

Forum:[Hack Forums](#)

Thread: [\[PHP\] The Alchemist's Admin Page Finder](#)

The Alchemist16 - November 8, 2012, 12:51 am

The Alchemist's Admin Page Finder

Hello Hackforums.

So, I finally finished my latest project. Very often, we get the administrator username and password of various websites but we do not find the admin page of the website. Well this is what you'll need then.

An admin page finder made in PHP.

Here's the code :

PHP Code

```
<?php
<html>
<head>
<meta http-equiv="author" content="The Alchemist"/>
<title>
Admin Page Finder
</title>
</head>
<body background=
"http://fc00.deviantart.net/fs70/i/2011/324/9/2/black___purple_textures_by_paralyzinglove-d4gscvx.j
pg">
<p align=center>
</p>
<p align="center"><font color="c0c0c0" size="5">Admin Page Finder</font></p>
<form method="POST" action="<?php $PHP_SELF; ?>">
<p align="center"><font color="c0c0c0">Enter website : </font>
<input type="text" name="url" value="http://" />
<br>
<input type="submit" name="submit" value="Check" />
</p>
<br>
<br>
<?php
//This code was created by The Alchemist
function urlExist($url)
{
    $handle = curl_init($url);
    if (false === $handle)
    {
        return false;
    }
    curl_setopt($handle, CURLOPT_HEADER, false);
```

```

        curl_setopt($handle, CURLOPT_FAILONERROR, true);
        curl_setopt($handle, CURLOPT_HTTPHEADER, Array(
"User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.15) Gecko/20080623 Firefo
x/2.0.0.15") ); // request as if Firefox
        curl_setopt($handle, CURLOPT_NOBODY, true);
        curl_setopt($handle, CURLOPT_RETURNTRANSFER, false);
        $connectable = curl_exec($handle);
        curl_close($handle);
        return $connectable;
}

if(isset($_POST['submit']) && isset($_POST['url']))
{
    $url= htmlentities($_POST['url']);
    if(filter_var($url, FILTER_VALIDATE_URL))
    {
        $trying = array('admin/', 'administrator/', 'admin1/', 'admin2/', 'admin3/', 'admin4/', 'admin5/',
'usuarios/',
        'usuario/', 'administrator/', 'moderator/', 'webadmin/', 'adminarea/', 'bb-admin/', 'adminLogin/',
'admin_area/',
        'panel-administracion/', 'instadmin/', 'memberadmin/', 'administratorlogin/', 'adm/',
'admin/account.php',
        'admin/index.php', 'admin/login.php', 'admin/admin.php', 'admin/account.php',
'admin_area/admin.php',
        'admin_area/login.php', 'siteadmin/login.php', 'siteadmin/index.php', 'siteadmin/login.html',
'admin/account.html',
        'admin/index.html', 'admin/login.html', 'admin/admin.html', 'admin_area/index.php',
'bb-admin/index.php', 'bb-admin/login.php',
        'bb-admin/admin.php', 'admin/home.php', 'admin_area/login.html', 'admin_area/index.html',
'admin/controlpanel.php', 'admin.php',
        'admincp/index.asp', 'admincp/login.asp', 'admincp/index.html', 'admin/account.html',
'adminpanel.html', 'webadmin.html',
        'webadmin/index.html', 'webadmin/admin.html', 'webadmin/login.html',
'admin/admin_login.html', 'admin_login.html',
        'panel-administracion/login.html', 'admin/cp.php', 'cp.php', 'administrator/index.php',
'administrator/login.php',
        'nsw/admin/login.php', 'webadmin/login.php', 'admin/admin_login.php', 'admin_login.php',
'administrator/account.php',
        'administrator.php', 'admin_area/admin.html', 'pages/admin/admin-login.php',
'admin/admin-login.php', 'admin-login.php',
        'bb-admin/index.html', 'bb-admin/login.html', 'acceso.php', 'bb-admin/admin.html',
'admin/home.html',
        'login.php', 'modelsearch/login.php', 'moderator.php', 'moderator/login.php',
'moderator/admin.php', 'account.php',
        'pages/admin/admin-login.html', 'admin/admin-login.html', 'admin-login.html', 'controlpanel.php',
'admincontrol.php',
        'admin/adminLogin.html', 'adminLogin.html', 'admin/adminLogin.html', 'home.html',
'rcjakar/admin/login.php',
        'adminarea/index.html', 'adminarea/admin.html', 'webadmin.php', 'webadmin/index.php',
'webadmin/admin.php',
        'admin/controlpanel.html', 'admin.html', 'admin/cp.html', 'cp.html', 'adminpanel.php',
'moderator.html',
        'administrator/index.html', 'administrator/login.html', 'user.html', 'administrator/account.html',
'administrator.html',

