

เปิดไฟล์ SQL_Lab.pcap

The screenshot shows the Wireshark interface with the SQL_Lab.pcap file loaded. The packet list on the left displays a series of HTTP requests and responses. Packet 13 is highlighted, showing a GET request for /dwa/vulnerabilities/sql/. The packet details pane on the right shows the structure of the HTTP request, including the method, URI, and various headers.

เช็ค packet ที่ 13

The screenshot shows the Wireshark interface with the SQL_Lab.pcap file loaded. The packet list on the left displays a series of HTTP requests and responses. Packet 13 is highlighted, showing a GET request for /dwa/vulnerabilities/sql/. The packet details pane on the right shows the structure of the HTTP request, including the method, URI, and various headers. The packet bytes pane at the bottom shows the raw data of the packet.

ค้นหา 1=1

The image shows a Wireshark packet capture of an HTTP stream. The packet list on the left shows three packets. The packet details pane on the right shows the HTTP request structure. The payload is a GET request to a vulnerable web application. The payload contains a SQL injection payload: `1=1`.

```

<div id="main_body">
<div class="body_padded">
<h1>Vulnerability: SQL Injection</h1>
<div class="vulnerable_code_area">
<form action="#" method="GET">
<p>
User ID:
<input type="text" size="15" name="id">
<input type="submit" name="Submit" value="Submit">
</p>
</form>
<pre>ID: 1=1<br />First name: admin<br />Surname: admin</pre>
</div>
<h2>More Information</h2>
<ul>
<li><a href="http://www.securiteam.com/securityreviews/SDPONIP76E.html" target="blank">http://www.securiteam.com/securityreviews/SDPONIP76E.html</a></li>
<li><a href="https://en.wikipedia.org/wiki/SQL_injection" target="blank">https://en.wikipedia.org/wiki/SQL_injection</a></li>
<li><a href="http://ferreh.mavituna.com/sql-injection-cheatsheet-oku/" target="blank">http://ferreh.mavituna.com/sql-injection-cheatsheet-oku/</a></li>
<li><a href="http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet" target="blank">http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet</a></li>
<li><a href="https://www.owasp.org/index.php/SQL_injection" target="blank">https://www.owasp.org/index.php/SQL_injection</a></li>
<li><a href="http://bobby-tables.com/" target="blank">http://bobby-tables.com/</a></li>
</ul>
</div>
<br />
</div>
<div class="clear">
</div>

