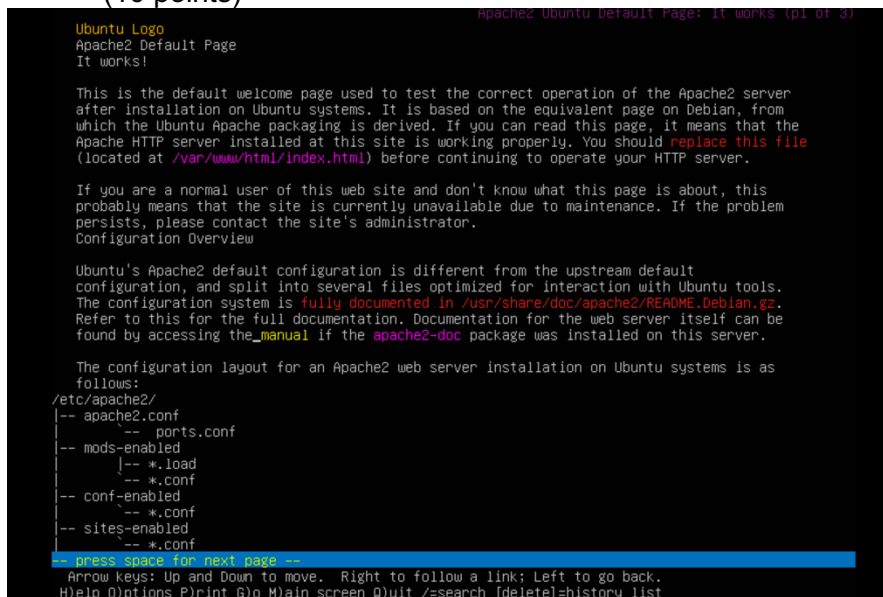


Lab 08 Template – Ethan Roepke

1. Screenshot of the default Apache page via Lynx
www.studentXX.230.com
(10 points)

A terminal window showing the output of the Lynx command. The title bar reads "Apache2 Ubuntu Default Page: It works (p1 of 3)". The content displays the Ubuntu Logo, the text "Apache2 Default Page", and "It works!". Below this, a paragraph explains that this is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It mentions that the page is based on the equivalent page on Debian and that if the user can read this page, it means the Apache HTTP server is working properly. A note advises replacing the file at /var/www/html/index.html before continuing to operate the HTTP server. Another paragraph explains that if a normal user doesn't know what the page is about, it probably means the site is currently unavailable due to maintenance. A link for "Configuration Overview" is provided. The next paragraph states that Ubuntu's Apache2 default configuration is different from the upstream default and is split into several files optimized for interaction with Ubuntu tools. It mentions that the configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz and refers to the full documentation. A link for the manual is provided. The final paragraph states that the configuration layout for an Apache2 web server installation on Ubuntu systems is as follows: /etc/apache2/. A list of files is shown: apache2.conf, ports.conf, mods-enabled, *.load, *.conf, conf-enabled, *.conf, sites-enabled, *.conf. A blue bar at the bottom of the terminal window contains the text "-- press space for next page --". Below the blue bar, a line of text provides arrow key instructions: "Arrow keys: Up and Down to move. Right to follow a link; Left to go back. H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list".

```
Apache2 Ubuntu Default Page: It works (p1 of 3)
Ubuntu Logo
Apache2 Default Page
It works!

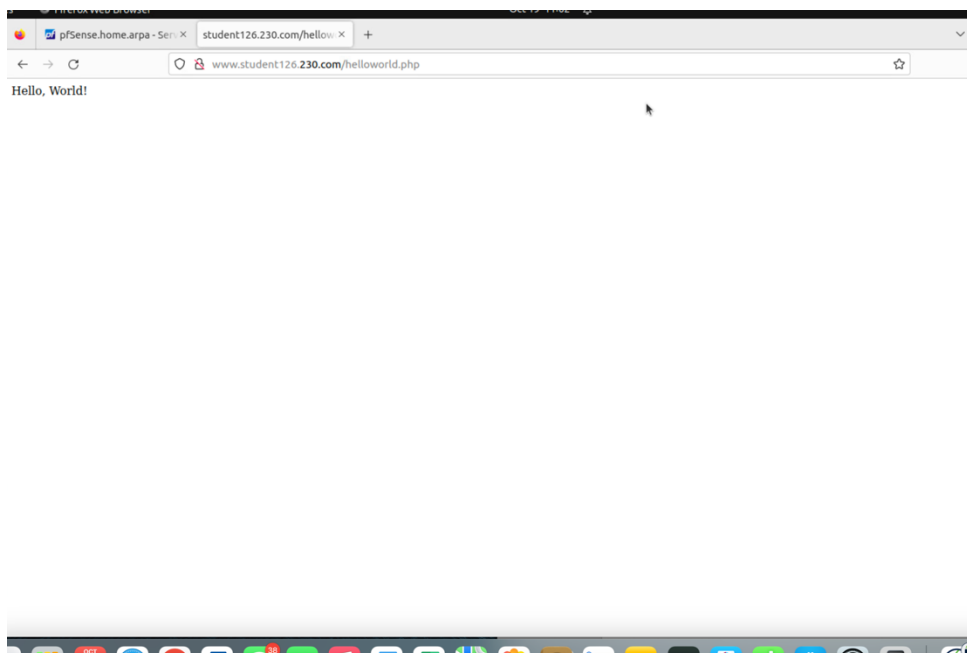
This is the default welcome page used to test the correct operation of the Apache2 server
after installation on Ubuntu systems. It is based on the equivalent page on Debian, from
which the Ubuntu Apache packaging is derived. If you can read this page, it means that the
Apache HTTP server installed at this site is working properly. You should replace this file
(located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this
probably means that the site is currently unavailable due to maintenance. If the problem
persists, please contact the site's administrator.
