HTExploit

Bypassing .htaccess Restrictions

Matías Katz & Maximiliano Soler

HTExploit - Bypassing .htaccess Restrictions

Introduction

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.

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.

Basic concepts

.htaccess - What is it and what is it for?

`.htaccess = hypertext access`

It is a distributed ***configuration file*** that allows each directory and subdirectory to have its own configuration, without the need of reconfiguring Apache's main settings file.

.htaccess usually uses the same syntax as the Web server's main configuration files.

Basic concepts

Why attack the protected directories?

Because is common to find...

- x Backup files
- x Configurations
- x Outdated versions
- x New developments
- x Admin Logins ;)

HTExploit - Bypassing .htaccess Restrictions

The Tool

What does mean *HTExploit*?

HTExploit (**H**iper**T**ext access **Exploit**)

It 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.

You will be able to list the contents of a directory protected this way, **bypassing the authentication process**.

HTExploit - Bypassing .htaccess Restrictions

Features

- x Free and Open Source.
- x User-friendly.
- x Flexible.
- x Modularized.
- x Reporting.
- x Integrated with other tools.
- x Multiplatform.

HTExploit - Bypassing .htaccess Restrictions

Why?

- An old weakness that is not used by others tools.
- A lot of websites recommending how to create wrong .htaccess.
- Not having found tools that met our needs.
- Research for fun and profit!

HTExploit - Bypassing .htaccess Restrictions

What is NOT HTExploit?

- x Not a one click Pwnage tool.
- x Not a replacement for others open source tools.
- x Not completely integrated with other solutions.

HTExploit - Bypassing .htaccess Restrictions

DEMO

Questions

```
  .d8888b.
 d88P  Y88b
      .d88P
     .d88P"
     888"
     888

     888
```

HTExploit - Bypassing .htaccess Restrictions

Links

HTExploit Web Site

http://www.mkit.com.ar/labs/htexploit

HTTP Authentication: Basic and Digest Access Authentication

http://tools.ietf.org/html/rfc2617

Apache Tutorial: .htaccess files

http://httpd.apache.org/docs/2.0/howto/htaccess.html

Common Configuration Problems: Issue #81 (090597)

http://www.apacheweek.com/issues/97-09-05#configerrors

Thank you!!

Matías Katz

Twitter: @matiaskatz

Maximiliano Soler

Twitter: @maxisoler

The potential of any tool or technique is limited only by the ***imagination*** of the user.