EP4 - CVE-2014-2323

SQL Injection no Lighttpd

Ciro S. Costa Marcela M. Terakado

Universidade de São Paulo

10 de Novembro de 2015

Sumário

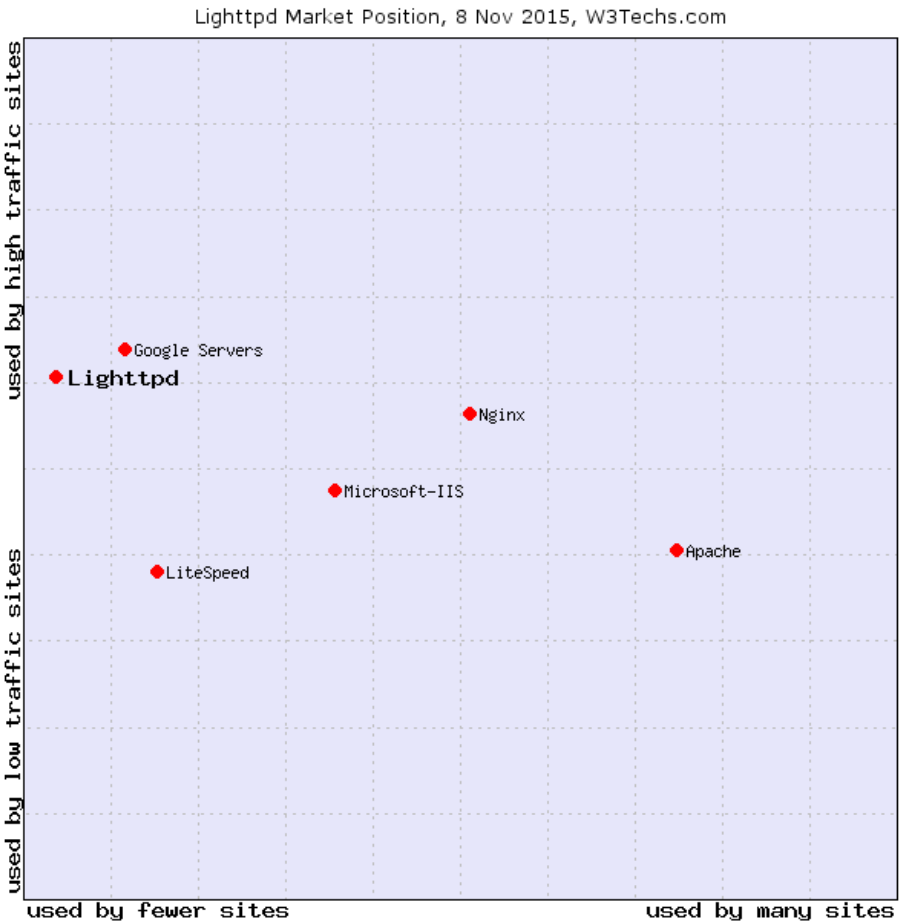
CVE-2014-2323

- 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

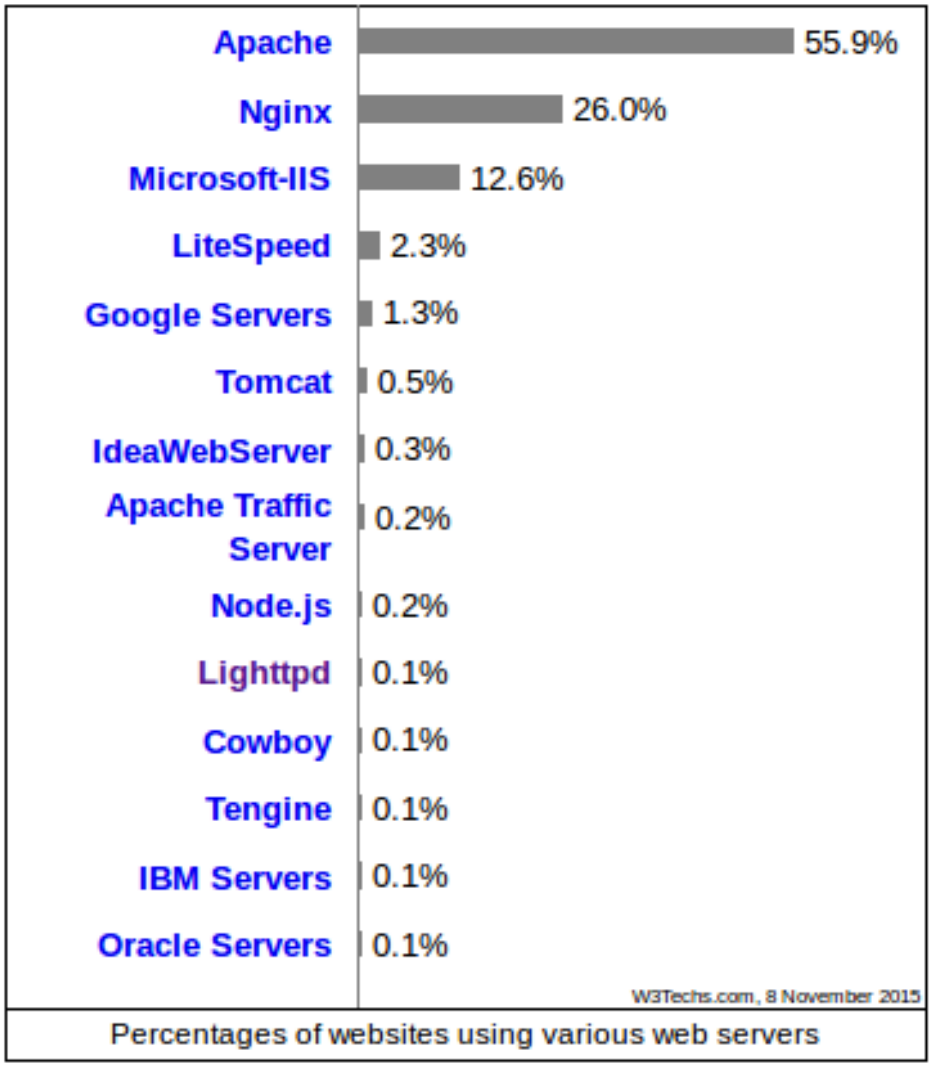
Lighttpd

O que é o Lighttpd?

Servidor HTTP para aplicações de alto desempenho.



