YGN ETHICAL HACKER GROUP

Security Advisory

Burglish Chat Input Flood Vulnerability

Discovered by: d0ubl3_h3lix
Date: Fri Feb 23, 2007
Threat Affected: DOS (Denial of Service), causing legitimate users unable to chat
Status: Fixed
Author: Ko Soe Min (Mark)
URL: http://www.burglish.com

Description:

Burglish Chat is the first and foremost chat that replaces users' typed Burglish characters to Unicode Burmese font.

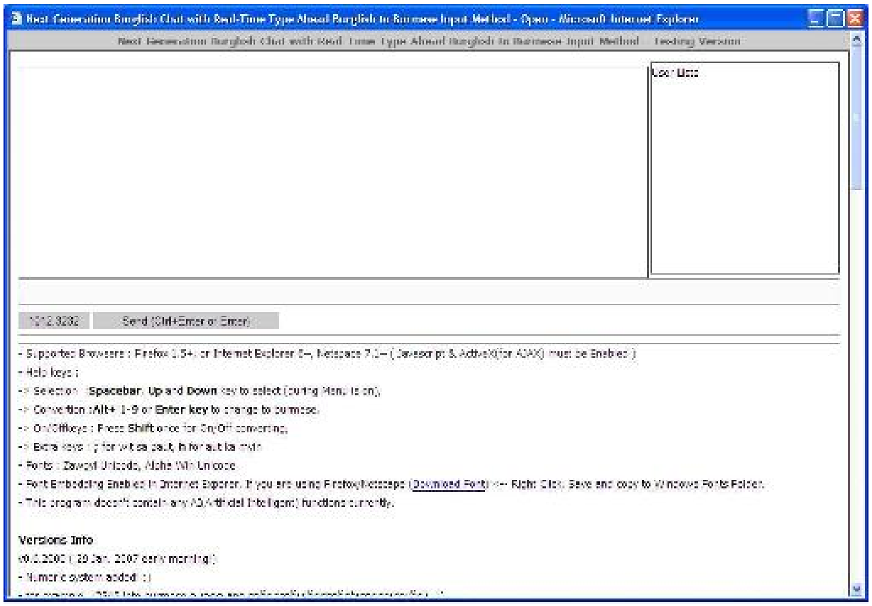
d0ubl3_h3lix's Last Note:

I am glad to see Mark had implemented a very good filter on inputs. Every developer should quickly be proactive to security response like him.

POF (Proof-Of-Concept)

Screenshots were captured with the aid of my friends living at different countries. Due to bad characters flood inputs which cause parsing errors, they can no longer able to chat. They do not see anything in chat window and cannot even type any texts. Please see the next pages.

Location One:

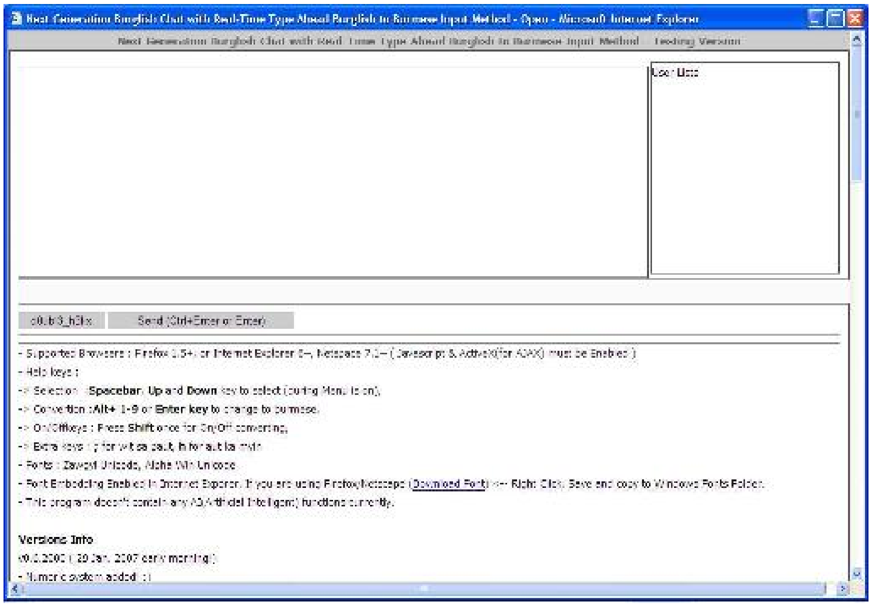


Next Generation Burglish Chat with Real-Time Type Ahead Burglish to Burmese Input Method - Opera - Microsoft Internet Explorer
Next Generation Burglish Chat with Real Time Type Ahead Burglish to Burmese Input Method - Testing Version
User Lists
1012.3282
Send (Ctrl+Enter or Enter)

- Supported Browsers : Firefox 1.5+, or Internet Explorer 6+, Netscape 7.1+ (Javascript & ActiveX(for AJAX) must be Enabled)
- Help keys :
-> Selection : **Spacebar**, **Up** and **Down** key to select (during Menu is on),
-> Convertion :**Alt+ 1-9** or **Enter key** to change to burmese.
-> On/Offkeys : Press **Shift** once for On/Off converting,
-> Extra keys : ; for wit sa pauk, h for auk ka myit
- Fonts : Zawgyi Unicode, Alphe Win Unicode
- Font Embedding Enabled in Internet Explorer. If you are using Firefox/Netscape (Download Font) <-- Right Click, Save and copy to Windows Fonts Folder.
- This program doesn't contain any AI(Artificial Intelligent) functions currently.