Configuration Overview

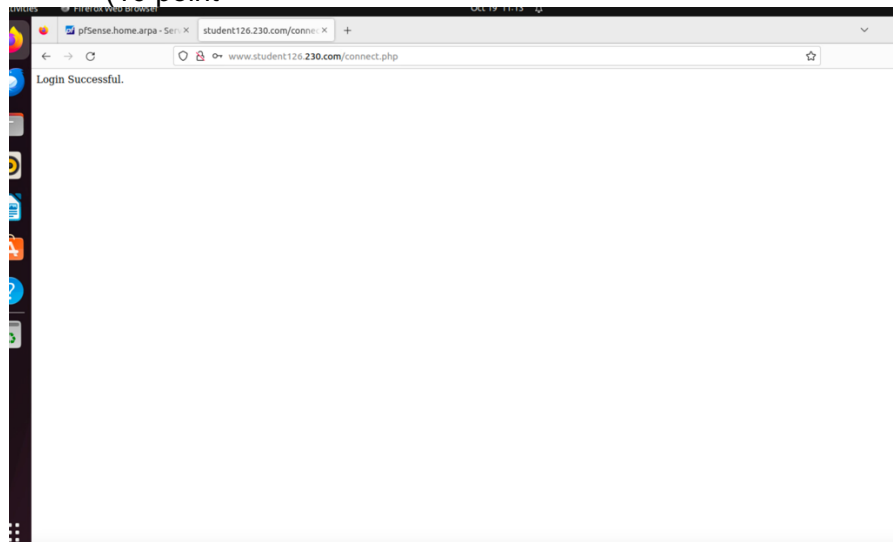
Ubuntu's Apache2 default configuration is different from the upstream default
configuration, and split into several files optimized for interaction with Ubuntu tools.
The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz.
Refer to this for the full documentation. Documentation for the web server itself can be
found by accessing the manual if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as
follows:
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
-- press space for next page --
Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

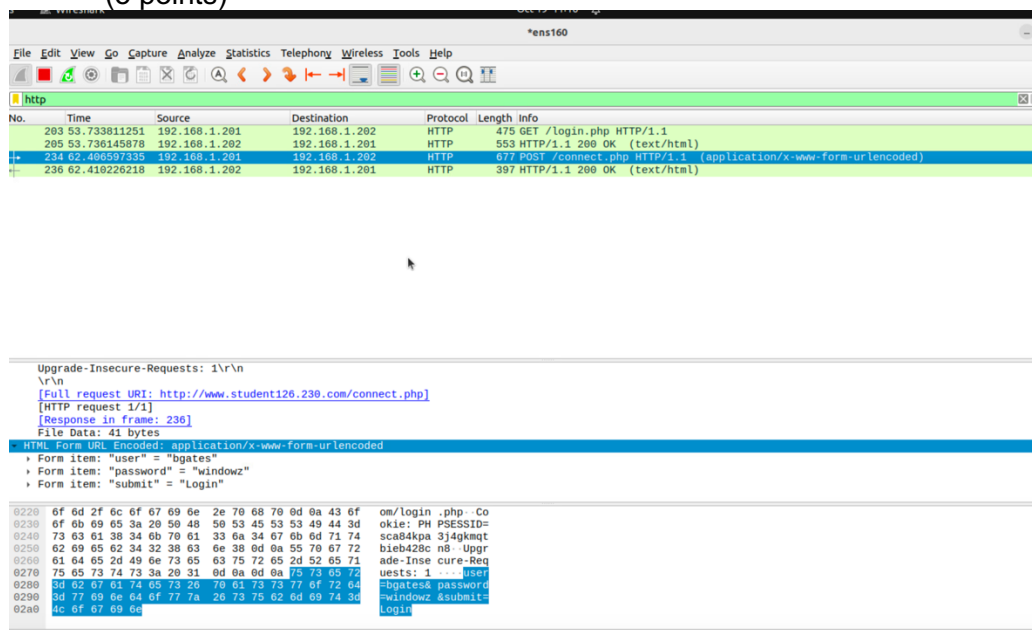
2. Screenshot of the Hello, world! PHP page via Firefox
www.studentXX.230.com/helloworld.php
(10 points)



3. Screenshot of one of the users logged into PHP web page via Firefox
www.studentXX.230.com/login.php
(10 point)



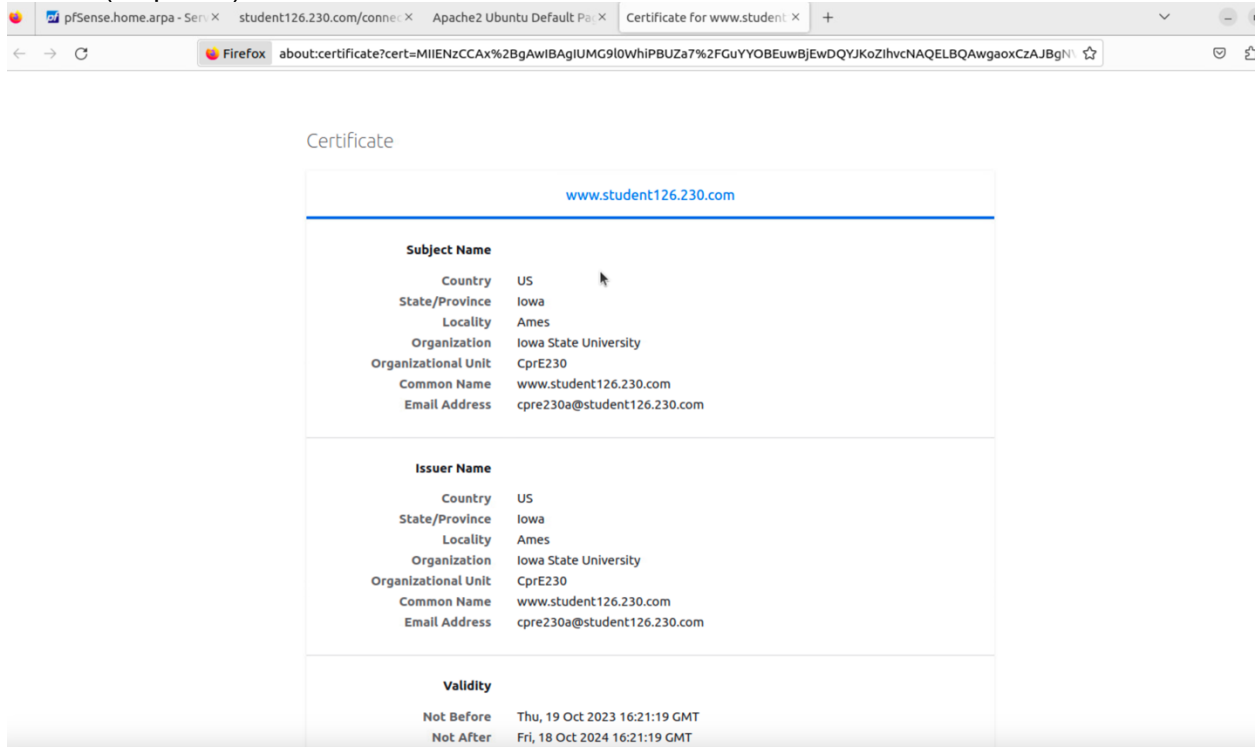
4. Screenshot of Wireshark showing the plaintext password when logging in
