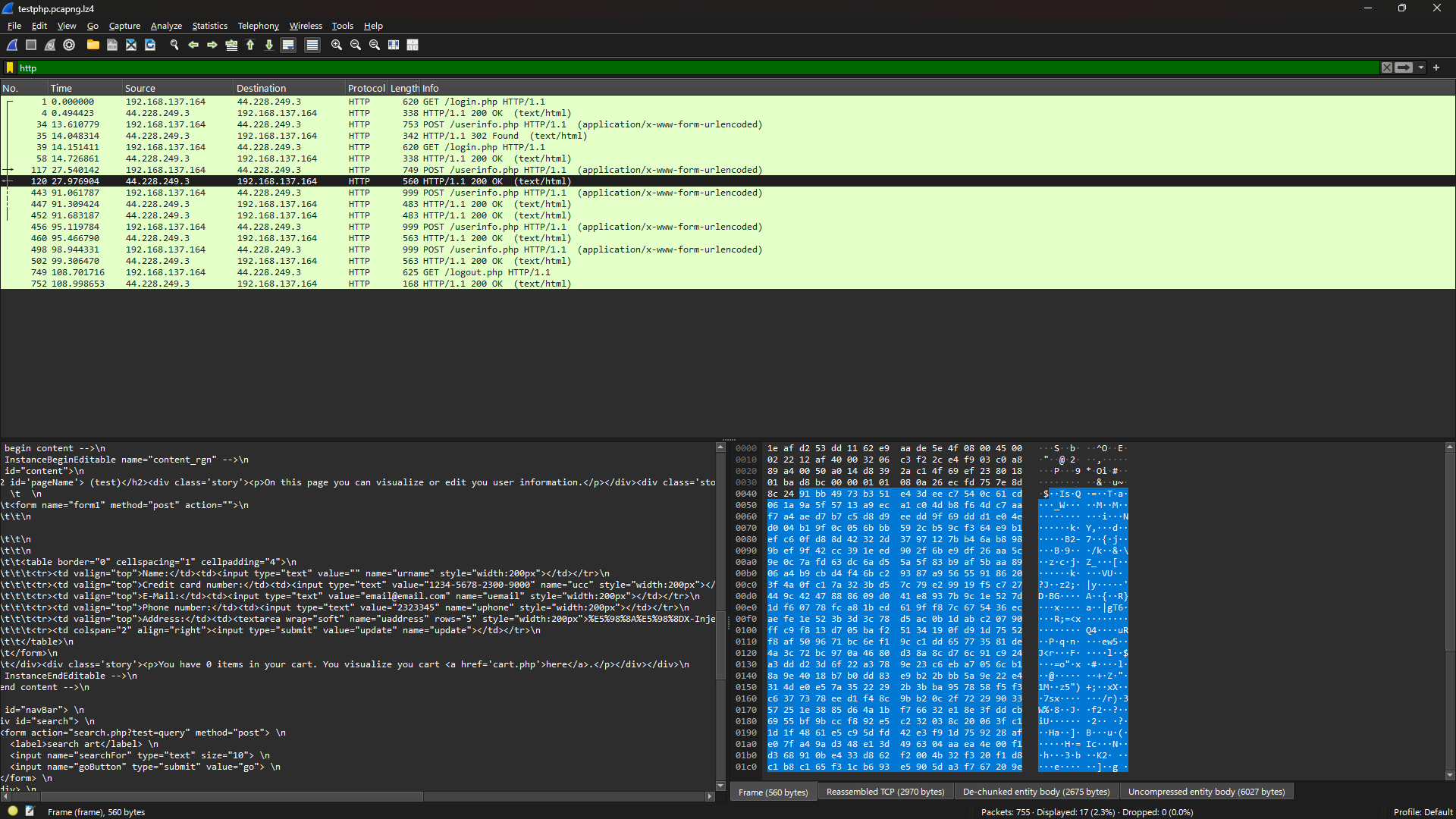
A screenshot of a computer

Description automatically generated

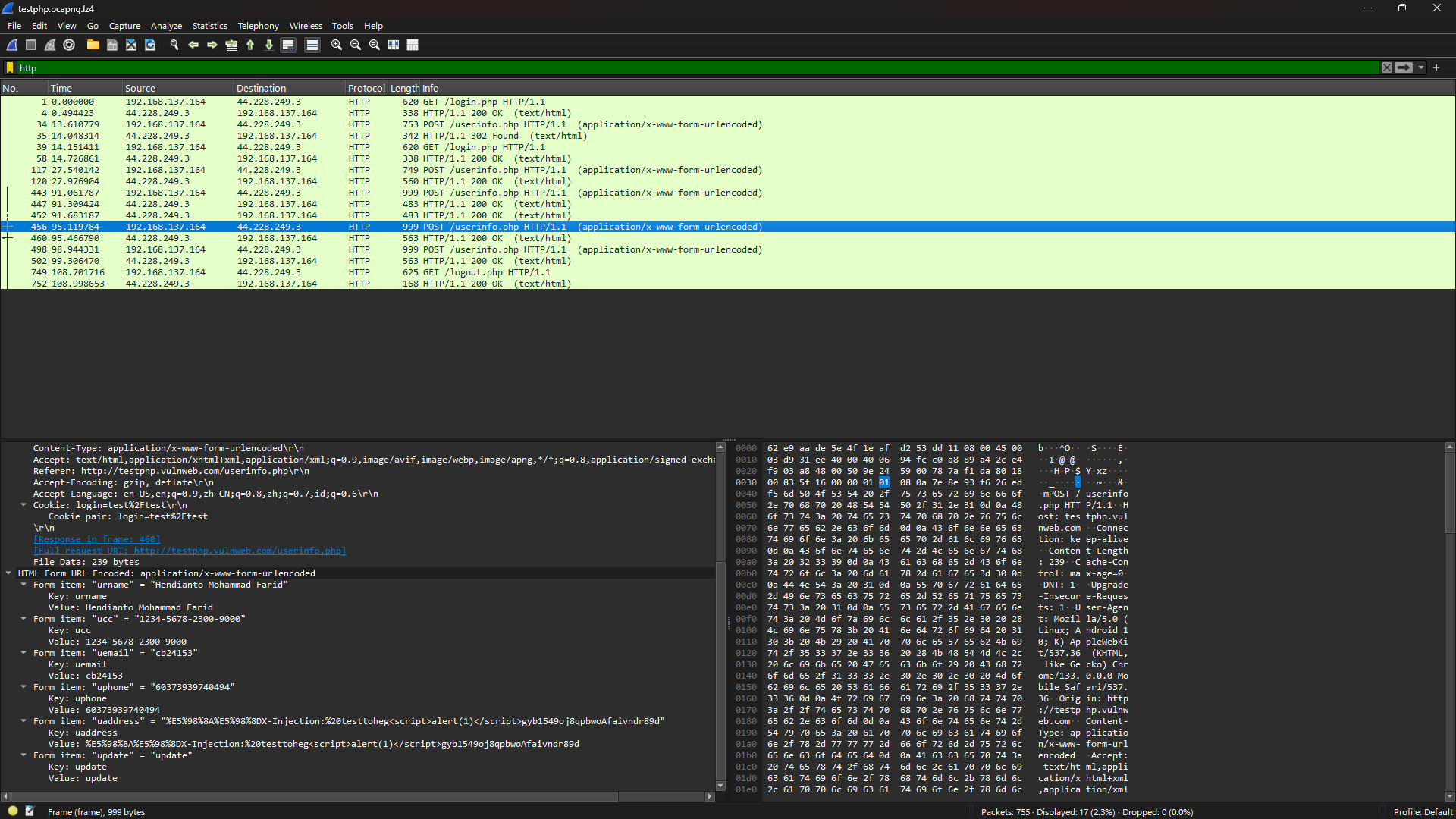
|  |
| --- |
| Frame 35: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF\_{E419A63D-D7AE-4D5C-A6F5-9C9AE503FE7F}, id 0  Ethernet II, Src: 62:e9:aa:de:5e:4f (62:e9:aa:de:5e:4f), Dst: 1e:af:d2:53:dd:11 (1e:af:d2:53:dd:11)  Internet Protocol Version 4, Src: 44.228.249.3, Dst: 192.168.137.164  Transmission Control Protocol, Src Port: 80, Dst Port: 40980, Seq: 2749, Ack: 1242, Len: 276  Hypertext Transfer Protocol, has 2 chunks (including last chunk)  HTTP/1.1 302 Found\r\n  Server: nginx/1.19.0\r\n  Date: Mon, 06 Jan 2025 16:52:47 GMT\r\n  Content-Type: text/html; charset=UTF-8\r\n  Transfer-Encoding: chunked\r\n  Connection: keep-alive\r\n  X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1\r\n  Location: login.php\r\n  \r\n  [Request in frame: 34]  [Time since request: 0.437535000 seconds]  [Request URI: /userinfo.php]  [Full request URI: http://testphp.vulnweb.com/userinfo.php]  HTTP chunked response  File Data: 14 bytes  Line-based text data: text/html (1 lines)  you must login |



