

# [TOOL] TCP/UDP Protocol Fuzzer (CIRT.DK)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00031.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 8 Jan 2006 13:44:50 +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>

-----

TCP/UDP Protocol Fuzzer (CIRT.DK)

---

## SUMMARY

## DETAILS

"Fuzzing" is an automated software testing technique that generates and submits random or sequential data to various areas of an application in an attempt to uncover security vulnerabilities.

For example, when searching for buffer overflows, a tester can simply generate data of various sizes and send it to one of the application entry points to observe how the application handles it.

Usage example (string overflow):

```
fuzz.pl -host 192.168.1.2 -port 80 -type string -load template.txt
```

Making the template:

Make a file where you can put any request into, and the place you want to Fuzz insert the tag <FUZZER>, if you need to count size of data you eg. like in a POST request of a HTTP server, use the tags <COUNT>data<COUNT>

[TOOL] TCP/UDP Protocol Fuzzer (CIRT.DK)

and <SIZE>, it could be done as follows:

POST /cgi-sys/FormMail.cgi HTTP/1.1  
Host: 127.0.0.1  
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.7.5)  
Gecko/20041128 Firefox/1.0 (Debian package 1.0-4)  
Keep-Alive: 300  
Connection: keep-alive  
Referer: <http://127.0.0.1/>  
Content-Type: application/x-www-form-urlencoded  
Content-Length: <SIZE>

<COUNT>recipient=test%40127.0.0.1&subject=Fuzzing&Name=test  
&email=test%40localhost& request=test<FUZZER>&redirect=/  
<COUNT>

You can also use hex values like \x41 or 0x41 values in the template if the protocol is binary.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:tools@xxxxxxx>> CIRT Tools.  
To keep updated with the tool visit the project's homepage at:  
<<http://www.cirt.dk/tools/fuzzer/fuzzer.txt>>  
<http://www.cirt.dk/tools/fuzzer/fuzzer.txt>

=====

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@xxxxxxxxxxxxxxxxx  
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====  
=====

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.



- Prev by Date: [\*\[EXPL\] BlueCoat WinProxy Buffer Overflow \(Host header, Exploit\)\*](#)
- Next by Date: [\*\[UNIX\] ADOdb SQL Injection and PHP Code Execution Vulnerabilities\*](#)
- Previous by thread: [\*\[EXPL\] BlueCoat WinProxy Buffer Overflow \(Host header, Exploit\)\*](#)
- Next by thread: [\*\[UNIX\] ADOdb SQL Injection and PHP Code Execution Vulnerabilities\*](#)

- Index(es):
  - ◆ *Date*
  - ◆ *Thread*