New issue

Jump to bottom

The function parameter [Route] has reflective XSS #4

Closed **Stellarsss** opened this issue on Jun 18, 2020 · 1 comment

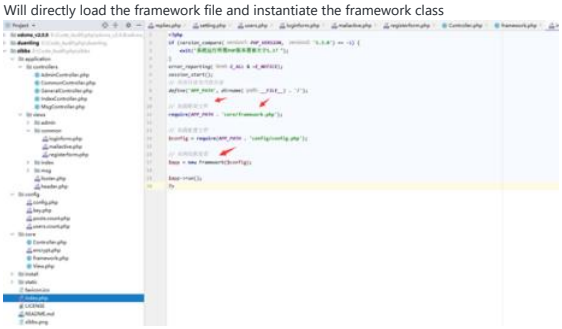
Stellarsss commented on Jun 18, 2020

First follow to the index.php entry file, which will load the frame file directly, so just visit the following address

`http://20.20.20.130:8000/zibbs/index.php`

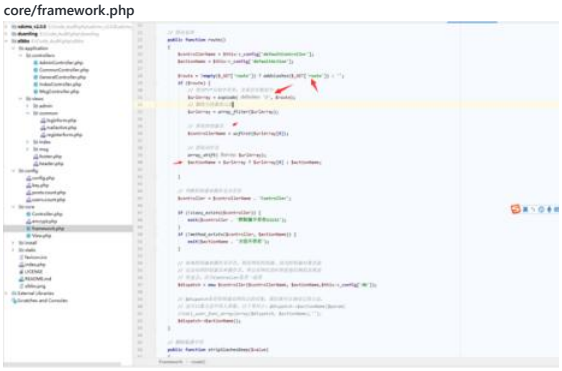
`http://20.20.20.130:8000/zibbs`

Will directly load the framework file and instantiate the framework class



Directly trace to the **core/framework.php** file. After analysis, this CMS handles the processing of each controller and operation through 【route】, wherein the parameter route is the controller name and action name to be filled in in this GET request.

core/framework.php

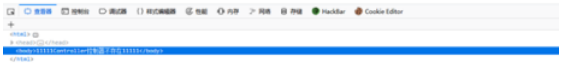


A normal GET request would look like this

http://20.20.20.130:8000/zibbs/index.php?route=admin/login

And here the parameter 【route】 is controllable, The value of the input parameter 【route】 is processed as follows, The value of the parameter【router】is first split through /, Such as route=aaa/bbb, the aaa Is the controller name,bbb for the action of, It also makes conditional judgments about whether the controller and the action name exist, When the Controller name does not exist, it will directly output "aaa Controller Controller does not exist 11111", as shown below

```php
// 路由处理
public function route()
{
    $controllerName = $this->_config['defaultController'];
    $actionName = $this->_config['defaultAction'];

    $route = !empty($_GET['route']) ? addslashes($_GET['route']) : '';
    if ($route) {
        // 使用"/"分割字符串，并保存在数组中
        $urlArray = explode( delimiter: '/', $route);
        // 删除空的数组元素
        $urlArray = array_filter($urlArray);

        // 获取控制器名
        $controllerName = ucfirst($urlArray[0]);

        // 获取动作名
        array_shift( &array: $urlArray);
        $actionName = $urlArray ? $urlArray[0] : $actionName;

    }

    // 判断控制器和操作是否存在
    $controller = $controllerName . 'Controller';

    if (!class_exists($controller)) {
        exit($controller . '控制器不存在11111');
    }
    if (!method_exists($controller, $actionName)) {
        exit($actionName . '方法不存在');
    }

    // 如果控制器和操作名存在，则实例化控制器，因为控制器对象里面
    // 还会用到控制器名和操作名，所以实例化的时候把他们俩的名称也
    // 传进去，结合Controller基类一起看
    $dispatch = new $controller($controllerName, $actionName,$this->_config['db']);

    // $dispatch保存控制器实例化后的对象，我们就可以调用它的方法，
    // 也可以像方法中传入参数，以下等同于：$dispatch->$actionName($param)
    //call_user_func_array(array($dispatch, $actionName),'');
    $dispatch->$actionName();
}
```

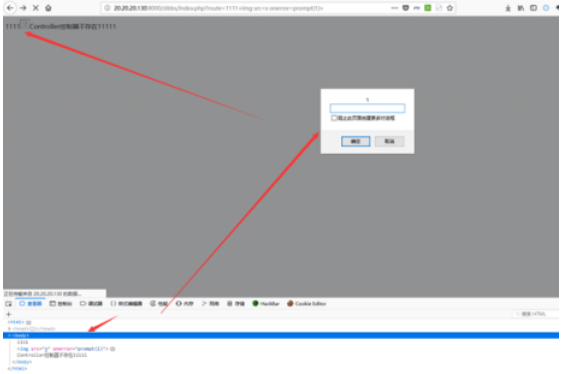


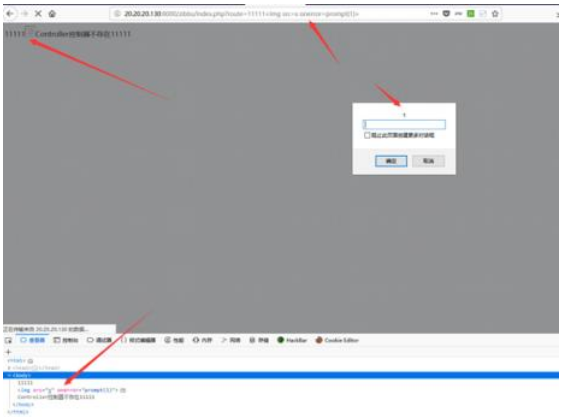
This is for the parameter 【route】, If the controller doesn't exist, The value of the input parameter 【route】 is displayed directly, And the following values, without XSS filtering, Only the addslashes() method is done here, and there is no XSS filtering function in this aspect

Because there is no filtering here, there is reflective XSS, which is tested as follows

Because of the split for / here, the regular XSS payload cannot be taken from a bomb frame, so using the following XSS payload can make a bomb fram

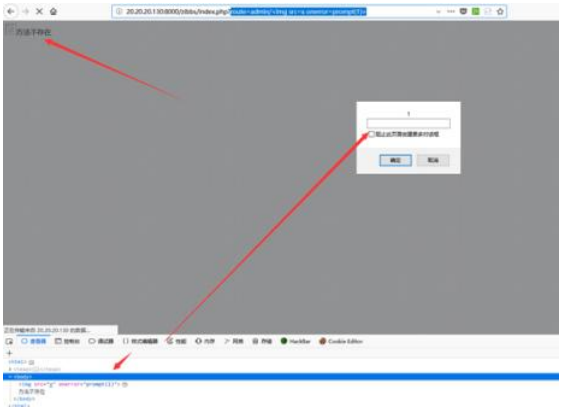
http://20.20.20.130:8000/zibbs/index.php?route=1111%3Cimg%20src=x%20onerror=prompt(1)%3E





The following test statement can also cause a pop-up as normal

route=admin/



Solution:
filter or encode special characters like this
<

"
'
&
%
... ...
and filter some keyword like this

script
javascript

... ...
or filter some label function which can run javascript like this
onclick
onerror
onload
... ...

Stellarsss closed this as completed on Jun 18, 2020

---

xujinliang commented on Jun 18, 2020 — Owner

3Q， you are a good man

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants