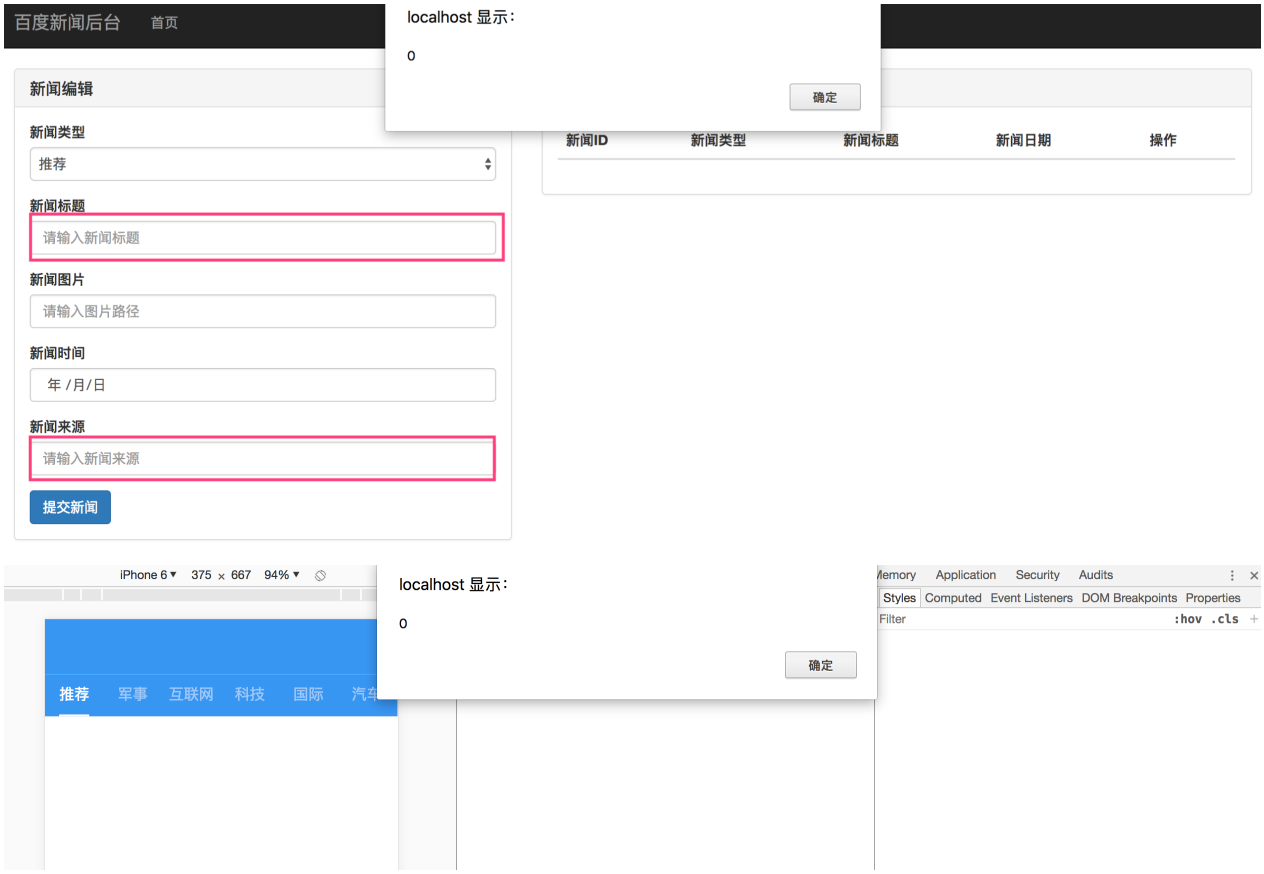
2017年7月2日 星期日

任务十四

XSS漏洞及修补

在后台页面的新闻标题和新闻来源的输入处有XSS漏洞。

输入</td><script>alert(0)</script><td>，会触发XSS。



使用PHP里的htmlspecialchars()函数，将/server/getnews.php里的'newstitle'=>$row['newsTitle']改为'newstitle'=>htmlspecialchars($row['newsTitle'])

```php
// 输出数据
$senddata=array();
while($row = mysqli_fetch_assoc($result)) {
    array_push($senddata,array(
    'newsid'=>$row['newsId'],
    'newstype'=>$row['newsType'],
    'newstitle'=>$row['newsTitle'],
    'newsimg'=>$row['newsImg'],
    'newstime'=>$row['newsTime'],
    'newssrc'=>$row['newsSrc']
    ));
}
```

```php
// 输出数据
$senddata=array();
while($row = mysqli_fetch_assoc($result)) {
    array_push($senddata,array(
    'newsid'=>$row['newsId'],
    'newstype'=>$row['newsType'],
    'newstitle'=>htmlspecialchars($row['newsTitle']),
    'newsimg'=>$row['newsImg'],
    'newstime'=>$row['newsTime'],
    'newssrc'=>htmlspecialchars($row['newsSrc'])
    ));
}
```

新闻列表

新闻ID	新闻类型	新闻标题	新闻日期	操作
20	推荐	</td><script>alert(0)</script><td>	2017-07-01	编辑 删除
16	科技	node express test	2016-06-11	编辑 删除
15	互联网	node express4	2017-06-09	编辑 删除
6	推荐	测试2	2017-06-04	编辑 删除
1	推荐	测试数据库第一条数据	2017-06-03	编辑 删除

如图，htmlspecialchars() 函数把预定义的字符转换为 HTML 实体。

预定义的字符是：

& （和号）成为 &

" （双引号）成为 "

' （单引号）成为 '

< （小于）成为 <

> （大于）成为 >

CSRF漏洞

因为该页面没有用到cookie也没有 get 和 post 请求。所以没做CSRF的修补。