|  |
| --- |
| /home/van/Pictures/logo-baru-uty-putih2.pnglogo-baru-uty-putih2**LAPORAN TUGAS BESAR**  **MANAJEMEN KEAMANAN KOMPUTER** |
| **UNRESTRICTED FILE UPLOAD TO REMOTE CODE EXECUTION (RCE)**  **KELOMPOK :**  **5180411091 DANANG AVAN MAULANA**  **5180411109 BAGAS TRI USADA**  **5180411126 MUHAMMAD NUR AZIZ MA'RUF**  **5180411066 FAYZAYA GANANG PUTRA**  **5180411144 SEM GILBERT**  **PROGRAM STUDI INFORMATIKA**  **FAKULTAS SAINS & TEKNOLOGI**  **UNIVERSITAS TEKNOLOGI YOGYAKARTA**  **YOGYAKARTA**  **2021** |

Unrestricted File Upload atau file upload yang tidak dibatasi menjadi salah satu masalah utama web security yang dapat mengancam keamanan website. Kerentanan ini biasa ditemukan di dalam fitur website yang digunakan untuk mengunggah file seperti foto, avatar, video, bukti transfer, dan lain-lain.

Meskipun fitur ini terlihat menarik, namun tidak jarang fitur ini digunakan peretas sebagai jalan masuk ke dalam sistem sehingga membahayakan web security Anda. Mereka juga bisa mengunggah dan mentransfer file yang berisi kode berbahaya untuk merusak halaman web Anda.

## Apa saja risiko yang dapat ditimbulkan ?

### Serangan sisi server

Peretas dapat melakukan serangan dari sisi server dengan cara mengunggah file dengan nama dan ekstensi yang sama dengan file yang berada di server. File yang diupload oleh peretas akan menimpa file asli di server sehingga website tidak dapat berfungsi lagi. Melalui metode ini, peretas juga bisa merusak web security sehingga memungkinkan file-file berbahaya lain seperti trojan atau pun virus dapat masuk ke dalam sistem website.

* Serangan DDoS

Peretas dapat melakukan serangan dengan metode DDoS, yaitu dengan cara mengunggah file-file berukuran besar. Serangan ini dapat melumpuhkan website karena adanya transaksi data dalam jumlah yang besar yang mengakibatkan lalu lintas website menjadi overload.

### Mengupload konten berbahaya

Peretas dapat mengunggah dokumen atau program yang terinfeksi dengan virus. File berbahaya tersebut dapat digunakan peretas untuk mengambil kendali server serta mendapat informasi sensitif dari server.

### Serangan sisi klien

Mengunggah file berbahaya dapat membuat situs web security menjadi lemah terhadap serangan sisi klien seperti cross-site content hijacking dan serangan XSS. Peretas juga bisa mengunggah file berbahaya yang dapat memicu kerentanan lain di perangkat yang digunakan oleh pengguna.

Basic File Upload pad PHP