ITSecTeam
IT Security Research & Penetration Testing Team

راهنمای استفاده از Havij 1.15

تیم تحقیقات امنیت و تست نفوذ آی تی
http://ItSecTeam.com

تهیه کننده:
r3dm0v3

www.ITSecTeam.com

ITSecTeam
IT Security Research & Penetration Testing Team

امکانات جدید

قابلیت ها

نصب

- **نرم افزار هویج چیست؟**
- **تزریق SQL یا SQL Injection چیست؟**
- **چه کسی باید از هویج استفاده کند؟**
- **نصب هویج**
- **حذف هویج**
- **رجیستر کردن برنامه**
- **بررسی وجود نسخه ی جدید**

شروع به کار

- **شروع سریع استفاده از هویج**
- **ذخیره و بازیابی اهداف**
- **دریافت اطلاعات (Info)**
- **استخراج اطلاعات جداول و دیتابیس ها**
  - استخراج اطلاعات
  - اعمال فیلتر بر روی دریافت اطلاعات
  - شروع دریافت اطلاعات از سطر دلخواه
  - استفاده از Group_Concat
  - دریافت اطلاعات یک سطر به صورت یکجا
  - ذخیره ی اطلاعات
  - تغییر اطلاعات یک سطر
  - حذف یک سطر
  - ایجاد یک سطر جدید
- **خواندن فایل ها**
- **اجرای دستورات سیستمی بر روی هدف**
- **پرس و جو (Query)**
- **پیدا کردن صفحه ی ورود مدیر**
- **کرک کردن پسوردهای MD5**

www.ITSecTeam.com

ITSecTeam
IT Security Research & Penetration Testing Team

تزریق به روش دستی

- **تعیین دیتابیس**
- **تعیین نوع متغییر**
- **تعیین کلمه ی کلیدی**
- **تعیین Syntax**
- **تعیین Syntax برای تزریق به روش چشم بسته (Blind)**
- **تعیین روش (Method)**
- **تزریق در فرم ها (متد POST)**

تنظیمات

- **تنظیمات ابتدایی**
  - تنظیم استفاده از پروکسی
  - تغییر فاصله (Space) در تزریق
  - نمایش تزریق های انجام شده
  - تزریق در صفحات URL Rewrite
  - تزریق در کوکی، user-agent و ...
- **تنظیمات پیشرفته**
  - برای تزریق به احراز هویت نیاز است!
  - تعیین کاراکترها برای تست در تزریق چشم بسته
  - تغییر هدر (Header) ها در تزریق
  - Time out
  - مقدار پیش فرض برای تزریق
  - Avoid using strings
  - Bypass illegal union
  - Try different syntaxes in union injection
  - Follow redirections
  - Column count
  - Do not find columns count in MsSQL with error
  - Bypass mod_security
  - Bypass WebKnight
  - جایگزینی عبارات دلخواه در تزریق
  - Time based method delay
  - Blind table prefix
  - Blind column prefix