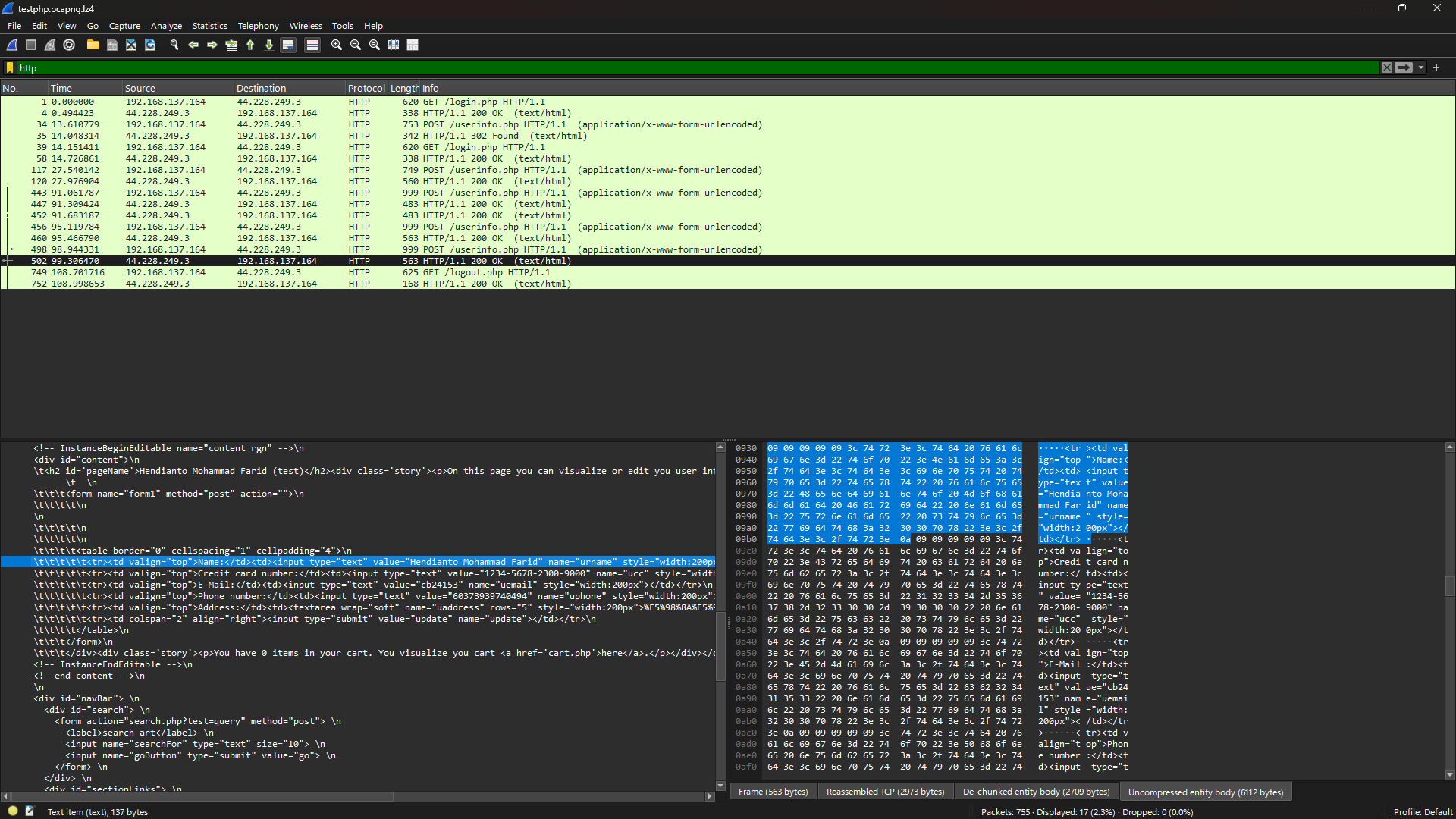
|  |
| --- |
| Frame 117: 749 bytes on wire (5992 bits), 749 bytes captured (5992 bits) on interface \Device\NPF\_{E419A63D-D7AE-4D5C-A6F5-9C9AE503FE7F}, id 0  Ethernet II, Src: 1e:af:d2:53:dd:11 (1e:af:d2:53:dd:11), Dst: 62:e9:aa:de:5e:4f (62:e9:aa:de:5e:4f)  Internet Protocol Version 4, Src: 192.168.137.164, Dst: 44.228.249.3  Transmission Control Protocol, Src Port: 40980, Dst Port: 80, Seq: 1796, Ack: 5773, Len: 683  Hypertext Transfer Protocol  POST /userinfo.php HTTP/1.1\r\n  Host: testphp.vulnweb.com\r\n  Connection: keep-alive\r\n  Content-Length: 20\r\n  [Content length: 20]  Cache-Control: max-age=0\r\n  Origin: http://testphp.vulnweb.com\r\n  DNT: 1\r\n  Upgrade-Insecure-Requests: 1\r\n  Content-Type: application/x-www-form-urlencoded\r\n  User-Agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Mobile Safari/537.36\r\n  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n  Referer: http://testphp.vulnweb.com/login.php\r\n  Accept-Encoding: gzip, deflate\r\n  Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7,id;q=0.6\r\n  \r\n  [Response in frame: 120]  [Full request URI: http://testphp.vulnweb.com/userinfo.php]  File Data: 20 bytes  HTML Form URL Encoded: application/x-www-form-urlencoded  Form item: "uname" = "test"  Key: uname  Value: test  Form item: "pass" = "test"  Key: pass  Value: test |