```

```

        'login.html','modelsearch/login.html','moderator/login.html','adminarea/login.html',
'panel-administracion/index.html',
        'panel-administracion/admin.html','modelsearch/index.html','modelsearch/admin.html',
'admincontrol/login.html',
        'adm/index.html','adm.html','moderator/admin.html','user.php','account.html',
'controlpanel.html','admincontrol.html',
        'panel-administracion/login.php','wp-login.php','adminLogin.php','admin/adminLogin.php',
'home.php','admin.php',
        'adminarea/index.php','adminarea/admin.php','adminarea/login.php',
'panel-administracion/index.php',
        'panel-administracion/admin.php','modelsearch/index.php','modelsearch/admin.php',
'admincontrol/login.php',
        'adm/admloginuser.php','admloginuser.php','admin2.php','admin2/login.php',
'admin2/index.php','usuarios/login.php',
        'adm/index.php','adm.php','affiliate.php','adm_auth.php','memberadmin.php',
'administratorlogin.php','admin.asp','admin/admin.asp',
        'admin_area/admin.asp','admin_area/login.asp','admin_area/index.asp','bb-admin/index.asp',
'bb-admin/login.asp',
        'bb-admin/admin.asp','pages/admin/admin-login.asp','admin/admin-login.asp',
'admin-login.asp','user.asp','webadmin/index.asp',
        'webadmin/admin.asp','webadmin/login.asp','admin/admin_login.asp','admin_login.asp',
'panel-administracion/login.asp',
        'adminLogin.asp','admin/adminLogin.asp','home.asp','adminarea/index.asp',
'adminarea/admin.asp','adminarea/login.asp',
        'panel-administracion/index.asp','panel-administracion/admin.asp','modelsearch/index.asp',
'modelsearch/admin.asp',
        'admincontrol/login.asp','adm/admloginuser.asp','admloginuser.asp','admin2/login.asp',
'admin2/index.asp','adm/index.asp',
        'adm.asp','affiliate.asp','adm_auth.asp','memberadmin.asp','administratorlogin.asp',
'siteadmin/login.asp','siteadmin/index.asp');
    foreach($trying as $sec)
    {
        $url=$url.'/'.$sec;
        if(urlExist($url))
        {
            echo '<p align="center"><font color="00FF00">'.$url.
' exists.<br>MATCH FOUND!!!</font></p>';
            exit;
        }
        else
        {
            echo '<p align="center"><font color="FFFF00">'.$url.' does not exist.</font></p>';
        }
    }
    echo
'<p align="center"><font color="c0c0c0" size="5">Could not find admin page.</font></p>';
}
else
{
    echo '<p align="center"><font color="c0c0c0" size="5">Invalid URL entered.</font></p>';
}
}
?>

```

</body>
</html>

Copy the code and save it in a file with .php extension and upload it to your free webhosting account. Then, surf the file. Enter the website url whose admin page you would like to search for. Press Check.

I hope you find this code to be useful.

Thats it...
Enjoy?

PLEASE GIVE FEEDBACK!!!

PigBacon - November 8, 2012, 3:35 am

To me it looks like you used [this guy's](#) Python code, and just copied it over to your PHP. Thoughts?

The Alchemist16 - November 8, 2012, 6:18 am

(Nov 8, 2012 04:35 AM)PigBacon Wrote: [\[CITE\]](#) To me it looks like you used [this guy's](#) Python code, and just copied it over to your PHP.

Thoughts?No, you're wrong... I didn't copy paste anything...?

First of all I dont know python and I never even look at the python section...?

Secondly, people who leech here are sure to get caught.... Cause its such a big forum...?

Thirdly, if you still think that my code is copied, you may manually compare my code with the python code...?

Please don't make wrong allegations...?

badbrains - November 8, 2012, 12:07 pm

(Nov 8, 2012 04:35 AM)PigBacon Wrote: [\[CITE\]](#) To me it looks like you used [this guy's](#) Python code, and just copied it over to your PHP.

Thoughts?

