

EP4 - CVE-2014-2323

SQL Injection no Lighttpd

Ciro S. Costa Marcela M. Terakado

Universidade de São Paulo

10 de Novembro de 2015

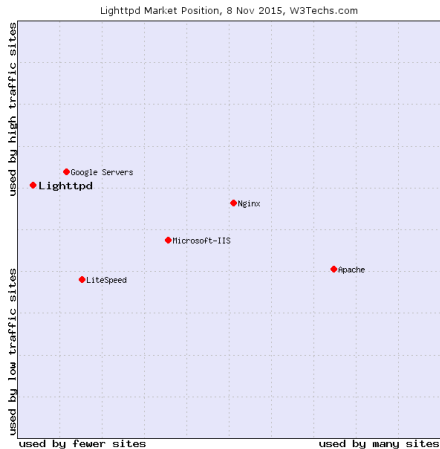
Sumário

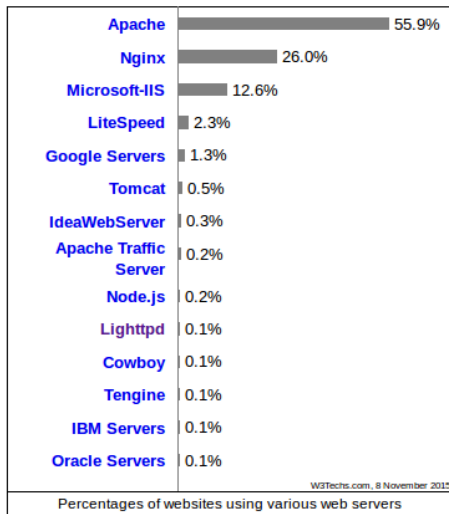
- 1 Lighttpd
- 2 Virtual Hosting
- 3 SQL Injection
- 4 Docker
- 5 Exploit
- 6 Correção

- SQL Injection
- Módulo de Virtual Hosting do Lighttpd (até a versão 1.4.34)
- Verificação de hostname
- Fácil exploração
- CVSS v2 Base Score: 7.5

O que é o Lighttpd?

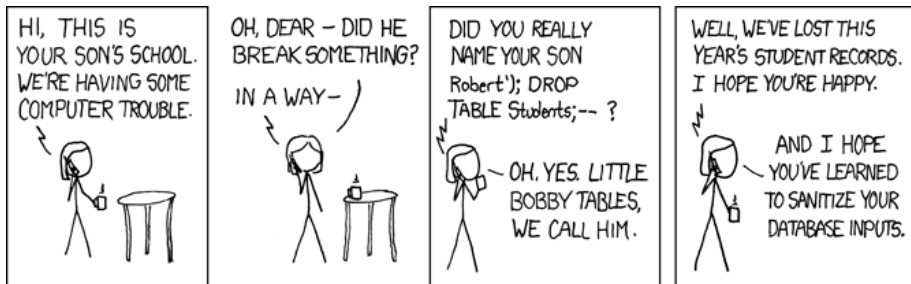
Servidor HTTP para aplicações de alto desempenho.



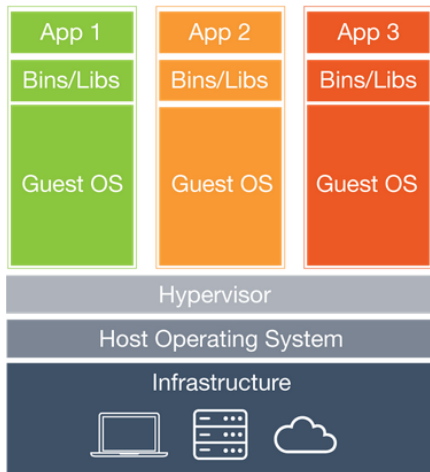


SQL Injection

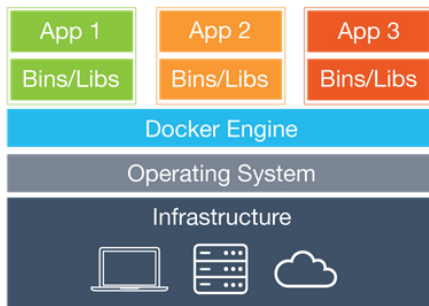
- Falha simples e bastante conhecida.
- Inserir código SQL por meio de uma entrada que não é validada ou verificada corretamente.



Docker



Virtual Machines



Containers

A falha

- request.c
- mod_mysql_vhost.c

- Verifica que entre '[]' apenas algo parecido com um endereço IPv6 pode aparecer.
- Só valida o número de porta correto se o próximo caractere é um ':'
- Não há o tratamento para o caso em que após o endereço IPv6 a string não termina.
- Servidor identifica corretamente se o hostname é válido de acordo com a gramática
- Problema: Se o próximo caractere é qualquer outra coisa, o resto do cabeçalho do host não está sujeito a qualquer tipo de verificação antes de serem armazenados.

- é inserido em uma consulta SQL sem qualquer escape.
- Problema: Permite que o invasor controle o que o banco de dados.

• request.c

```
40 1 /* IPv6 address */
2 if (host->ptr[0] == '[') {
3     char *c = host->ptr + 1;
4     int colon_cnt = 0;
5
6     /* check portnumber */
7     for (; *c && *c != ':'; c++) {
8         if (*c == ':') {
9             if (++colon_cnt > 7) {
10                 return -1;
11             }
12         } else if (!light_isxdigit(*c) && '.' != *c) {
13 +-- 11 lines: return -1;
14         for (c += 2; *c; c++) {
15             if (!light_isdigit(*c)) {
16                 return -1;
17             }
18         }
19     }
20     return 0;
21 }
22
40 1 /* IPv6 address */
2 if (host->ptr[0] == '[') {
3     char *c = host->ptr + 1;
4     int colon_cnt = 0;
5
6     /* check the address inside [...] */
7     for (; *c && *c != ':'; c++) {
8         if (*c == ':') {
9             if (++colon_cnt > 7) {
10                 return -1;
11             }
12         } else if (!light_isxdigit(*c) && '.' != *c) {
13 +-- 11 lines: return -1;
14         for (c += 2; *c; c++) {
15             if (!light_isdigit(*c)) {
16                 return -1;
17             }
18         }
19     }
20     else if ('\0' != *(c+1)) {
21         /* only a port is allowed to follow [...] */
22         return -1;
23     }
24     return 0;
25 }
26
```

- mod_mysql_vhost.c

[illegible]

```

3  /* build and run SQL query */
4  buffer_copy_string(buffer(p->tmp_buf, p->conf.mysql_pre);
5  if (p->conf.mysql_post-used) {
6      /* escape the uri.authority */
7      unsigned long to_len;
8
9      /* 'to' has to be 'from len * 2 + 1' */
10     buffer_prepare_append(p->tmp_buf, (con->uri.authority->used - 1) * 2 + 1);
11
12     to_len = mysql_real_escape_string(p->conf.mysql,
13     p->tmp_buf->ptr + p->tmp_buf->used - 1,
14     con->uri.authority->ptr, con->uri.authority->used - 1);
15     p->tmp_buf->used += to_len;
16
17     buffer_append_string_buffer(p->tmp_buf, p->conf.mysql_post);
18 }

```

- <https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-2323>
- http://download.lighttpd.net/lighttpd/security/lighttpd_sa_2014_01.txt
- <http://redmine.lighttpd.net/projects/lighttpd/repository/revisions/2959/diff/>