Lighttpd

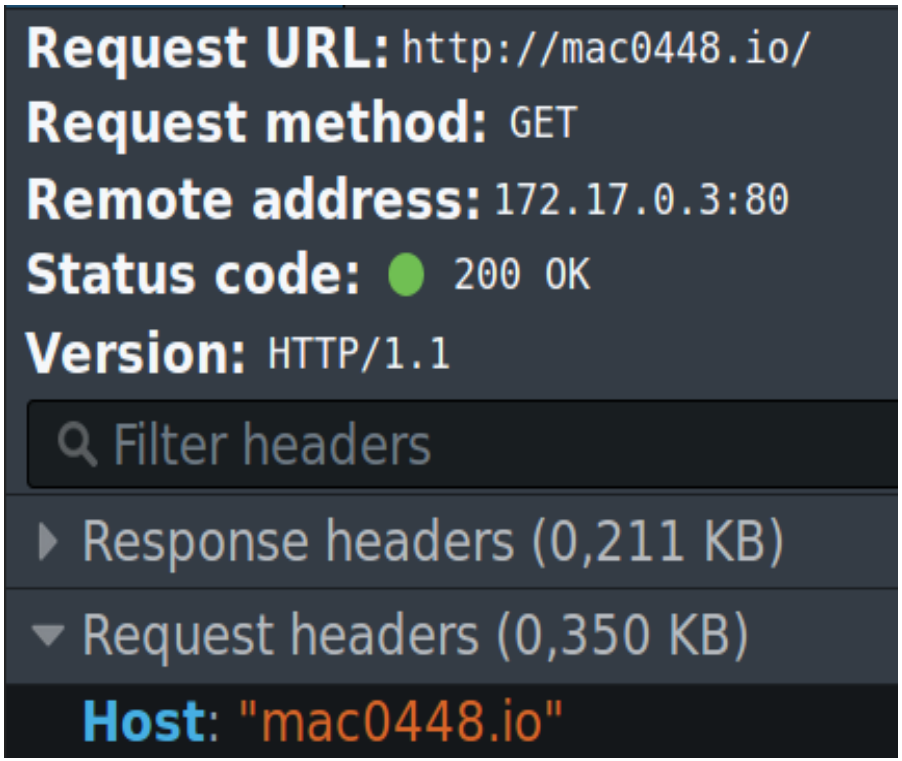


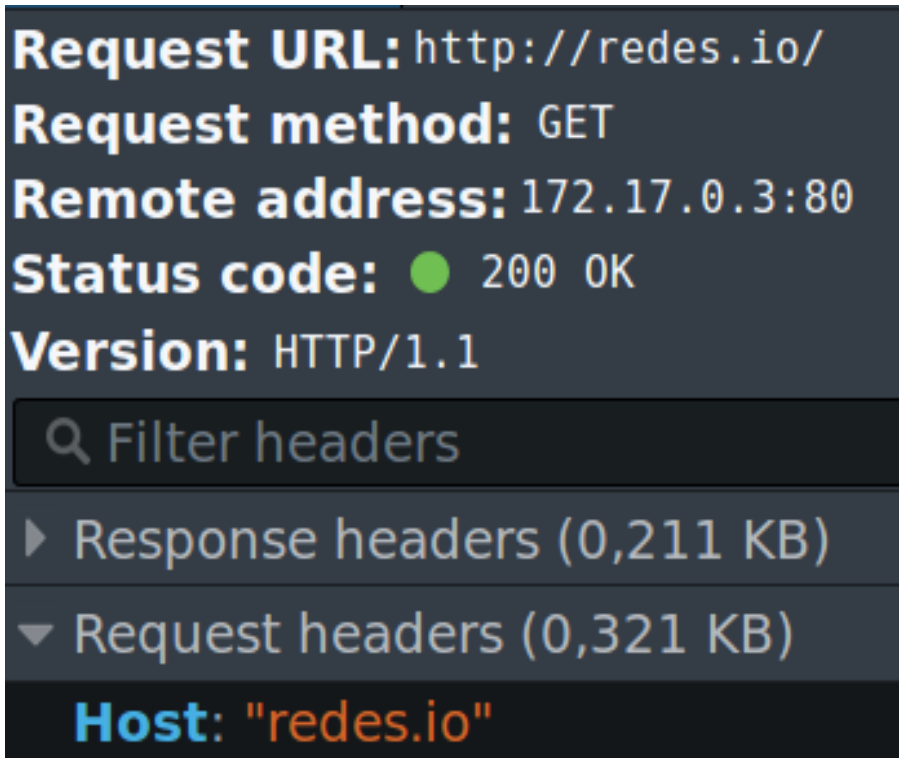
Percentages of websites using various web servers

Virtual Hosting

