< 6번 워게임 풀이문서 >

김구민



다음과 같은 사이트가 주어진다. Hint, reference!, README 글을 보면 다음과 같다.

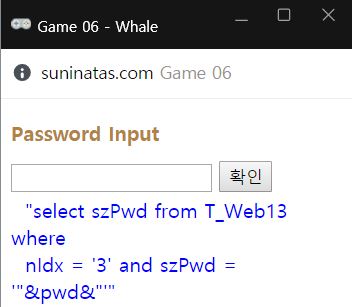
**[Hint]**



**[reference!]**



**[README]**



================================================================

나머지 Wating과 열공열공 글은 문제를 푸는데 도움이 되지 않아보인다.

Hint의 내용대로 suninatas’s Writing인 README를 확인해보면 SQL 쿼리문이 주어진다.

**select szPwd from T\_Web**

**where nIdx = '3' and szPwd = ' "&pwd&" '**

↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓

**T\_Web에서 szPwd를 고르는데**

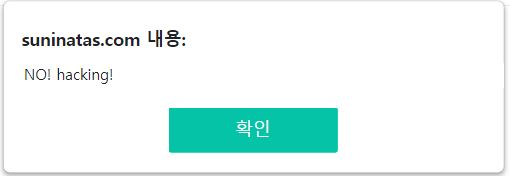
**nidx가 3이고 szPwd가 "&pwd&"인 szPwd를 찾자는 의미**

텍스트 박스 안에 들어갈 내용은 szPwd에 대한 내용, 즉 “&pwd&”에 대한 내용이다.

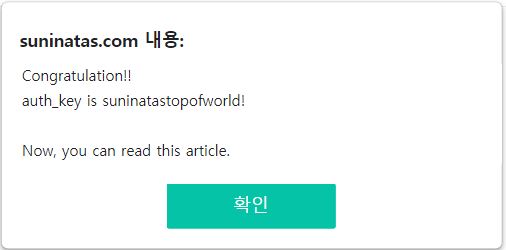
여기서 ‘로 따옴표가 열리기 때문에 ‘를 한 번 더 써서 닫아주고 or (true인 내용)으로 true값을 만들고 --(주석)로 뒤에 나오는 ‘를 무효화시키는 꼼수를 써보았다.

그래서 텍스트 박스 안에 ‘ or (2>1) --라는 내용을 적어보았다.

그러나 NO Hacking이라는 문구와 함께 실패했다.



그래서 괄호를 제거하고 다시 ‘ or 2>1 --의 내용을 입력해보았다.

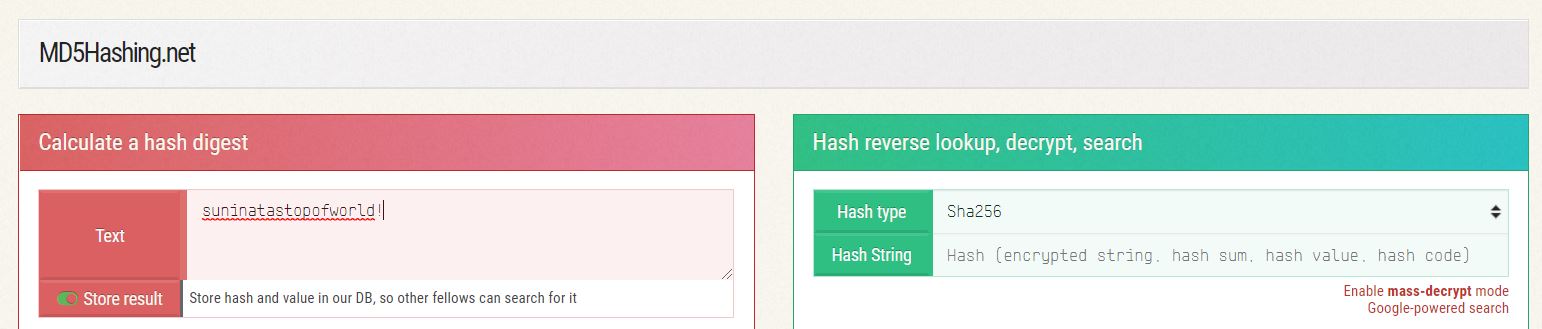


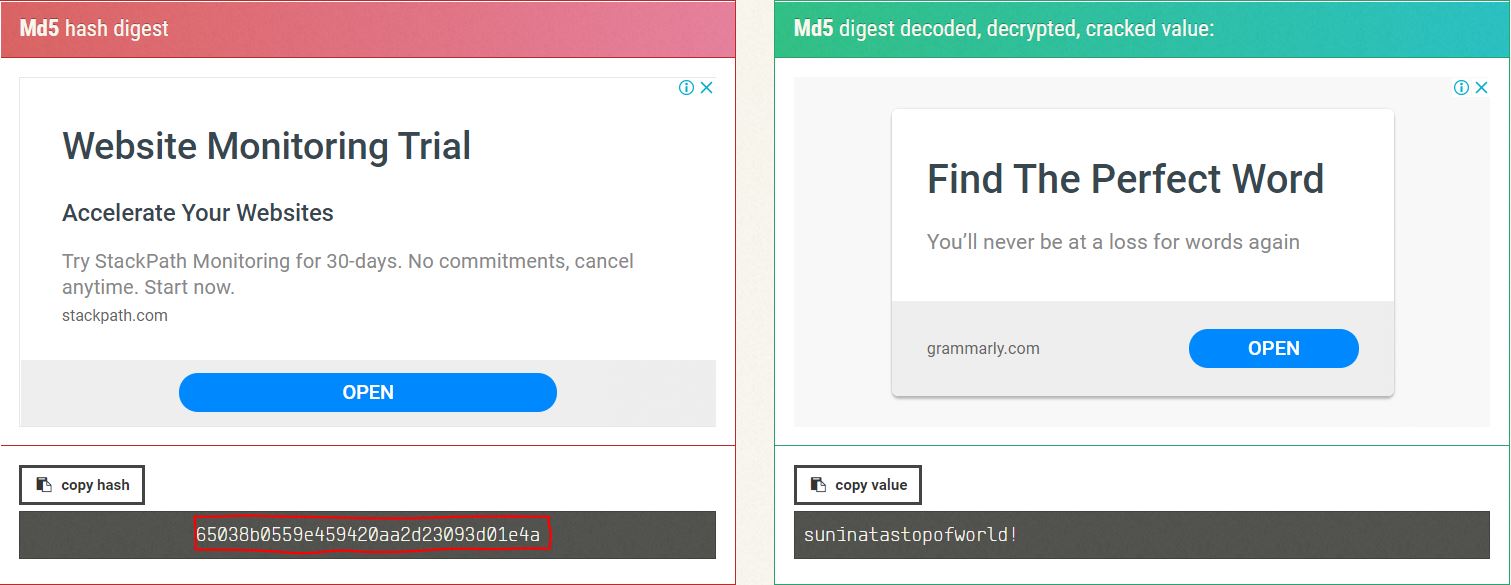
하지만 또 접근권한이 없다는 경고 창이 떴다!



