Sharad Dixit

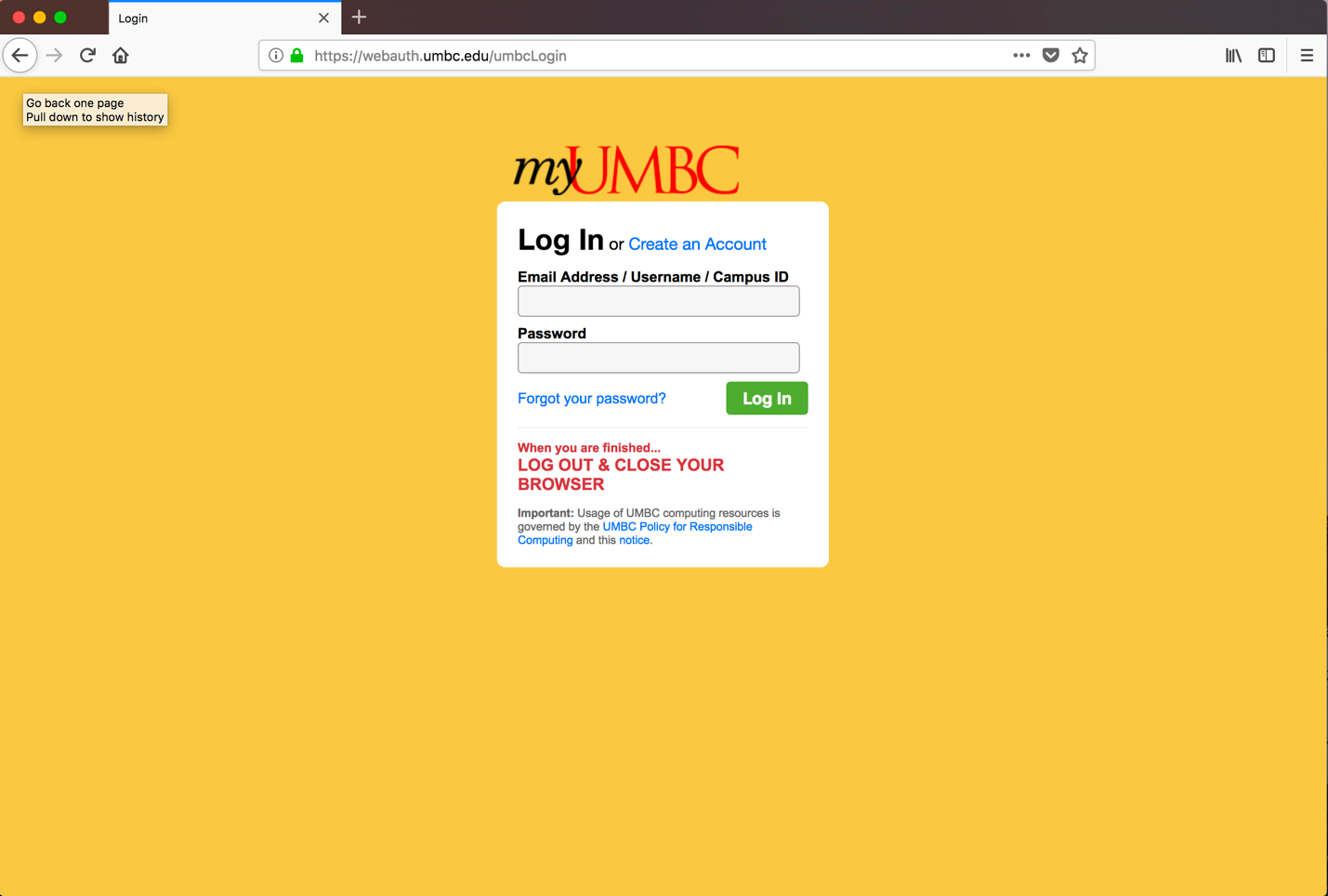
CMSC 487 Introduction to Network Security