Definição

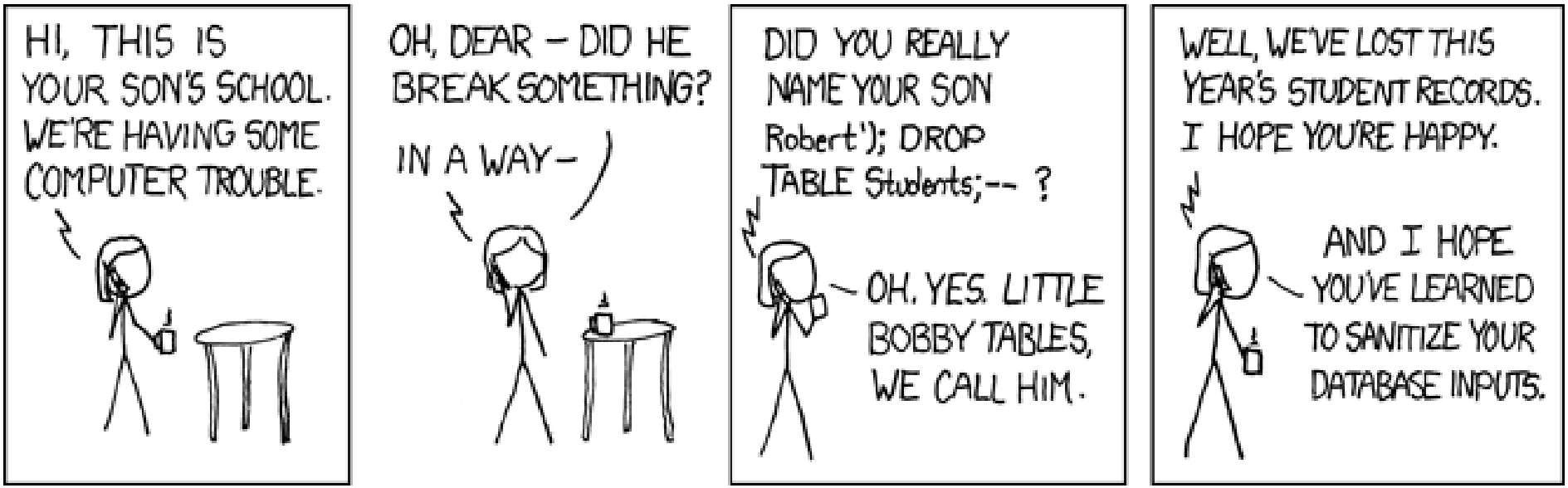
Método utilizado para hospedar mais de um nome de domínio cuja resolução se faz a um mesmo IP