www.ITSecTeam.com

ITSecTeam
IT Security Research & Penetration Testing Team

- Table list for blind guessing
- Column list for blind guessing

forum.ITSecTeam.com

ITSecTeam
IT Security Research & Penetration Testing Team

امکانات جدید

1. بایپس کردن WebKnight اضافه شد.
2. بایپس کردن mod_security بهتر شد.
3. پشتیبانی از Unicode اضافه شد.
4. یک روش جدید برای پیدا کردن جداول و ستون ها در MsSQL اضافه شد.
5. امکان ادامه دادن استخراج جداول و ستون ها اضافه شد.
6. امکان جایگزینی دلخواه عبارات در تزریق ها اضافه شد.
7. امکان تغییر مقدار پیش فرض برای تزریق هنگام استفاده از %Inject_Here% اضافه شد.
8. امکان تعیین پیشوند برای جداول و ستون ها در حالت چشم بسته (Blind) اضافه شد.
9. امکان استفاده از لیست جداول و ستون های دلخواه اضافه شد.
10. امکان تنظیم Time out فراهم شد.
11. یک سایت کرکر جدید اضافه شد.
12. رفع اشکال: یک مشکل در مرتبط با دستور SELECT
13. رفع اشکال: پیدا کردن ستون رشته ای
14. رفع اشکال: دریافت اطلاعات چندین ستون در MsSQL
15. رفع اشکال: پیدا کردن تعداد ستون ها در MySQL
16. رفع اشکال: syntax اشتباه در تزریق از نوع رشته ای در Access
17. رفع اشکال: نتایج مثبت اشتباه حذف شدند
18. رفع اشکال: دریافت اطلاعات در صفحات url-encode شده
19. رفع اشکال: بارگذاری پروژه های ذخیره شده
20. رفع اشکال: تعدادی خطا در دریافت اطلاعات در MsSQL
21. رفع اشکال: یک مشکل در Access هنگام حدس زدن جداول و ستون ها
22. رفع اشکال: یک مشکل هنگام استفاده از پروکسی
23. رفع اشکال: مشکل فعال سازی remote desktop در ویندوز 2008
24. رفع اشکال: نتایج غلط در پیدا کردن تعداد ستون ها
25. رفع اشکال: هنگامی که روش مبتنی بر خطا در MsSQL با شکست مواجه می شود
26. رفع اشکال: یک مشکل در ذخیره ی اطلاعات
27. رفع اشکال: مشکل تشخیص دیتابیس Oracle و PostgreSQL

www.ITSecTeam.com

ITSecTeam
IT Security Research & Penetration Testing Team

قابلیت ها

موارد	نسخه ی رایگان	نسخه ی حرفه ای
1. دیتابیس های مورد پشتیبانی همراه با روش های تزریق:	✓	✓
a. MsSQL 2000/2005 with error	✓	✓
b. MsSQL 2000/2005 no error union based	✓	✓
c. MsSQL Blind	✗	✓
d. MsSQL time based	✗	✓
e. MySQL union based	✓	✓
f. MySQL Blind	✓	✓
g. MySQL error based	✓	✓
h. MySQL time based	✓	✓
i. Oracle union based	✓	✓
j. Oracle error based	✗	✓
k. PostgreSQL union based	✗	✓
l. MsAccess union based	✓	✓
m. MsAccess Blind	✗	✓
n. Sybase (ASE)	✓	✓
m. Sybase (ASE) Blind	✗	✓
2. پشتیبانی از HTTPS	✗	✓
3. پشتیبانی از پروکسی	✓	✓
4. تشخیص خودکار دیتابیس	✓	✓
5. تشخیص خودکار نوع متغییر (عدد یا رشته)	✓	✓
6. تشخیص خودکار کلمه ی کلیدی (پیدا کردن تفاوت بین پاسخ مثبت و منفی)	✓	✓
7. امتحان گرامر (syntax) های مختلف تزریق	✓	✓
8. تنظیمات برای جایگزین کردن فاصله (space) با ...,+,**/در مقابل IDSیا فیلتر ها	✓	✓
9. عدم استفاده از رشته ها (دور زدن فیلتر های مشابه (magic_quotes	✓	✓
10. امکان وارد کردن گرامرهای تزریق بصورت دلخواه	✓	✓
11. امکان اجرای query دلخواه با قابلیت نمایش نتیجه	✗	✓
12. دور زدن مشکل illegal union	✓	✓
13. قابلیت انتخاب هدر های http بصورت دلخواه (مانند referrer و user-agent)	✓	✓