**Assignment 1**

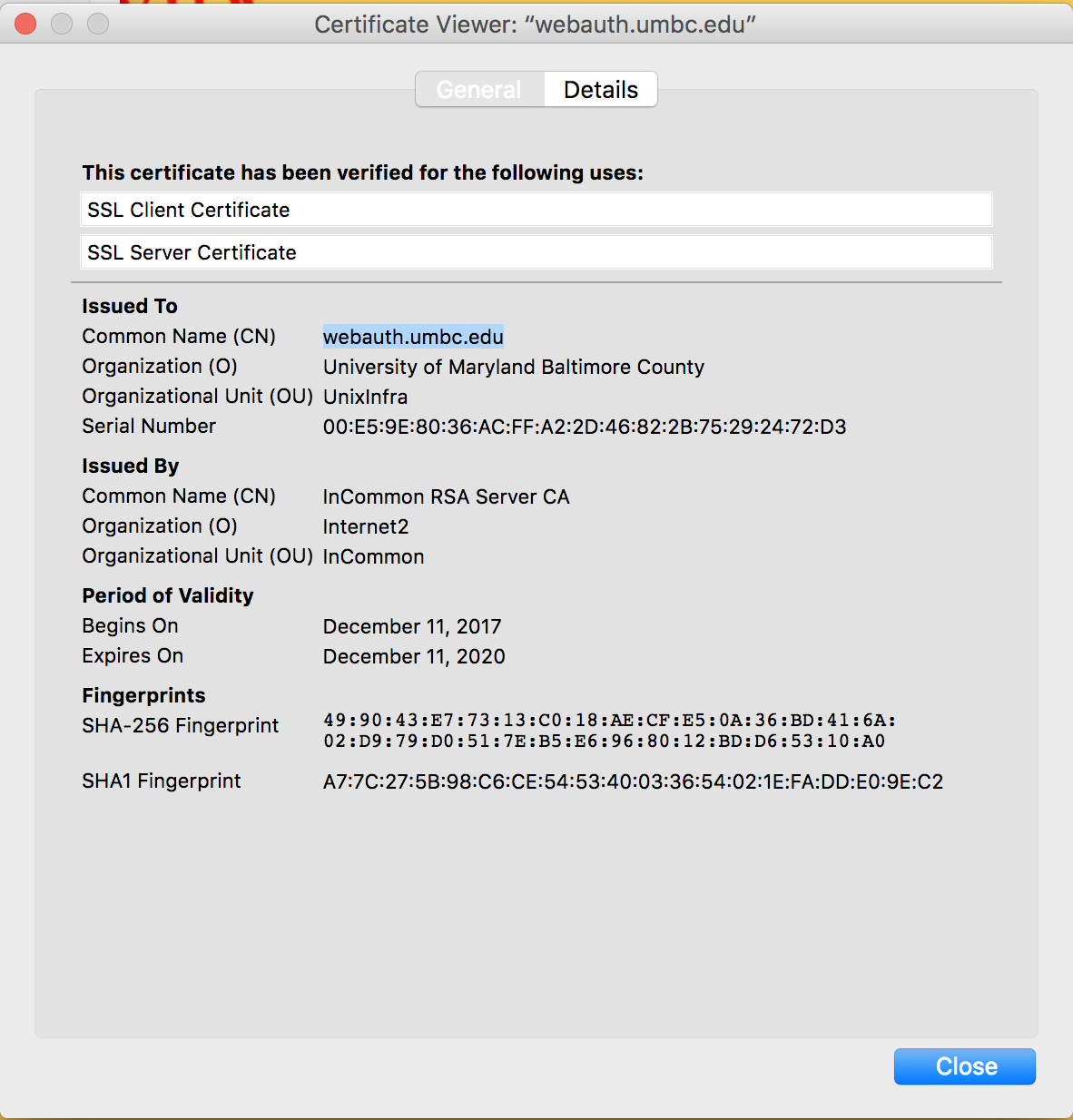
* **Objective:**

The objective of this assignment was to explore man in the middle attacks against SSL/TLS encrypted connections. Tools SSLstrip and SSLsplit are used to implement man in the middle attack and extract user login information by directing users internet traffic to attackers hoax server and then implementing SSLstrip and SSLsplit to extract information of user.

* **Methodology:**



The above figure depicts the browser when neither SSLstrip nor SSLsplit has been executed. In the figure above connection is secured with https. The https protocol is secured because it is encrypted whereas http is not. There when a user sends login information on a secured https connection then their login information cannot be read by the attacker as it is encrypted whereas when the information is send over http then the information could be read by the attacker.