|  |
| --- |
| Frame 120: 560 bytes on wire (4480 bits), 560 bytes captured (4480 bits) on interface \Device\NPF\_{E419A63D-D7AE-4D5C-A6F5-9C9AE503FE7F}, id 0  Ethernet II, Src: 62:e9:aa:de:5e:4f (62:e9:aa:de:5e:4f), Dst: 1e:af:d2:53:dd:11 (1e:af:d2:53:dd:11)  Internet Protocol Version 4, Src: 44.228.249.3, Dst: 192.168.137.164  Transmission Control Protocol, Src Port: 80, Dst Port: 40980, Seq: 8249, Ack: 2479, Len: 494  [3 Reassembled TCP Segments (2970 bytes): #118(1238), #119(1238), #120(494)]  Hypertext Transfer Protocol, has 2 chunks (including last chunk)  HTTP/1.1 200 OK\r\n  Server: nginx/1.19.0\r\n  Date: Mon, 06 Jan 2025 16:53:01 GMT\r\n  Content-Type: text/html; charset=UTF-8\r\n  Transfer-Encoding: chunked\r\n  Connection: keep-alive\r\n  X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1\r\n  Set-Cookie: login=test%2Ftest\r\n  Content-Encoding: gzip\r\n  \r\n  [Request in frame: 117]  [Time since request: 0.436762000 seconds]  [Request URI: /userinfo.php]  [Full request URI: http://testphp.vulnweb.com/userinfo.php]  HTTP chunked response  Content-encoded entity body (gzip): 2675 bytes -> 6027 bytes  File Data: 6027 bytes  Line-based text data: text/html (119 lines)  <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"\n  "http://www.w3.org/TR/html4/loose.dtd">\n  <html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHTMLIsLocked="false" -->\n  <head>\n  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">\n  \n  <!-- InstanceBeginEditable name="document\_title\_rgn" -->\n  <title>user info</title>\n  <!-- InstanceEndEditable -->\n  <link rel="stylesheet" href="style.css" type="text/css">\n  <!-- InstanceBeginEditable name="headers\_rgn" -->\n  <!-- here goes headers headers -->\n  <!-- InstanceEndEditable -->\n  <script language="JavaScript" type="text/JavaScript">\n  <!--\n  function MM\_reloadPage(init) { //reloads the window if Nav4 resized\n  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {\n  document.MM\_pgW=innerWidth; document.MM\_pgH=innerHeight; onresize=MM\_reloadPage; }}\n  else if (innerWidth!=document.MM\_pgW || innerHeight!=document.MM\_pgH) location.reload();\n  }\n  MM\_reloadPage(true);\n  //-->\n  </script>\n  \n  </head>\n  <body> \n  <div id="mainLayer" style="position:absolute; width:700px; z-index:1">\n  <div id="masthead"> \n  <h1 id="siteName"><a href="https://www.acunetix.com/"><img src="images/logo.gif" width="306" height="38" border="0" alt="Acunetix website security"></a></h1> \n  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></h6>\n  <div id="globalNav"> \n  \t<table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>\n  \t<td align="left">\n  \t\t<a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="artists.php">artists\n  \t\t</a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> | \n  \t\t<a href="guestbook.php">guestbook</a> | \n  \t\t<a href="AJAX/index.php">AJAX Demo</a>\n  \t</td>\n  \t<td align="right">\n  \t<a href='logout.php'>Logout test</a>\t</td>\n  \t</tr></table>\n  </div> \n  </div> \n  <!-- end masthead --> \n  \n  <!-- begin content -->\n  <!-- InstanceBeginEditable name="content\_rgn" -->\n  <div id="content">\n  \t<h2 id='pageName'> (test)</h2><div class='story'><p>On this page you can visualize or edit you user information.</p></div><div class='story'>\n  \t \n  \t\t\t<form name="form1" method="post" action="">\n  \t\t\t\t\n  \n  \t\t\t\t\n  \t\t\t\t\n  \t\t\t\t<table border="0" cellspacing="1" cellpadding="4">\n  \t\t\t\t\t<tr><td valign="top">Name:</td><td><input type="text" value="" name="urname" style="width:200px"></td></tr>\n  \t\t\t\t\t<tr><td valign="top">Credit card number:</td><td><input type="text" value="1234-5678-2300-9000" name="ucc" style="width:200px"></td></tr>\n  \t\t\t\t\t<tr><td valign="top">E-Mail:</td><td><input type="text" value="email@email.com" name="uemail" style="width:200px"></td></tr>\n  \t\t\t\t\t<tr><td valign="top">Phone number:</td><td><input type="text" value="2323345" name="uphone" style="width:200px"></td></tr>\n  \t\t\t\t\t<tr><td valign="top">Address:</td><td><textarea wrap="soft" name="uaddress" rows="5" style="width:200px">%E5%98%8A%E5%98%8DX-Injection:%20testtoheg<script>alert(1)</script>gyb1549oj8qpbwoAfaivndr89d</textarea></td></tr>\n  \t\t\t\t\t<tr><td colspan="2" align="right"><input type="submit" value="update" name="update"></td></tr>\n  \t\t\t\t</table>\n  \t\t\t</form>\n  \t\t\t</div><div class='story'><p>You have 0 items in your cart. You visualize you cart <a href='cart.php'>here</a>.</p></div></div>\n  <!-- InstanceEndEditable -->\n  <!--end content -->\n  \n  <div id="navBar"> \n  <div id="search"> \n  <form action="search.php?test=query" method="post"> \n  <label>search art</label> \n  <input name="searchFor" type="text" size="10"> \n  <input name="goButton" type="submit" value="go"> \n  </form> \n  </div> \n  <div id="sectionLinks"> \n  <ul> \n  <li><a href="categories.php">Browse categories</a></li> \n  <li><a href="artists.php">Browse artists</a></li> \n  <li><a href="cart.php">Your cart</a></li> \n  <li><a href="login.php">Signup</a></li>\n  \t <li><a href="userinfo.php">Your profile</a></li>\n  \t <li><a href="guestbook.php">Our guestbook</a></li>\n  \t\t<li><a href="AJAX/index.php">AJAX Demo</a></li>\n  \t </li> \n  </ul> \n  </div> \n  <div class="relatedLinks"> \n  <h3>Links</h3> \n  <ul> \n  <li><a href="http://www.acunetix.com">Security art</a></li> \n  \t <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP scanner</a></li>\n  \t <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/">PHP vuln help</a></li>\n  \t <li><a href="http://www.eclectasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li> \n  </ul> \n  </div> \n  <div id="advert"> \n  <p>\n  <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0" width="107" height="66">\n  <param name="movie" value="Flash/add.swf">\n  <param name=quality value=high>\n  <embed src="Flash/add.swf" quality=high pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?P1\_Prod\_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66"></embed>\n  </object>\n  </p>\n  </div> \n  </div> \n  \n  <!--end navbar --> \n  <div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> | &copy;2019\n  Acunetix Ltd \n  </div> \n  <br> \n  <div style="background-color:lightgray;width:100%;text-align:center;font-size:12px;padding:1px">\n  […]<p style="padding-left:5%;padding-right:5%"><b>Warning</b>: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you un  </div>\n  </div>\n  </body>\n  <!-- InstanceEnd --></html>\n |



