

[NT] Multiple DUWare Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0061.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/18/03

To: list@securiteam.com

Date: 18 Dec 2003 16:40:06 +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 DUWare Vulnerabilities

SUMMARY

<<http://www.duware.com>> DUportal Pro is "a professional Web portal and online community. DUportal Pro contains numerous advanced features such as Web-based administration, Articles, Banner Ads, Event Calendar, Classified Ads, Web link directory, Downloads, Entertainment, Message Board, Picture Gallery, News, E-Commerce, Members Directory, Polls, and Business Directory, and more that can be downloaded online. All modules are customizable via Web-based Admin panel, together with size, skins, and themes".

Almost all, if not ALL of the products offered by DU Ware seem to have been done with an extremely minimal understanding and/or concern of security, and very important aspects of web security such as, but not limited to: unique session ID's, input validation, and many more. Their software relies HEAVILY on hidden tags, client side input validation, and security through obscurity. Examples of some of the consequences of this weakly implemented/nonexistent security are script execution, arbitrary file upload, account hijacking, database exposure, query tampering, and code injection and server compromise.

DETAILS

Securiteam: [NT] Multiple DUWare Vulnerabilities

Vulnerable systems:

- * DU Portal version 3.0

Remote File Upload:

Anywhere there are places to upload a picture, or file on DUPortal you can upload a script, or file of your liking. The only limits really are size. The only requirement to exploit this vulnerability is a web browser. Simply save the page to your hard drive, edit out all the client side validation and an attacker may upload any file they wish. This can allow for script execution on the host machine as well as host compromise.

Script Execution:

Script execution in DU Software Products can take place in a number of ways. The most serious of these is by using the previously mentioned file upload vulnerability to upload any script of your liking. Using that particular method it is obviously not very hard to compromise the security of the entire host. Another way is by injecting script into items that have to be approved by the administrator of the portal. This can also be manipulated by tampering with the hidden form value by the name of "APPROVED".

If the item you add requires approval by the administrator, then any code you inject into a particular item will be executed by the administrator unknowingly, thus allowing an attacker to carry out administrative functions via the admin. It is also possible for a user to inject script into their username value, as well as other components and have it executed in the browsers of the portals visitors.

Account Hijacking:

Having an administrator execute commands and script for an attacker can be bad news, but it is even worse when an attacker can take over the administrative account, or any other account at will. This is not hard to do and only requires a browser and text editor to execute. Because DU Portal assigns no specific user session id, and relies on hidden fields to change information, it is simple to reset the password of ANY account in the DU Portal database. It is also possible to tamper with cookie data, and gain limited access to arbitrary accounts.

Privilege Escalation:

When registering an account on a DU Portal installation, a malicious user is able to set them to any user level they like by altering the hidden form field value for "U_ACCESS" It is initially set to user, but anyone with a text editor and web browser can change this to admin.

Query Tampering:

There is little input validation and/or sanitization in DU Portal, so tampering with database queries is not a difficult task. Below is a list of the affected components.

- * search.asp
- * password.asp

Securiteam: [NT] Multiple DUWare Vulnerabilities

- * channel.asp
- * register.asp
- * type.asp
- * detail.asp
- * post.asp
- * submit.asp

This may not be all of them, but it should be most of them. JeiAr hopes that the list above will be incentive enough for the developer to secure all of the portal's components, including any not previously mentioned.

Hidden Form Value Weakness:

As JeiAr has mentioned before, this portal system relies HEAVILY on client side validation and especially on hidden form fields/values. By saving any number of pages of a DU Portal an editing, an attacker can manipulate much data. Examples include but are not limited to administrative action, impersonating other users, changing shop prices, account hijacking, and much more.

Plain Text And Database Disclosure Weakness:

No passwords in the DU Portal database are encrypted. They are also shown in plain text in the admin panel. This is a problem because it can be used by an attacker or malicious administrator to compromise the integrity of users that have a bad habit of using the same password everywhere. The database by default is also available for download at the following location

<http://localhost/database/DUportal.mdb>

This can be avoided however by setting the proper permissions for the directory in which the database is located in or better yet move the entire database to an offline directory.

Exploits:

An proof of concept exploit is available at (HTML format):

<<http://www.gulftech.org/vuln/DUd3.html>>

<http://www.gulftech.org/vuln/DUd3.html>.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:security@gulftech.org>>
JeiAr.

=====

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

=====

=====

Securiteam: [NT] Multiple DUWare Vulnerabilities

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.