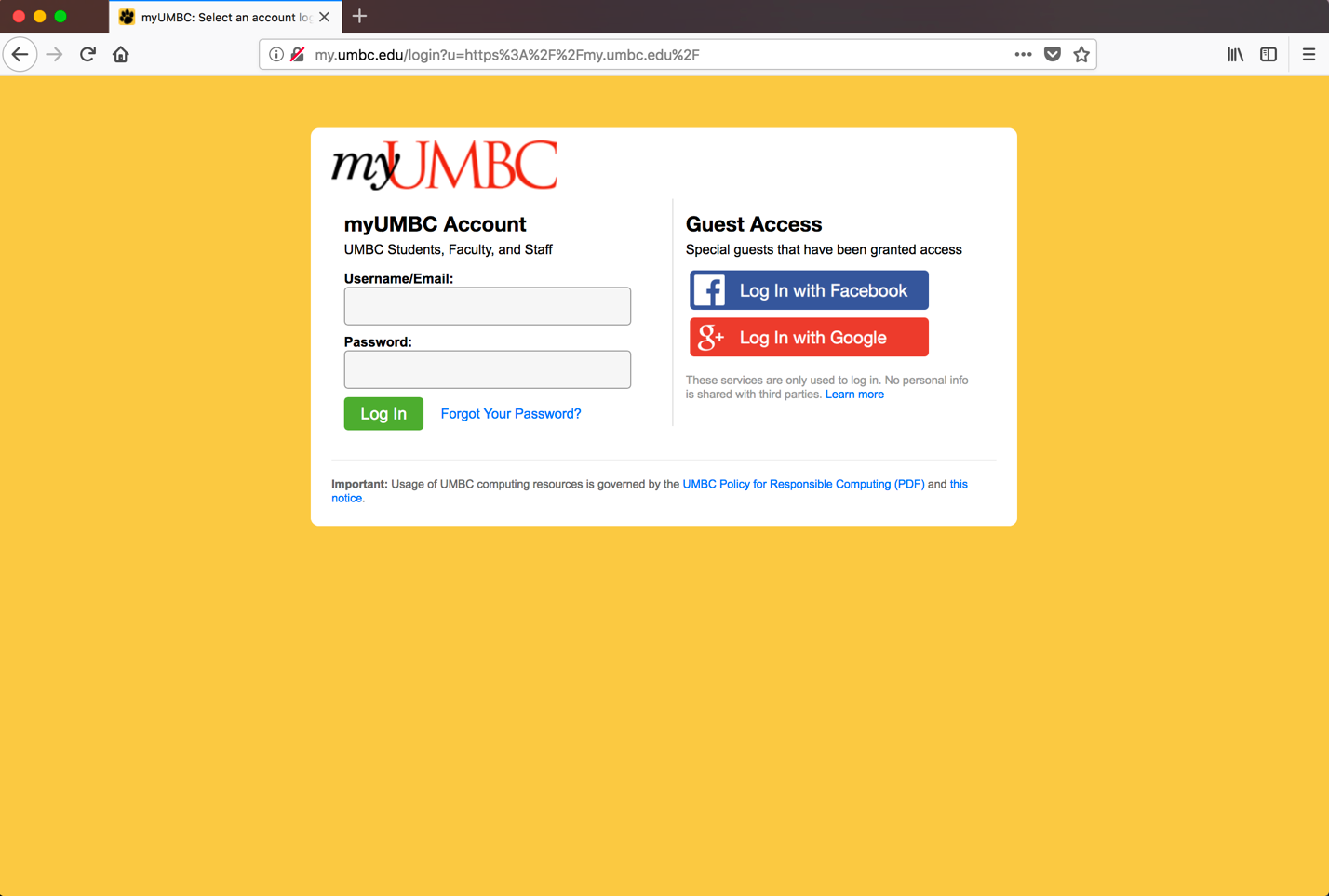
The above figure depicts the certificate of website which is secured by https protocol. This certificate is before SSLstrip or SSLsplit has been executed, that is why it is an authorized certificate. When an attack is launched then certificate is removed, and a hoax certificate is implanted so that the user does not get to know that an attack has been launched. The certificate is issued by ‘internet2’ will change after we use SSLstrip or SSLsplit.

