[web] 마법봉

해쉬에 마법을 부여하면 그 어떤 것도 뚫릴지어니...

If you enchant a hash, Anything will breakthrough...

제출

View Source

?

```php
<?php
show_source(__FILE__);
$flag = "if_you_solved";
$input = $_GET['flag'];
if(md5("240610708") == sha1($input)){
    echo $flag;
}
else{
    echo "Nah...";
}
?>
```

Nah...

소스는 이러하다

input을 sha1 해쉬코드로 변환해 만약 그것이 md5(”240610708”)과 동일하면 플래그를 출력하는 듯 하다.

그럼 input값으로 md5(”240610708”)의 결과값을 sha1으로 복호화 한 값을 넣었으면 좋겠지만 아쉽게도 내 지식상으로 sha1을 복호화 할수 있는 방법은 없... 있나?

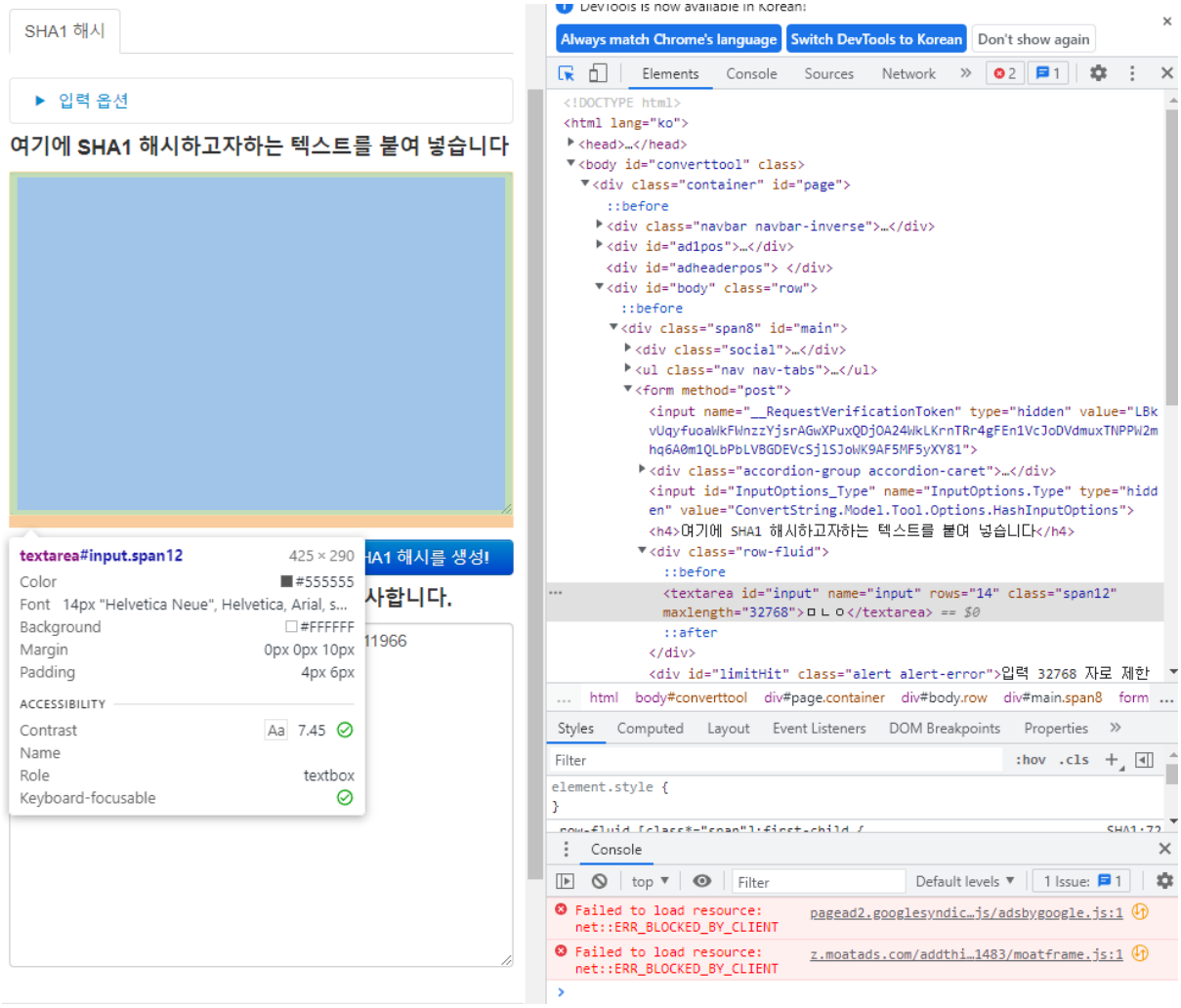
아무튼 md5(”240610708”) = 0E462097431906509019562988736854이다.

