Experiment No: 9

**Aim:** To Demonstrate on web backdoor.

**Theory:**

At the start the company had no security and it was an internal website so it had trusted its employees.But there was an attack on the website from an internal source who had aided an external attacker. So the company had to face huge losses and loose valuable customers.

**Early Attack Phase Detection:**

Attackers are vulnerable to discovery in the early stages of the campaign before they have had the opportunity to mature their ability to start using your remote access infrastructure and thus remove or downgrade their use of backdoor Trojans as a primary means of access. Their goal is to cause losses to the organization and make the vulnerable for more losses.

**Dead Analysis**

As there was no security anyone and everyone could assess the website and see its content.

* Login to the website.
* Gain Access to the system.
* Obtain the access to data.

**Live Analysis**

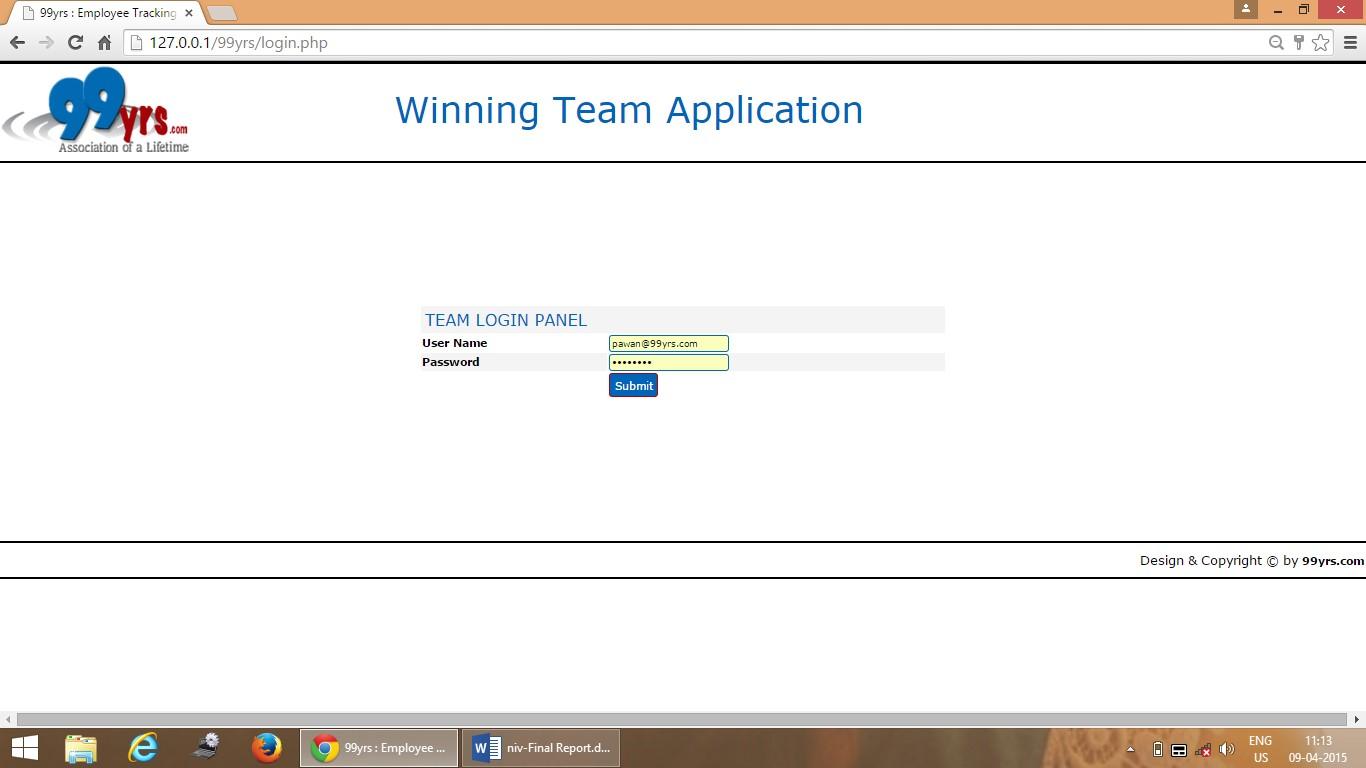
1. Before any login mac id of a system is obtained.