OP is right. The array is in a completely different order dude.

BTW OP, use a multi curl handler. it will be much faster.

DashPHP - November 8, 2012, 12:51 pm

This is very nice. It works brilliantly. Good work mate :)

PigBacon - November 8, 2012, 1:44 pm

(Nov 8, 2012 01:07 PM)PeopleUnderTheStairs Wrote: [\[CITE\]](#) OP is right. The array is in a completely different order dude.

BTW OP, use a multi curl handler. it will be much faster.

I could steal code from you, reorder some stuff and claim it was my own if I wanted to.

I'm just saying, I looked, and jesus christ, he has everything from that one, even the more obscure ones which no-one would ever think of.

That's all I'm saying. ?

badbrains - November 8, 2012, 3:29 pm

Dude, aside from the xboxhuge array, there's little to no similarity.

His array has 167 keys less

Quote:[0/357] admin/

[1/357] administrator/
[2/357] admin1/
[3/357] administrator/
[4/357] moderator/
[5/357] webadmin/
[6/357] adminarea/
[7/357] bb-admin/
[8/357] adminLogin/
[9/357] admin_area/
[10/357] panel-administracion/
[11/357] instadmin/
[12/357] memberadmin/
[13/357] administratorlogin/
[14/357] adm/
[15/357] admin/account.php
[16/357] admin/index.php
[17/357] admin/login.php
[18/357] admin/admin.php
[19/357] admin/account.php
[20/357] admin_area/admin.php
[21/357] admin_area/login.php
[22/357] siteadmin/login.php
[23/357] siteadmin/index.php
[24/357] siteadmin/login.html
[25/357] admin/account.html
[26/357] admin/index.html
[27/357] admin/login.html
[28/357] admin/admin.html
[29/357] admin_area/index.php
[30/357] bb-admin/index.php
[31/357] bb-admin/login.php
[32/357] bb-admin/admin.php
[33/357] admin/home.php
[34/357] admin_area/login.html
[35/357] admin_area/index.html
[36/357] admin/controlpanel.php
[37/357] admin.php
[38/357] admincp/index.asp
[39/357] admincp/login.asp
[40/357] admincp/index.html
[41/357] admin/account.html
[42/357] adminpanel.html
[43/357] webadmin.html
[44/357] webadmin/index.html
[45/357] webadmin/admin.html
[46/357] webadmin/login.html
[47/357] admin/admin_login.html
[48/357] admin_login.html
[49/357] panel-administracion/login.html
[50/357] admin/cp.php
[51/357] cp.php
[52/357] administrator/index.php
[53/357] administrator/login.php

[54/357] nsw/admin/login.php
[55/357] webadmin/login.php
[56/357] admin/admin_login.php
[57/357] admin_login.php
[58/357] administrator/account.php
[59/357] administrator.php
[60/357] admin_area/admin.html
[61/357] pages/admin/admin-login.php
[62/357] admin/admin-login.php
[63/357] admin-login.php
[64/357] bb-admin/index.html
[65/357] bb-admin/login.html
[66/357] bb-admin/admin.html
[67/357] admin/home.html
[68/357] login.php
[69/357] modelsearch/login.php
[70/357] moderator.php
[71/357] moderator/login.php
[72/357] moderator/admin.php
[73/357] account.php
[74/357] pages/admin/admin-login.html
[75/357] admin/admin-login.html
[76/357] admin-login.html
[77/357] controlpanel.php
[78/357] admincontrol.php
[79/357] admin/adminLogin.html
[80/357] adminLogin.html
[81/357] admin/adminLogin.html
[82/357] home.html
[83/357] rcjakar/admin/login.php
[84/357] adminarea/index.html
[85/357] adminarea/admin.html
[86/357] webadmin.php
[87/357] webadmin/index.php
[88/357] webadmin/admin.php
[89/357] admin/controlpanel.html
[90/357] admin.html
[91/357] admin/cp.html
[92/357] cp.html
[93/357] adminpanel.php
[94/357] moderator.html
[95/357] administrator/index.html
[96/357] administrator/login.html
[97/357] user.html
[98/357] administrator/account.html
[99/357] administrator.html
[100/357] login.html
[101/357] modelsearch/login.html
[102/357] moderator/login.html
[103/357] adminarea/login.html
[104/357] panel-administracion/index.html
[105/357] panel-administracion/admin.html
[106/357] modelsearch/index.html