ITSecTeam
IT Security Research & Penetration Testing Team

14. بازخوانی کوکی از سایت برای احراز هویت	✓	✓
15. احراز هویت به روش Http Basic و Digest	✓	✓
16. تزریق در صفحات URL Rewrite	✗	✓
17. دور زدن فایروال mod_security و فایروال های مشابه	✗	✓
18. دور زدن فایروال WebKnight و فایروال های مشابه	✗	✓
19. نتیجه ی real time	✓	✓
20. حدس زدن جدول ها و ستون ها در (mysql<5همچنین در (blindو MsAccess	✓	✓
21. گرفتن سریع جدول ها و ستون ها برای mysql	✓	✓
22. ادامه دادن دریافت جداول و ستون ها	✗	✓
23. اجرای دستورات SQL در دیتابیس Oracle	✗	✓
24. جایگزینی عبارات دلخواه در تزریق ها	✗	✓
25. قابلیت All in one request برای گرفتن همزمان یک سطر از اطلاعات با هر تعداد ستون	✗	✓
26. امکان ذخیره مستقیم اطلاعات در فایل با فرمتdump	✗	✓
27. امکان ذخیره مستقیم اطلاعات در فایل با فرمتXML	✗	✓
28. امکان نمایش اینجکشن های انجام شده توسط برنامه (Show Requests)	✗	✓
29. اضافه شدن فعال سازی ریموت دسکتاپ	✗	✓
30. روش های متعدد برای استخراج جداول و ستون ها	✗	✓
31. جستجوگر صفحه ی ورود سریع	✓	✓
32. کرکر MD5به صورت آنلاین	✓	✓
33. دریافت اطلاعات DBMS	✓	✓
34. دریافت جداول، ستون ها و اطلاعات	✓	✓
35. اجرای دستور (فقط (mssql	✓	✓
36. خواندن فایل ها ی سیستم (فقط (mysql	✓	✓
37. Insert/update/deleteاطلاعات	✓	✓
38. پشتیبانی از Unicode	✗	✓

ITSecTeam
IT Security Research & Penetration Testing Team

نصب

نرم افزار هویج چیست؟

هویج یک ابزار شناسایی و بهره برداری از آسیب پذیری تزریق SQL یا همان SQL Injection می باشد. هویج این امکان را فراهم می سازد تا تنها با چند کلیک تمام فرایند تست و بررسی وجود آسیب پذیری و همچنین اکسپلویت کردن آن را به صورت خودکار انجام دهید.

تزریق SQL یا SQL Injection چیست؟

تزریق SQL یک آسیب پذیری شایع در وب سایت ها می باشد که ناشی از عدم بررسی کافی بر روی ورودی های کاربر است. در این آسیب پذیری نفوذگر با تزریق جملاتی به دستور SQL نوشته شده توسط برنامه نویس می تواند نتیجه ی پرس و جو (query) را تغییر دهد و دستورات دلخواه خود را اجرا کند. به این کار Exploit کردن این آسیب پذیری می گویند که می تواند منجر به افشای اطلاعات حساس، تغییر اطلاعات، حذف اطلاعات و یا حتی دسترسی کامل به سیستم شود.

چه کسی باید از هویج استفاده کند؟

نرم افزار هویج برای متخصصان امنیت، مدیران سایت ها، برنامه نویسان تحت وب، متخصصان تست نفوذ، علاقه مندان به هک و امنیت و تمامی کسانی که مایلند امنیت سایت خود را مورد آزمایش قرار دهند قابل استفاده است.

www.ITSecTeam.com

ITSecTeam
IT Security Research & Penetration Testing Team

نصب هویج

موارد مورد نیاز برای نصب هویج:

- سیستم عامل ویندوز
- فایل setup برنامه
- Internet Explorer 5.5 یا ورژن بالاتر
- 6MB فضای خالی بر روی دیسک سخت

