

## RE: Script for find domino's users

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-02/0166.html>

---

*From:* Jay D. Thomson ([jthomson@appsecinc.com](mailto:jthomson@appsecinc.com))

*Date:* 02/08/02

From: "Jay D. Thomson" <[jthomson@appsecinc.com](mailto:jthomson@appsecinc.com)>

To: <[bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)>

Date: Fri, 8 Feb 2002 12:45:47 -0800

Simon,

Proper ACL management is certainly required to provide security, however in this case it still won't prevent an attacker from remotely verifying a mail user's existence. The key lies in the fact that Domino web servers will return a "401" unauthorized response if the database actually exists, and a "404" nonexistent URI if the database does not. Since user mail databases are created by default when users are registered, this is a simple and easy way to test for existence.

This can be easily tested by opening a web browser and attempting to access a known good mail database and then one that is known to be nonexistent.

Obviously, if the anonymous user can actually access/read a user's mail database, that server has much bigger problems than what I describe above!

There are several things administrators can do beyond what you describe eliminate this issue:

1) Choose not to allow email through the web (Application Security, Inc. recommends this for reasons I won't go into here)

2) Force nonexistent mail/\*.nsf database access attempts to return a 401 unauthorized using a complex set of HTTP redirection rules set up in the server's server document. Attackers can generally get around this by using HTTP escape characters (i.e. %61).

Either way, administrators are going to want to run regular security scans against their Domino based webservers in order to see just what an attacker could determine/break. Here at Application Security, Inc. (ASI) we're are preparing to debut a new penetration testing tool specifically geared for Domino webservers. This tool will not only tell you if users can be determined remotely, but it will also test mail database security, proper ACL management, the existence of serious remote vulnerabilities, user password strength, poor authentication mechanisms and more. This is a lot of stuff for one or two people to keep straight on however many servers a

RE: Script for find domino's users

## SecurityFocus Bugtraq: RE: Script for find domino's users

company has; so we're attempting to remove the both the burden and reduce the possibility of human error due to caffeine burnout.

More information on our new pentesting offering is available at my company's website: [www.appsecinc.com](http://www.appsecinc.com).

Regards,

---

Jay D. Thomson  
Tel: 212-490-6022  
Fax: 212-490-6456  
E-mail: [jthomson@appsecinc.com](mailto:jthomson@appsecinc.com)  
Web: [www.appsecinc.com](http://www.appsecinc.com)  
Application Security, Inc. – Protection Where it Counts –

This isn't a proof of concept, but more a probe for misconfigured database ACL's.

If a Domino web server doesn't have a redirection URL for /mail/\* mail files, then you rely on the access control for each mail file.

Two things can be done to avoid this :

- 1 – Change the ACL on sensitive databases ( /mail/\* , names.nsf ) to :  
Anonymous – No access  
[Default] – No access
- 2 – Within the Server Document for each server, ensure that "Allow HTTP clients to browse databases:" is set to "No"

I believe that all versions of Domino server from 4.5 upwards are susceptible to badly configured ACL's. Any good administrator would have a hold of this already.

```
#!/usr/local/bin/php -q  
<?
```

```
<snip>
```

```
</snip>
```

```
fclose ($fd);
```

```
?>
```

- 
- **Previous message:** [Geoff Sweet: "RE: MSN contact list disclosure"](#)
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)