2. If the mac id, obtained is authorized, only then can it have access to the main page for login

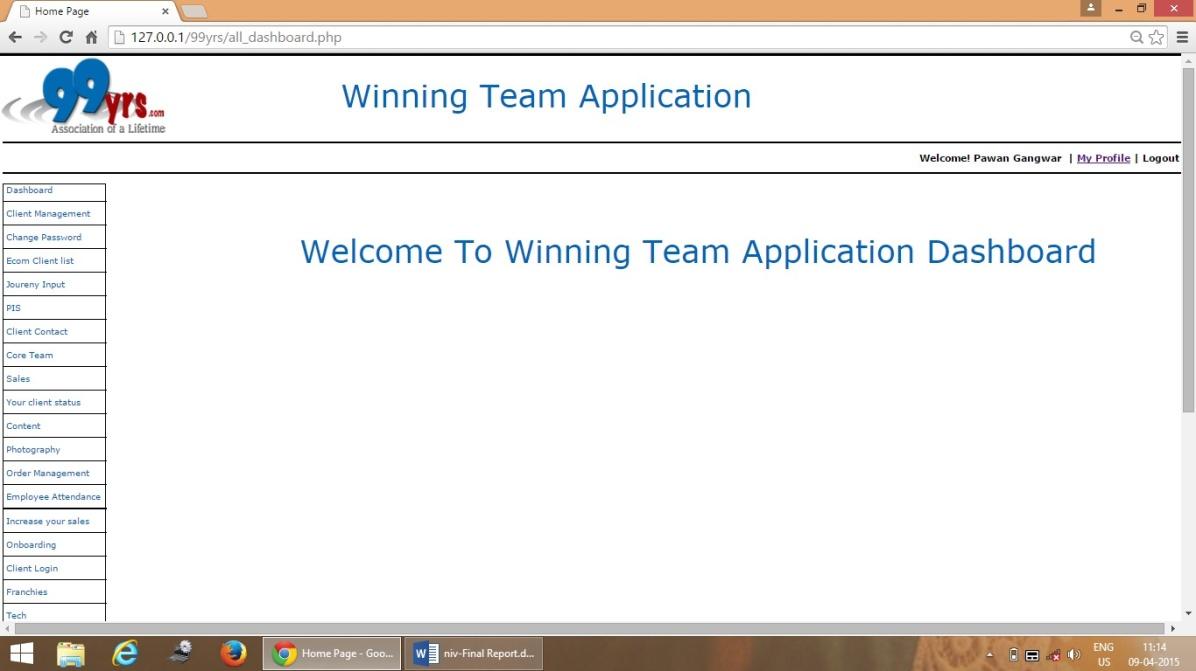
3. If the mac id is not authorized, further login in not possible for that particular system.

