

دروس في حماية المنتديات

والان نتطرق الى الدرس الاول وهو التعديل على ملف الكونفك (config) الموجود في مجلد (includes) :

▪ افتح الملف ببرنامج الفرونت بيج او اي برنامج اخر ثم قم بعمل بحث عن

قم بتغيير امس المجلدين admincp – modcp باي اسم تختاره

وبعدها ابحث عن

كود:PHP

```
$config['Misc']['admincpdir'] = 'admincp';  
$config['Misc']['modcpdir'] = 'modcp';
```

نقوم باستبدال الكلمتين admincp - modcp إلى الأسماء الجديدة.

▪ تغير الـ prefix من ملف الـ config

ابحث عن:

كود:PHP

```
$config['Misc']['****ieprefix'] = 'bb';
```

واستبدل الـ bb الى شي اخر مثلا bsb

▪ تعديل في ملف الـ config لحمايتك من الاوامر التخريبية

افتح ملف الكونفك وابحث عن

```
canrunqueries
```

وستجدها بهذا الشكل

```
$canrunqueries = "";
```

كلما عليك فعله هو وضع رقم عضويتك فقط بداخل هذه العلامة '1' و**ثم احفظها وهذا يتيح لك ايضا اضافة اوامر لقاعدة البيانات من لوحة التحكم**

▪ **تشفير الـ config وتغيير مساره واسمه (انا لاافضله ولكم الحرية في تنفيذه)**

○ **قم بنسخ ملف الكونفك على جهازك وسمه باي اسم تريده مثلا gulf ونقله لمجلد اخر مثلا الى admincp فسيصبح المسار admincp/gulf.php**

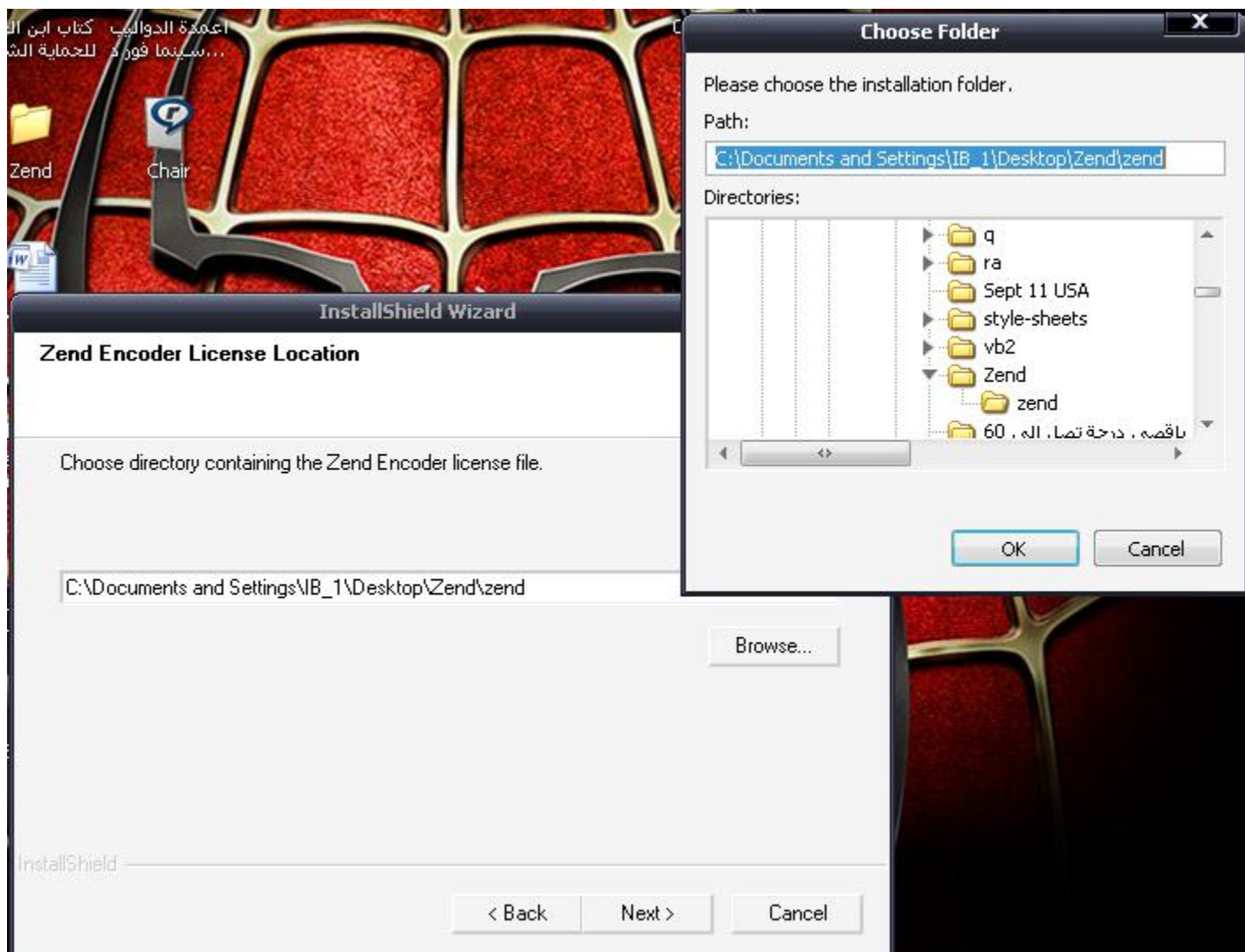
والان قم بالتعديل على class_core.php وهو موجود في includes و**قم بتغيير اسم config.php بالاسم الذي اخترته (gulf)** وايضا غير المسار من include/config.php الى المسار الجديد الذي اخترته (admincp/gulf.php) وكذلك غير المسار في ملف init.php