|  |
| --- |
| Frame 456: 999 bytes on wire (7992 bits), 999 bytes captured (7992 bits) on interface \Device\NPF\_{E419A63D-D7AE-4D5C-A6F5-9C9AE503FE7F}, id 0  Ethernet II, Src: 1e:af:d2:53:dd:11 (1e:af:d2:53:dd:11), Dst: 62:e9:aa:de:5e:4f (62:e9:aa:de:5e:4f)  Internet Protocol Version 4, Src: 192.168.137.164, Dst: 44.228.249.3  Transmission Control Protocol, Src Port: 43080, Dst Port: 80, Seq: 934, Ack: 418, Len: 933  Hypertext Transfer Protocol  POST /userinfo.php HTTP/1.1\r\n  Host: testphp.vulnweb.com\r\n  Connection: keep-alive\r\n  Content-Length: 239\r\n  [Content length: 239]  Cache-Control: max-age=0\r\n  DNT: 1\r\n  Upgrade-Insecure-Requests: 1\r\n  User-Agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Mobile Safari/537.36\r\n  Origin: http://testphp.vulnweb.com\r\n  Content-Type: application/x-www-form-urlencoded\r\n  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n  Referer: http://testphp.vulnweb.com/userinfo.php\r\n  Accept-Encoding: gzip, deflate\r\n  Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7,id;q=0.6\r\n  Cookie: login=test%2Ftest\r\n  Cookie pair: login=test%2Ftest  \r\n  [Response in frame: 460]  [Full request URI: http://testphp.vulnweb.com/userinfo.php]  File Data: 239 bytes  HTML Form URL Encoded: application/x-www-form-urlencoded  Form item: "urname" = "Hendianto Mohammad Farid"  Key: urname  Value: Hendianto Mohammad Farid  Form item: "ucc" = "1234-5678-2300-9000"  Key: ucc  Value: 1234-5678-2300-9000  Form item: "uemail" = "cb24153"  Key: uemail  Value: cb24153  Form item: "uphone" = "60373939740494"  Key: uphone  Value: 60373939740494  Form item: "uaddress" = "%E5%98%8A%E5%98%8DX-Injection:%20testtoheg<script>alert(1)</script>gyb1549oj8qpbwoAfaivndr89d"  Key: uaddress  Value: %E5%98%8A%E5%98%8DX-Injection:%20testtoheg<script>alert(1)</script>gyb1549oj8qpbwoAfaivndr89d  Form item: "update" = "update"  Key: update  Value: update |

