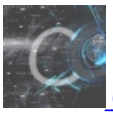
SDUTSec - WEB——Writeup

原创

@北陌 于 2019-01-25 10:43:34 发布 316 收藏 1

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_43921596/article/details/86636795



1.easy MD5-1

首先右键查看源代码

```
think carefully
<!--
**
if($_POST['param1']!==$_POST['param2'] && md5($_POST['param1'])===md5($_POST['param2'])){
    die("seclab507{*******}");
}
else{
    echo "think carefully";
}


-->
```


代码的意思为

param1和param2的值不同但他们的MD5值相同

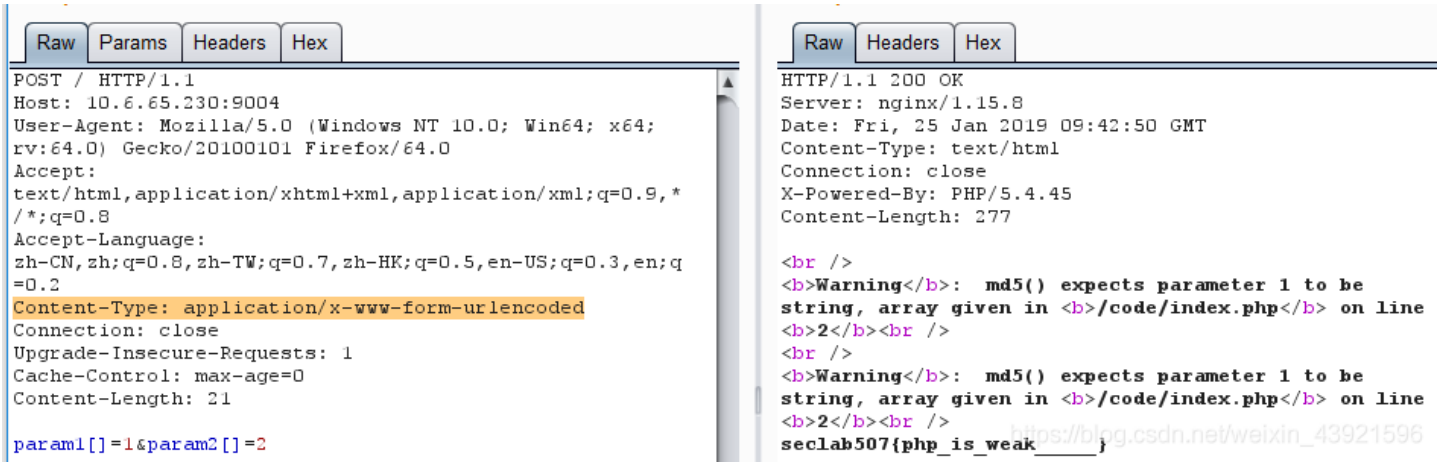
===强类型，md5的值不进行类型转换，当作字符串处理．需要用数组进行绕过：

```
param1[]=1&param2[]=2
```

POST请求进行抓包改包，用BurpSuite，但是需要加上一行字符串

```
Content-Type: application/x-www-form-urlencoded
```

不知道为什么要加，网上说这是最常见的 POST 提交数据的方式，记住就ok



2.MD5 collision

```
no
<!--
if((string)$_POST['p1']!==(string)$_POST['p2'] && md5($_POST['p1'])===md5($_POST['p2'])){
    die("seclab507{******}");
}
else{
    echo "no";
}
-->
```

代码的意思为
强制类型转换p1和p2为`string`，且转换后p1和p2的值不同但是MD5值相同
这里就需要php中MD5碰撞的漏洞

```
p1=%4d%c9%68%ff%0e%e3%5c%20%95%72%d4%77%7b%72%15%87%d3%6f%a7%b2%1b%dc%56%b7%4a%3d%c0%78%3e%7b%95%18%af%bf%a2%00%a8%28%4b%f3%6e%8e%4b%55%b3%5f%42%75%93%d8%49%67%6d%a0%d1%55%5d%83%60%fb%5f%07%fe%a2
```

中间用&连接

```
p2=%4d%c9%68%ff%0e%e3%5c%20%95%72%d4%77%7b%72%15%87%d3%6f%a7%b2%1b%dc%56%b7%4a%3d%c0%78%3e%7b%95%18%af%bf%a2%02%a8%28%4b%f3%6e%8e%4b%55%b3%5f%42%75%93%d8%49%67%6d%a0%d1%d5%5d%83%60%fb%5f%07%fe%a2
```

POST请求不要忘了加上

```
Content-Type: application/x-www-form-urlencoded
```

Request

Raw | Params | Headers | Hex

```
POST / HTTP/1.1
Host: 10.6.65.230:9005
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:64.0) Gecko/20100101 Firefox/64.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*
/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q
=0.2
Content-Type: application/x-www-form-urlencoded
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 391

p1=%4d%c9%68%ff%0e%e3%5c%20%95%72%d4%77%7b%72%15%87%d3%6
f%a7%b2%1b%dc%56%b7%4a%3d%c0%78%3e%7b%95%18%af%bf%a2%00
%a8%28%4b%f3%6e%8e%4b%55%b3%5f%42%75%93%d8%49%67%6d%a0%
d1%55%5d%83%60%fb%5f%07%fe%a2&p2=%4d%c9%68%ff%0e%e3%5c%
20%95%72%d4%77%7b%72%15%87%d3%6f%a7%b2%1b%dc%56%b7%4a%3
d%c0%78%3e%7b%95%18%af%bf%a2%02%a8%28%4b%f3%6e%8e%4b%55
%b3%5f%42%75%93%d8%49%67%6d%a0%d1%d5%5d%83%60%fb%5f%07%
fe%a2
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: nginx/1.15.8
Date: Fri, 25 Jan 2019 10:26:17 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.4.45
Content-Length: 35

seclab507{[redacted]}
```