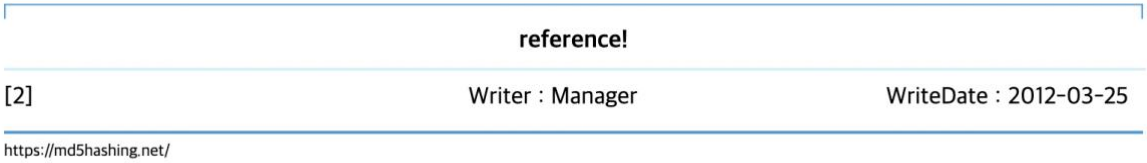
SuNiNaTaS 6

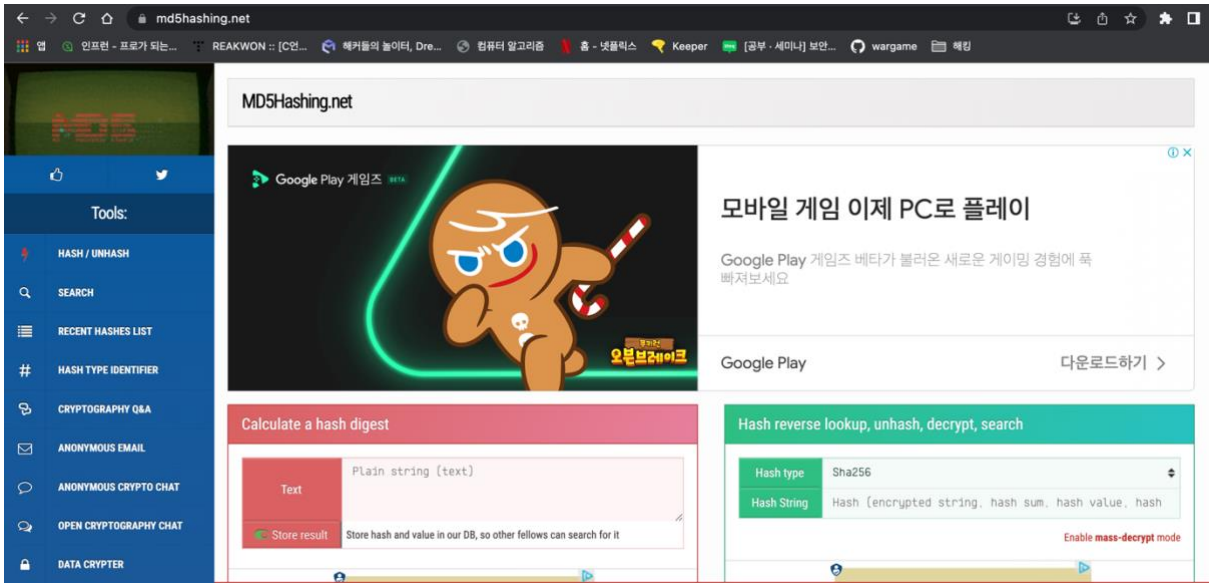
처음 들어가면 다음과 같은 문제 페이지가 주어집니다.

우선 1번부터 차례 차례 글을 읽어봅니다.

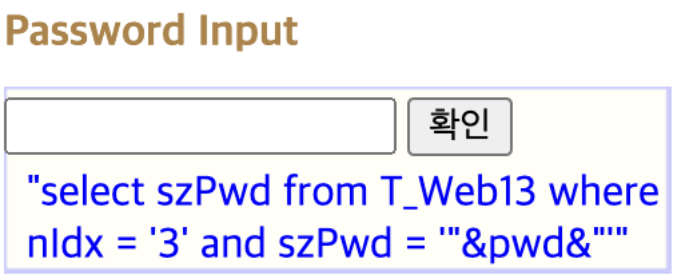
Suninatas의 글을 읽으라는 힌트입니다.



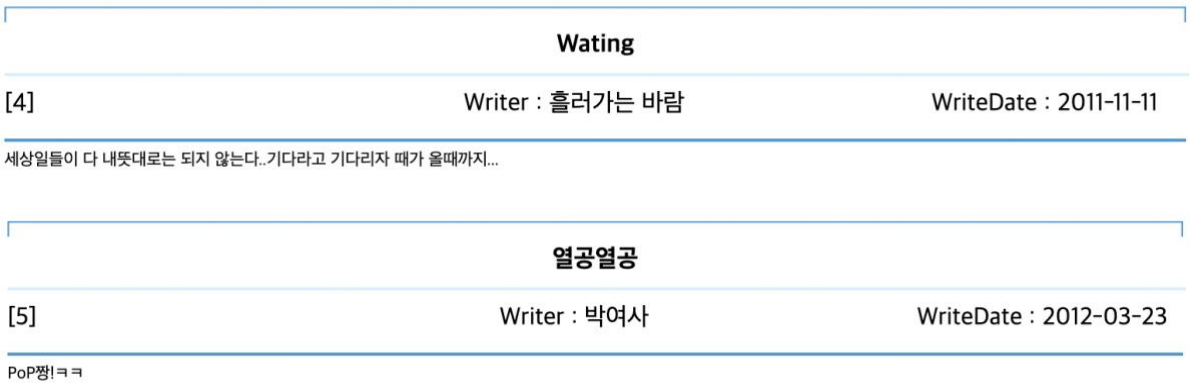
Md5hasing.net의 주소입니다.