[107/357] modelsearch/admin.html
[108/357] admincontrol/login.html
[109/357] adm/index.html
[110/357] adm.html
[111/357] moderator/admin.html
[112/357] user.php
[113/357] account.html
[114/357] controlpanel.html
[115/357] admincontrol.html
[116/357] panel-administracion/login.php
[117/357] wp-login.php
[118/357] adminLogin.php
[119/357] admin/adminLogin.php
[120/357] home.php
[121/357] admin.php
[122/357] adminarea/index.php
[123/357] adminarea/admin.php
[124/357] adminarea/login.php
[125/357] panel-administracion/index.php
[126/357] panel-administracion/admin.php
[127/357] modelsearch/index.php
[128/357] modelsearch/admin.php
[129/357] admincontrol/login.php
[130/357] adm/admloginuser.php
[131/357] admloginuser.php
[132/357] admin2.php
[133/357] admin2/login.php
[134/357] admin2/index.php
[135/357] adm/index.php
[136/357] adm.php
[137/357] affiliate.php
[138/357] adm_auth.php
[139/357] memberadmin.php
[140/357] administratorlogin.php
[141/357] admin.asp
[142/357] admin/admin.asp
[143/357] admin_area/admin.asp
[144/357] admin_area/login.asp
[145/357] admin_area/index.asp
[146/357] bb-admin/index.asp
[147/357] bb-admin/login.asp
[148/357] bb-admin/admin.asp
[149/357] pages/admin/admin-login.asp
[150/357] admin/admin-login.asp
[151/357] admin-login.asp
[152/357] user.asp
[153/357] webadmin/index.asp
[154/357] webadmin/admin.asp
[155/357] webadmin/login.asp
[156/357] admin/admin_login.asp
[157/357] admin_login.asp
[158/357] panel-administracion/login.asp
[159/357] adminLogin.asp

[160/357] admin/adminLogin.asp
[161/357] home.asp
[162/357] adminarea/index.asp
[163/357] adminarea/admin.asp
[164/357] adminarea/login.asp
[165/357] panel-administracion/index.asp
[166/357] panel-administracion/admin.asp
[167/357] modelsearch/index.asp
[168/357] modelsearch/admin.asp
[169/357] admincontrol/login.asp
[170/357] adm/admloginuser.asp
[171/357] admloginuser.asp
[172/357] admin2/login.asp
[173/357] admin2/index.asp
[174/357] adm/index.asp
[175/357] adm.asp
[176/357] affiliate.asp
[177/357] adm_auth.asp
[178/357] memberadmin.asp
[179/357] administratorlogin.asp
[180/357] siteadmin/login.asp
[181/357] siteadmin/index.asp

The Alchemist16 - November 8, 2012, 7:25 pm

(Nov 8, 2012 01:07 PM)PeopleUnderTheStairs Wrote: [\[CITE\]](#) OP is right. The array is in a completely different order dude.

BTW OP, use a multi curl handler. it will be much faster.Thanks for the appreciation mate...

(Nov 8, 2012 01:51 PM)Dharmesh Wrote: [\[CITE\]](#) This is very nice. It works brilliantly. Good work mate :)Thanks for the appreciation...

(Nov 8, 2012 02:44 PM)PigBacon Wrote: [\[CITE\]](#) I could steal code from you, reorder some stuff and claim it was my own if I wanted to.

I'm just saying, I looked, and jesus christ, he has everything from that one, even the more obscure ones which no-one would ever think of.

That's all I'm saying. ?Finally some appreciation... Thanks mate...

(Nov 8, 2012 04:29 PM)PeopleUnderTheStairs Wrote: [\[CITE\]](#) Dude, aside from the xboxhuge array, there's little to no similarity.

His array has 167 keys less

Well... Regarding the keys, I think I should have put them in another txt file and use file handler to check for pages... In this way, my code would have looked better and it would have been easier to add keys whenever possible...

Thanks for the feedback guys...

Hycca - November 9, 2012, 12:09 am

Vulnerable to XSS/HTML code injection, no multi handle.

FroFro - November 9, 2012, 2:21 am

Spoiler ([Click to View](#))

As Exodius said, it's vulnerable. You need to fix it ?

The Alchemist16 - November 9, 2012, 2:41 am

(Nov 9, 2012 01:09 AM)?Exodius Wrote: [\[CITE\]](#) Vulnerable to XSS/HTML code injection, no multi handle.Thanks for the notice mate...

