Challenge 9

http://192.168.2.11/sqli/sql7/ [Level: Advanced]

- Which parameter is vulnerable?

  url parameter is vulnerable.

- Provide test case to confirm the sql injection vulnerability

  The application does a URL decode on the input. Note that the application uses mysql_real_escape_string and the input is going as string; yet it is vulnerable.

  The following code demonstrates this:

```
$comments=mysql_real_escape_string($_POST['comments']);

$url=mysql_real_escape_string($_POST['url']);

$query  = "Insert into temp values('".$comments."','".urldecode($url)."')";
```

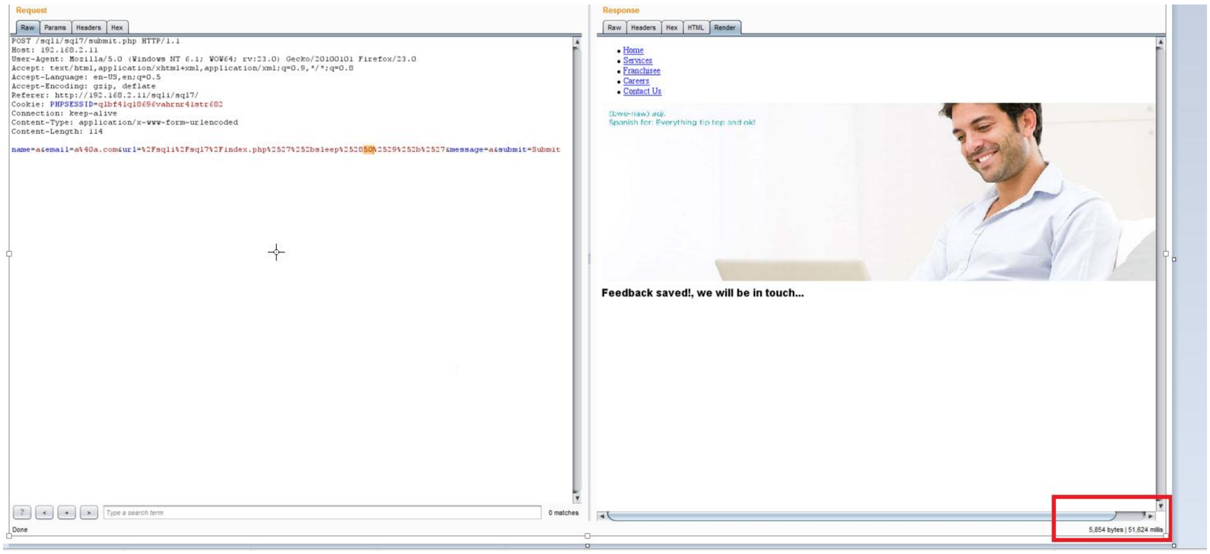
When you inject %2527; mysql_real_escape_string will not sanitize it as it is not a single quote. When the sql is executed, the urldecode function converts %2527 to %27 which is single quote and make it vulnerable.

We need to url encode our attack. As the injection is in Insert statement, we will have to use time delay function. We can inject:

‘+sleep(50)+’

Now, we need to encode our attack:

url=%2Fsqli%2Fsql7%2Findex.php%2527%252bsleep%252850%2529%252b%2527



You can verify that the response took over 50 seconds.

Further reading:

Some real world examples of such SQL Injection are listed below:

- http://www.securityfocus.com/archive/1/469258
- http://www.securityfocus.com/archive/1/480575