

ABSTRAK

Judul : Analisa celah keamanan pada Wordpress terhadap serangan
Unrestricted File upload

Nama : Dani Kharisma

Program Studi : Teknik Informatika

Keamanan dan kerahasiaan data merupakan hal yang wajib diperhatikan dan dilindungi oleh setiap pengembang website. *Wordpress* merupakan salah satu *Content Management System* yang digunakan oleh sekitar 1,7 juta pengembang *website* diseluruh dunia. beberapa *plugin* pada *wordpress* masih memiliki celah keamanan yang berbahaya, seperti *plugins* yang digunakan untuk proses mengunggah file. dengan memanfaatkan celah keamanan *file upload* pada website seorang attacker dapat mengambil informasi penting yang terdapat pada sebuah website. *Unrestricted file upload* merupakan sebuah celah keamanan yang dapat mengancam keamanan *website*. Kerentanan ini biasanya terdapat dalam fitur website yang digunakan untuk mengunggah file seperti foto, avatar, video, dan lain-lain. Pada pengujian ini peneliti akan melakukan serangan *Unrestricted File upload* terhadap *plugin* yang memiliki celah dengan mengunggah file berbahaya dan peneliti berhasil melakukan eksploitasi kedalam *webserver*. hasil dari penelitian ini adalah untuk melihat dampak dari serangan *Unrestricted File upload* terhadap situs berbasis *Wordpress*, sehingga dapat dilakukan proses perbaikan lebih lanjut terhadap situs XYZ.

Kata kunci : *Unrestricted file upload, Wordpress, exploit*

ABSTRACT

Title : Analyze security holes in WordPress against attacks
Unrestricted File upload

Name : Dani Kharisma

Study Program : Information Technology

Data security and confidentiality are things that must be considered and protected by every website developer. Wordpress is one of the Content Management Systems that is used by around 1.7 million website developers worldwide. some plugins on wordpress still have dangerous security holes, like plugins that are used to process files. by exploiting the vulnerability of uploaded files on the website an attacker can retrieve important information contained on a website. Unrestricted *file upload* is a security hole that can threaten website security. This vulnerability is usually found in website features that are used to upload files such as photos, avatars, videos, and others. In this test, researchers will attack the Unrestricted *File upload* against plugins that have loopholes by uploading malicious files and the researchers have successfully exploited the website XYZ webserver. the result of this research is to look at the impact of the Unrestricted *File upload* attack on Wordpress-based sites, so that further improvements can be made to sites owned by website XYZ.

Keywords : *Unrestricted file upload, Wordpress, exploit*