**SGB.or.id PHP Code Injection**

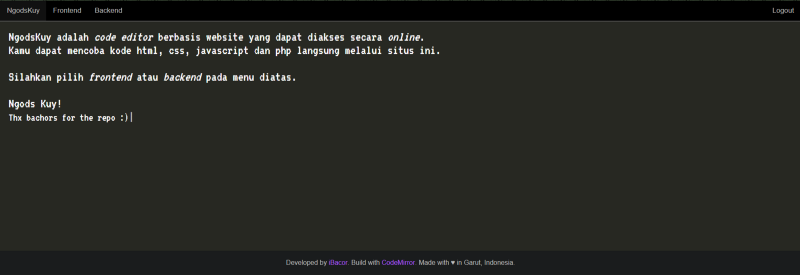
Sharing Gil’s Blog (SGB) merupakan salah satu komunitas besar yang ada di Indonesia yang didalamnya terdapat berbagai macam pemuda lintas generasi yang sangat kompak dalam berbagai hal. Ini dapat dilihat dari deskripsi SGB dari situs officialnya [sgb.or.id](https://sgb.or.id/).



Sebagian besar dari mereka adalah remaja-remaja aktif dalam dunia IT dari berbagai bidang. Sehingga segala sesuatu tentang tips & trik hampir semuanya bermula dari komunitas ini.

Beberapa waktu lalu, saya dan teman saya sudah pernah melakukan testing ke situs milik SGB, khususnya pada bagian daftar member resmi mereka member.sgb.or.id. Celah ini sangat fatal, beberapa privasi member mereka berhasil kami dapatkan, sampai mereka meminta kami untuk menolong memperbaiki celah tersebut dan melakukan pembaruan data.

Kali ini, saya sendiri kembali melakukan testing pada salah satu subdomain milik mereka, dimana subdomain ini berisi sebuah Code Editor bernama **Ngods.**Pada Editor Ngods ini kita dapat menuliskan code lalu secara otomatis code itu di perlihatkan secara online (in-Browser Code Editor). Ngods berbasis sebuah plugins opensource bernama [**CodeMirror**](https://github.com/codemirror/codemirror).



ngods.sgb.or.id

Mendengar kabar bahwa tools ini baru saja dirilis oleh mereka, saya langsung sangat tertarik!!! Langsung saja, saya menuju menu Backend, dimana pada halaman ini kita bisa menuliskan kode server-side yaitu PHP.

***Service ngods.sgb.or.id sudah ditutup semenjak saya menulis wripte up ini. Jadi, saya hanya akan menjabarkan secara tulisan tanpa gambar.***

Setelah saya mencoba-coba menuliskan code PHP sederhana, ternyata ada sebuah filtering/fungsi yang tidak diperbolehkan. Sehingga, beberapa kali evil code yang saya tulis tidak berhasil berjalan dengan sempurna.

Saya hanya bisa melakukan scanning directory dan files melalui code PHP sederhana yang saya buat :

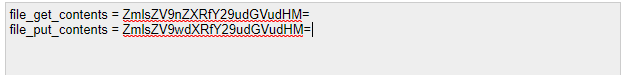
*<?php var\_dump(scandir(‘/tmp’)); var\_dump($\_SERVER); ?>*

2 Code ini sangat membantu saya melakukan information gathering, dimana saya mampu melihat seluruh struktur file dan folder yang ada pada server mereka ([**Scandir PHP Function**](http://php.net/manual/en/function.scandir.php)). Dan tentunya, saya berhasil menemukan **IP ASLI**server mereka di balik **CLOUDFLARE (**[**$\_SERVER Predefined Variables**](http://php.net/manual/en/reserved.variables.server.php)**)**.

Fungsi yang saya maksud tidak dipebolehkan contohnya fungsi-fungsi nakal seperti fopen, curl, file\_get\_contents, file\_put\_contents, dan lainnya untuk membuat sebuah file dan membaca file lokal tidak bisa dijalankan. Editor menunjukkan sebuah peringatan “**Function disabled**”.

Tidak mundur begitu saja, pikiran saya secara mudah menebak bagaimana membypass hal ini. Tidak memakan waktu lama, langsung saja fungsi tersebut dengan mudahnya saya lewati tanpa halangan yang berarti.

Bypass tersebut saya lakukan dengan cara mengubah nama fungsi PHP tersebut menjadi sebuah encode Base64.



Merubah nama fungsi ke Base64 untuk mengecoh filtering.

Cukup dengan 2 fungsi ini saya sudah leluasa mengupload sebuah PHP Backdoor ke server mereka. Berikut isi code saya yang lebih lengkap.



Code yang saya gunakan untuk masuk ke dalam Server SGB.or.id

Fungsi pada variable **$a** merupakan fungsi **file\_put\_contents** dan variable **$b**adalah fungsi **file\_get\_contents.**

Jika ada kata-kata sedikitpun yang mengandung fungsi-fungsi nakal tadi maka editor akan menghasilkan pesan “Function Disabled”. Karena itu pada code diatas, saya buat semuanya nampak bersih sehingga fungsi-fungsi nakal tidak ikut terbawa (Untung saja base64\_decode tidak difilter :D).

Code diatas tadi akan membuat sebuah file baru pada document root milik sgb.or.id yang berisi **IndoXploit PHP Backdoo**r yang saya ambil pada link tertera pada variable **$b**. (sgb.or.id/backdoor.php)

Setelah saya coba mengecek secara langsung, dan benar saja backdoor saya sudah berhasil masuk pada server mereka tanpa ada halangan, filter yang awalnya memblokir fungsi nakal tersebut juga dengan mudahnya dapat dilewati begitu saja.

Oke sekian writeup dari saya, sayang sekali service ngods mereka tutup pada saat saya menulis writeup ini. Sehingga apa yang saya jelaskan tidak dipenuhi dengan bukti gambar secara langsung :(

Semoga bermanfaat.