# ANALISIS FILE UPLOAD VULNERABILITY DAN PENCEGAHAN DENGAN FILE CONTENT VALIDATION

**Jose Alnevo Theora**

## ABSTRAK

*File Upload Vulnerability* merupakan sebuah kerentanan yang terdapat pada sebuah *website* yang disebabkan oleh karena ketidaksempuranaan penulisan kode program. Dimana dengan adanya kerentanan tersebut, memungkinkan orang yang tidak memiliki kewenangan untuk menggunggah file berbahaya seperti *backdoor* kedalam sistem atau server website tersebut. Tujuan dari penelitian ini bertujuan untuk Dapat mengetahui hal terkait File Upload Vulnerability, Dapat membuat aplikasi berbasis website yang bisa mencegah masuknya backdoor kedalam sistem, Dapat menjadikan referensi untuk penelitian terkait. Sehingga untuk mencegah hal tersebut diperlukannya pencegahan *File Upload Vulnerability* dengan cara melakukan *File Content Validation* dimana cara ini akan menyeleksi *file* yang akan diunggah kedalam *website*. Dimana proses *filtering file* dilakukan dengan cara *filtering* ekstensi file, dan selanjutnya isi atau *content* pada file tersebut akan dicek, apakah mengandung *string* yang biasa terdapat pada *backdoor*, Jika *file* tersebut terindikasi sebagai *backdoor* karena adanya kecocokan pada *string* tersebut, maka *file* tersebut tidak akan bisa masuk atau diunggah, dan jika file tersebut aman, maka file tersebut akan bisa masuk atau diunggah kedalam sistem. Dari hasil percobaan *File Content validation* dengan mengunggah sebanyak 150 file didapatkan hasil yaitu, sebanyak 30 *executable file* dan 6 *PHP backdoor file* tidak bisa masuk kedalam server yang telah disediakan. Sehingga dengan menggunakan *File Content Validation* bisa mencegah masuknya *executable file dan PHP backdoor file* kedalam server.

Kata Kunci : *File Upload Vulnerability, file,* sistem, *server*.

# ANALISIS FILE UPLOAD VULNERABILITY DAN PENCEGAHAN DENGAN FILE CONTENT VALIDATION

**Jose Alnevo Theora**

## ABSTRACT

File Upload Vulnerability is a vulnerability found on a website caused by the imperfect writing of program code. Wherewith these vulnerabilities, it is possible for people who do not have the authority to upload malicious files such as backdoors into the system or website server. The purpose of this study is to be able to find out things related to File Upload Vulnerability, Can create website-based applications that can prevent backdoor entry into the system, Can make references for related research. So to prevent this, it is necessary to prevent File Upload Vulnerability by doing File Content Validation where this method will select files to be uploaded to the website. Where the file filtering process is done by filtering the file extension, and then the contents of the file will be checked, whether it contains a string that is usually found in the backdoor. If the file is indicated as a backdoor because of a match in the string, then the file will not be able to enter or uploaded, and if the file is safe, then the file will be able to enter or be uploaded to the system. From the results of the File Content validation experiment by uploading 150 files, the results obtained are, as many as 30 executable files and 6 PHP backdoor files cannot enter the server that has been provided. So using File Content Validation can prevent the entry of executable files and PHP backdoor files into the server.

Keyword : *File Upload Vulnerability*, *file*, system, *server*.