Password Blacklist tab

To Access

From the Login Admin page, you may enable the option. If you click the **Password Blacklist** tab, tools for creating custom blacklists are available.

Option	Description	Default
Password file used	The automatically selected file is recommended unless you generate your own blacklist file. ☰ Automatically select blacklist | Num & Let: 0, Special: 0, Min Len: 1, Custom: 0, Word Count: 1000 | Num & Let: 0, Special: 0, Min Len: 5, Custom: 0, Word Count: 1000 | Num & Let: 0, Special: 0, Min Len: 7, Custom: 0, Word Count: 1000 | Num & Let: 0, Special: 0, Min Len: 9, Custom: 0, Word Count: 1000 | Num & Let: 0, Special: 1, Min Len: 1, Custom: 0, Word Count: 1000 | Num & Let: 0, Special: 1…	Automatically select blacklist

Introduction

Password blacklists lists fill a role in securing accounts from becoming compromised. It uses a list of commonly used passwords to prevent their use and therefore help prevent accounts from becoming compromised. The feature incorporates several lists that complement a wide range of algorithmic password restrictions. The feature can be set to automatically set the best password list, or one can be chosen.

How Likely is this Threat?

Well-known security expert Mark Burnett, better known as xato, mentions in one of his articles that nearly 40% of us use the same top 100 passwords. So without any password restrictions, and 10 attempts per account, one would need to try about 60 accounts before one was compromised. This, of course, can be done with a bot, and thousands of accounts could be checked in mere seconds.

Are Strict Algorithmic Password Constraints Enough?

Algorithmic password constraints are a good start, but the password blacklist addresses a different area of password checking. That is organic patterns. Given any set of algorithmic constraints, there will always be a common set of "Organic Patterns" that emerge. Common passwords include keyboard patterns, the word "password", movie names, pet names, dates and sports. The 4 most popular being: 123456, password, 12345678 & qwerty. Require a number and a letter and the 4 most popular are now: abc123, 1qaz2wsx, 123qwe & trustno1. Require both a special character and a number and we get l58jkdjp!, p@ssw0rd, !qaz2wsx & 1qaz!qaz.
Since algorithmic password constraints are published, an attacker need only set some filters to quickly find the most likely passwords for any algorithmic password constraints. Algorithmic constraints may help in choosing better passwords, but it does not address the "organic" nature of password selection.

Will it Affect Performance?

The password blacklist has been tested with up to 65,000 blacklisted passwords, with no noticeable effect on performance. The default number of passwords is 1000.

Auto Select Option

The auto select option chooses the "best" blacklist for your install. It makes this decision based on the following criteria, in this order: Number and Character, Special Characters, Minimum Length of Password, Custom or Default & Number of Passwords. The longest password length without going over your password length preference will be chosen. Then preference is given to custom generated blacklists, and finally, if a tie exists, preference is given to the blacklist with the most number of passwords.

Password Blacklist Tools

The password blacklist tools are found on the "Password Blacklist" tab of the "Login Preferences" in the control panels of your tiki install. They allow you to create a custom blacklist for your tiki install. The blacklists that come with tiki cover a wide range of settings, but naturally, can't cover every configuration perfectly. A "perfect" list may be generated here. You may also choose to change the number of blacklisted words, or use different published lists.

How to use

1.1.1. Choose your password list

There are many lists but the perhaps the best place to start is the most commonly published passwords. These are conglomerated from security experts from compromised passwords and accounts. The words are then ranked by popularity. The size of the list you can upload to tiki depends on your maximum execution time and maximum file upload size. Typically 1 million passwords are no issue, with slightly higher settings 2 million is easily handled. Please note that after you are done generating your passwords, its recommended you use the "Delete Temporary Index" button to remove these passwords from your database. They take up a lot of room and don't serve any purpose after the lists have been generated.

1.1.2. Upload your list

When you upload your list, it's indexed and placed in the database. The second set of tools now becomes visible, where you are able to generate a password list that tiki will use to blacklist passwords.

1.1.3. Generate your blacklist

The default configuration settings in this step are your current password settings. So long as you are generating this password list for the current tiki install, and you are going to keep your current password settings, the only option you may need to change is the number of passwords to generate. This setting is actually a limit to the number of passwords, so if your original list was not large enough, and your password constraints are very strict, there may be fewer passwords in your final list. When a list is saved, it places a file on the server and allows you to switch between files. Default files will never be overridden, but if you generate two lists with the exact same constraints, the previous file will be deleted and the new blacklist will replace it.

Related pages

- https://xato.net/10-000-top-passwords-6d6380716fe0#.ty2peww21
- http://blog.nfrontsecurity.com/2016/05/microsoft-attempts-to-blacklist-common-passwords/
- https://github.com/danielmiessler/SecLists
- https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Your-Pa-word-doesn-t-matter/ba-p/731984

Alias names for this page:
Blacklist | Blacklists | PasswordBlacklists | PasswordBlacklist | Password Blacklist | PasswordsBlacklists | Passwords Blacklists | Passwords Blacklist | PasswordsBlacklists