

# [EXPL] Invision Power Board Army System Mod SQL Injection Exploit

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00041.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 13 Feb 2006 19:27:23 +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>

-----  
Invision Power Board Army System Mod SQL Injection Exploit  
-----

## SUMMARY

" <<http://mods.invisionize.com/db/index.php/f/3347>> Army System v2.1 is a very popular mods that has a ranking system built-in. This multiple player rpg can easily be installed on every Invision Power Board v2.x.x"

Army System is prone to an SQL injection vulnerability. This issue is due to a failure in the application to properly sanitize user-supplied input passed to the "userstat" parameter, before being used in an SQL query. A specially crafted URL could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation.

## DETAILS

### Vulnerable Systems:

- \* Invision Board: 2.0.0 Final PHP: 4.1.0 and above
- \* Invision Board: 2.0.1 PHP: 4.3.0 and above
- \* Invision Power Board Army System Mod 2.1 and prior

### Exploit:



[EXPL] Invision Power Board Army System Mod SQL Injection Exploit

```
↓  
if ( strpos( $buffer, "<td class='pformleft'  
width=\"35%\">Name</td>\" ) ) {  
$infos['md5'] = strip_tags ( fgets(  
$handle ) );  
break;  
↓  
↓  
↓  
  
fclose ($handle);  
  
if (count($infos) == 1) return $infos;  
return false;  
↓  
?>
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:unsecure@xxxxxxxxxxxx> fRoGGz  
SecuBox Labs.

=====  
=====

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

=====  
=====

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.