

ABSTRACT

Media information obtained through a Website requires security that can cover the vulnerabilities in the Website. For example WCMS Wordpress, and Drupal which is a WCMS Platform originally used as Blogs, Online sites, even E-Commerce, but along with its development, Wordpress has evolved into an advanced and customizable WCMS for more sophisticated Websites such as E-Commerce, banking, media, Real Estate, etc, as well as Drupal WCMS. WordPress and Drupal are the basis of WCMS that is often exposed to attacks from Passwords with several different methods, such as Dictionary or Brute-Force (changing the entire data).

Most users use WordPress and Drupal services to create a weak password so that there is a security gap that is used by people who are not responsible. An analysis related to password security in Greece shows that the average length of Password is only 7 characters, which is relatively weak of the recommended Password is 16 characters. Forensic investigation is an important process in this study to determine the evidence of invalidity and criminal activity that occurs in WCMS. Dictionary Attack is a technique or attack method used to break into any Password that has the possibility, by using Wordlist.

This research will collect evidence (Evidence) from attacks using the Dictionary Tools. The method used to find Forensic evidence in research is by taking Log data from Web Server that is used, as well as Logs from Wordpress and Drupal, then Logs that have been obtained from Web Server and WCMS adjusted from time, day / date, and IP attacker / intruder.

Therefore this research will use some Tools as a comparison object to perform penetration testing of each account in WCMS, with this analysis the expected results later from each Log or Password list that has been penetrated there is a solution of attack on WCMS by installing Plug-In or Module on each WCMS. The settlement of the problems contained in this study using the standard Password that has been recommended is 16 characters, as well as installation of Plug-In or Module on each WCMS.

Keyword : Dictionary Attack, Wordlist, Log File, WCMS, Wordpress, Drupal, Forensics

ABSTRAK

Media informasi yang diperoleh melalui sebuah *Website* membutuhkan keamanan yang dapat menutup celah keamanan dalam *Website*. Contohnya *WCMS Wordpress*, dan *Drupal* yang merupakan *Platform WCMS* yang awal mulanya digunakan sebagai *Blog*, situs *Online*, bahkan *E-Commerce*, namun seiring dengan perkembangannya, *Wordpress* telah berkembang menjadi *WCMS* yang canggih dan mampu diubah – ubah untuk keperluan *Website* yang lebih rumit seperti *E-Commerce*, perbankan, media, *Real Estate*, dan sebagainya begitu pula dengan *WCMS Drupal*. *Wordpress* dan *Drupal* merupakan basis dari *WCMS* yang seringkali terkena serangan dari *Password* dengan beberapa metode berbeda, seperti *Dictionary* atau *Brute-Force* (mengubah keseluruhan data).

Kebanyakan pengguna memakai jasa *Wordpress* dan *drupal* membuat *Password* yang lemah sehingga ada celah keamanan yang dimanfaatkan oleh orang yang tidak bertanggung jawab. Sebuah analisis yang berkaitan dengan keamanan *Password* di Yunani menunjukkan bahwa panjang rata-rata *Password* hanya 7 karakter, yang relatif lemah dari *Password* yang direkomendasikan adalah 16 karakter. Investigasi Forensik merupakan proses penting dalam penelitian ini untuk menentukan bukti ketidakabsahan dan aktivitas kriminal yang terjadi pada *WCMS*. *Dictionary Attack* adalah Teknik atau metode serangan yang digunakan untuk membobol setiap *Password* yang memiliki kemungkinan, dengan menggunakan *Wordlist*.

Penelitian ini akan mengumpulkan berbagai bukti (*Evidence*) dari serangan menggunakan *Tools Dictionary*. Metode yang digunakan untuk menemukan bukti Forensik dalam penelitian yaitu dengan mengambil data *Log* dari *Web Server* yang digunakan, serta *Log* dari *Wordpress* dan *Drupal*, kemudian *Log* yang telah diperoleh dari *Web Server* dan *WCMS* disesuaikan dari waktu, hari / tanggal, dan *IP* penyerang / penyusup.

Oleh karena itu penelitian ini akan menggunakan beberapa *Tools* sebagai bahan perbandingan untuk melakukan pengujian penetrasi setiap akun dalam *WCMS* dengan analisis ini diharapkan nantinya dari setiap *Log* maupun daftar *Password* yang telah di penetrasi ada solusi dari serangan terhadap *WCMS* dengan melakukan pemasangan *Plug-In* atau *Module* pada tiap *WCMS*. Adapun penyelesaian dari masalah yang terdapat dalam penelitian ini dengan menggunakan standar *Password* yang telah direkomendasikan yaitu 16 karakter, serta pemasangan *Plug-In* atau *Module* pada setiap *WCMS*.

Keyword : *Dictionary Attack*, *Wordlist*, *Log File*, *WCMS*, *Wordpress*, *Drupal*, *Forensik*