* **SSLSTRIP:**

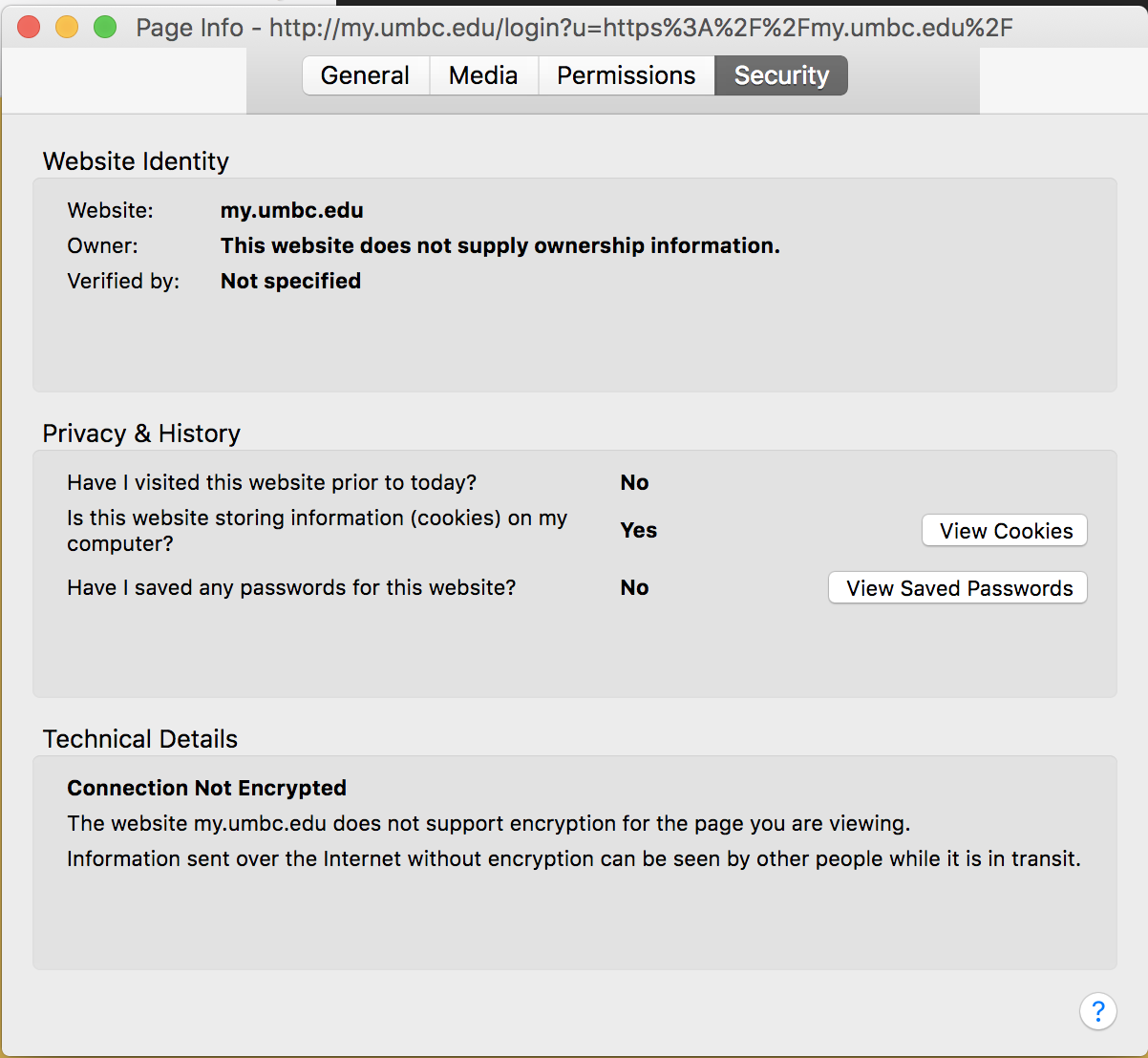
SSLSTRIP is the man in the middle attack tool that allows the attacker to manipulate internet traffic and capture data such as usernames and password. It works by converting https request to http.

Working:

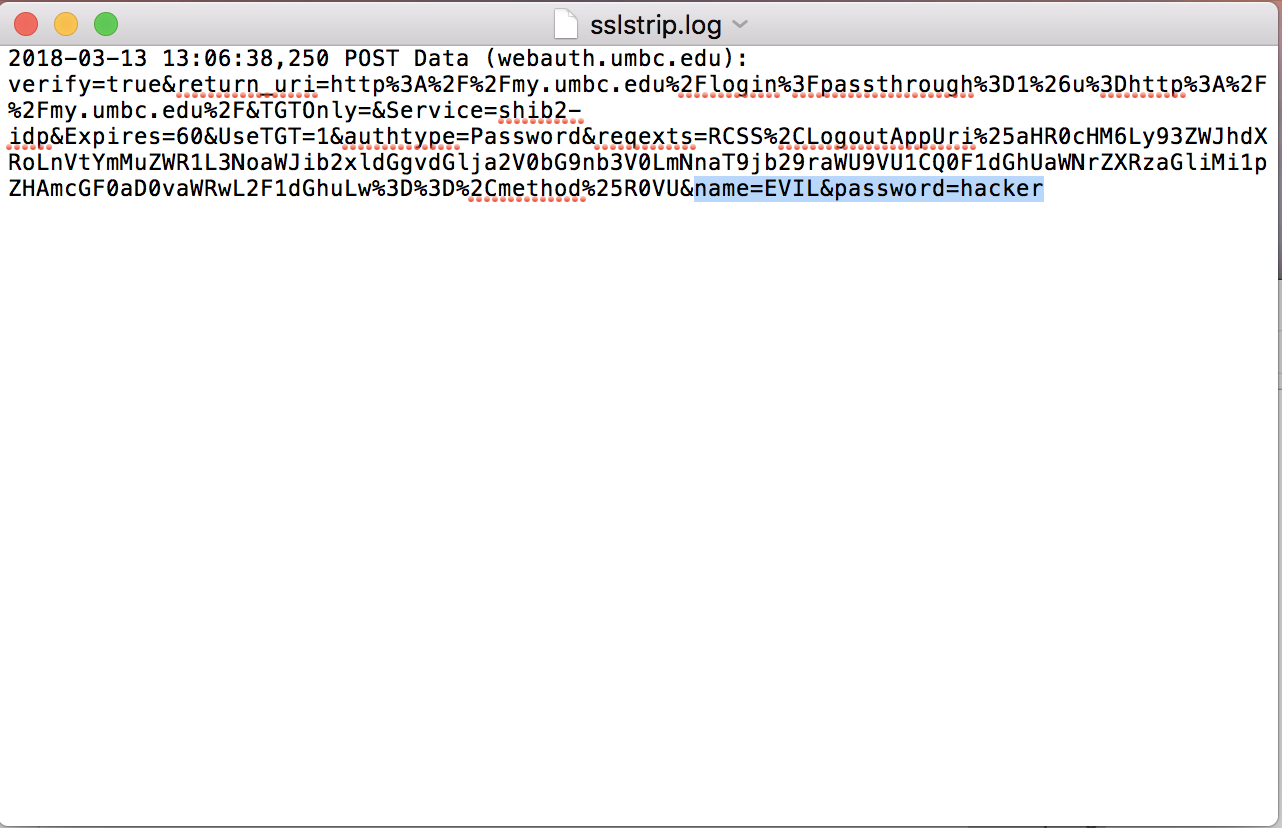
* First, we need to get our hands-on targets internet traffic which is done by tricking the router in sending the internet traffic to our computer instead of the website the user is trying to connect with.
* Then we run SSLstrip on kali Linux on our computer which basically extracts the information user enters on the website and stores in our computer.