○ **والان سنقوم بعملية التشفير والتي تتم ببرنامج الزند Zend**
❖ **حمل البرنامج مع الكراك من هنا**

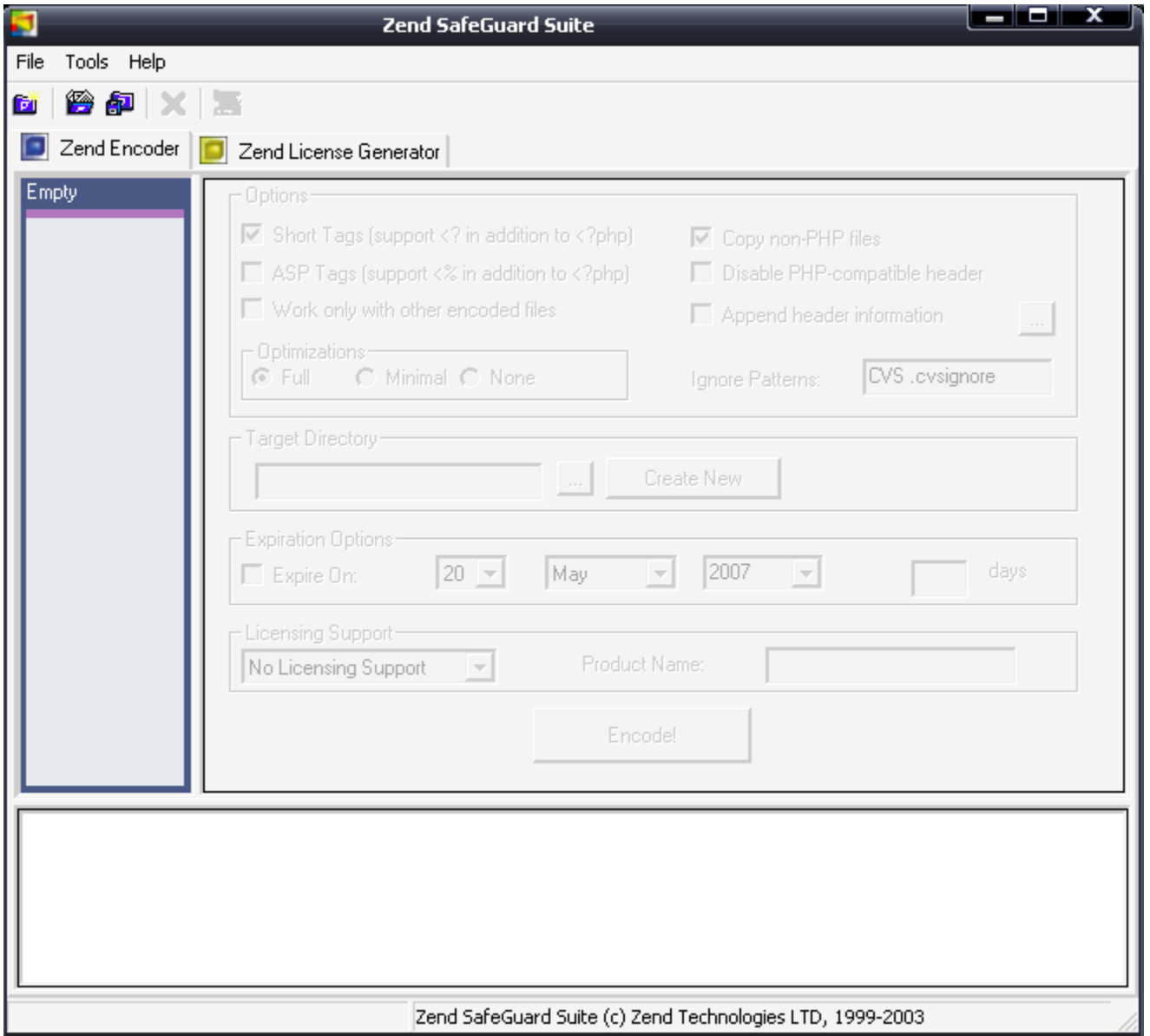
قم ب**تنصيب البرنامج انضر الى الصورة**



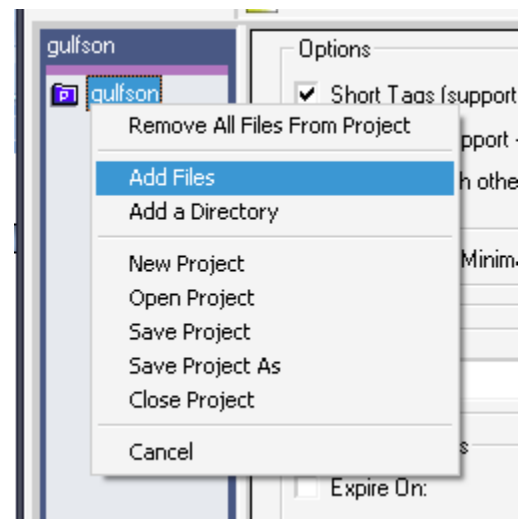