(Nov 9, 2012 03:21 AM)-Matt_ Wrote: [\[CITE\]](#) Spoiler [\(Click to View\)](#)

As Exodius said, it's vulnerable. You need to fix it ?

Thanks for the notice mate... I'm gonna fix it...

FroFro - November 9, 2012, 2:41 am

(Nov 9, 2012 03:41 AM)The Alchemist16 Wrote: [\[CITE\]](#) Thanks for the notice mate...

Thanks for the notice mate... I'm gonna fix it...

Sent you a PM about it ?

Hope you get it fixed ?

The Alchemist16 - November 9, 2012, 3:04 am

Exodius and Matt... Thanks a lot for notifying me... I've added XSS filter...

This is the code now :

Spoiler [\(Click to View\)](#)PHP Code

```
<?php
<html>
<head>
<meta http-equiv="author" content="The Alchemist"/>
<title>
Admin Page Finder
</title>
</head>
<body background=
"http://fc00.deviantart.net/fs70/i/2011/324/9/2/black___purple_textures_by_paralyzinglove-d4gscvx.jp
g">
<p align=center>
</p>
<p align="center"><font color="c0c0c0" size="5">Admin Page Finder</font></p>
<form method="POST" action="">
<p align="center"><font color="c0c0c0">Enter website : </font>
<input type="text" name="url" value="http://" />
<br>
<input type="submit" name="submit" value="Check"/>
</p>
<br>
<br>
<?php
//This code was created by The Alchemist
function xss_protect($data, $strip_tags = false, $allowed_tags = "") {
    if($strip_tags) {
        $data = strip_tags($data, $allowed_tags . "<b>");
    }
}
```

```

    if(strpos($data, "script") !== false) {
$result = str_replace("script","scr<b></b>ipt", htmlentities($data, ENT_QUOTES));
    } else {
$result = htmlentities($data, ENT_QUOTES);
    }

    return $result;
}
function urlExist($url)
{
    $handle = curl_init($url);
    if (false === $handle)
    {
        return false;
    }
    curl_setopt($handle, CURLOPT_HEADER, false);
    curl_setopt($handle, CURLOPT_FAILONERROR, true);
    curl_setopt($handle, CURLOPT_HTTPHEADER, Array(
"User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.15) Gecko/20080623 Firefo
x/2.0.0.15" )); // request as if Firefox
    curl_setopt($handle, CURLOPT_NOBODY, true);
    curl_setopt($handle, CURLOPT_RETURNTRANSFER, false);
    $connectable = curl_exec($handle);
    curl_close($handle);
    return $connectable;
}

if(isset($_POST['submit']) && isset($_POST['url']))
{
    $url= htmlentities(xss_protect($_POST['url']));
    if(filter_var($url, FILTER_VALIDATE_URL))
    {
        $trying = array('admin/', 'administrator/', 'admin1/', 'admin2/', 'admin3/', 'admin4/', 'admin5/', 'usuarios/',
        'usuario/', 'administrator/', 'moderator/', 'webadmin/', 'adminarea/', 'bb-admin/', 'adminLogin/',
'admin_area/',
        'panel-administracion/', 'instadmin/', 'memberadmin/', 'administratorlogin/', 'adm/', 'admin/account.php',
        'admin/index.php', 'admin/login.php', 'admin/admin.php', 'admin/account.php',
'admin_area/admin.php',
        'admin_area/login.php', 'siteadmin/login.php', 'siteadmin/index.php', 'siteadmin/login.html',
'admin/account.html',
        'admin/index.html', 'admin/login.html', 'admin/admin.html', 'admin_area/index.php',
'bb-admin/index.php', 'bb-admin/login.php',
        'bb-admin/admin.php', 'admin/home.php', 'admin_area/login.html', 'admin_area/index.html',
'admin/controlpanel.php', 'admin.php',
        'admincp/index.asp', 'admincp/login.asp', 'admincp/index.html', 'admin/account.html',
'adminpanel.html', 'webadmin.html',
        'webadmin/index.html', 'webadmin/admin.html', 'webadmin/login.html', 'admin/admin_login.html',
'admin_login.html',
        'panel-administracion/login.html', 'admin/cp.php', 'cp.php', 'administrator/index.php',
'administrator/login.php',
        'nsw/admin/login.php', 'webadmin/login.php', 'admin/admin_login.php', 'admin_login.php',
'administrator/account.php',
        'administrator.php', 'admin_area/admin.html', 'pages/admin/admin-login.php',