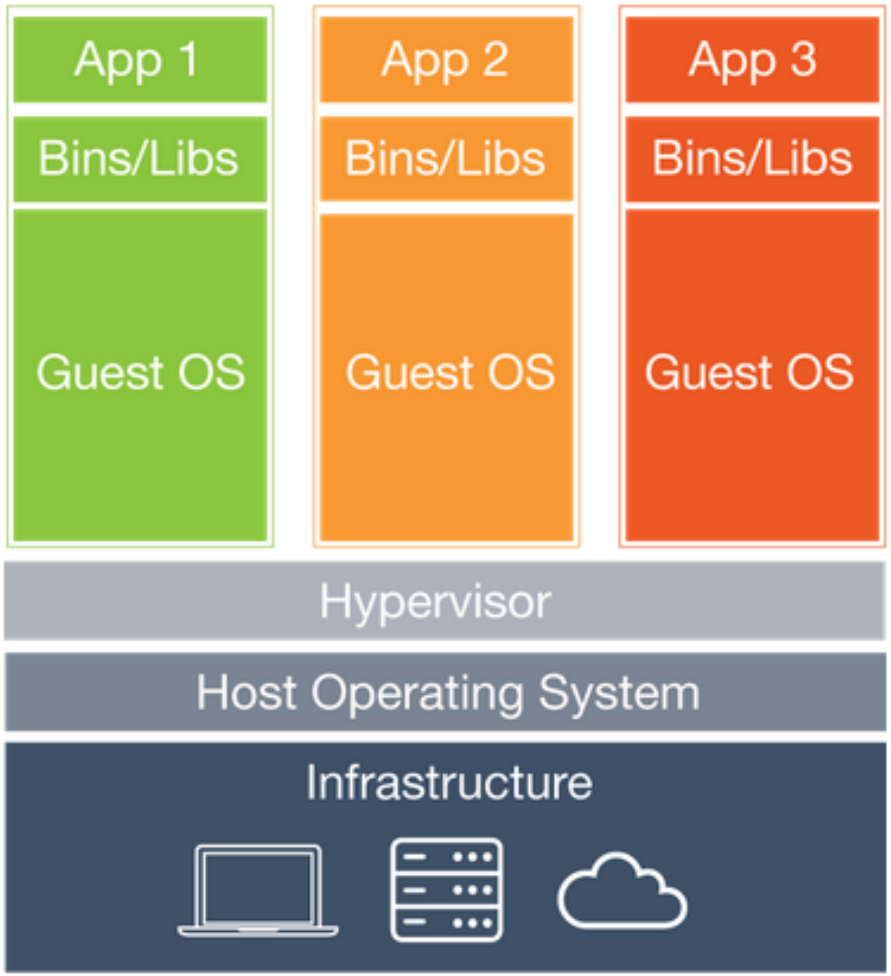


SQL Injection

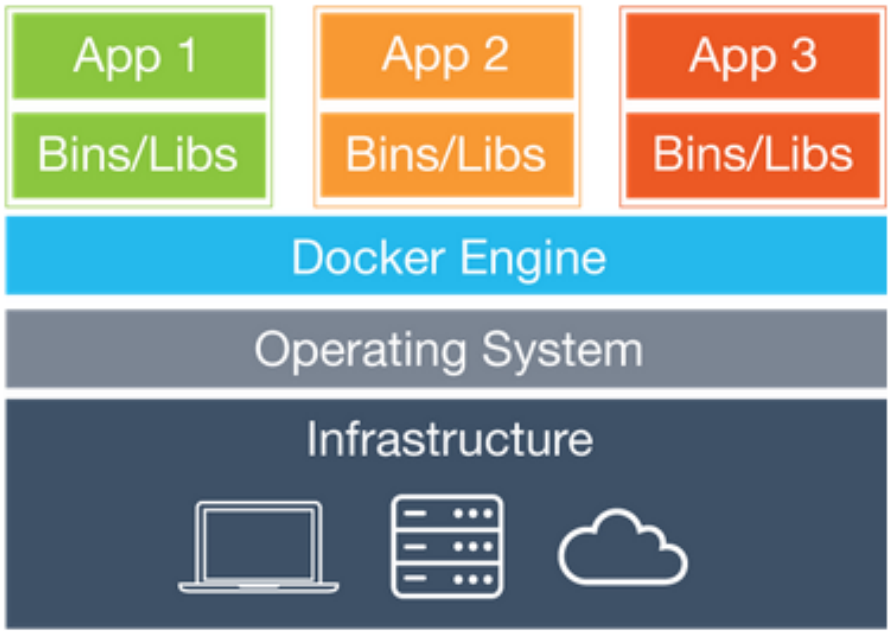
- Falha simples e bastante conhecida.
- Inserir código SQL por meio de uma entrada que não é validada ou verificada corretamente.



Docker



Virtual Machines



Containers

A falha

- request.c
- mod_mysql_vhost.c

request.c

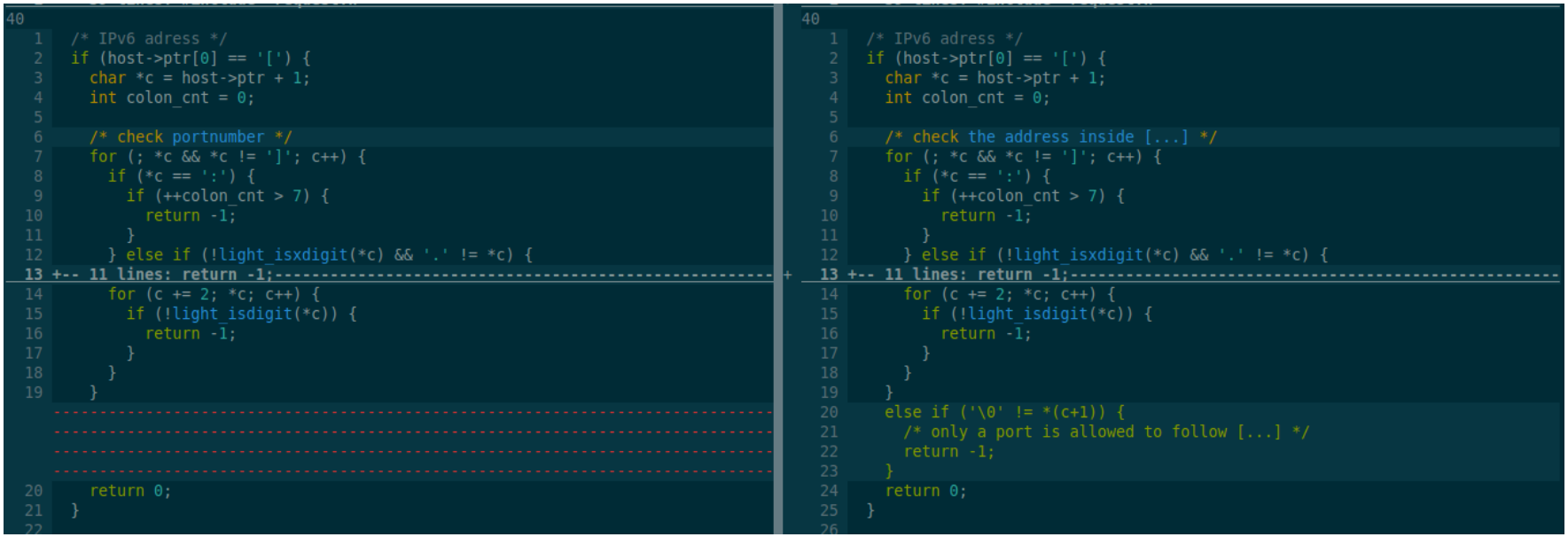
- Verifica que entre '[]' apenas algo parecido com um endereço IPv6 pode aparecer.
- Só valida o número de porta correto se o próximo caractere é um ':'
- Não há o tratamento para o caso em que após o endereço IPv6 a string não termina.
- Servidor identifica corretamente se o hostname é válido de acordo 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.