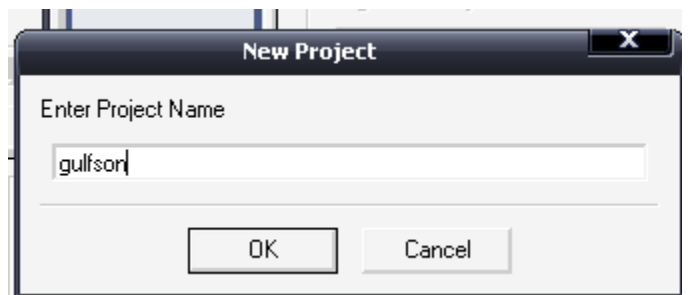
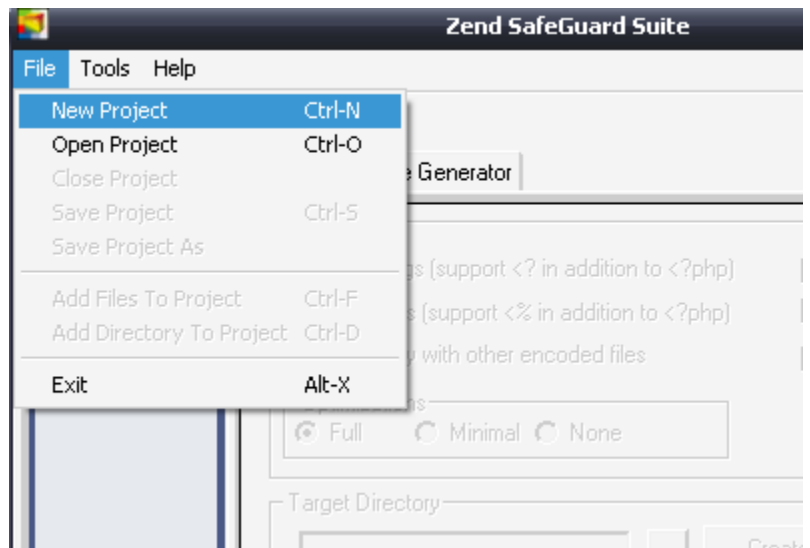
اختر الخيار الثاني بعدها



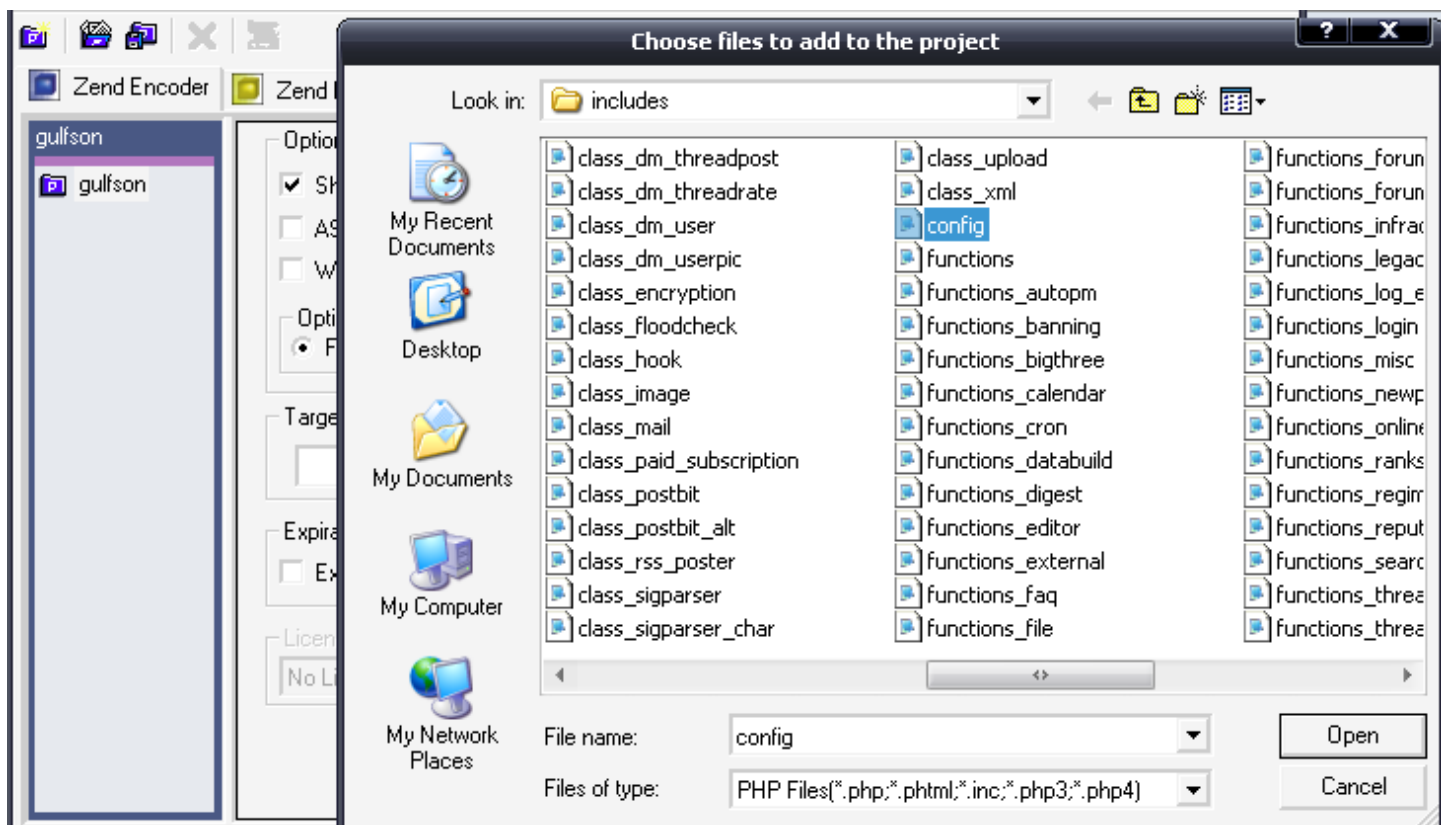
اذهب الى المجلد الذي فتحت الضغط عنه
وبعد الانتهاء من التنصيب ادخل الى البرنامج



