MOAUB

Abysssec Research

1) Advisory information

Title	: Luftguitar CMS Vulnerability: Upload arbitrary file
Affected	: Luftguitar CMS 2.0.2
Discovery	: www.abysssec.com
Vendor	: ---
Impact	: Ciritical
Contact	: shahin [at] abysssec.com , info [at] abysssec.com
Twitter	: @abysssec

2) Vulnerability Information

Class

1- **Upload arbitrary file**

Impact

An attacker may leverage this issue to have arbitrary script code execute in the browser of an unsuspecting user. This may help the attacker steal cookie-based authentication credentials and launch other attacks.

Also it's possible to upload a malicious script and run arbitrary command on target server.

Remotely Exploitable

Yes

Locally Exploitable

No

3) Vulnerabilities detail

1- Arbitrary Upload file:

This CMS have Upload arbitrary file valnerability with Image Gallery.

you can upload your file with this path:

http://Example.com/Backstage/Components/FreeTextBox/ftb.imagegallery.aspx

Uploaded files will be placing in this path:

http://Example.com/Images/