```

```

'admin/admin-login.php','admin-login.php',
'bb-admin/index.html','bb-admin/login.html','acceso.php','bb-admin/admin.html','admin/home.html',
'login.php','modelsearch/login.php','moderator.php','moderator/login.php','moderator/admin.php',
'account.php',
'pages/admin/admin-login.html','admin/admin-login.html','admin-login.html','controlpanel.php',
'admincontrol.php',
'admin/adminLogin.html','adminLogin.html','admin/adminLogin.html','home.html',
'rcjekar/admin/login.php',
'adminarea/index.html','adminarea/admin.html','webadmin.php','webadmin/index.php',
'webadmin/admin.php',
'admin/controlpanel.html','admin.html','admin/cp.html','cp.html','adminpanel.php','moderator.html',
'administrator/index.html','administrator/login.html','user.html','administrator/account.html',
'administrator.html',
'login.html','modelsearch/login.html','moderator/login.html','adminarea/login.html',
'panel-administracion/index.html',
'panel-administracion/admin.html','modelsearch/index.html','modelsearch/admin.html',
'admincontrol/login.html',
'adm/index.html','adm.html','moderator/admin.html','user.php','account.html','controlpanel.html',
'admincontrol.html',
'panel-administracion/login.php','wp-login.php','adminLogin.php','admin/adminLogin.php',
'home.php','admin.php',
'adminarea/index.php','adminarea/admin.php','adminarea/login.php',
'panel-administracion/index.php',
'panel-administracion/admin.php','modelsearch/index.php','modelsearch/admin.php',
'admincontrol/login.php',
'adm/admloginuser.php','admloginuser.php','admin2.php','admin2/login.php','admin2/index.php',
'usuarios/login.php',
'adm/index.php','adm.php','affiliate.php','adm_auth.php','memberadmin.php',
'administratorlogin.php','admin.asp','admin/admin.asp',
'admin_area/admin.asp','admin_area/login.asp','admin_area/index.asp','bb-admin/index.asp',
'bb-admin/login.asp',
'bb-admin/admin.asp','pages/admin/admin-login.asp','admin/admin-login.asp','admin-login.asp',
'user.asp','webadmin/index.asp',
'webadmin/admin.asp','webadmin/login.asp','admin/admin_login.asp','admin_login.asp',
'panel-administracion/login.asp',
'adminLogin.asp','admin/adminLogin.asp','home.asp','adminarea/index.asp',
'adminarea/admin.asp','adminarea/login.asp',
'panel-administracion/index.asp','panel-administracion/admin.asp','modelsearch/index.asp',
'modelsearch/admin.asp',
'admincontrol/login.asp','adm/admloginuser.asp','admloginuser.asp','admin2/login.asp',
'admin2/index.asp','adm/index.asp',
'adm.asp','affiliate.asp','adm_auth.asp','memberadmin.asp','administratorlogin.asp',
'siteadmin/login.asp','siteadmin/index.asp');
foreach($trying as $sec)
{
$url=$url.'/'.$sec;
if(urlExist($url))
{
echo '<p align="center"><font color="00FF00">'.$url.' exists.<br>MATCH FOUND!!!</font></p>';
exit;
}
else
{

```

```

    echo '<p align="center"><font color="FFFF00">'. $url.'. does not exist.</font></p>';
  }
}
echo '<p align="center"><font color="c0c0c0" size="5">Could not find admin page.</font></p>';
}
else
{
    echo '<p align="center"><font color="c0c0c0" size="5">Invalid URL entered.</font></p>';
}
}
?>
</body>
</html>

```

Will be updating the main thread soon...

Hycca - November 9, 2012, 3:58 am

Well if not the fact that that part:

PHP Code

```
<?php
```

```
<form method="POST" action="<?php $PHP_SELF; ?>">
```

Is not properly coded, it would be vulnerable. What you wanted to use is `<?php echo $_SERVER['PHP_SELF'] ?>` which would be vulnerable to XSS. Never use `$PHP_SELF`.