اتبع الصور



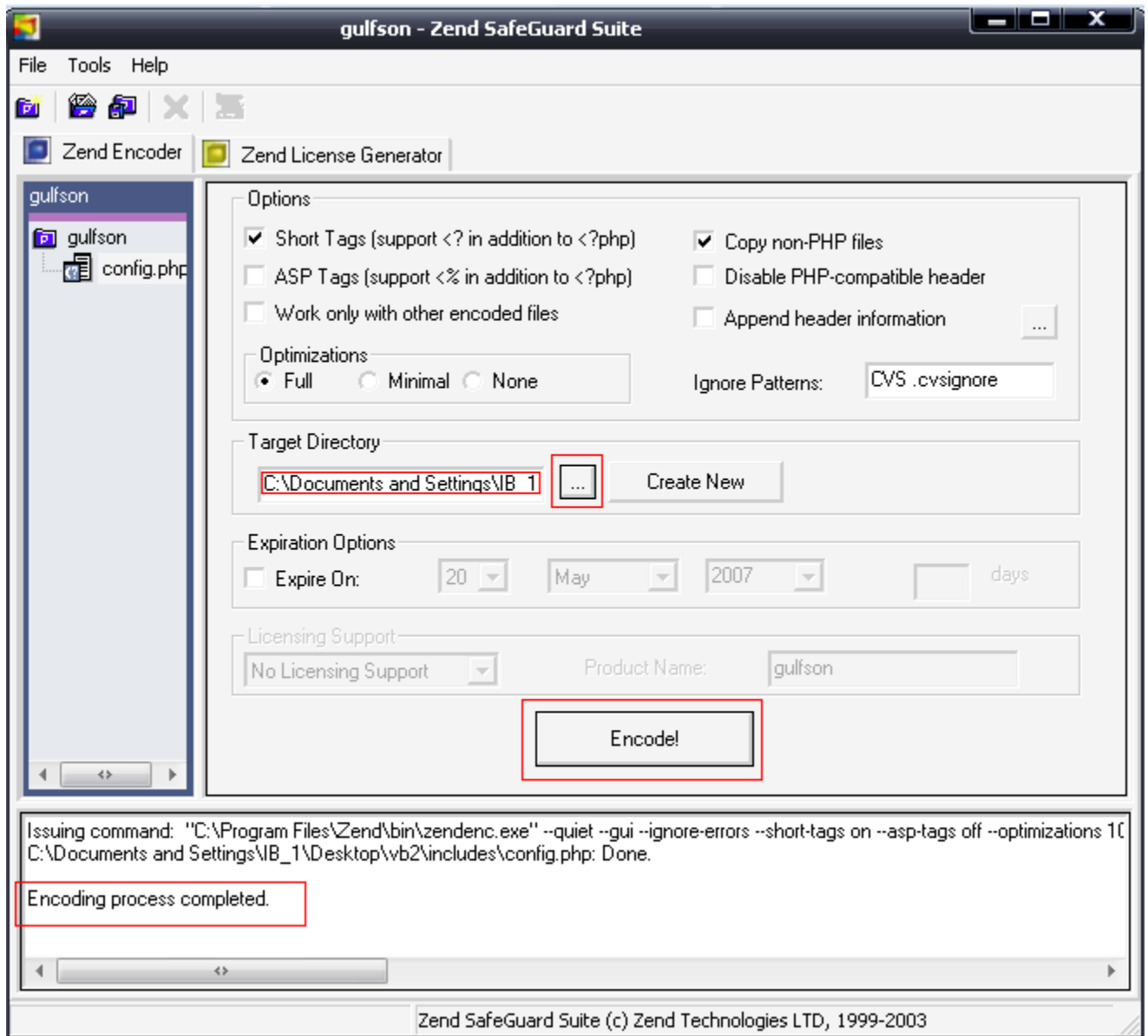
واختار ملف الكونفك



وبعد ما اخترت الملف قم بتحديد مكان حفظ النسخة الجديدة المشفرة من الكونفك (مثلا على سطح المكتب)

واضغط على encode!

وسيتم التشفير وتظهر رسالة بالاسفل كما موضح بالصورة

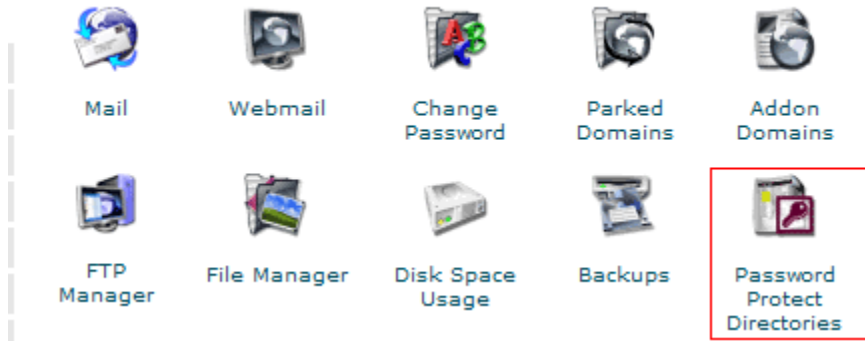


وها قد انتهينا من التشفير

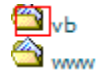
الدرس الثاني وهو وضع جدار ناري للملفات:

حماية مجلدات المنتدى الآتية من السي بنل (admincp - modcp - includes) :

ادخل الى السي بنل وثم اختار



وبعدھا انقر على صورة مجلد الـ VB



وبعدھا انقر على اسم المجلد (admincp - modcp - includes) وليس الصورة (طبعا تعدل عليهم واحد واحد)
وبعد الضغط على الاسم سنتقل الى هذه الصورة

Active Users

iqmasters

Delete User

User Name:

Password:


Add/modify authorized user

Change Password

بعدها



بعدها

 Directory requires a password to access via the web (you must check this to activate password protection).