해쉬에 마법을 넣으라고 하니 아마도 php의 sha1함수에 취약점이 있겠거니 싶어 서치하던 참에 **매직해시**라는 것을 발견했다.

PHP상에서 0e로 시작하는 문자열의 뒤가 모두 숫자인 경우 해당 문자열을 float 형태(지수형태)로 인식한다!

따라서 0e123 같은 경우 0^123이 되어 결국 0이 된다는 거다.

그렇다면 sha1($input)의 결과가 0이 나오면 if문은 참이 된다.



sha1($input)값이 0e로 시작하는 암호문을 찾기 위해.. 웹크롤링을 할 생각이다

```
from selenium import webdriver
from webdriver_manager.chrome import ChromeDriverManager
from time import sleep

#path = "C:\webcrowling\chromdriver.exe"
driver = webdriver.Chrome(ChromeDriverManager().install())
driver.get("https://www.convertstring.com/ko/Hash/SHA1")
sleep(2)



element = driver.find_element_by_id("input")
btn = driver.find_element_by_xpath('//*[@id="submit"]')
out = driver.find_element_by_id("output")
i = 1

while not out.text.startswith("0E"):
    element.send_keys(i)
    btn.click()
    #창이 새로고침되면서 저장한 변수들이 날아가버림
    element = driver.find_element_by_id("input")
```

```
    btn = driver.find_element_by_xpath('//*[@id="submit"]')
    out = driver.find_element_by_id("output")
    element.clear() #입력된 내용을 지워줌
    sleep(2)
    i += 1


print(out.text)
```

어라라.. 근데 저 sleep(2)를 기다리며 생각해보니 분명 파이썬에 sha1으로 디코딩해주는 함수 라이브러리가 있을 거 같다.....

그리고 찾아보니 있었다.. 코드를 작성해서 0e로 시작하는 sha1 값을 구했다.