4. So only authorized systems will have access to the site.

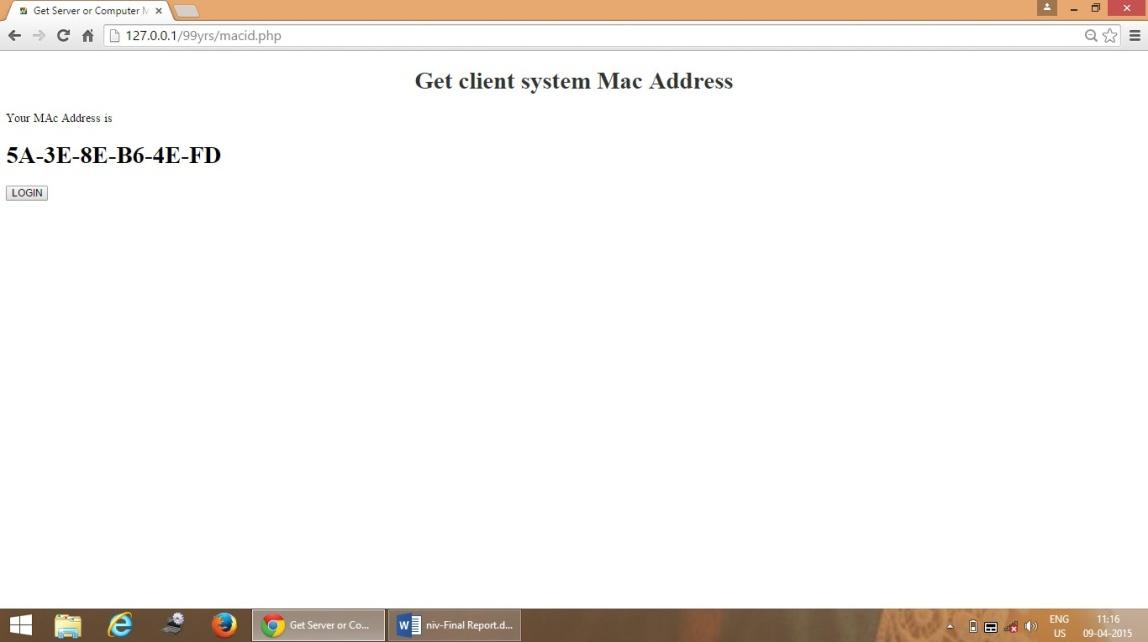
*Snapshot 1: Login without security.*



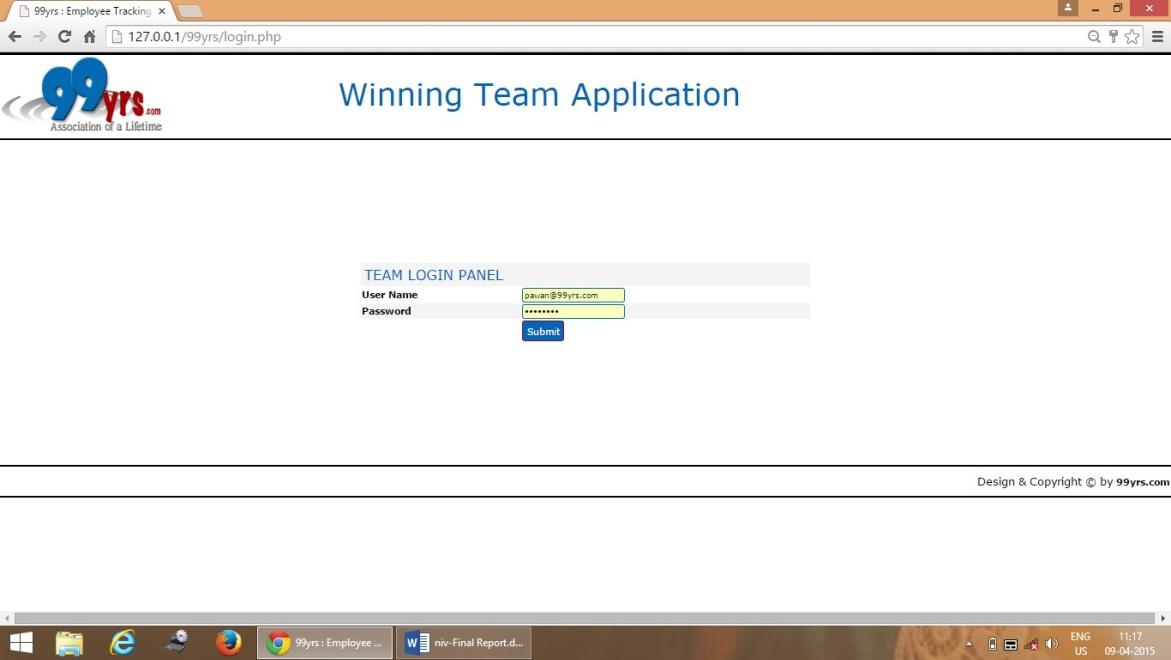
*Snapshot 2: Direct access to the site*



*Snapshot 3: Access with mac id Authorization*



*Snapshot 4: Access after Authorization*



**Conclusion:**

As we have seen the importance of security, it has become a necessary thing for every organization to have it. No one can be trusted, so proper authorization has to be given to every individual in an organization. We have seen that default passwords also cause problems, so it’s necessary to change the default passwords to our own new ones.