Protected Resource Name (will display in browser's password mask):

Save

والان انتهينا من الحماية للمجلدات المذكورة.

الدرس الثالث وهو الكلمات الممنوعة:

لتحصين المنتدى من اكواد التحويل وتعطيل كل اكواد الهتمل بكشل كامل والاستغناء عن الكلمات الممنوعه التي تسبب مشاكل بالمنتدى وبنفس الوقت تعمل بظاً

اتبع الشرح التالي

افتح ملف `newthread.php` الموجود بمجلد المنتدى الرئيسي

وابحث عن

رمز:

```
$newpost['title'] =& $vbulletin->GPC['subject'];
```

اضف تحته بشكل مباشر

رمز:

```
if (preg_match('/<|>/', $newpost['title'])) {  
$newpost['title'] = str_replace(array("<", ">"), array("&lt;", "&gt;"), $newpost['title']);  
}
```

وهو من صنع ادمن (Gulfsun)

الدرس الرابع وهو مسح رقم الاصداره اسفل المنتدى:

توجه الى لوحة التحكم وبعدها الى البحث في العبارات وبعدها ابحث عن العبارة التالية

كود:PHP

Powered by vBulletin Version {1}
Copyright ©2000 -
{2}, Jelsoft Enterprises Ltd.

واستبدالها بالتالي:

كود:PHP

Powered by vBulletin
Copyright ©2000 - {2}, Jelsoft Enterprises Ltd.

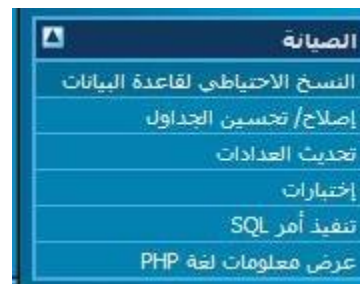
- وكذلك لاتنسى حذف مجلد الانستول نهائيا
- والباسورد الذي ستستعمله يجب ان يكون مؤلف من رموز (*%^&\$%#@)
- واخذ باك اب دوري كل اسبوع (وسنشرح الطريقة)

الدرس الرابع وهو اخذ باك اب للمنتدى بطريقتين:

يعد الباك اب من اهم الطرق للحفاظ على موقعك في حال تعرضه لاي اختراق او تخريب وسنشرح طريقة اخذ الباك اب عن طريق لوحة التحكم والسي بنل

(a) اخذ باك اب عن طريق لوحة التحكم المنتدى

توجه الى لوحة التحكم واتبع التعليمات على الصورة



بعدها نحدد نعم لكل

النسخ الاحتياطي لقاعدة البيانات

مساعدة ?

النسخ الاحتياطي لقاعدة البيانات

نسخ قاعدة البيانات عن طريق PHP فقط يستحسن في حالة قواعد البيانات الصغيرة إذا يمكن أن يتم إيقاف العملية بسبب الخروج عن الوقت المحدد. الحفظ أو النسخ الاحتياطي إلى المزود عن طريق سطر الأوامر موثوق أكثر.

مساعدة ?

حدود قاعدة البيانات للإدراج في النسخ الاحتياطي

اسم الحدود	نعم الكل	الكل لا
access	<input checked="" type="radio"/>	<input type="radio"/>
adminhelp	<input checked="" type="radio"/>	<input type="radio"/>
administrator	<input checked="" type="radio"/>	<input type="radio"/>
adminlog	<input checked="" type="radio"/>	<input type="radio"/>
adminmessage	<input checked="" type="radio"/>	<input type="radio"/>
adminutil	<input checked="" type="radio"/>	<input type="radio"/>
announcement	<input checked="" type="radio"/>	<input type="radio"/>
announcementread	<input checked="" type="radio"/>	<input type="radio"/>
attachment	<input checked="" type="radio"/>	<input type="radio"/>
attachmentpermission	<input checked="" type="radio"/>	<input type="radio"/>
attachmenttype	<input checked="" type="radio"/>	<input type="radio"/>
attachmentviews	<input checked="" type="radio"/>	<input type="radio"/>

وعندما تضغط على اذهب سيتم تحميلها لجهازك

<input type="radio"/>	نعم	7	userpromotion
<input type="radio"/>	نعم	7	usertextfield
<input type="radio"/>	نعم	7	usertitle
<input type="radio"/>	نعم	7	word
<input type="radio"/>	نعم	7	postindex

مساعدة النسخ الاحتياطي لقاعدة البيانات في ملف على المزود

تحذير: مسار الملف المحدد هنا سيحفظ النسخة الاحتياطية ضمن جذر الويب، هذا يعني بأن أي شخص يمكن أن يحمّله. ننصح بتحديد موقع أكثر أمناً لتخزين نسخك الاحتياطية.