Versions Info
v0.0.2000 (20 Jan, 2007 early morning)
- Numeric system added :)

Location Two:

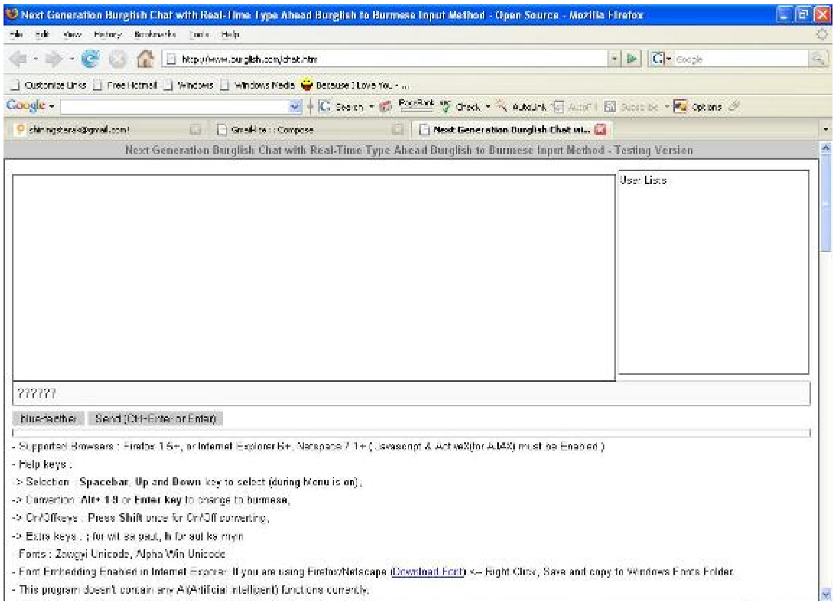


Next Generation Burglish Chat with Real-Time Type Ahead Burglish to Burmese Input Method - Opera - Microsoft Internet Explorer
Next Generation Burglish Chat with Real Time Type Ahead Burglish to Burmese Input Method - Testing Version
User Lists
d0ub13_h3lix
Send (Ctrl+Enter or Enter)

- Supported Browsers : Firefox 1.5+, or Internet Explorer 6+, Netscape 7.1+ (Javascript & ActiveX(for AJAX) must be Enabled)
- Help keys :
-> Selection : **Spacebar**, **Up** and **Down** key to select (during Menu is on),
-> Convertion :**Alt+ 1-9** or **Enter key** to change to burmese.
-> On/Offkeys : Press **Shift** once for On/Off converting,
-> Extra keys : ; for wit sa pauk, h for auk ka myit
- Fonts : Zawgyi Unicode, Alphe Win Unicode
- Font Embedding Enabled in Internet Explorer. If you are using Firefox/Netscape (Download Font) <-- Right Click, Save and copy to Windows Fonts Folder.
- This program doesn't contain any AI(Artificial Intelligent) functions currently.

Versions Info
v0.0.2000 (20 Jan, 2007 early morning)
- Numeric system added :)

Location Three:


Next Generation Burglish Chat with Real-Time Type Ahead Burglish to Burmese Input Method - Open Source - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.burglish.com/chat.htm
Google
Customize Links Free Hotmail Windows Windows Media Because I Love You - ...
Google
Search PageRank Check AutoLink AutoFill Subscribe Options
Gmail - Inbox : Compose
Next Generation Burglish Chat wi...
User Lists
??????
Bluefeather
Send (Ctrl+Enter or Enter)
Download Font

Next Generation Burglish Chat with Real-Time Type Ahead Burglish to Burmese Input Method - Testing Version

- Supported Browsers : Firefox 1.5+, or Internet Explorer 6+, Netscape 7.1+ (Javascript & ActiveX(for AJAX) must be Enabled)
- Help keys :
-> Selection : **Spacebar**, **Up** and **Down** key to select (during Menu is on),
-> Convertion: **Alt+ 1-9** or **Enter key** to change to burmese,
-> On/Offkeys : Press **Shift** once for On/Off converting,
-> Extra keys : ; for wit sa paut, **h** for aut ka myit
- Fonts : Zawgyi Unicode, Alpha Win Unicode
- Font Embedding Enabled in Internet Explorer. If you are using Firefox/Netscape (Download Font) <-- Right Click, Save and copy to Windows Fonts Folder.
- This program doesn't contain any AI(Artificial Intelligent) functions currently.