New issue

Jump to bottom

Bug:V1.1.9 Cross Site Scripting Vulnerability #8

Open **Richard1266** opened this issue on Mar 6, 2019 · 0 comments

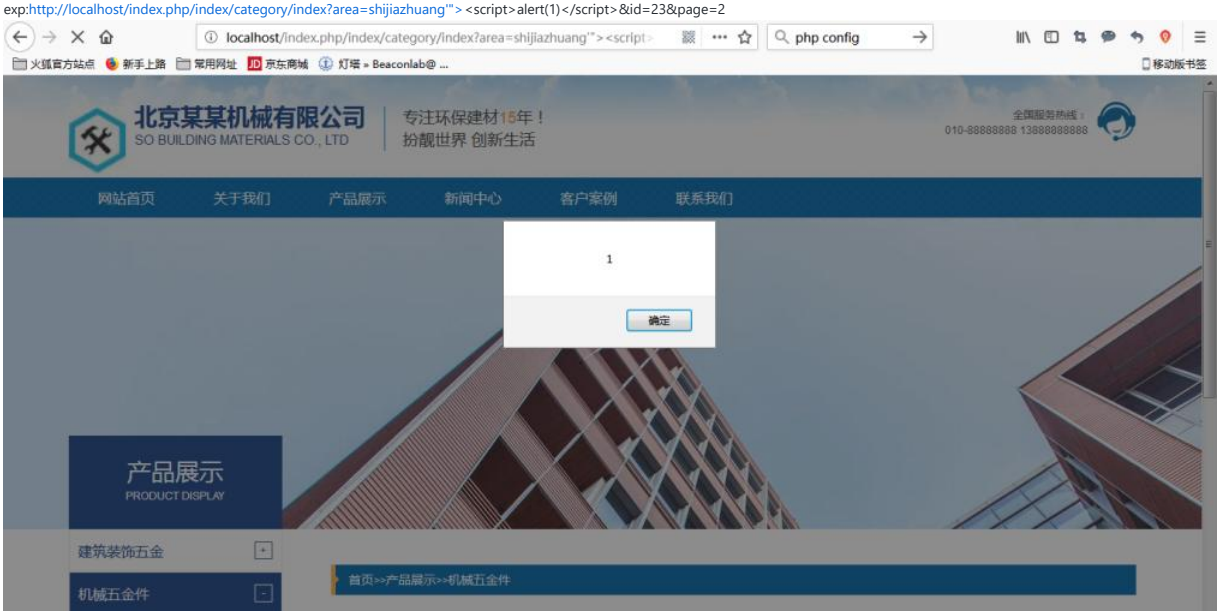
Richard1266 commented on Mar 6, 2019 • edited

There is an Reflective Cross Site Scripting vulnerability in your latest version of the CMS v1.1.9
Download link: "http://img.yunucms.com/o_1d1n2lp3h1g0m1rjfvf818epqmua.zip?attname="

In the YUNUCMSv1.1.9\app\extend\com\Page.php, No filtering to url in the upurl( ) function:

```
protected function upurl($url){
    if (config('sys.url_model') == 3) {
        $url = preg_replace('/page\/*\//',''.$url);
        $url = str_replace([ "?", '='], ['', '/'], $url);
        if (isset($_GET["ctitle"])) {
            $url = "/".$_GET["ctitle"].'/'.$url;
        }
    }
    return $url;
```

Steps To Reproduce:
Open below URL in browser which supports flash.
url:http://localhost/index.php/index/category/index?[xsspayload]&id=23&page=2
exp:http://localhost/index.php/index/category/index?area=shijiazhuang'"><script>alert(1)</script>&id=23&page=2



Fix:
Filter the url parameter

Richard1266 changed the title ~~Bug:Cross Site Scripting Vulnerability~~ Bug:V1.1.9 Cross Site Scripting Vulnerability on Mar 8, 2019

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant