ctf 中php 弱类型,CTF中PHP代码审计小tips-弱类型==与===比较

转载

他们迂回误会 于 2021-04-03 14:22:33 发布 44 收藏
文章标签： ctf 中php 弱类型
阅读次数

MiniProject_PHP_Code_audit-3 Writeup

整体逻辑：

这段代码的逻辑是用户输入username和password两个参数，如果username和password的值不相等，再判断username和password字符串的 sha1 散列值与类型是否相等，如果相等才输出flag值。

考点：

这段代码中有一个逻辑点，怎么样使的两个值不相等，但是sha1()后的值相等。===会比较类型，比如bool sha1()函数和md5()函数存在着漏洞，sha1()函数默认的传入参数类型是字符串型，那要是给它传入数组呢会出现错误，使sha1()函数返回错误，也就是返回false，这样一来===运算符就可以发挥作用了，需要构造username和password既不相等，又同样是数组类型。

=== 在进行比较的时候，会先判断两种字符串的类型是否相等，再比较。

== 在进行比较的时候，会先将字符串类型转化成相同，再比较。

PS：URL可以传递数组参数，形式是链接：xxx.com?x[]=1&x[]=2&x[]=3

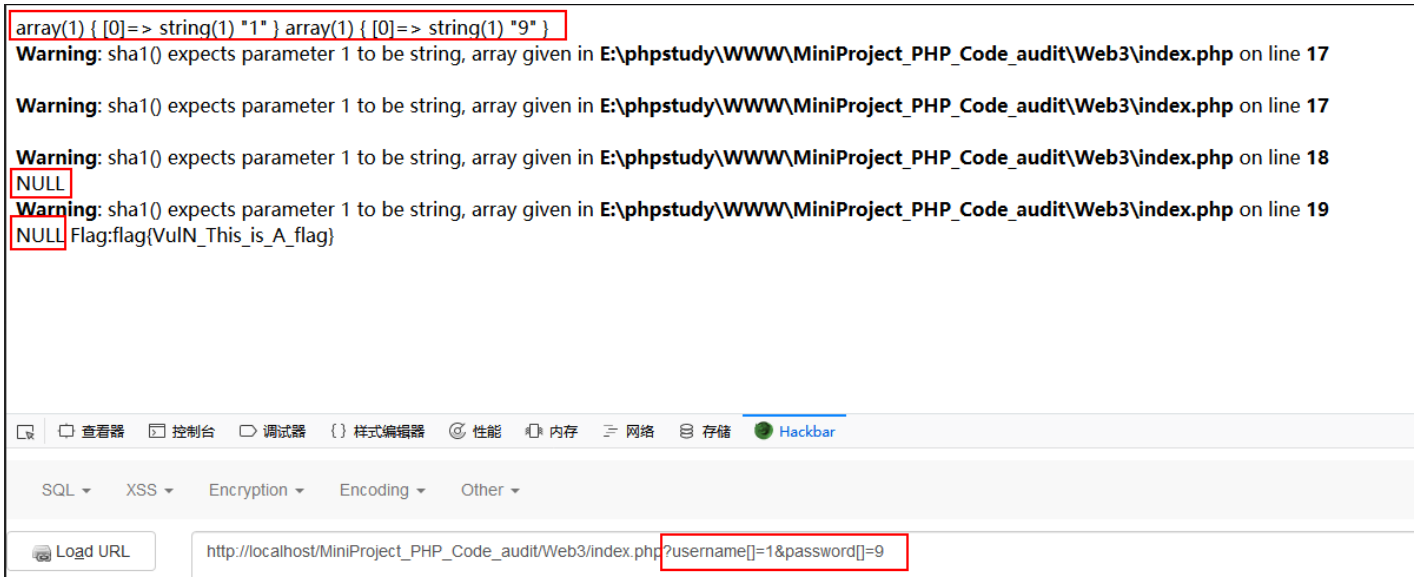
这样就提交了一个x[]={1,2,3}的数组。 如果使用sha1对一个数组进行加密，返回的将是NULL，NULL===NULL。

测试代码：

通过打印出传入的值以及类型，以及sha()后的值和类型看看如何绕过：

```php
<?php
/** Created by PhpStorm. ... */

    $flag = 'flag{VulN_This_is_A_flag}';
    var_dump($_GET['username']);
    var_dump($_GET['password']);
    if (isset($_GET['username']) and isset($_GET['password']))
    {
        if ($_GET['username'] == $_GET['password']){
            echo '<p>You password can not be your username !</p>';
        }
        else if (sha1($_GET['username']) === sha1($_GET['password'])){  //计算字符串的 sha1 散列值
            var_dump(sha1($_GET['username']));
            var_dump(sha1($_GET['password']));
            die('Flag:'.$flag);
        }
        else{
            echo '<p>Invalid password</p>';
        }
    }
    else{
        echo '<p>Login first</p>';
    }
?>
```



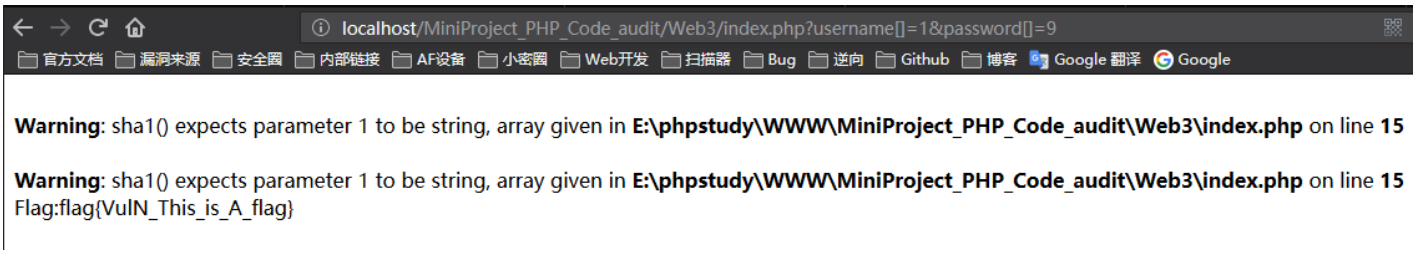
Writeup：

分析代码逻辑，发现GET了两个字段username和password，获得flag要求的条件是：username != password & sha1(username) == sha1(password)，可以利用sha1()函数的漏洞来绕过。

如果把这两个字段构造为数组，如：?name[]=a&password[]=q，这样在第一处判断时两数组确实是不同的，但在PHP中，sha1 是不能处理数组的，sha1(数组)会返回null，所以sha1 (a[])==null,sha1 (b[])==null，sha1 (a[])=sha1 (b[])=null,这样就可以了。

在第二处判断时由于sha1()函数无法处理数组类型，将报错并返回false，if 条件成立，获得flag。经验证md5()函数同样存在此漏洞。

index.php?username[]=1&password[]=9


localhost/MiniProject_PHP_Code_audit/Web3/index.php?username[]=1&password[]=9
官方文档 漏洞来源 安全圈 内部链接 AF设备 小密圈 Web开发 扫描器 Bug 逆向 Github 博客 Google 翻译 Google
Warning: sha1() expects parameter 1 to be string, array given in E:\phpstudy\WWW\MiniProject_PHP_Code_audit\Web3\index.php on line 15
Warning: sha1() expects parameter 1 to be string, array given in E:\phpstudy\WWW\MiniProject_PHP_Code_audit\Web3\index.php on line 15
Flag:flag{VulN_This_is_A_flag}

参考链接：