The Alchemist16 - November 9, 2012, 7:19 am

(Nov 9, 2012 04:58 AM)?Exodius Wrote: [\[CITE\]](#) Well if not the fact that that part:

PHP Code

```
<?php
```

```
<form method="POST" action="<?php $PHP_SELF; ?>">
```

Is not properly coded, it would be vulnerable. What you wanted to use is `<?php echo $_SERVER['PHP_SELF'] ?>` which would be vulnerable to XSS. Never use `$PHP_SELF`. Didn't quite get you. You said PHP Code

```
<?php echo $_SERVER['PHP_SELF'] ?>
```

is vulnerable to XSS. Also, not to use `$PHP_SELF`.

Do you mean I should modify the code and make it :

PHP Code

```
<?php
```

```
<form method="POST" action="<?php echo $_SERVER['PHP_SELF']; ?>">
```

Am I right??

badbrains - November 9, 2012, 8:00 am

>Vulnerable

doesn't matter as it doesn't store data from other users lol.

The Alchemist16 - November 9, 2012, 9:56 am

(Nov 9, 2012 09:00 AM)PeopleUnderTheStairs Wrote: [\[CITE\]](#) >Vulnerable

doesn't matter as it doesn't store data from other users lol.

You're absolutely right...?

But its a good practise to make codes that are not vulnerable...??

Hycca - November 9, 2012, 5:55 pm

(Nov 9, 2012 08:19 AM)The Alchemist16 Wrote: [\[CITE\]](#) Didn't quite get you. You said PHP Code `<?php echo $_SERVER['PHP_SELF']; ?>` is vulnerable to XSS. Also, not to use `$PHP_SELF`.

Do you mean I should modify the code and make it :

PHP Code

`<?php`

`<form method="POST" action="<?php echo $_SERVER['PHP_SELF']; ?>">`

Am I right??

PHP Code

`<?php $PHP_SELF; ?>`"

Well first of all there's no such thing as `$PHP_SELF` nowadays, it does nothing. It will be treated as a variable that was never set which will result in it being blank. Actually, it would be blank either way because you didn't use 'echo' before it. What you WANTED to use was PHP Code

`<?php echo $_SERVER['PHP_SELF']; ?>` which as I said is vulnerable to XSS because it reflects the whole URL on the page without filtering it.

If you would use `$_SERVER['PHP_SELF']` someone could enter let's say

<http://127.0.0.1/admin.php/>"><script>alert('XSS')</script>.

So no, you shouldn't use either one of them because 1st one does nothing and 2nd one is vulnerable to XSS. Leave it like PHP Code

`<?php`

`<form method="POST" action="">`

The Alchemist16 - November 9, 2012, 8:40 pm

(Nov 9, 2012 06:55 PM)?Exodius Wrote: [\[CITE\]](#) PHP Code

`<?php $PHP_SELF; ?>`"

Well first of all there's no such thing as `$PHP_SELF` nowadays, it does nothing. It will be treated as a variable that was never set which will result in it being blank. Actually, it would be blank either way because you didn't use 'echo' before it. What you WANTED to use was PHP Code

`<?php echo $_SERVER['PHP_SELF']; ?>` which as I said is vulnerable to XSS because it reflects the whole URL on the page without filtering it.

If you would use `$_SERVER['PHP_SELF']` someone could enter let's say

<http://127.0.0.1/admin.php/>"><script>alert('XSS')</script>.

So no, you shouldn't use either one of them because 1st one does nothing and 2nd one is vulnerable to XSS. Leave it like PHP Code

`<?php`

`<form method="POST" action="">`

Ok... Thanks for explaining... Making the changes...

'An0ny - December 2, 2012, 7:57 am

Is the vurn fixed? I'm going to implent it on my site.

nicksaban1 - December 2, 2012, 8:00 am

(Nov 8, 2012 04:35 AM)PigBacon Wrote: [\[CITE\]](#) To me it looks like you used [this guy's](#) Python code, and just copied it over to your PHP.

Thoughts?

The code is completely different. The only thing similar is the search array.

OP: I am impressed with your php coding. Good job!

The Alchemist16 - December 23, 2012, 6:26 am

(Dec 2, 2012 08:57 AM)ExploitZ Wrote: [\[CITE\]](#) Is the vurn fixed? I'm going to implent it on my site. Yup... The vulnerability is fixed... Look up on the second page of the thread..

(Dec 2, 2012 09:00 AM)Nick Saban Wrote: [\[CITE\]](#) The code is completely different. The only thing similar is the search array.

OP: I am impressed with your php coding. Good job!
Thanks a lot for the appreciation mate...
More to come...