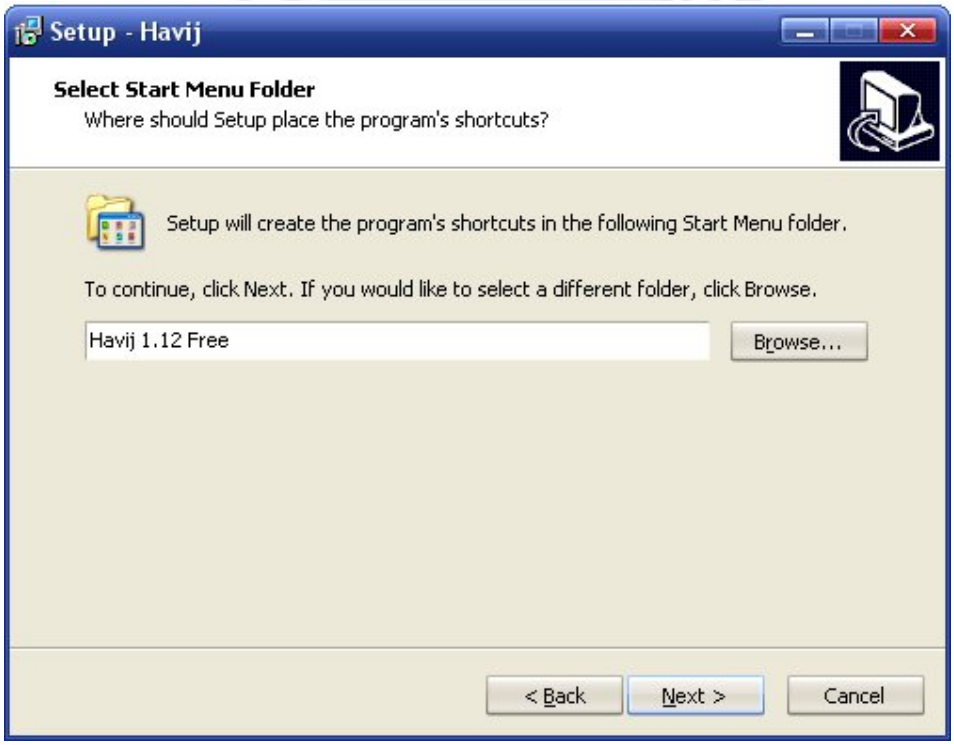
دقت کنید که حتما فایل نصب برنامه را از سایت ItSecTeam.com و یا منبع معتبر دیگری دریافت کرده باشید.

برای شروع نصب فایل setup برنامه را اجرا نمایید. پنجره ی زیر باید نمایش داده شود.

بر روی Next کلیک نموده تا نصب ادامه پیدا کند و صفحه ی زیر نمایش داده شود.

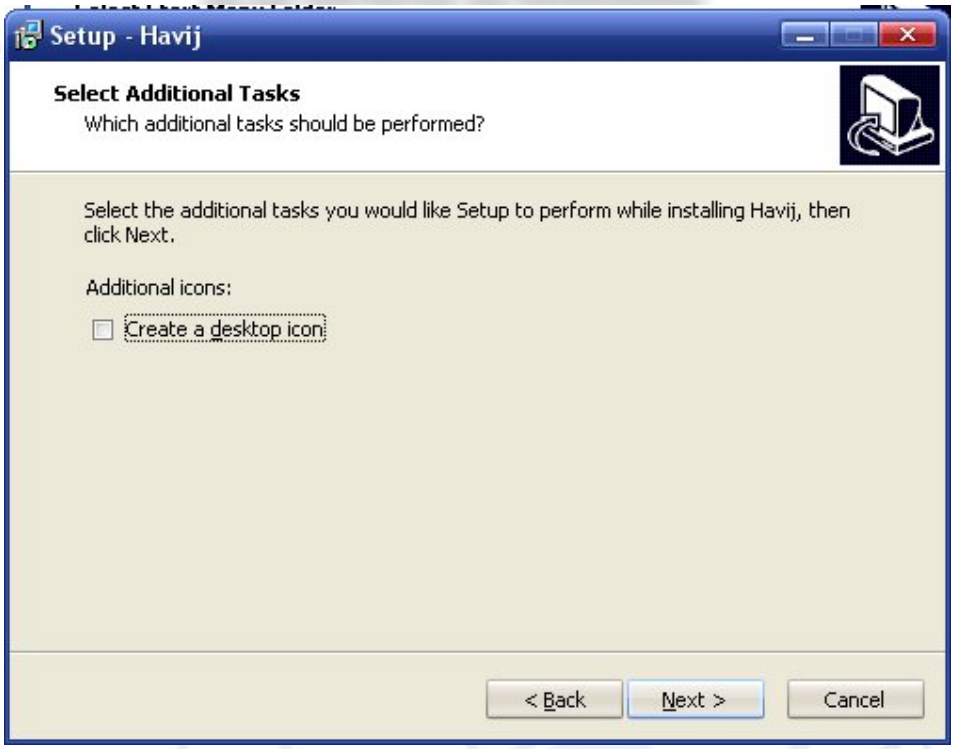
ITSecTeam

در صفحه ی بالا شما باید آدرس محلی را که هویج آنجا نصب خواهد شد وارد کنید، می توانید مسیر پیش فرض را تغییر ندهید و بر روی Next کلیک کنید تا وارد مرحله ی بعد شوید.