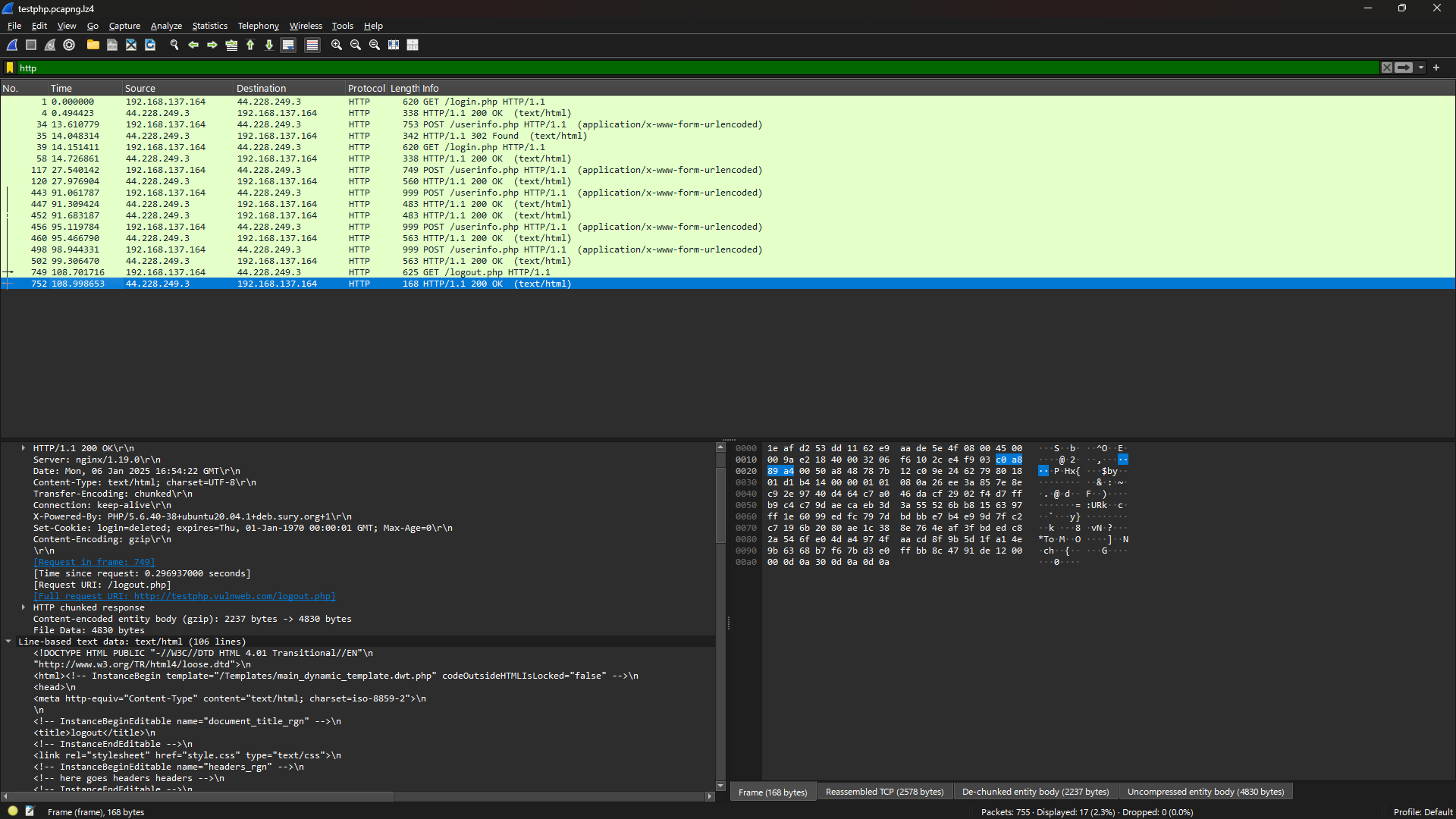


|  |
| --- |
| Frame 502: 563 bytes on wire (4504 bits), 563 bytes captured (4504 bits) on interface \Device\NPF\_{E419A63D-D7AE-4D5C-A6F5-9C9AE503FE7F}, id 0  Ethernet II, Src: 62:e9:aa:de:5e:4f (62:e9:aa:de:5e:4f), Dst: 1e:af:d2:53:dd:11 (1e:af:d2:53:dd:11)  Internet Protocol Version 4, Src: 44.228.249.3, Dst: 192.168.137.164  Transmission Control Protocol, Src Port: 80, Dst Port: 43080, Seq: 5867, Ack: 2800, Len: 497  [3 Reassembled TCP Segments (2973 bytes): #500(1238), #501(1238), #502(497)]  Hypertext Transfer Protocol, has 2 chunks (including last chunk)  HTTP/1.1 200 OK\r\n  Server: nginx/1.19.0\r\n  Date: Mon, 06 Jan 2025 16:54:12 GMT\r\n  Content-Type: text/html; charset=UTF-8\r\n  Transfer-Encoding: chunked\r\n  Connection: keep-alive\r\n  X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1\r\n  Content-Encoding: gzip\r\n  \r\n  [Request in frame: 498]  [Time since request: 0.362139000 seconds]  [Request URI: /userinfo.php]  [Full request URI: http://testphp.vulnweb.com/userinfo.php]  HTTP chunked response  Content-encoded entity body (gzip): 2709 bytes -> 6112 bytes  File Data: 6112 bytes  Line-based text data: text/html (119 lines)  <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"\n  "http://www.w3.org/TR/html4/loose.dtd">\n  <html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHTMLIsLocked="false" -->\n  <head>\n  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">\n  \n  <!-- InstanceBeginEditable name="document\_title\_rgn" -->\n  <title>user info</title>\n  <!-- InstanceEndEditable -->\n  <link rel="stylesheet" href="style.css" type="text/css">\n  <!-- InstanceBeginEditable name="headers\_rgn" -->\n  <!-- here goes headers headers -->\n  <!-- InstanceEndEditable -->\n  <script language="JavaScript" type="text/JavaScript">\n  <!--\n  function MM\_reloadPage(init) { //reloads the window if Nav4 resized\n  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {\n  document.MM\_pgW=innerWidth; document.MM\_pgH=innerHeight; onresize=MM\_reloadPage; }}\n  else if (innerWidth!=document.MM\_pgW || innerHeight!=document.MM\_pgH) location.reload();\n  }\n  MM\_reloadPage(true);\n  //-->\n  </script>\n  \n  </head>\n  <body> \n  <div id="mainLayer" style="position:absolute; width:700px; z-index:1">\n  <div id="masthead"> \n  <h1 id="siteName"><a href="https://www.acunetix.com/"><img src="images/logo.gif" width="306" height="38" border="0" alt="Acunetix website security"></a></h1> \n  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></h6>\n  <div id="globalNav"> \n  \t<table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>\n  \t<td align="left">\n  \t\t<a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="artists.php">artists\n  \t\t</a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> | \n  \t\t<a href="guestbook.php">guestbook</a> | \n  \t\t<a href="AJAX/index.php">AJAX Demo</a>\n  \t</td>\n  \t<td align="right">\n  \t<a href='logout.php'>Logout test</a>\t</td>\n  \t</tr></table>\n  </div> \n  </div> \n  <!-- end masthead --> \n  \n  <!-- begin content -->\n  <!-- InstanceBeginEditable name="content\_rgn" -->\n  <div id="content">\n  \t<h2 id='pageName'>Hendianto Mohammad Farid (test)</h2><div class='story'><p>On this page you can visualize or edit you user information.