المسار واسم الملف لحفظ النسخ الاحتياطي إليه: **forumbackup-04-18-2007-e6813.sql/.** (مزدك (server) يجب أن يكون قادراً على الكتابة في هذا المجلد (عادة تغيير التراخيص إلى 0777)

والطريقة الأخرى الشائعة – اذهب لمجلد **admincp** واعطه التصريح 777 وفي بعض الأحيان لاتحتاج لهذا التصريح وبعدها انزل اكثر الى الاسفل بنفس الصفحة في لوحة التحكم واضغط على حفظ

```

جاري تنفيذ العملية على : holiday
جاري تنفيذ العملية على : icon
جاري تنفيذ العملية على : imagecategory
جاري تنفيذ العملية على : imagecategorypermission
جاري تنفيذ العملية على : language
جاري تنفيذ العملية على : mailqueue

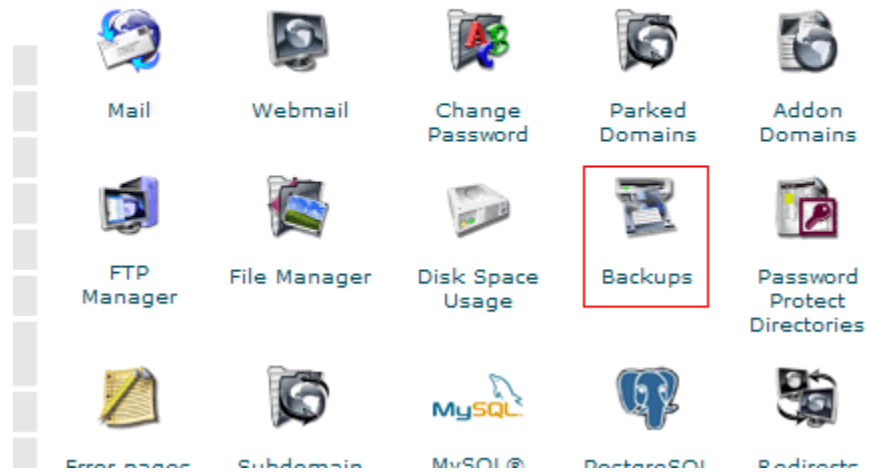
```

وستحفظ في مجلد الـ VB وبعدين حملها على جهازك اذا كنت ترغب او انقلها لمجلد مخصص لحفظ النسخة ولاتنسى وضع الحماية عليه ويجب ان تظهر رسالة بالاخير تقول تم النسخ بنجاح وبعدها نرجع التصريح لـ 755

(b) اخذ باك اب عن طريق السي بنل

وهي تتميز بكونها شاملة اي باك اب للموقع كله توجه الى cpanel وتابع الصورة

Update your contact information here.



تابع

Full Backup

[Generate/Download a Full Backup](#)

اضغط هنا

Full backups can only be used for moving your account to another server or keeping a local copy of your account

Home Directory

Download a home directory Backup

Restore a Home Directory Backup

Download a MySQL Database Backup

test vb1

Restore a MySQL Database

وهناك 3 طرق لاختذ الباك اب وسنأخذ الافضل والاهم

CPANEL 10

Full Backup

Previous full backups saved in home directory:

No Previous Backups

Generate/Download a Full Backup

Backup Destination: Home Directory

Email Address:

Remote Server (FTP/SCP only):

Remote User (FTP/SCP only):

Remote Password (FTP/SCP only):

Port (FTP/SCP only)

Remote Dir (FTP/SCP only)

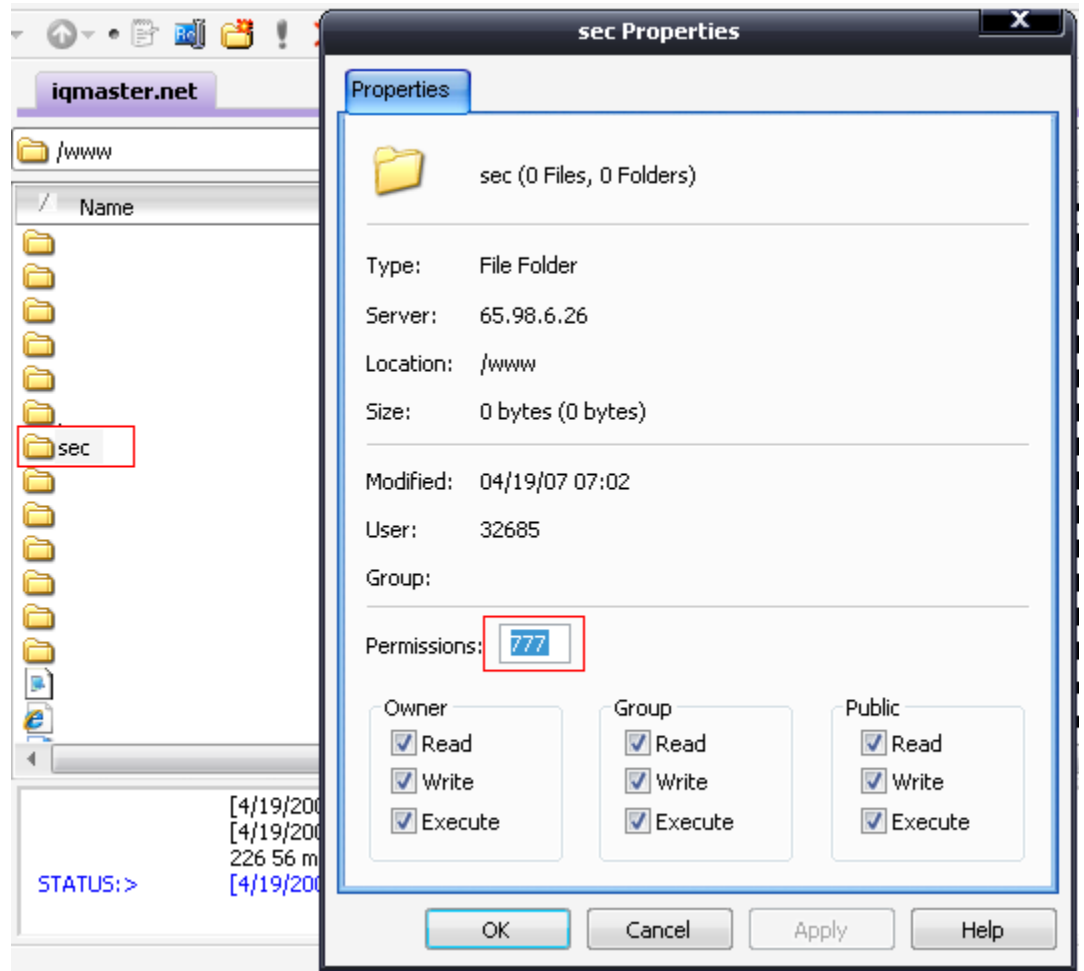
[Go Back]