그러다가 그 전 reference의 글을 보지 않았다는 사실이 떠올라서 확인해보았다.

해당 사이트를 들어가보니 해싱 사이트였다. 그래서 아까 알아냈던 auth\_key를 해싱하기로 했다.



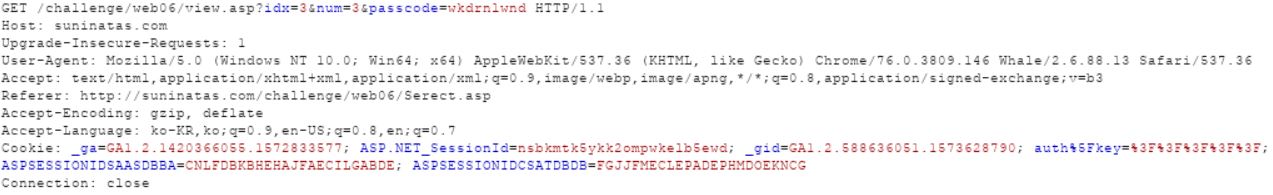


해싱된 결과값은 65038b0559e459420aa2d23093d01e4a이다.

쿼리문을 입력할 때 프록시를 이용해 Burp-Suite를 사용하면 아래와 같은 소스가 나온다.



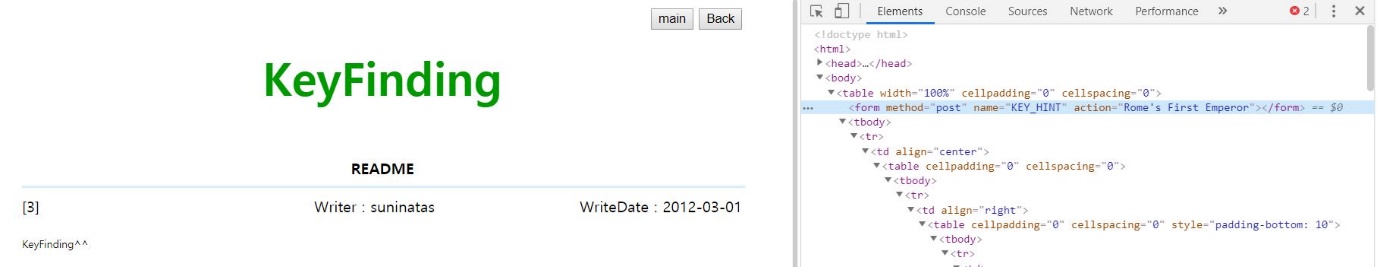
인증키(auth%5Fkey)를 65038b0559e459420aa2d23093d01e4a로 바꿔주고 Forward



또 인증키를 65038b0559e459420aa2d23093d01e4a로 바꿔주고 Forward 시키면



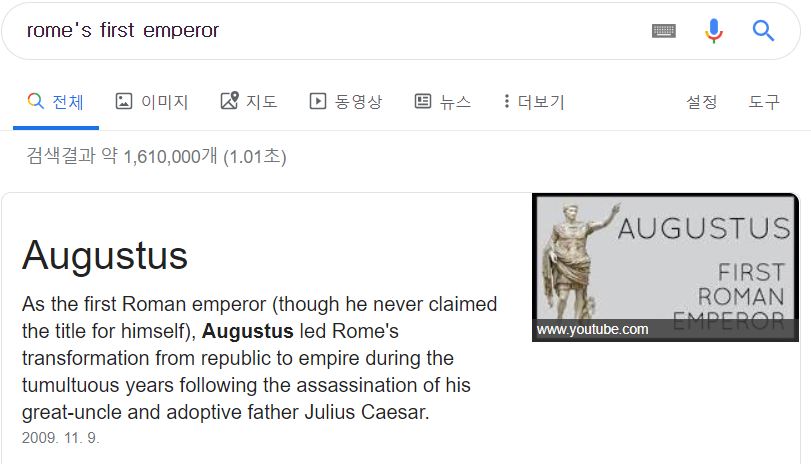
다음과 같은 KeyFinding이라는 새 창이 뜬다!! F12를 눌러서 소스를 확인해보았다.



소스를 보다보니 위의 그림과 같이

<form method="post" name="KEY\_HINT" action="Rome'sFirst Emperor"> 소스를 확인할 수 있다.

그래서 로마의 첫번째 황제가 누군지 구글링해보았다.



답은 Augustus였다.