</p></div><div class='story'>\n  \t \n  \t\t\t<form name="form1" method="post" action="">\n  \t\t\t\t\n  \n  \t\t\t\t\n  \t\t\t\t\n  \t\t\t\t<table border="0" cellspacing="1" cellpadding="4">\n  \t\t\t\t\t<tr><td valign="top">Name:</td><td><input type="text" value="Hendianto Mohammad Farid" name="urname" style="width:200px"></td></tr>\n  \t\t\t\t\t<tr><td valign="top">Credit card number:</td><td><input type="text" value="1234-5678-2300-9000" name="ucc" style="width:200px"></td></tr>\n  \t\t\t\t\t<tr><td valign="top">E-Mail:</td><td><input type="text" value="cb24153" name="uemail" style="width:200px"></td></tr>\n  \t\t\t\t\t<tr><td valign="top">Phone number:</td><td><input type="text" value="60373939740494" name="uphone" style="width:200px"></td></tr>\n  \t\t\t\t\t<tr><td valign="top">Address:</td><td><textarea wrap="soft" name="uaddress" rows="5" style="width:200px">%E5%98%8A%E5%98%8DX-Injection:%20testtoheg<script>alert(1)</script>gyb1549oj8qpbwoAfaivndr89d</textarea></td></tr>\n  \t\t\t\t\t<tr><td colspan="2" align="right"><input type="submit" value="update" name="update"></td></tr>\n  \t\t\t\t</table>\n  \t\t\t</form>\n  \t\t\t</div><div class='story'><p>You have 0 items in your cart. You visualize you cart <a href='cart.php'>here</a>.</p></div></div>\n  <!-- InstanceEndEditable -->\n  <!--end content -->\n  \n  <div id="navBar"> \n  <div id="search"> \n  <form action="search.php?test=query" method="post"> \n  <label>search art</label> \n  <input name="searchFor" type="text" size="10"> \n  <input name="goButton" type="submit" value="go"> \n  </form> \n  </div> \n  <div id="sectionLinks"> \n  <ul> \n  <li><a href="categories.php">Browse categories</a></li> \n  <li><a href="artists.php">Browse artists</a></li> \n  <li><a href="cart.php">Your cart</a></li> \n  <li><a href="login.php">Signup</a></li>\n  \t <li><a href="userinfo.php">Your profile</a></li>\n  \t <li><a href="guestbook.php">Our guestbook</a></li>\n  \t\t<li><a href="AJAX/index.php">AJAX Demo</a></li>\n  \t <li><a href="../logout.php">Logout</a></li> \n  </ul> \n  </div> \n  <div class="relatedLinks"> \n  <h3>Links</h3> \n  <ul> \n  <li><a href="http://www.acunetix.com">Security art</a></li> \n  \t <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP scanner</a></li>\n  \t <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/">PHP vuln help</a></li>\n  \t <li><a href="http://www.eclectasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li> \n  </ul> \n  </div> \n  <div id="advert"> \n  <p>\n  <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0" width="107" height="66">\n  <param name="movie" value="Flash/add.swf">\n  <param name=quality value=high>\n  <embed src="Flash/add.swf" quality=high pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?P1\_Prod\_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66"></embed>\n  </object>\n  </p>\n  </div> \n  </div> \n  \n  <!--end navbar --> \n  <div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> | &copy;2019\n  Acunetix Ltd \n  </div> \n  <br> \n  <div style="background-color:lightgray;width:100%;text-align:center;font-size:12px;padding:1px">\n  […]<p style="padding-left:5%;padding-right:5%"><b>Warning</b>: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you un  </div>\n  </div>\n  </body>\n  <!-- InstanceEnd --></html>\n |