```

เช็ค packet ที่ 19 และค้นหา 1=1

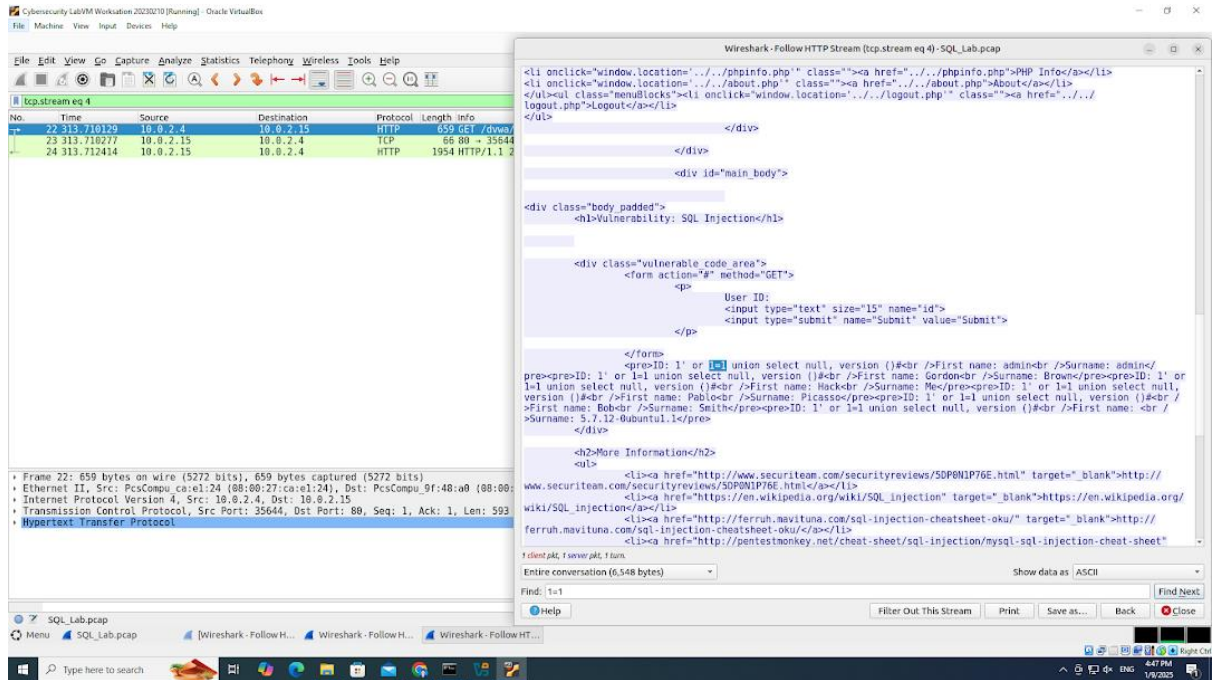
The image shows a Wireshark packet capture of an HTTP stream. The packet list on the left shows three packets. The packet details pane on the right shows the HTTP request structure. The payload is a GET request to a vulnerable web application. The payload contains a SQL injection payload: `1=1`.

```

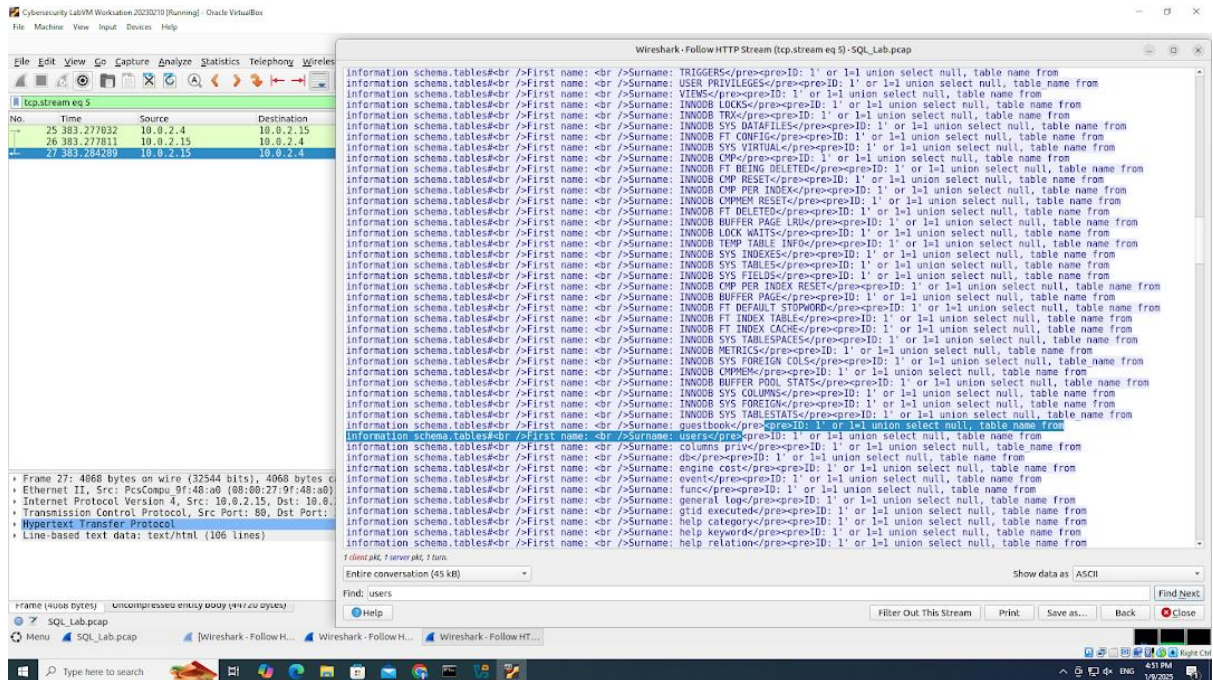
</div>
<div id="main_body">
<div class="body_padded">
<h1>Vulnerability: SQL Injection</h1>
<div class="vulnerable_code_area">
<form action="#" method="GET">
<p>
User ID:
<input type="text" size="15" name="id">
<input type="submit" name="Submit" value="Submit">
</p>
</form>
<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: admin<br />Surname: admin</pre>
</div>
<h2>More Information</h2>
<ul>
<li><a href="http://www.securiteam.com/securityreviews/SDPONIP76E.html" target="blank">http://www.securiteam.com/securityreviews/SDPONIP76E.html</a></li>
<li><a href="https://en.wikipedia.org/wiki/SQL_injection" target="blank">https://en.wikipedia.org/wiki/SQL_injection</a></li>
<li><a href="http://ferreh.mavituna.com/sql-injection-cheatsheet-oku/" target="blank">http://ferreh.mavituna.com/sql-injection-cheatsheet-oku/</a></li>
<li><a href="http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet" target="blank">http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet</a></li>
<li><a href="https://www.owasp.org/index.php/SQL_injection" target="blank">https://www.owasp.org/index.php/SQL_injection</a></li>
<li><a href="http://bobby-tables.com/" target="blank">http://bobby-tables.com/</a></li>
</ul>
</div>
<br />
</div>
<div class="clear">
</div>

```

เช็ค packet ที่ 22 และค้นหา 1=1



เช็ค packet ที่ 25 และค้นหา users



เช็ค packet ที่ 28 และค้นหา users

The screenshot displays the Wireshark network protocol analyzer interface. The main window is titled 'Wireshark - Follow HTTP Stream (tcp.stream eq 6) - SQL_Lab.pcap'. The packet list on the left shows a list of captured packets, with packet 28 selected. The packet details pane on the right shows the structure of the selected packet, which is an HTTP GET request. The request body contains a form with a 'User ID' input field and a 'Submit' button. The packet bytes pane at the bottom shows the raw data of the packet.

เมื่อลองเอาแฮชที่ถูก hash ไปลองถอด hash จะได้ว่า charley