وسرّصك رساله على البريد تخبرك بأنه تم اخذ الباك اب للموقع
وستجدها بالموقع ونهاية الملف tar.gz

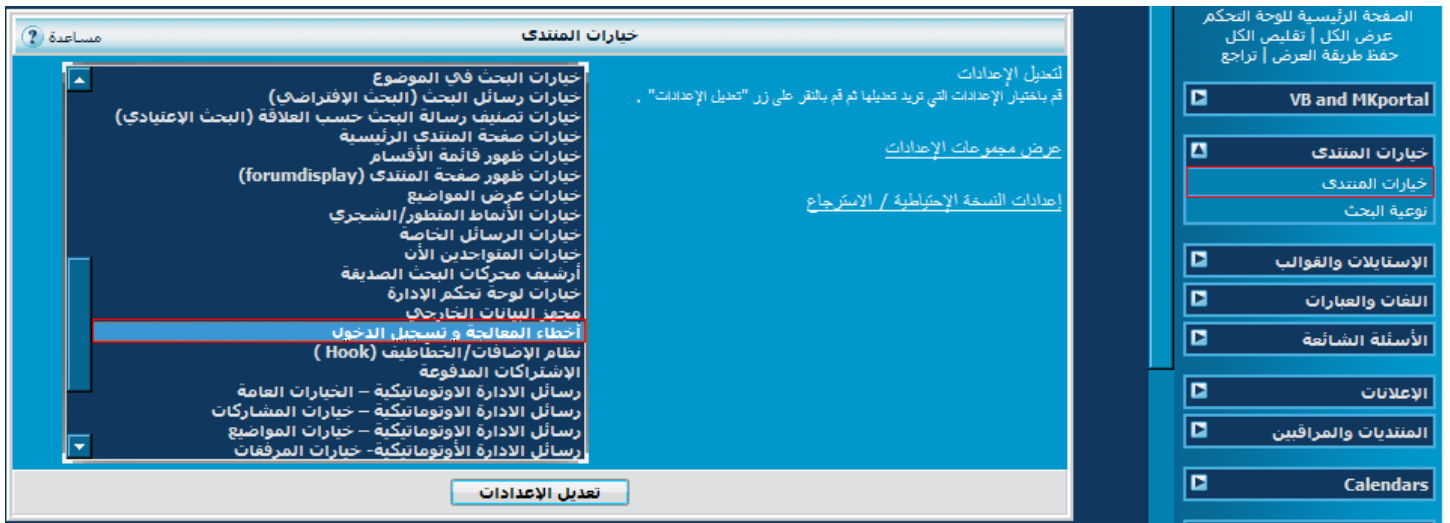
■ والافضل تحميل الباك اب لجهازك حتى لاتسرق او وضعها في مجلد خاص محمي

الدرس الخامس وهو مراقبة من يحاول دخول لوحة التحكم:

افتح مجلد الـ VB باي برنامج FTP وقم بوضع مجلد جديد باي اسم مثلا sec واعطه التصريح 777 وذلك بضغط رايت كليك على المجلد وثم تختار
CHMOD



بعدها توجه الى لوحة تحكم المنتدى واختار خيارات المنتدى ثم اخطاء المعالجة وتسجيل الدخول



وفي اول فراغ قم بكتابة مسار الملف

مساعدة ? أخطاء المعالجة و تسجيل الدخول

تسجيل أخطاء قاعدة البيانات في ملف

إذا كنت تريد تسجيل كافة أخطاء قاعدة البيانات في ملف، أدخل المسار إلى الملف هنا. سوف يتم حفظ الملف على الشكل {filename}.log.

الرجاء لاحظ بأن المجلد الذي سيتم إنشاء الملف به يجب أن يكون قابل للكتابة من قبل المزود.

تسجيل فشل الدخول إلى لوحة تحكم الإدارة في ملف

إذا كنت تريد تسجيل كافة المحاولات الفاشلة لدخول لوحة تحكم الإدارة إلى ملف، أدخل

وبذلك ستصلك معلومات عند ادخال اي باسورد بالخطأ في لوحة التحكم

الدرس السادس وهو إخفاء ملفات موقعك عن العيون:

افتح ملف تكست في جهازك وضع بداخله الكلمات الموجودة بالاسفل وسمي اسم التكتست robots وارفعه لمجلد المنتدى وتستطيع ان تستعمله لإخفاء اي مجلد اخر

```
User-agent: Mediapartners-Google*
Disallow:
User-agent: *
Disallow: admincp.php
Disallow: /admincp/index.php
Disallow: /images/
Disallow: /includes/
Disallow: /includes/cron/
Disallow: /includes/datastore/
Disallow: /includes/paymentapi/
Disallow: /includes/xml/
Disallow: /massy/
Disallow: /modcp/index.php
Disallow: /install/
Disallow: /customprofilepics/
Disallow: /customavatars/
Disallow: /cpstyles/
Disallow: /clientscript/
Disallow: /archive/
```

```
Disallow: /cron/  
Disallow: /datastore/  
Disallow: /paymentapi/  
Disallow: /xml/  
Disallow: /modcp/
```