A screenshot of a computer

Description automatically generated

|  |
| --- |
| Frame 749: 625 bytes on wire (5000 bits), 625 bytes captured (5000 bits) on interface \Device\NPF\_{E419A63D-D7AE-4D5C-A6F5-9C9AE503FE7F}, id 0  Ethernet II, Src: 1e:af:d2:53:dd:11 (1e:af:d2:53:dd:11), Dst: 62:e9:aa:de:5e:4f (62:e9:aa:de:5e:4f)  Internet Protocol Version 4, Src: 192.168.137.164, Dst: 44.228.249.3  Transmission Control Protocol, Src Port: 43080, Dst Port: 80, Seq: 2800, Ack: 6364, Len: 559  Hypertext Transfer Protocol  GET /logout.php HTTP/1.1\r\n  Host: testphp.vulnweb.com\r\n  Connection: keep-alive\r\n  DNT: 1\r\n  Upgrade-Insecure-Requests: 1\r\n  User-Agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Mobile Safari/537.36\r\n  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n  Referer: http://testphp.vulnweb.com/userinfo.php\r\n  Accept-Encoding: gzip, deflate\r\n  Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7,id;q=0.6\r\n  Cookie: login=test%2Ftest\r\n  Cookie pair: login=test%2Ftest  \r\n  [Response in frame: 752]  [Full request URI: http://testphp.vulnweb.com/logout.php] |



