

Forum:[Hack Forums](#)

Thread: [Bypass .htaccess authentication](#)

airwawekz - September 29, 2014, 10:16 am

A .htaccess (hypertext access) file is a directory-level configuration file supported by several web servers, that allows for decentralized management of web server configuration.

Code The original purpose of .htaccess - reflected in its name - was to allow per-directory access control, by for example requiring a password to access the content. Nowadays however, the .htaccess files can override many other configuration settings including content type and character set, CGI handlers, etc.

What does like a .htaccess file content ?

Code AuthName "h4xx0r top security"

AuthType Basic

AuthUserFile "/home/site/www/r00t/.htpasswd"

Require valid-user

How to bypass it ? That is the question !

First of all where is the vulnerability ?

The vuln is when a .htaccess file use <Limit></limit> in the code.

The <Limit> tag is used to restrict enclosed access controls to only certain HTTP methods

So a vulnerable file would look like this :

Code AuthName "h4xx0r top security"

AuthType Basic

AuthUserFile "/home/site/www/r00t/.htpasswd"

<Limit GET POST>

Require valid-user

</Limit>

So now how to bypass it ?

When you want to access to a web page you have a request like this :

Code GET http://127.0.0.1/index.php

Host: 127.0.0.1

So, simply use another http method that GET or POST :

Code Code:

RW http://127.0.0.1/index.php

Host: 127.0.0.1

To do this, you can use for example the addon on firefox : Live HTTP Headers

1. Open Live HTTP Headers, make sure that Capture checkbox is checked.
2. Go to a website with a .htaccess authentication page.
3. When the pop up of login is prompted click cancel.
4. Now find the website in the history of Live HTTP Headers's window
5. Click on replay

6. Where is written GET change it by another http method
7. Click Replay of this window (6)