The above figure depicts when the SSLstrip attack has been executed, where it can be seen that the network of the user has been compromised and that the https connection has been changed to http which is not secured. Therefore, man in the middle attack works as now whatever Username and Password details will be added by the user will extracted by the attacker.



The above figure depicts the certificate after the SSLstrip attack, where the original certificate is removed as the connection changes from https to http. Therefore, with this now the attacker could extract all the information which the user enters on the website.

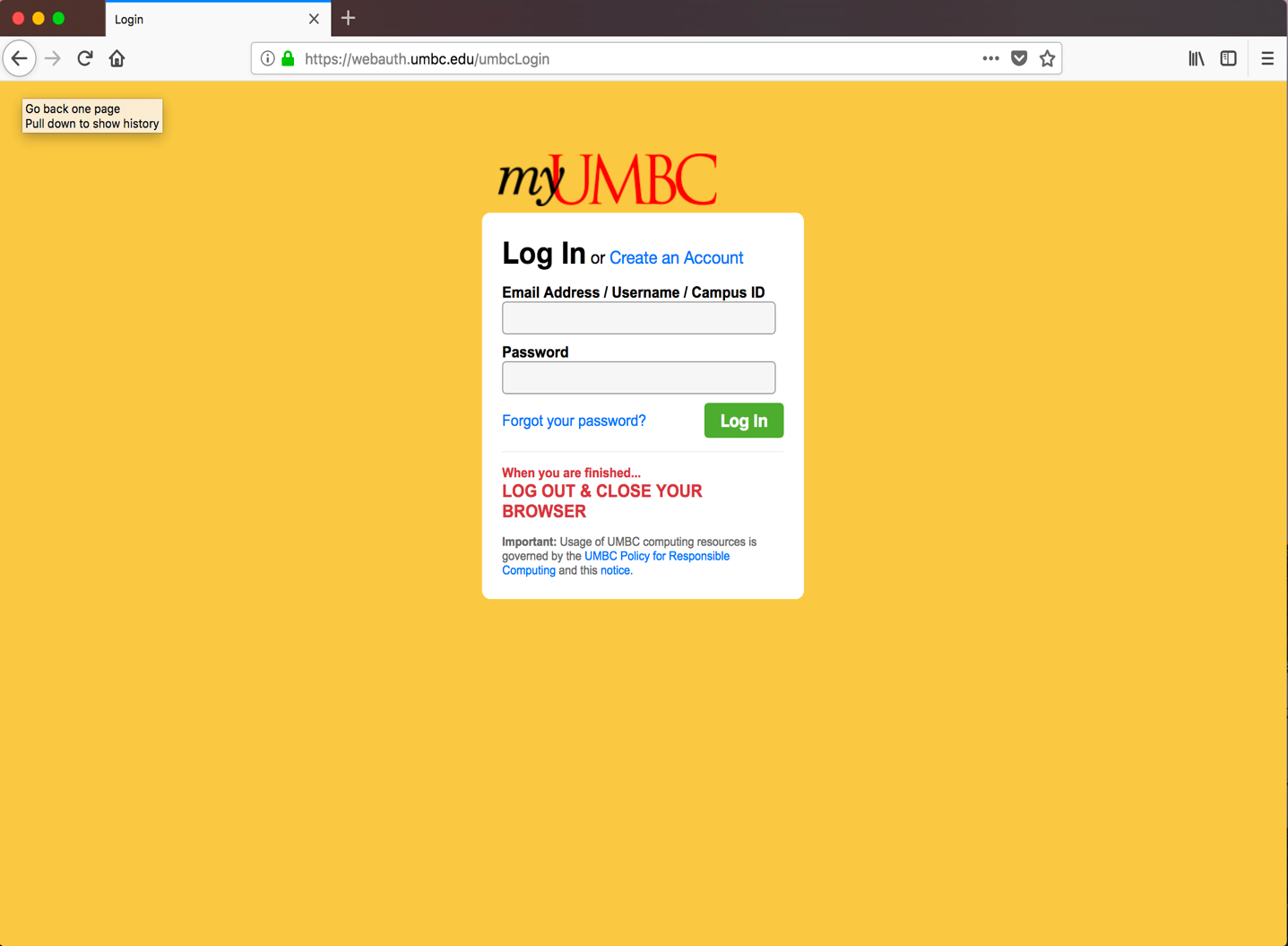


The above figure depicts the output of the sslstrip.log with login details extracted. The username: EVIL and password: hacker was entered by the user when http connection was there that is when SSLstrip attack was executed.

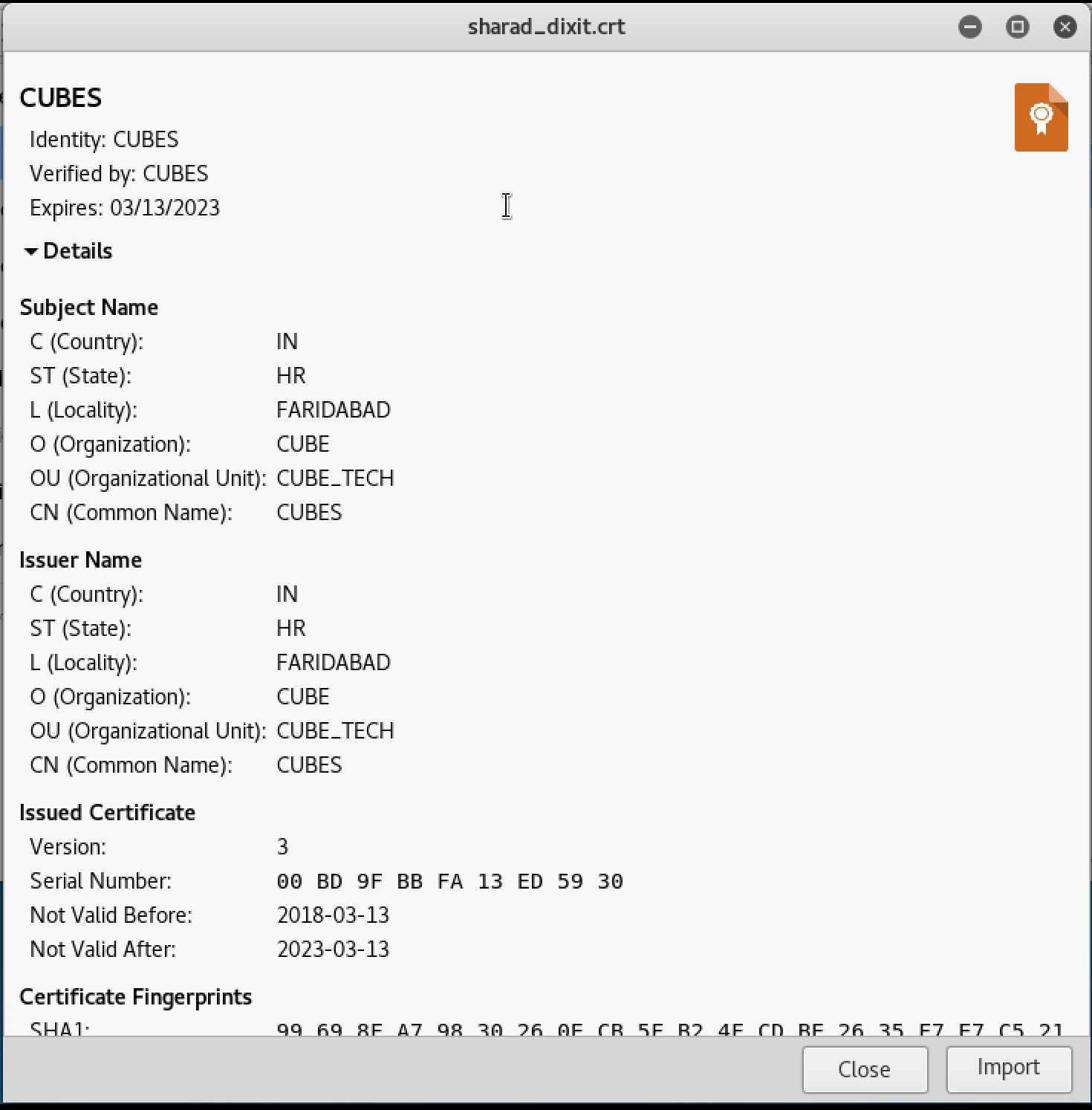
* **SSLSPLIT**:

SSLsplit is a generic TLS/SSL proxy for performing man in the middle attacks on all kind of secure communication protocols. SSLsplit act as a man in the middle attack where the client traffic is redirected to the server where SSLsplit is being executed, and the user thinks that his connection is connected to the original server.