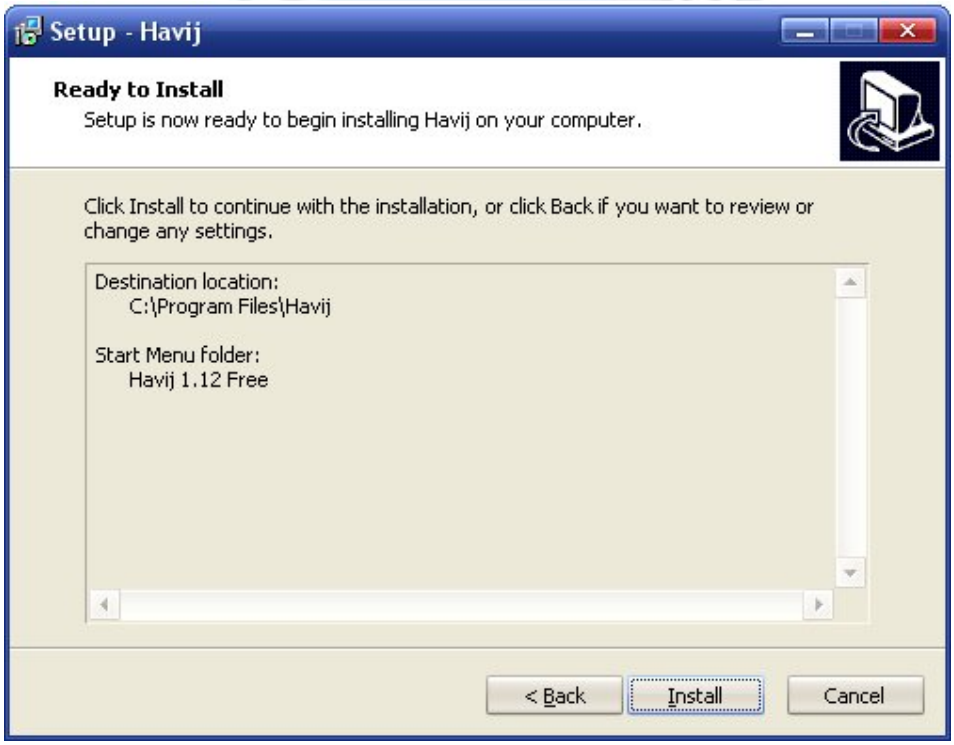


در این مرحله شما باید نام پوشه ای که در Start Menu برای برنامه ایجاد می شود وارد کنید. می توانید این نام را تغییر ندهید و بر روی Next کلیک کنید.