mod_mysql_vhost.c

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

Correção

- request.c



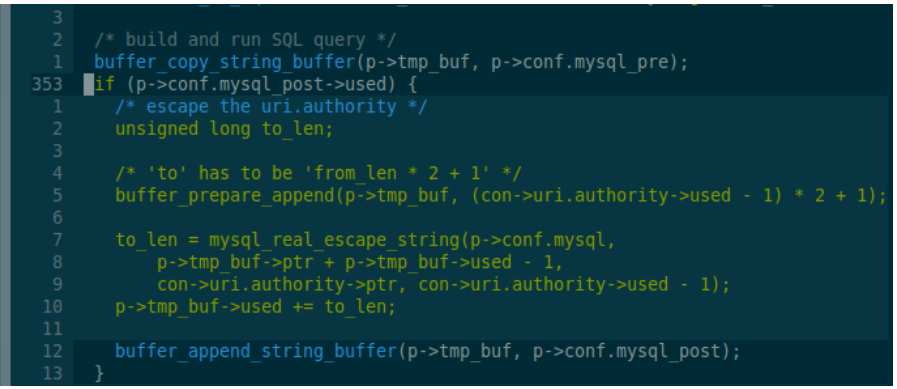
```
/* IPv6 adress */
if (host->ptr[0] == '[') {
  char *c = host->ptr + 1;
  int colon_cnt = 0;

  /* check portnumber */
  for (; *c && *c != ']'; c++) {
    if (*c == ':') {
      if (++colon_cnt > 7) {
        return -1;
      }
    } else if (!light_isxdigit(*c) && '.' != *c) {
+-- 11 lines: return -1;----------
      for (c += 2; *c; c++) {
        if (!light_isdigit(*c)) {
          return -1;
        }
      }
    }
    return 0;
  }
```

```
/* IPv6 adress */
if (host->ptr[0] == '[') {
  char *c = host->ptr + 1;
  int colon_cnt = 0;

  /* check the address inside [...] */
  for (; *c && *c != ']'; c++) {
    if (*c == ':') {
      if (++colon_cnt > 7) {
        return -1;
      }
    } else if (!light_isxdigit(*c) && '.' != *c) {
+-- 11 lines: return -1;----------
      for (c += 2; *c; c++) {
        if (!light_isdigit(*c)) {
          return -1;
        }
      }
    }
    else if ('\0' != *(c+1)) {
      /* only a port is allowed to follow [...] */
      return -1;
    }
    return 0;
  }
```

Correção

- mod_mysql_vhost.c

```
/* build and run SQL query */
buffer_copy_string_buffer(p->tmp_buf, p->conf.mysql_pre);
if (p->conf.mysql_post->used) {
  buffer_append_string_buffer(p->tmp_buf, con->uri.authority);
  buffer_append_string_buffer(p->tmp_buf, p->conf.mysql_post);
}
```

