qerogram Update : CVE-2021-45003 ... on Feb 23 History

..

report_img	9 months ago
README.md	9 months ago
ptms_exploit.py	9 months ago

README.md

PTMS

license MIT

Author

Qerogram

Version

php 7.2.24 PTMS version 2022.01.18

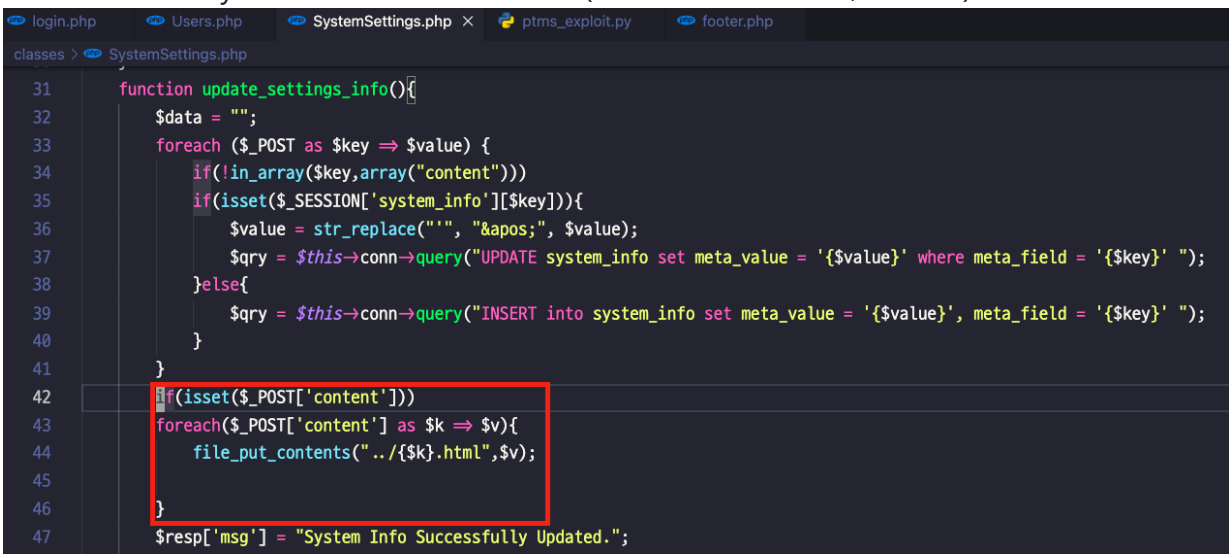
Vulnerability

RCE(Remote Code Execution) via File Upload

Chains the three vulnerabilities below and uses them.

1. **Insecure Permission Check**
   It does not check user permission when using the arbitrary file writing function.

2. **Arbitrary File Write Function**
   Limited arbitrary file write function exists.(Possible extension, "html".)



3. **Local File Include**
   the error handling page with the extension "html" is loaded through the keyword "include".

Therefore, we can overwrite the "404.html" file, which is an error handler page, with a webshell payload, as if overwriting the SEH handler code, and then invoke the error page to **trigger an RCE vulnerability.**

Reference

[1] Download WebApp from Vendor