ITSecTeam



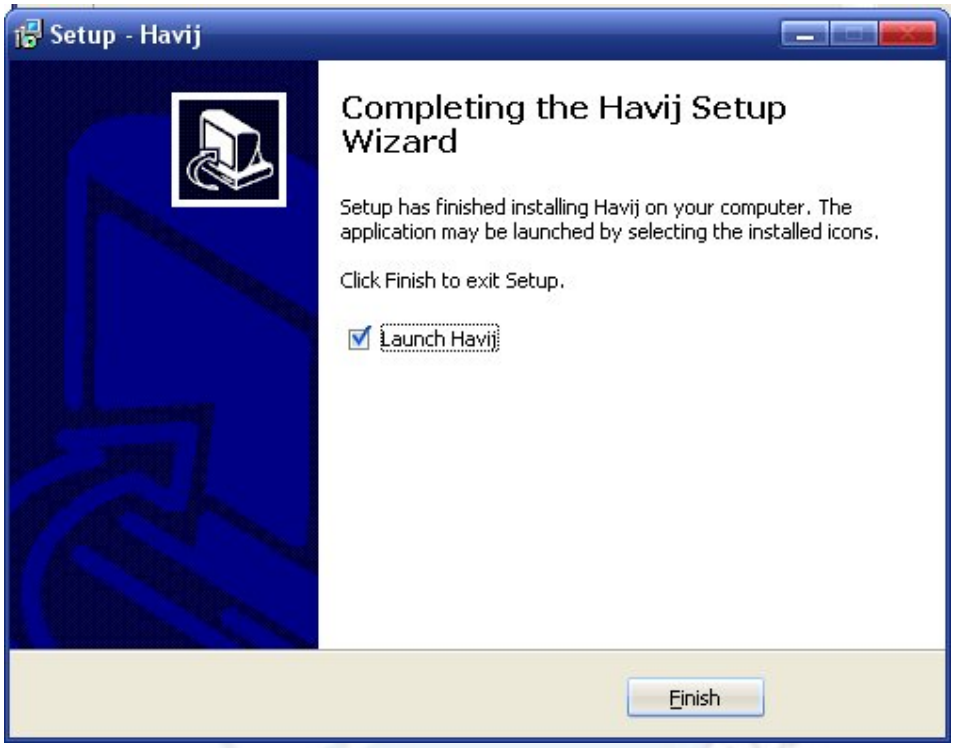
اگر تمایل دارید تا یک میانبر در دسکتاپ ایجاد شود گزینه ی Create a desktop icon را تیک بزنید. با کلیک بر روی Next خلاصه ای از اطلاعات نصب به صورت زیر نمایش داده می شود.



با کلیک بر روی Install نصب آغاز می شود.

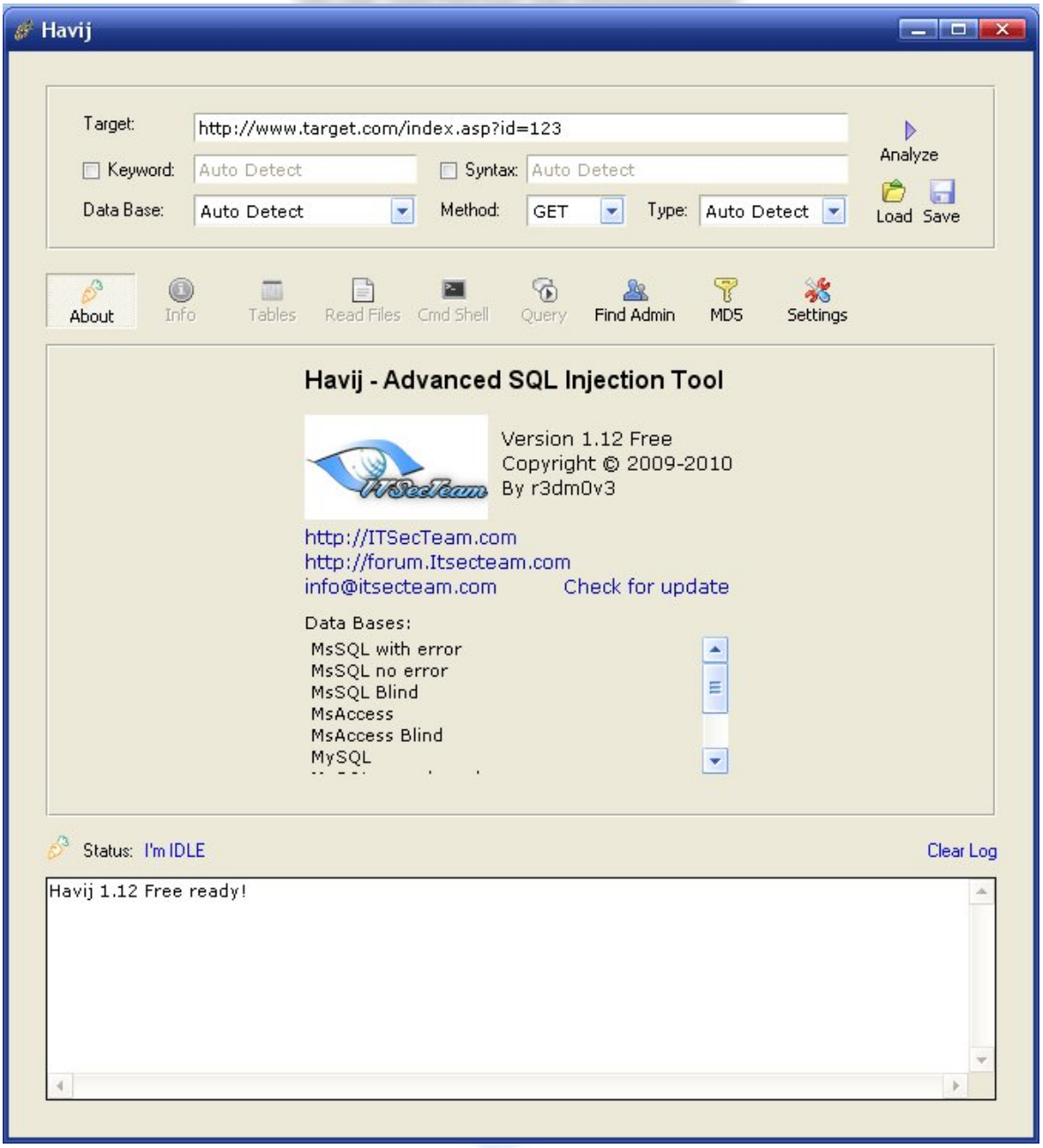
ITSecTeam
IT Security Research & Penetration Testing Team