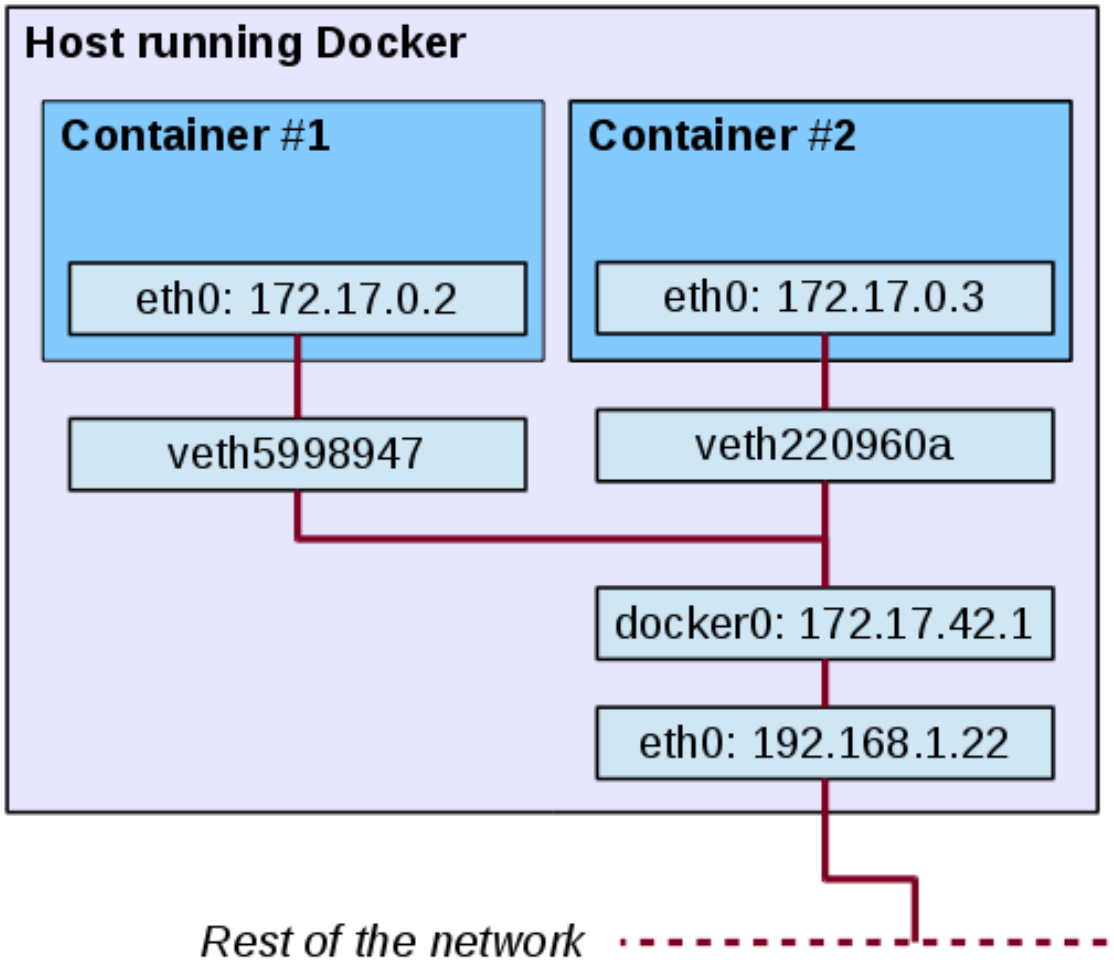


```
/* build and run SQL query */
buffer_copy_string_buffer(p->tmp_buf, p->conf.mysql_pre);
if (p->conf.mysql_post->used) {
  /* escape the uri.authority */
  unsigned long to_len;

  /* 'to' has to be 'from_len * 2 + 1' */
  buffer_prepare_append(p->tmp_buf, (con->uri.authority->used - 1) * 2 + 1);

  to_len = mysql_real_escape_string(p->conf.mysql,
      p->tmp_buf->ptr + p->tmp_buf->used - 1,
      con->uri.authority->ptr, con->uri.authority->used - 1);
  p->tmp_buf->used += to_len;

  buffer_append_string_buffer(p->tmp_buf, p->conf.mysql_post);
}
```

Referências

- 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/

Docker


Host running Docker
Container #1
eth0: 172.17.0.2
Container #2
eth0: 172.17.0.3
veth5998947
veth220960a
docker0: 172.17.42.1
eth0: 192.168.1.22
Rest of the network