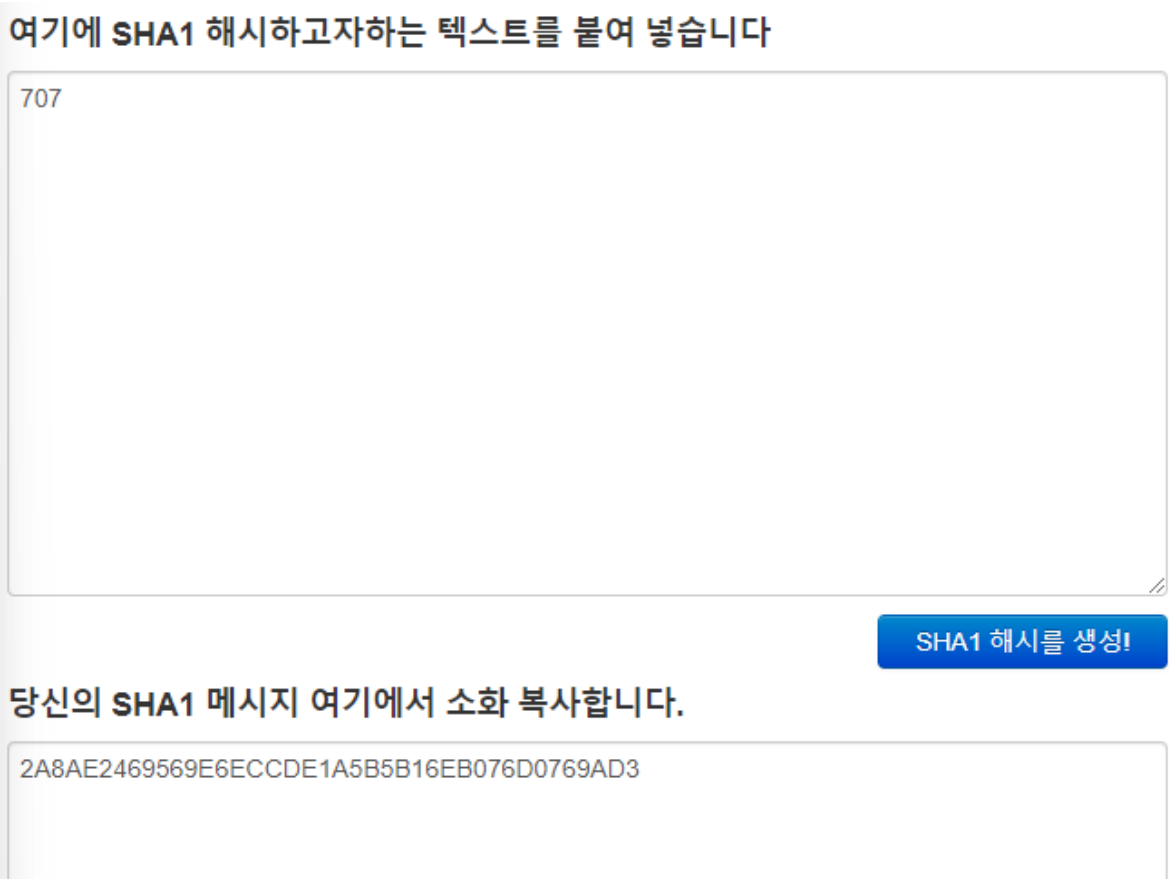
```
import hashlib
i = 45 #웹크롤링 기다리면서 45까지 해당값이 나오지 않는다는 걸 알았다..
h = hashlib.sha1()

while True:
    h.update(str(i).encode('utf8'))
    res = h.hexdigest()
    if res.startswith("0e"):
        print(res)
        print(i)
        break
    else: i+=1
```

```
*** Remote Interpreter Reinitialized ***
0e99338d28982d3f3debeb143eaa0d3b13cbd37b
707
>>>
```

결과는 707이다.

근데 안된다



보니까 사이트 값이랑 출력 결과값이 다르다;;

```
import hashlib
i = 45


while True:
    h = hashlib.sha1()
    h.update(str(i).encode('utf8'))
    res = h.hexdigest()
    if res.startswith("0e"):
        print(res)
        print(str(i).encode('utf8'))
        break
    else: i+=1
```

함수를 잘못사용해서 그런가보다..^^ update 메소드 보고 눈치챘어야 했는데 아무튼 결과로는 234가 나왔다.

근데 그래도 안된다.

맞다.. 매직해쉬에 해당되려면 0e 뒤에 나오는 문자가 모두 숫자여야 했다...

```
import hashlib
i = 234
while True:
    h = hashlib.sha1()
    h.update(str(i).encode('utf8'))
    res = h.hexdigest()
    if res.startswith("0e") and res[3:].isdigit():
        print(res)
        print(str(i).encode('utf8'))
        break
    else: i+=1
```

로 다시 코드를 돌렸다.

그런데 지금 15분이 지났는데 결과가 안나온다

결과 코드가 어지간히 긴가보다...

걍 구글링 해도 나오지 않을까?

sha1	40	10932435112	0e07766915004133176347055865026311692244

고맙게도.. 인터넷이 정보의 장이라 불리는데는 이유가 있으며...

결과가 10932435112 정도나 되니까 지금까지 출력이 안되는 것이다.

아무튼 입력으로 10932435112를 주니 키 값이 나왔다!