پس از پایان نصب پنجره ی زیر نمایش داده می شود که این موضوع را به اطلاع شما می رساند.



اگر مایلید تا پس از نصب، برنامه ی هویج را اجرا کنید گزینه ی Launch Havij را تیک بزنید و بر روی Finish کلیک کنید.

ITSecTeam

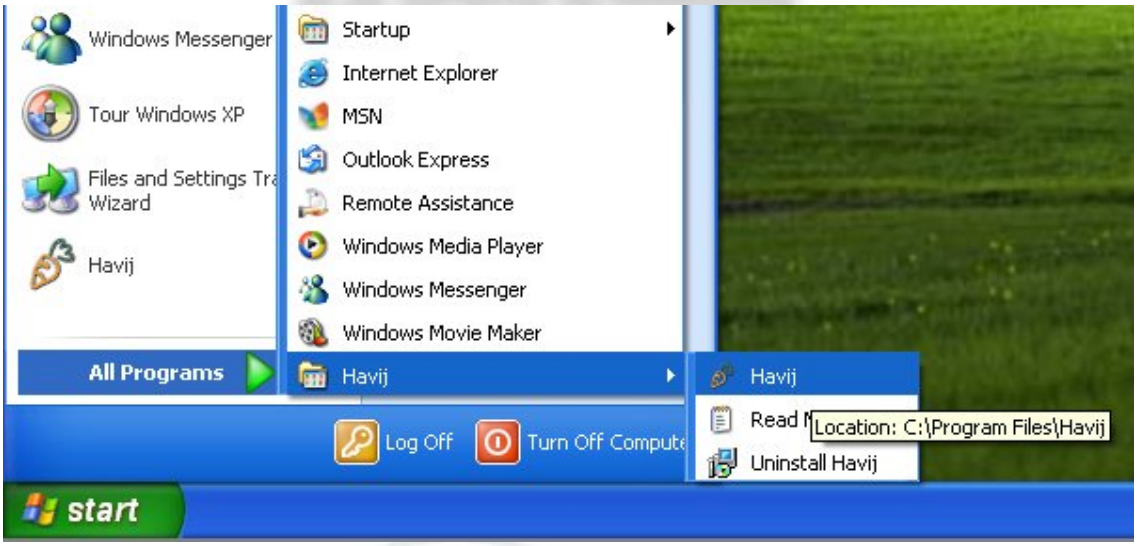


نصب هویج با موفقیت به پایان رسید.

برای اجرای هویج می توانید از منوی Start گزینه ی All Programs یا Program Files را انتخاب کرده و وارد پوشه ی Havij شده و برنامه ی Havij را انتخاب کنید و یا از طریق میانبر برنامه در میز کار (desktop) به هویج دسترسی پیدا کنید.

توجه: نرم افزار هویج برای تزریق در سایتها احتیاج به ارتباط با اینترنت دارد. در صورتی که از برنامه های دیواره ی آتش (Firewall) استفاده می کنید، مجوز دسترسی به اینترنت را به هویج بدهید.

