HTExploit:
Bypassing htaccess Restrictions

Black Hat USA 2012 – White Paper

Matías Katz (@matiaskatz)

Maximiliano Soler (@maxisoler)

July 2012

Table of Contents

Introduction

Our research is based on Web servers, especially Apache and how the .htaccess files are configured in relation to the authorization and authentication on a directory and/or file [1].

It is essential to mention that this is NOT a new attack technique or vulnerability into the Web server [2]. *HTExploit* is a tool that allows you to bypass the restrictions and go one step further; using different attacks vectors to find vulnerabilities that in a traditional way could not be displayed.

HTExploit takes advantage of a weakness in the implementation of the .htaccess file directives related to standard HTTP requests and how they are interpreted [3].

Why attack the protected directories?

Today is common to find lazy administrators and/or developers, using directories located on the same Web server to save backups files, configurations, their own jobs, outdated versions or new developments to be implemented in the future.

These directories are interesting from the security perspective, because if they are protected by an authentication and authorization process, it is for a reason. [4].

Problem with protecting directories

When directories are created and protection through directives in the .htaccess is desired, it is usually done without many specifications, looking for the simplest and most functional way, by using *Basic* or *Digest Authentication* [5].

Since this configuration works, many important security considerations are being ignored and no enhancements are being implemented.

Motivation

Before starting to develop *HTExploit*, we searched for similar tools and verified if they complied with the features that we have thought of. We did not find any tool that already covered our ideas.

In some found tools, it was possible to modify the HTTP methods, but without the possibility of exploiting or bypassing their protections.

Not having found tools that met our needs, we prepared the roadmap to start developing our tool, focusing on how to take advantage of misconfigurations in the .htaccess files.

HTExploit

HTExploit **[6]** is an open-source tool written in Python that exploits a weakness in the way that .htaccess files can be configured to protect a web directory with an authentication process. By using this tool anyone would be able to list the contents of a directory protected this way, bypassing the authentication process.

The tool provides modularity, by allowing the tester to fully perform an analysis on the protected website of the following attacks: SQL Injection, Local File Inclusion, Remote File Inclusion and others.

The main characteristic of this tool is that all of the analyses performed are done inside the protected directory, not from the publicly accessible site.

Conclusions

When authentication and authorization mechanisms are implemented, especially for Web servers using htaccess configuration files, it is necessary not only to declare the traditional HTTP methods. It is also necessary to restrict access to those unknown.

From the developer perspective it is mandatory to perform the necessary security checks, to be able to rely on more than just the configuration files.

References

[1] **Apache Tutorial: .htaccess files**
http://httpd.apache.org/docs/2.0/howto/htaccess.html

[2] **Common Configuration Problems: Issue #81 (090597)**
http://www.apacheweek.com/issues/97-09-05#configerrors

[3] **HTTP Authentication: Basic and Digest Access Authentication**
http://tools.ietf.org/html/rfc2617

[4] **Authentication, Authorization and Access Control**
http://httpd.apache.org/docs/2.4/howto/auth.html

[5] **Password Formats**
http://httpd.apache.org/docs/current/misc/password_encryptions.html

[6] **HTExploit Web Site**
http://www.mkit.com.ar/labs/htexploit

About us

Matías Katz (@matiaskatz) is a Penetration Tester who specializes in Web security analysis. He loves to build simple tools to perform discovery and exploitation on any software or network. He is the founder of Mkit Argentina, a company that specializes in penetration testing and code auditing services. Also, he is Super Mario World master!!

Maximiliano Soler (@maxisoler) lives in Buenos Aires, Argentina and currently works as Security Analyst, in an International Bank. Maxi has discovered vulnerabilities in different applications Web and Microsoft's products.