Case Study 3:

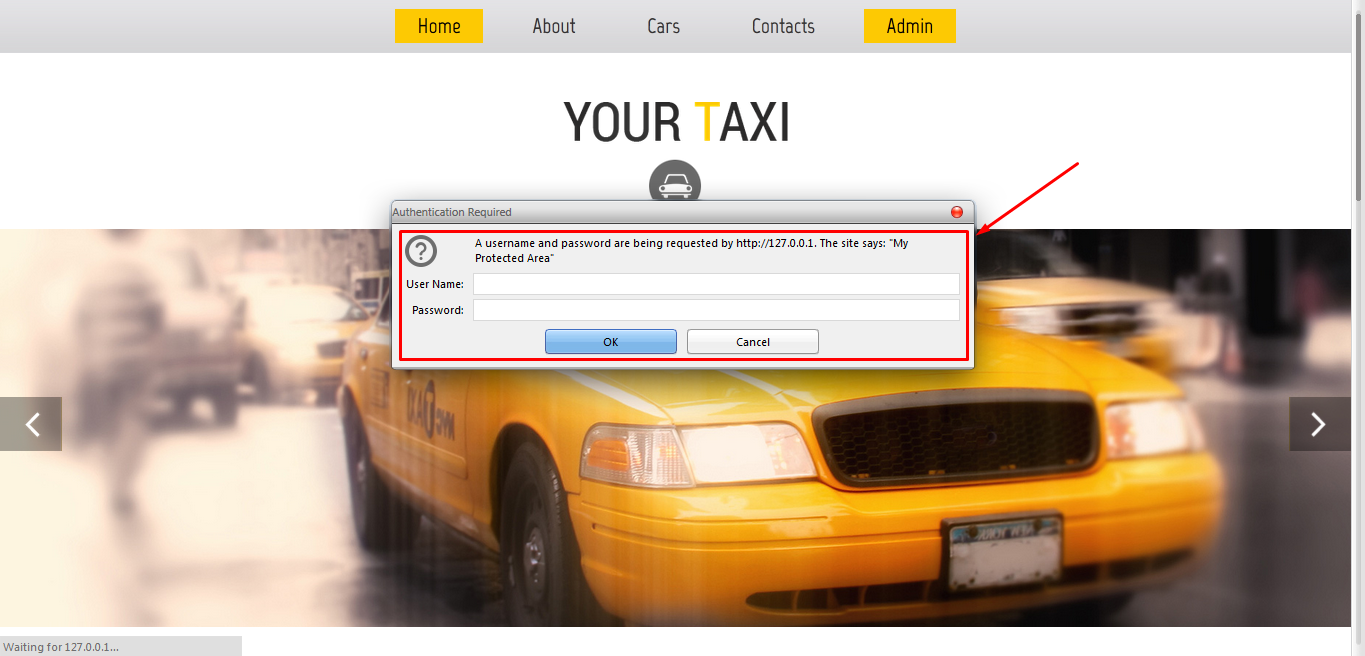
Attack:

* Insecure Direct object Access
* Security Misconfiguration
* Sensitive Data Exposure

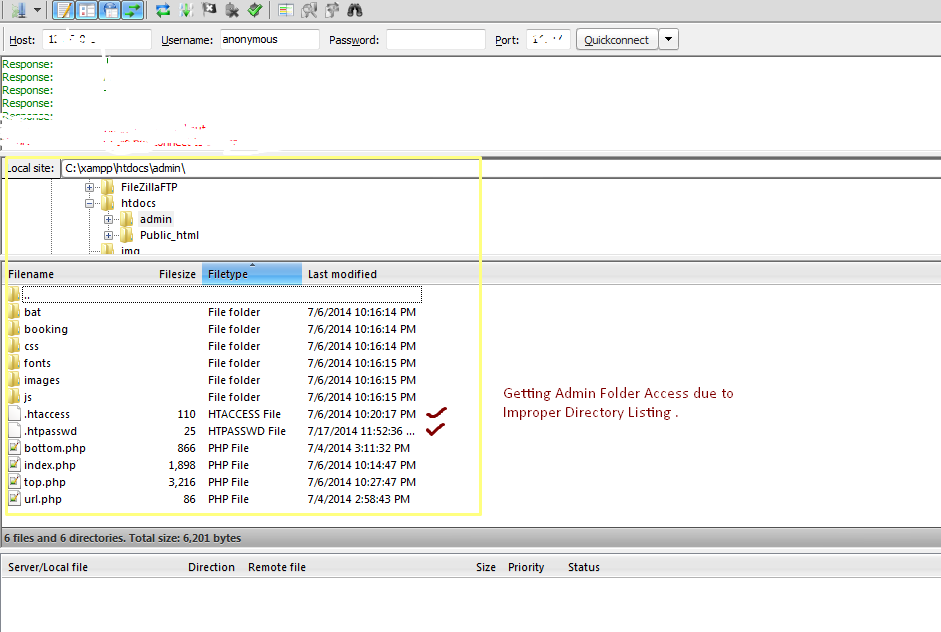
Mission: To get access to the secure admin area using a FTP misconfiguration which gives access to the sensitive .htaccess file and change its password.

Solution :

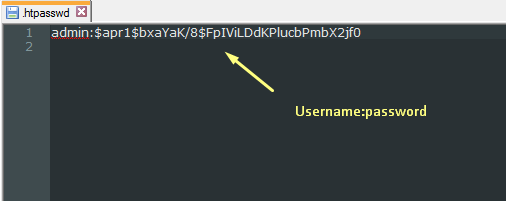
1). When you try to open the admin/index.php . A pop up will ask for username and password. So you cannot get access to any file within the admin folder section until you enter the correct password and username.

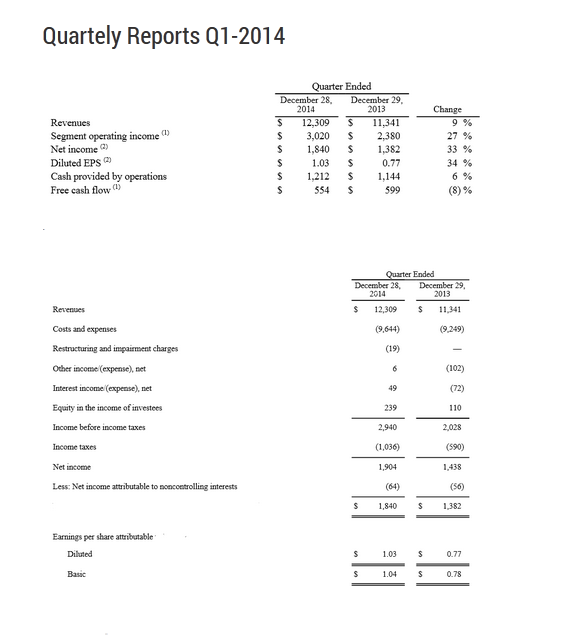


2). To see the content inside the admin area, try to login the using FTP Anonymous Client. This will let you to see all the file directories.



4). Now go to admin folder and then .htpasswd open the file and you can see the password and username. Now enter the credential and you can see the sensitive information.





5). To Change the username and password edit “username:password “ . [There is colon in between and it should be in a single line]