|  |
| --- |
| Frame 752: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits) on interface \Device\NPF\_{E419A63D-D7AE-4D5C-A6F5-9C9AE503FE7F}, id 0  Ethernet II, Src: 62:e9:aa:de:5e:4f (62:e9:aa:de:5e:4f), Dst: 1e:af:d2:53:dd:11 (1e:af:d2:53:dd:11)  Internet Protocol Version 4, Src: 44.228.249.3, Dst: 192.168.137.164  Transmission Control Protocol, Src Port: 80, Dst Port: 43080, Seq: 8840, Ack: 3359, Len: 102  [3 Reassembled TCP Segments (2578 bytes): #750(1238), #751(1238), #752(102)]  Hypertext Transfer Protocol, has 2 chunks (including last chunk)  HTTP/1.1 200 OK\r\n  Server: nginx/1.19.0\r\n  Date: Mon, 06 Jan 2025 16:54:22 GMT\r\n  Content-Type: text/html; charset=UTF-8\r\n  Transfer-Encoding: chunked\r\n  Connection: keep-alive\r\n  X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1\r\n  Set-Cookie: login=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0\r\n  Content-Encoding: gzip\r\n  \r\n  [Request in frame: 749]  [Time since request: 0.296937000 seconds]  [Request URI: /logout.php]  [Full request URI: http://testphp.vulnweb.com/logout.php]  HTTP chunked response  Content-encoded entity body (gzip): 2237 bytes -> 4830 bytes  File Data: 4830 bytes  Line-based text data: text/html (106 lines)  <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"\n  "http://www.w3.org/TR/html4/loose.dtd">\n  <html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHTMLIsLocked="false" -->\n  <head>\n  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">\n  \n  <!-- InstanceBeginEditable name="document\_title\_rgn" -->\n  <title>logout</title>\n  <!-- InstanceEndEditable -->\n  <link rel="stylesheet" href="style.css" type="text/css">\n  <!-- InstanceBeginEditable name="headers\_rgn" -->\n  <!-- here goes headers headers -->\n  <!-- InstanceEndEditable -->\n  <script language="JavaScript" type="text/JavaScript">\n  <!--\n  function MM\_reloadPage(init) { //reloads the window if Nav4 resized\n  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {\n  document.MM\_pgW=innerWidth; document.MM\_pgH=innerHeight; onresize=MM\_reloadPage; }}\n  else if (innerWidth!=document.MM\_pgW || innerHeight!=document.MM\_pgH) location.reload();\n  }\n  MM\_reloadPage(true);\n  //-->\n  </script>\n  \n  </head>\n  <body> \n  <div id="mainLayer" style="position:absolute; width:700px; z-index:1">\n  <div id="masthead"> \n  <h1 id="siteName"><a href="https://www.acunetix.com/"><img src="images/logo.gif" width="306" height="38" border="0" alt="Acunetix website security"></a></h1> \n  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></h6>\n  <div id="globalNav"> \n  \t<table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>\n  \t<td align="left">\n  \t\t<a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="artists.php">artists\n  \t\t</a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> | \n  \t\t<a href="guestbook.php">guestbook</a> | \n  \t\t<a href="AJAX/index.php">AJAX Demo</a>\n  \t</td>\n  \t<td align="right">\n  \t\t</td>\n  \t</tr></table>\n  </div> \n  </div> \n  <!-- end masthead --> \n  \n  <!-- begin content -->\n  <!-- InstanceBeginEditable name="content\_rgn" -->\n  <div id="content">\n  \t<div class="story">\n  \t\t<h1 id="pageName">You have been logged out. See you back soon.</h1>\n  \t</div>\n  </div>\n  <!-- InstanceEndEditable -->\n  <!--end content -->\n  \n  <div id="navBar"> \n  <div id="search"> \n  <form action="search.php?test=query" method="post"> \n  <label>search art</label> \n  <input name="searchFor" type="text" size="10"> \n  <input name="goButton" type="submit" value="go"> \n  </form> \n  </div> \n  <div id="sectionLinks"> \n  <ul> \n  <li><a href="categories.php">Browse categories</a></li> \n  <li><a href="artists.php">Browse artists</a></li> \n  <li><a href="cart.php">Your cart</a></li> \n  <li><a href="login.php">Signup</a></li>\n  \t <li><a href="userinfo.php">Your profile</a></li>\n  \t <li><a href="guestbook.php">Our guestbook</a></li>\n  \t\t<li><a href="AJAX/index.php">AJAX Demo</a></li>\n  \t </li> \n  </ul> \n  </div> \n  <div class="relatedLinks"> \n  <h3>Links</h3> \n  <ul> \n  <li><a href="http://www.acunetix.com">Security art</a></li> \n  \t <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP scanner</a></li>\n  \t <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/">PHP vuln help</a></li>\n  \t <li><a href="http://www.eclectasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li> \n  </ul> \n  </div> \n  <div id="advert"> \n  <p>\n  <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0" width="107" height="66">\n  <param name="movie" value="Flash/add.swf">\n  <param name=quality value=high>\n  <embed src="Flash/add.swf" quality=high pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?P1\_Prod\_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66"></embed>\n  </object>\n  </p>\n  </div> \n  </div> \n  \n  <!--end navbar --> \n  <div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> | &copy;2019\n  Acunetix Ltd \n  </div> \n  <br> \n  <div style="background-color:lightgray;width:100%;text-align:center;font-size:12px;padding:1px">\n  […]<p style="padding-left:5%;padding-right:5%"><b>Warning</b>: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you un  </div>\n  </div>\n  </body>\n  <!-- InstanceEnd --></html>\n |

* 1. Record and report your findings about the data that appeared in Wireshark from accessing the websites.

File all report

1. Access Point Security
   1. Suggest any wireless access point used in the market to strengthen security in a home wireless environment. Based on its function, justify your choice of the access point based on the security point of view.
   2. Provide a reference for the product selection.

**Marking Guide**

|  |  |  |  |
| --- | --- | --- | --- |
| Item | 0 | In between | Full mark |
| Front page | Not provide |  | Provide all |
| Task 5 | Not provide | Missing task and not complete | Provide all and complete |
| Task 6 | Not provide | Missing task and not complete | Provide all and complete |
| List of references | Not provide |  | Correct and complete |