

New issue

[Jump to bottom](#)

Reflected-XSS vulnerabilities via '/common/library/Page.php'

#1

Open zhujietao opened this issue on Oct 14 · 1 comment

zhujietao commented on Oct 14

Which version of yii-shopwind do you testing?

V3.4.3

Expected behavior

login web system

Actual behavior

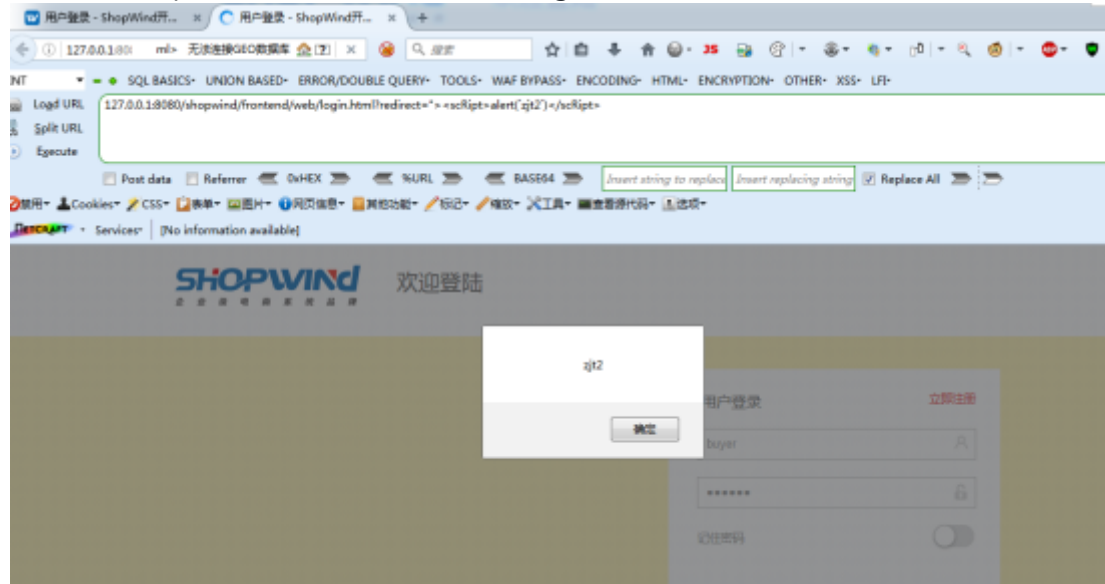
login Reflected-XSS vulnerabilities in the login page of yii-shopwind .

Steps to reproduce the behavior

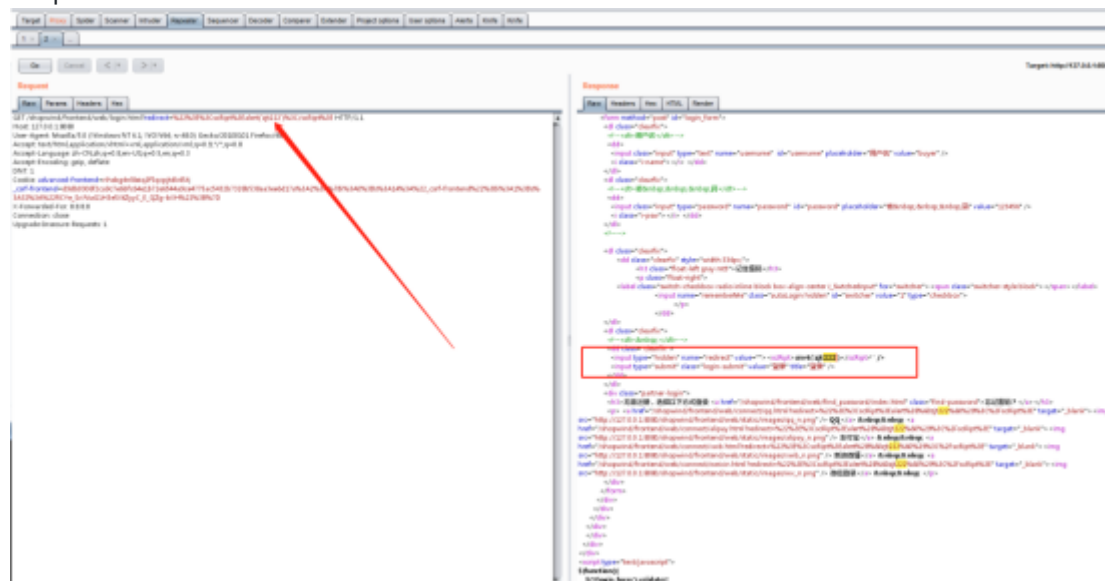
POC:%22%3E%3CscRipt%3Ealert(%60zjt2%60)%3C/scRipt%3E

1. open browser load login pag.

2. add the vuln parameter(redirect) after the login url and insert POC.



Burp Suite validated



zhujietao commented on Oct 14

Author

vulnerabilities page and point.

troller.php | 全局搜索 | SiteController.php | HandlerStack.php | Page.php | Page.php | UserController.php | Page.php | 全局搜索

```
127 > {
128 >     $model = new \frontend\library\Menu();
129 >     if(($curitem != null) && ($curmenu == null)) {
130 >         return $model->curitem($curitem);
131 >     }
132 >     return ArrayHelper::merge($model->curitem($curitem), $model->curmenu($curmenu));
133 > }
134 > }
135 > /**
136 >  * 在ACTION执行前跳转
137 >  * 跳转到登录页面后，如登录成功，跳回到
138 >  * $param string $redirect
139 >  */
140 > public static function redirect($redirect = null)
141 > {
142 >     // $loginUrl = Yii::$app->user->loginUrl;
143 >     $loginUrl = Url::toRoute(['user/login', 'redirect' => $redirect]);
144 >
145 >     if(Yii::$app->request->isAjax) {
146 >         Yii::$app->getResponse()->format = Response::FORMAT_JSON;
147 >         Yii::$app->getResponse()->data = ['done' => false, 'icon' => 'warning', 'msg' => Yii::t('yii', 'Login Required'), 'loginUrl' => $loginUrl];
148 >         return false;
149 >     }
150 >     return Yii::$app->getResponse()->redirect($loginUrl);
151 > }
152 > }
153 > /**
154 >  * 页面的公共参数
155 >  * $param string $page as: mall|user|store
156 >  */
157 > public static function getAssign($page = '', $options = null)
158 > {
159 >     $params = [
160 >         'icp_number' => isset(Yii::$app->params['icp_number']) ? Yii::$app->params['icp_number'] : null,
161 >         'statistics_code' => isset(Yii::$app->params['statistics_code']) ? Yii::$app->params['statistics_code'] : null,
162 >     ];
163 >
164 >     if(in_array($page, ['mall', 'store'])) {
165 >         $params['hot_keywords'] = explode(',', Yii::$app->params['hot_keywords']);
166 >
167 >         $model = new \frontend\models\CartForm();
168 >         $params['casts_top'] = $model->getCart();
169 >     }
170 >
171 >     return $params;
172 > }
173 > }
174 > /**
175 >  * 将相对地址修改为绝对地址，以适应不同的应用显示
176 >  * @desc 主要是处理图片路径，不要使用在js文件路径（以免引起跨域问题）
177 >  */
178 > public static function urlFormat($url = '', $default = '')
179 > {
```



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