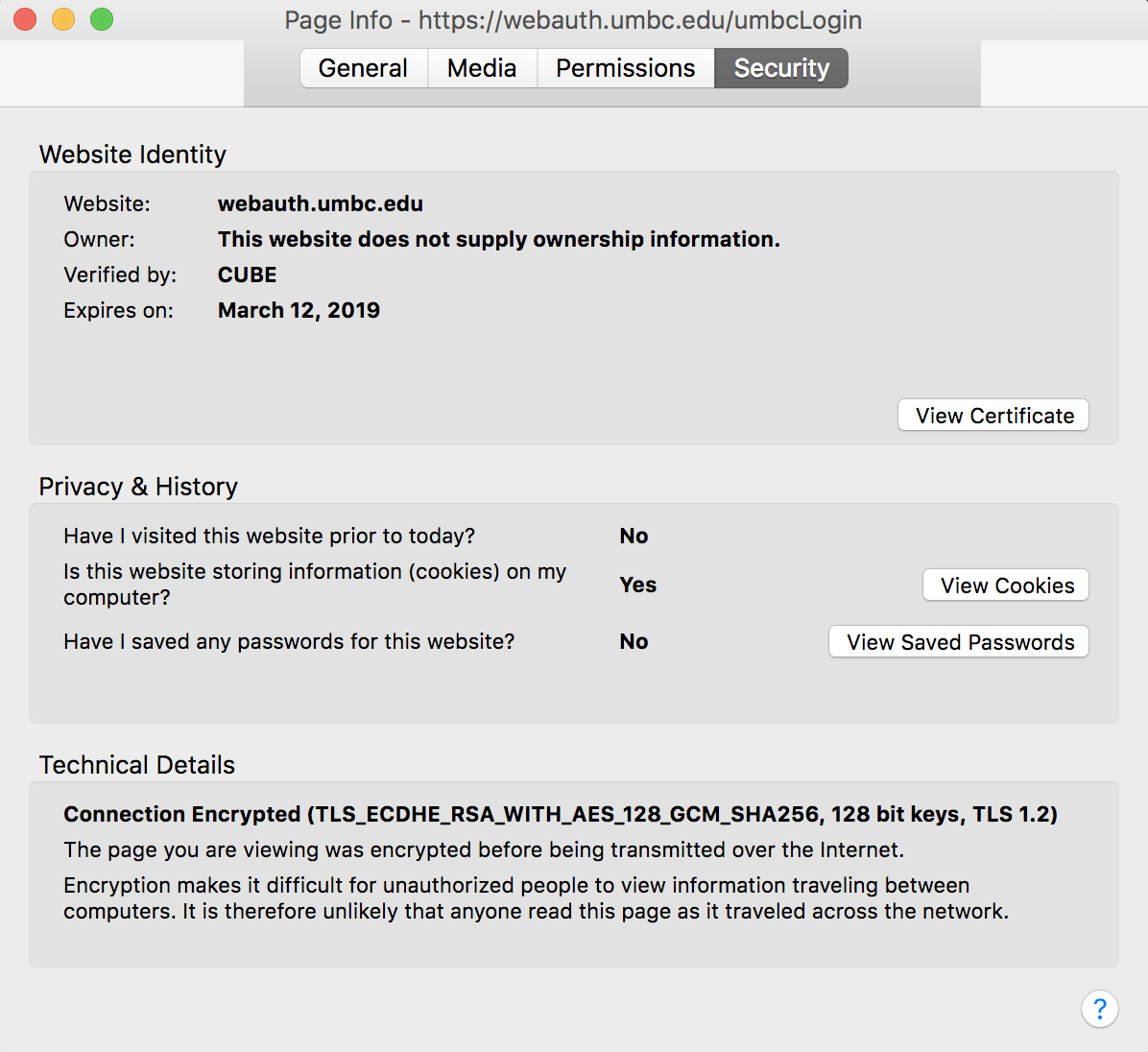
SSLsplit creates a certificate and there by pretends to be original server to the client. For doing so, it generates a certificate and signs it with a private key.



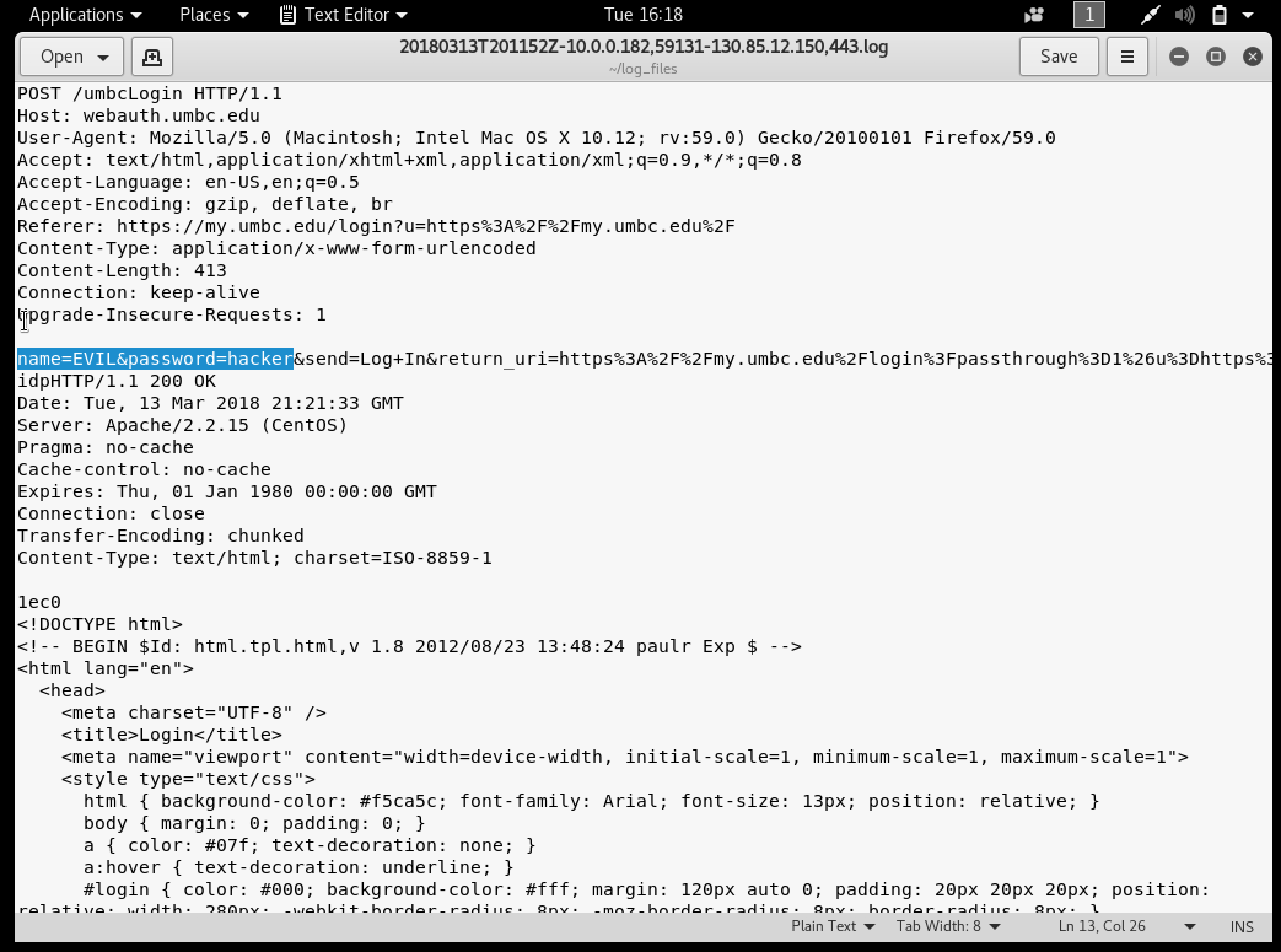
The above figure depicts browser when SSLsplit has been executed. It can been seen that the certificate created is working that’s why the connection is appearing to be secured.



The above figure depicts the certificate created with a key. This certificate is named ‘CUBES’ and after creation it is imported in the Firefox . Hence now when the SSLsplit is launched with the certificate and the key then man in the middle attack works as the user thinks that he is connecting to original server, but it gets connected to the attacker’s server.



The above figure depicts that our certificate has been implanted in the host network and works as this certificate is used for having a secured connection. Therefore, attackers server pretends to be the original server and gets verified by the hoax certificate that is CUBE in this case, which was created by the attacker. Hence the user accesses the website and believes that the connection is secured and is connected to original server but what happens is that the connection is to attackers server and it’s verified by attackers certificate. Therefore, attacker extracts information from the user in this way through SSLsplit.



The above figure depicts the output of the log file where the attackers extract the information of the user. The highlighted statement in the output is what attacker extracted from the user. Therefore, attacker successfully obtains login information of user through SSLsplit.

* **Conclusion**

Tools SSLsplit and SSLstrip were successfully implemented to implement man in the middle attack against SSL/TLS encrypted by removing SSL/TLS encryption from the targets computer. Further the compromised target computer login information was extracted and hence giving successful man in the middle attack.