

## RE: SQL Injection – retrieving all rows

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-03/0074.html>

---

**From:** Zacharias Pigadas ([zpig@space.gr](mailto:zpig@space.gr))

**Date:** 03/21/02

From: "Zacharias Pigadas" <[zpig@space.gr](mailto:zpig@space.gr)>

To: "mel" <[meling@scan-associates.net](mailto:meling@scan-associates.net)>

Date: Thu, 21 Mar 2002 09:04:18 +0200

Hello,

I will have to disappoint you but in that case you have to run multiple queries as follows:

Suppose this is your SQL injection string:

SELECT field1, field2 FROM table where 1=1 : This will return you the first row in the table say value1, value2

Second query will be something like that:

SELECT field1, field2 FROM table where 1=1 AND (((field1 NOT IN (value1)) AND (field2 NOT IN (value2)))): This will return you the second row in the table say value21, value22

third query:

SELECT field1, field2 FROM table where 1=1 AND (((field1 NOT IN (value1,value21)) AND (field2 NOT IN (value2,value22)))): This will return you the second row in the table say value31, value32

Well you get the idea....

This can be scripted...

Zach

> -----Original Message-----

> From: mel [<mailto:meling@scan-associates.net>]

> Sent: Wednesday, March 20, 2002 1:25 PM

> To: [pen-test@securityfocus.com](mailto:pen-test@securityfocus.com)

> Subject: SQL Injection – retrieving all rows

>

>

> Hi,

>

> I've been able to enumerate over 50 plus tables in a recent pen-test,

## SecurityFocus Penetration: RE: SQL Injection – retrieving all rows

> now come the hard part – I want to dump data from the most important  
> table that contains user names and passwords. However, the ASP app  
> that I exploit only returns one row at a time. Is there anyway to  
> overcome this?  
>  
> I've been looking for apps that return multiple rows (such as search, etc)  
> but to know avail. I've tried dumping asp codes using BULK INSERT, but  
> the command is only available for system account. Creating an stored  
> procedure does not seem to work as well :(  
>  
> Now, I'm thinking of writing a script that dump the data one at a time,  
> but I would like the advice from fellow pen-testers first.  
>  
> Cheers,  
>  
> --mel  
>  
>

---

> -----  
> This list is provided by the SecurityFocus Security Intelligence  
> Alert (SIA)  
> Service. For more information on SecurityFocus' SIA service which  
> automatically alerts you to the latest security vulnerabilities  
> please see:  
> <https://alerts.securityfocus.com/>  
>  
>

---

This list is provided by the SecurityFocus Security Intelligence Alert (SIA)  
Service. For more information on SecurityFocus' SIA service which  
automatically alerts you to the latest security vulnerabilities please see:  
<https://alerts.securityfocus.com/>

---

- **Previous message:** [Alex S. Harasic: "Re: Send output to file in SQL"](#)
- **In reply to:** [mel: "SQL Injection – retrieving all rows"](#)
- **Next in thread:** [Kevin Spett: "Re: SQL Injection – retrieving all rows"](#)
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)