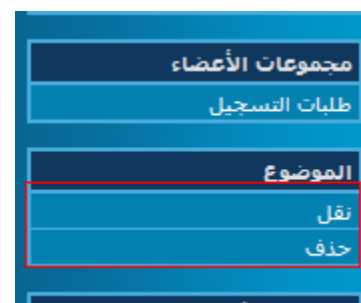
الدرس السادس وهو سكرابت الخطاء:

وهو يقوم بتوجه الزائر من الصفحة الخطاء الى المكان الذي تريده وانت تتحكم بالصفحات مثل اضافة كتابة بانها الصفحة الخطاء ووضع رابط او تحويل تلقائي للتركيب اتبع التعليمات

- ❖ حمل الملف من [هنا](#)
- ❖ عدل على ملف **error.php** كما مذكور بداخله
- ❖ عدل على ملف **htaccess**. باي محرر وضع عنوان موقعك
- ❖ حمل مجلد **err** الى موقعك
- ❖ ضع ملف **htaccess**. في مجلد منتدك الرئيسي واذا كان موجود افتحه واضف ما بداخل **htaccess**. الي في جهازك الى ما كان موجود بموقعك

الدرس السادس وهو حماية المنتدى من مراقبيك:

اذا كنت لاتثق باحد المراقبين او حصل خلاف فالافضل ان تعمل التالي لان هناك خيار حذف كل مواضيع المنتدى من لوحة تحكم المراقبين



توجه الى [vb/modcp/thread.php](#) وقم بتغير اسم هذا الملف **thread.php**

الدرس السادس وهو حماية قوية بواسطة CrackerTracker :

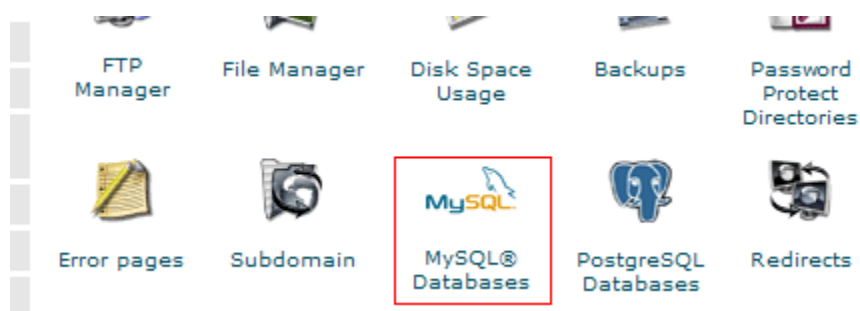
هاك قوي جدا يحمي منتدك من اي عملية سكرت ويحتوي على ملف **log_fileinjects.txt** و **counter.txt** تسجل به كل عمليات الاختراق مع الاي بي

- ❖ حمل الملف من [هنا](#)
- ❖ ادخل الى مجلد موقعك وارفع له مجلد **elog** واعط الملفين الموجودين بداخله تصريح 666
- ❖ وبعدها ارفع المنتج من لوحة تحكم المنتدى وبذلك يتم التركيب بنجاح

دروس مفيدة في حال اختراق او تعطل المنتدى

الدرس السادس وهو استرجاع باسورد الادمن اذا انسرق:

افتح السي بنل واتبع الصور



بعدها

Access Hosts:

localhost

Host (% wildcard is allowed):

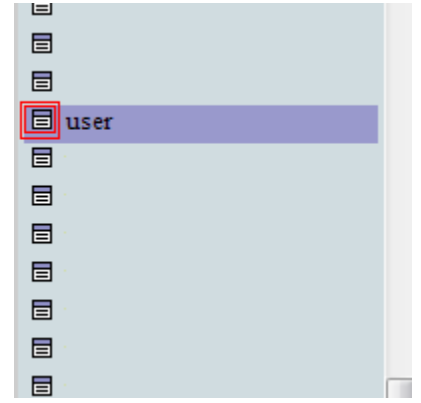
Add Host

phpMyAdmin















You can use phpMyAdmin to administer your MySQL databases in a web based environment.

[Go Back]

بعدها اختر قاعدة بيانات منتدك ثم اختر منها **user**



وستلاحظ الاسم والباسورد قم بحفظه عندك وفي حال اختراقك اضغط على علامة القلم

		userid	usergroupid	membergroupids	displaygroupid	username	password
 		1	6		0	IQmasters	i9f60ba'
 		2	10		0	moon light	t22cb0
 		3	7		7	ᐃáá äĩÑæí	7: :930e68a
 		4	2		0	bishbish	051765
 		12	2		0	khattab	9447bcf
 		5	6		0	BebO_IRQ	1846f9
 		6	2		0	ammar tiger	e74a64

وبعدها

- ✓ ادخل لموقعك ببرنامج FTP وغير تصريح مجلد المنتدى (vb) الى 751 وذلك بضغط رايت كليك على المجلد وبعدها اختار CHMOD وقم بالتعديل هناك وكرر هذا التصريح على جميع الملفات التي لاتحتاج الى تصريح 777 (ولاكن احفظ تصاريح المجلدات القديمة حتى اذا اخطئت بها تستطيع ان ترجعها)
- ✓ قم بفحص المنتدى عند انتهائك من اي درس حتى ترى اذا كان يعمل بشكل جيد

MBSMGROUP PC SOFT 2008
Thanks for gulfson.com