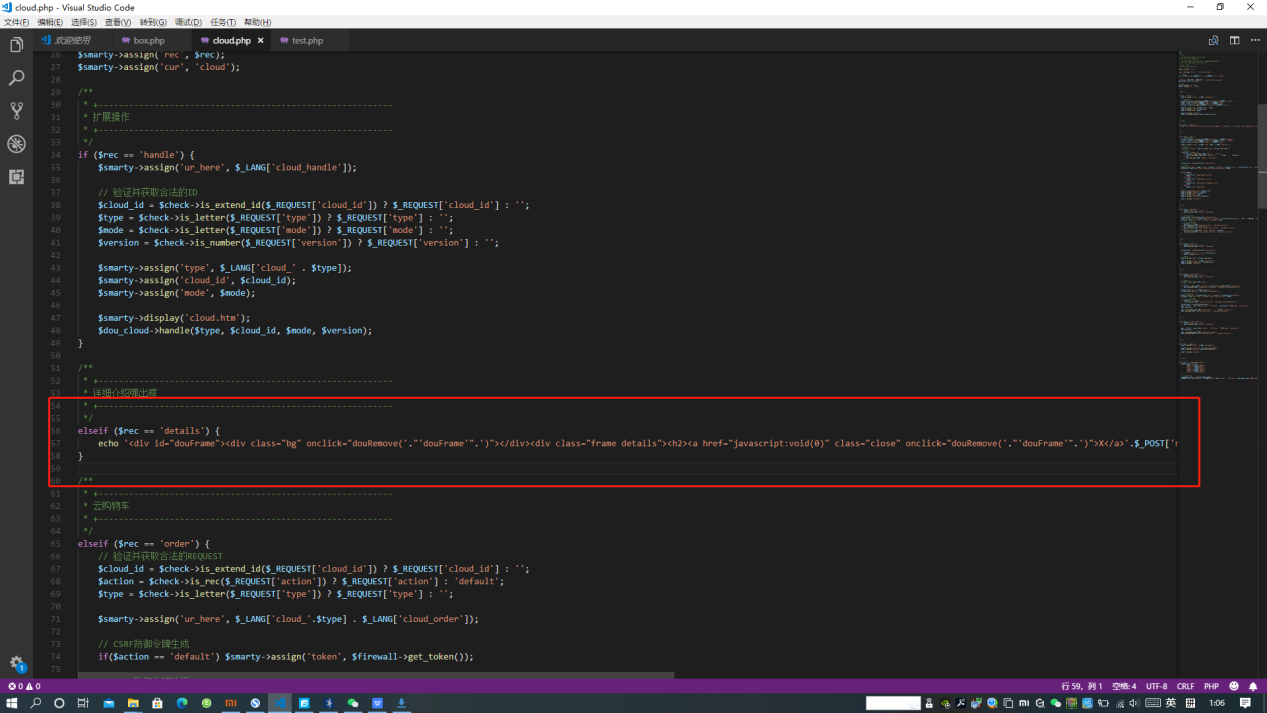
<http://61.155.169.167:81/uploads/userup2/1838/DouPHP_1.6_Release_20210120.zip>

/admin/cloud.php



echo '<div id="douFrame"><div class="bg" onclick="douRemove('."'douFrame'".')"></div><div class="frame details"><h2><a href="javascript:void(0)" class="close" onclick="douRemove('."'douFrame'".')">X</a>'.$\_POST['name'].'</h2><div class="content"><iframe frameborder="0" hspace="0" src="'.$\_POST['frame'].'" width="100%" height="600">' . $\_LANG['cloud\_frame\_cue'] . '</iframe></div></div></div>';

After copying it out, you can see that it is a php output statement echo

The focus is $\_POST['name']

This is where you can pass parameters. Look at the front and back, you can confirm that there is xss here, and you can directly enter <script>alert(1)</script>. If you are not sure, you can substitute this for testing.

The basic structure has been completed, and then just look at how to trigger this statement.

Looking up there is a judgment, the condition is：$rec == 'details'

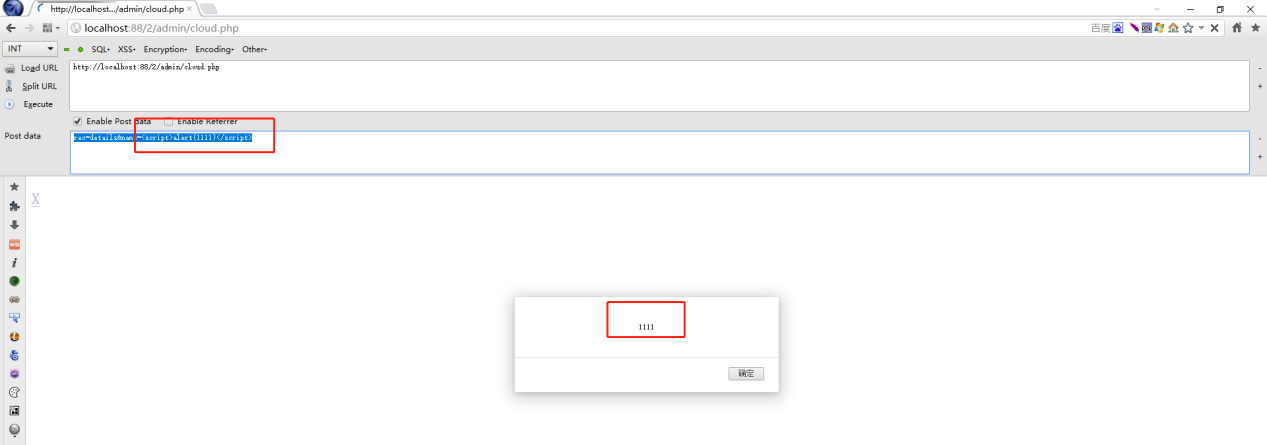
Then find out where this $rec comes from

Then look up,$rec = $check->is\_rec($\_REQUEST['rec']) ? $\_REQUEST['rec'] : 'default';

There is a statement like this on line 19, you can see that $rec comes from this way.

This is a ternary operator, for example a?b:c first judge whether a is true, if it is true, the return value is b, if a is false, then return c. Here you need to let rec be details, then enter rec=details.

So finally: post incoming data：rec=details&name=<script>alert(1111)</script>



Of course, you need to log in