Md5hasing.net의 모습

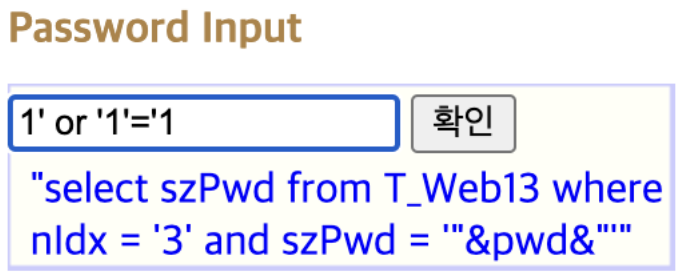


3번 글은 비밀번호가 필요합니다.



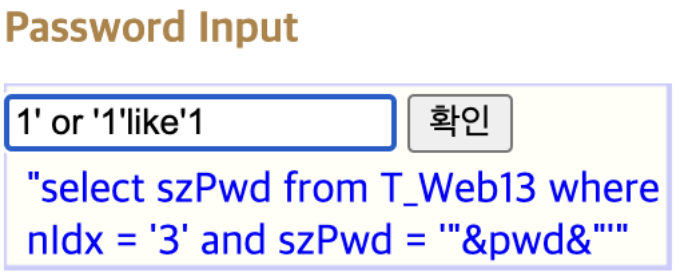
4번과 5번 글은 큰 의미가 없는 글로 보여집니다.

우선 suninatas의 글을 읽기 위해 비밀번호를 통과해야 합니다.
아래 쪽에 sql문이 주어졌으니 sql injection으로 통과를 시도합니다.

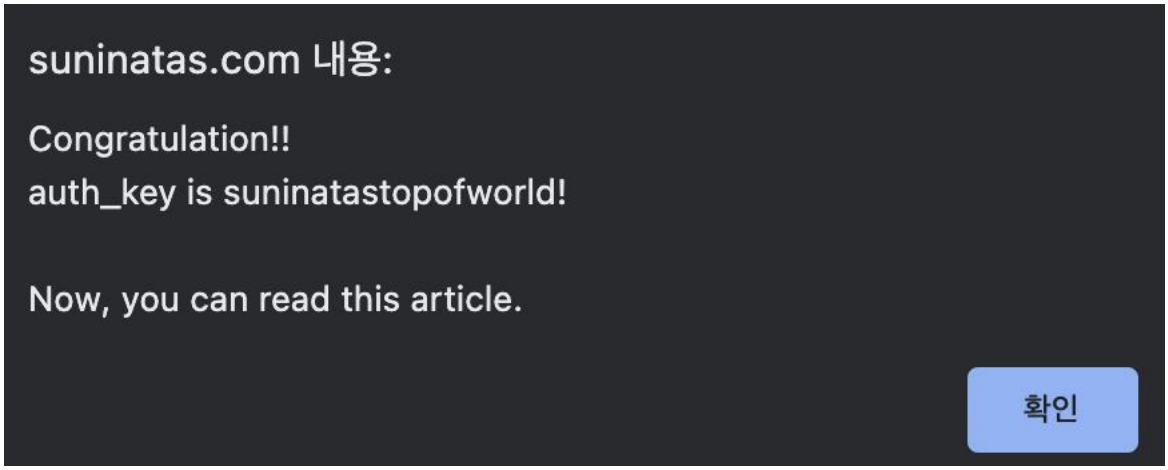


1′ or ′1′=′1 을 삽입합니다

제대로 되지 않습니다. 이후 여러 시도들을 해보니 = , and , union , select 등 많은 구문이 필터링 되고 있었습니다. 필터링이 안 되고 있는 것을 찾아보니 like 가 가능했습니다.

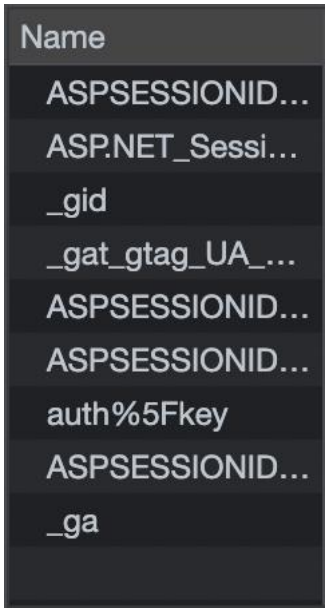


= 연산자를 like 로 바꾸어 시도합니다.



잘 작동되어 글을 읽을 수 있게 됩니다.
그리고 여기에 auth_key 라고 나타난 suninatastopofworld!를 혹시나 하여 시도해 보았지만 auth key 가 아니었습니다.

쿠키를 확인해보니 auth key 라는 쿠키가 존재합니다.



쿠키의 값으로 suninatastopofworld!를 넘겨주었지만 실패합니다.
Md5 를 이용하여 해싱하여

```
65038b0559e459420aa2d23093d01e4a
```

를 넘겨주었지만 실패합니다.
이 후 글의 내용을 확인해봅니다.

README

[3]	Writer : suninatas	WriteDate : 2012-03-01

KeyFinding^^

Key 를 찾으라는 내용의 글입니다.
소스를 확인해봅니다.

```
<body class="vsc-initialized"> == $0
  <table width="100%" cellpadding="0" cellspacing="0">
    <form method="post" name="KEY_HINT" action="Rome's First Emperor"></form>
    <tbody>
```

Key hint 로 rome's first emperor 가 주어졌습니다.

정답은 Augustus