

Dictionary Password Recovery Tool for Salted Md5's

Due to increased interest for salted Md5's over the last months, the Md5This Team would like to share the small tool we created to recover salted Md5 passwords (commonly used nowadays in web applications and forums - e.g. VBulletinBoard and InvisionPowerBoard).

The tool has just been created so bare with us. Feedback appreciated. It's been written in java to maintain platform independency. We are planning to improve it and also write it in C in order to improve it's speed.

Currently it's not supporting brute force attacks only dictionary (the dictionary will have to be provided by you). We have already uploaded a couple of wordlists (a small one of 3MB and a big one of 200MB in case you need one to get started). You will need to install JRE (Java Runtime Environment - get the latest one from <http://java.sun.com/javase/downloads> if you don't have one installed already) on your pc in order to run it like any other application created in java. Installation:

Download, unzip and run Md5This Tool jar file.

Usage: (simple explanation)

A. Choose your usage from the Method selection box before starting:

- Md5 method is the traditional Md5 algorithm for passwords hashed once. Salt not needed. A valid Md5 string needs to be provided in the Md5 text box in order to get a result if this method is selected.
- E107 method is a password hashed twice. For example a password "hello" would hash to "5d41402abc4b2a76b9719d911017c592" and then "5d41402abc4b2a76b9719d911017c592" is hashed to "69a329523ce1ec88bf63061863d9cb14". Salt not needed. A valid Md5 string needs to be provided in the Md5 text box in order to get a result if this method is selected.
- VBulletin method is a password "hello" hashed to "5d41402abc4b2a76b9719d911017c592", then add a salt "testsalt" to "5d41402abc4b2a76b9719d911017c592" which will form "5d41402abc4b2a76b9719d911017c592testsalt" and then this string hashed to "b9a8f3032597bc73d564a6c846787f5b". A valid Md5 string and a salt (which you have already found by some means!--Not taking questions on this, one it's your responsibility) needs to be provided in the Md5 text box in order to get a result if this method is selected.
- InvisionPowerBoard method is a password "hello" hashed to "5d41402abc4b2a76b9719d911017c592", then a salt "testsalt" hashed to "315240c61218a4a861ec949166a85ef0" and the "315240c61218a4a861ec949166a85ef05d41402abc4b2a76b9719d911017c592" hashes hashed to Md5 hash "74223e0c12d03f63572265bca9588dd9". A valid Md5 string and a salt (which you have already found by some means!--Not taking questions on this, one it's your responsibility) needs to be provided in the Md5 text box in order to get a result if this method is selected.

B. Enter a valid Md5 hash in the md5 text box and a salt (if needed - according to the method selected--see above.)

C. Press the Get Wordlist & Start button, navigate to your wordlist and select it. You will get a message with the approximate time the application will take to scan through the entire list according to the size of the wordlist. Different processor configurations though will result to different timings. The time is computed according to the PC on which it was tested but there shouldn't be a big difference for wordlists smaller than 200MB. The application might look like it's not responding during execution time but it's actually working very fast that's why it happens (look on your task manager and you will see it's actually running!). If your password is found the application will stop and display your password in plaintext, otherwise it will scan the entire wordlist and display a "--not found--" message in the password field.

Furthermore, an Md5 simple calculator is provided at the bottom for convenience.

Tool Download Link:

<http://www.md5this.com/bYMd5ThiS.rar> A small wordlist (the one used by Cain&Abel):

<http://www.md5this.com/Wordlist.zip>

a bigger wordlist will be uploaded soon.