(5 points)



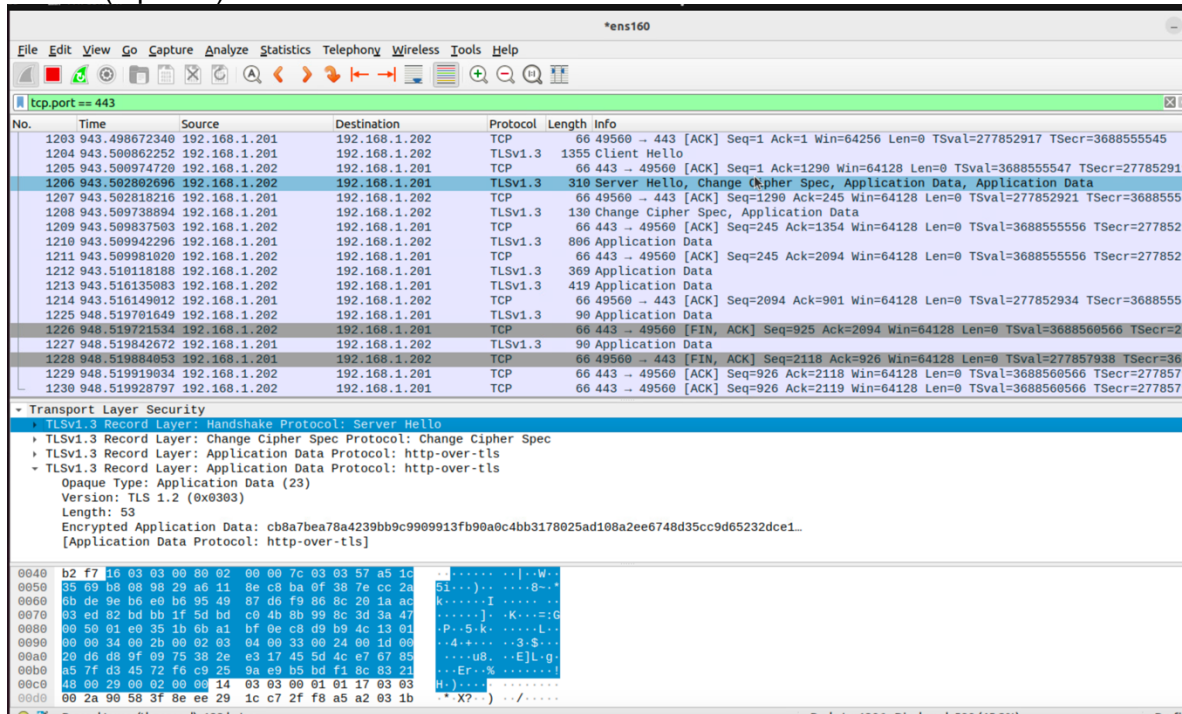
5. Screenshot of the Apache default page on HTTPS via Firefox
<https://www.studentXX.230.com>
(10 points)



6. Screenshot of the SSL certificate (10 points)



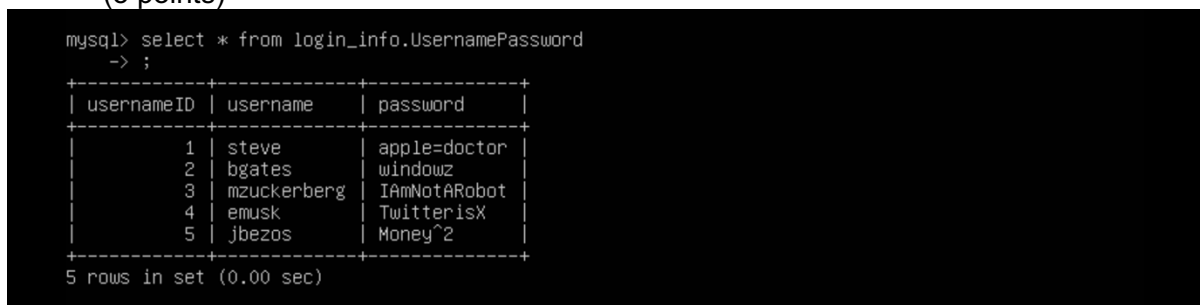
7. Screenshot of Wireshark showing an encrypted packet when logging in (5 points)



8. Screenshot of the profile page, via Firefox <https://studentXX.230.com/profile.php> (10 points)



9. Screenshot of the database, with changed username and password (5 points)



10. **Description of what SQL injection is, and how you might go about preventing it**
(10 points)

SQL injection allows attackers to access information that was no intended to be displayed by using a malicious SQL code.

A way to preventing outside attackers from using SQL injection by utilizing parametrized queries. This will be allow you use to reuse them for similar applications and wont need to create separate queries for each case.

11. **Screenshot of NAT rule(s)**
(5 points)

<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	37.56.23.100	*	105.148.172.204	993 (IMAP/S)	192.168.1.204	993 (IMAP/S)	mail - nagios secure imap login		
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	37.56.23.100	*	105.148.172.204	587 (SUBMISSION)	192.168.1.204	587 (SUBMISSION)	mail - nagios secure IMAP		
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	37.56.23.100	*	105.148.172.204	110 (POP3)	192.168.1.204	110 (POP3)	mail - nagios mail pop		
www - nagios check													
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	37.56.23.100	*	105.148.172.202	80 (HTTP)	192.168.1.202	80 (HTTP)	www - check nagios HTTP		
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	37.56.23.100	*	105.148.172.202	443 (HTTPS)	192.168.1.202	443 (HTTPS)	www - check nagios HTTPS		

Add Add Delete Save Separator

12. **Screenshot of successful Nagios queries against web services.**
(10 points)

<