

RE: News Item: UN warns on password 'explosion'

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2006-12/msg00183.html>

- *From:* "Pranav Lal" <pranav.lal@xxxxxxxxx>
 - *Date:* Thu, 7 Dec 2006 06:17:25 +0530
-

Hi Saqib and all,

The problem with most implementations of captcha is that they are absolutely inaccessible to users with disabilities. Google has recently done some work to make the system accessible but then how many people with implement that?

Pranav

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxxx [<mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx>] On Behalf Of Saqib Ali
Sent: Tuesday, December 05, 2006 5:48 PM
To: Andrew Aris
Cc: security-basics
Subject: Re: News Item: UN warns on password 'explosion'

Interesting feedback.

I implemented a discussion forum at ASU (university) for Objectivity DB using the email auth that i mentioned in my last email. So here are some of my thoughts about the issues that you raise.

1) True. If there was a spam attack it would generate lot of bounce backs, which could in turn a cause a DOS scenario. However we never received such a attack (I guess the forum wasn't popular enough ;))
But my .procmail was setup to /dev/null any non-standard emails, so I didn't see any bounce back cause by spams.

2) True. I don't have a solution to this. Maybe only allowing 1 post / hour is a way to mitigate this.

3) Captcha should solve this issue, and issues #1 and #2 as well. Granted captcha requires additional work on part of the user, but isn't typing a 5 digit number easier then remembering usernames/password for X number of forums ??? In my opinion using captcha is much more easier and convenient for users. I know some people might not agree with this.

Just a thought....

RE: News Item: UN warns on password 'explosion'

saqib

<http://www.full-disk-encryption.net>

On 12/5/06, Andrew Aris <andrew@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

Nice idea, but it does have some flaws..

- 1) Any attempts to spam the forum using invalid email addresses will result in the form sending large amounts of wasted e-mail out, followed by receiving large amounts of bounces back.
- 2) You could use it to "attack" peoples mail boxes by posting a lot to a forum with their email address, generating lots of "authorisation" messages to their address.
- 3) Authorisation emails would probably be easy enough to automate a response to – allowing spammers to post on the forum. Sure you could use image verification but then you wouldn't have many posters as not many would be bothered to go through the hassle.

All of the above combine to make it an unattractive idea to forum admins.

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxxx [<mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx>] On Behalf Of Saqib Ali
Sent: 04 December 2006 14:53
To: security-basics
Subject: News Item: UN warns on password 'explosion'

Nothing new: Username + Password reuse will make the net less secure which in turn make people wary of spending money online.

Still a good read.

My question is why so many online discussion forum require logon to post messages? Currently I have 20+ discussion forum account for the various vendors that I deal with (e.g. citrix, wise, altiris, active batch etc) .

Why can't they be like mailing lists where the username+password is optional/not-required.

Discussion forums use username+password as mean to

- 1) control access,
- 2) tie the post to a email address; and
- 3) prevent anonymous spam.

Alternatively this can also be achieved by simply requiring email address along with post, and then sending a authorization email to the poster before making the post visible on the forum. This will achieve the same effect, and the user will not be burdened with remembering username+password for each forum where they make posts.

Saqib Ali, CISSP, ISSAP
<http://www.full-disk-encryption.net>

Saqib Ali, CISSP, ISSAP
<http://www.full-disk-encryption.net>

This list is sponsored by: ByteCrusher

Detect Malicious Web Content and Exploits in Real-Time.
Anti-Virus engines can't detect unknown or new threats.
LinkScanner can. Web surfing just became a whole lot safer.

http://www.explabs.com/staging/promotions/xern_lspro.asp?loc=sfmaildetect

This list is sponsored by: ByteCrusher

Detect Malicious Web Content and Exploits in Real-Time.
Anti-Virus engines can't detect unknown or new threats.
LinkScanner can. Web surfing just became a whole lot safer.

http://www.explabs.com/staging/promotions/xern_lspro.asp?loc=sfmaildetect