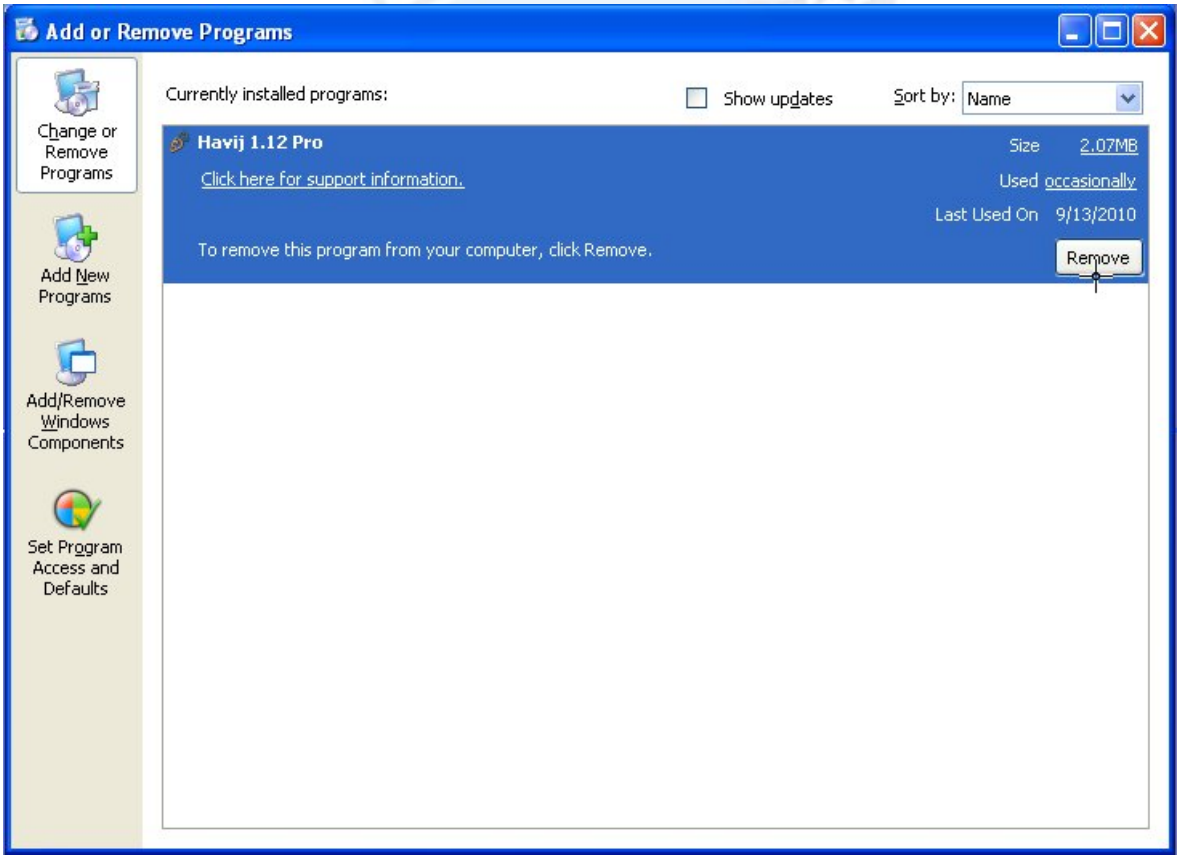
ITSecTeam



مراحل بالا برای تمام نسخه های برنامه یکسان است.

حذف هویج

برای حذف برنامه ی هویج وارد Control Panel شوید و گزینه ی Add or Remove Programs را انتخاب کنید. در لیست برنامه ی Havij را پیدا کنید.



سپس بر روی Remove کلیک کنید. یک سوال از شما پرسیده می شود که آیا می خواهید برنامه را حذف کنید یا خیر، روی Yes کلیک کنید. سپس مراحل حذف به صورت خودکار انجام می شود و در پایان پیغام زیر مبتنی بر اینکه برنامه با موفقیت حذف شد نمایش داده می شود.

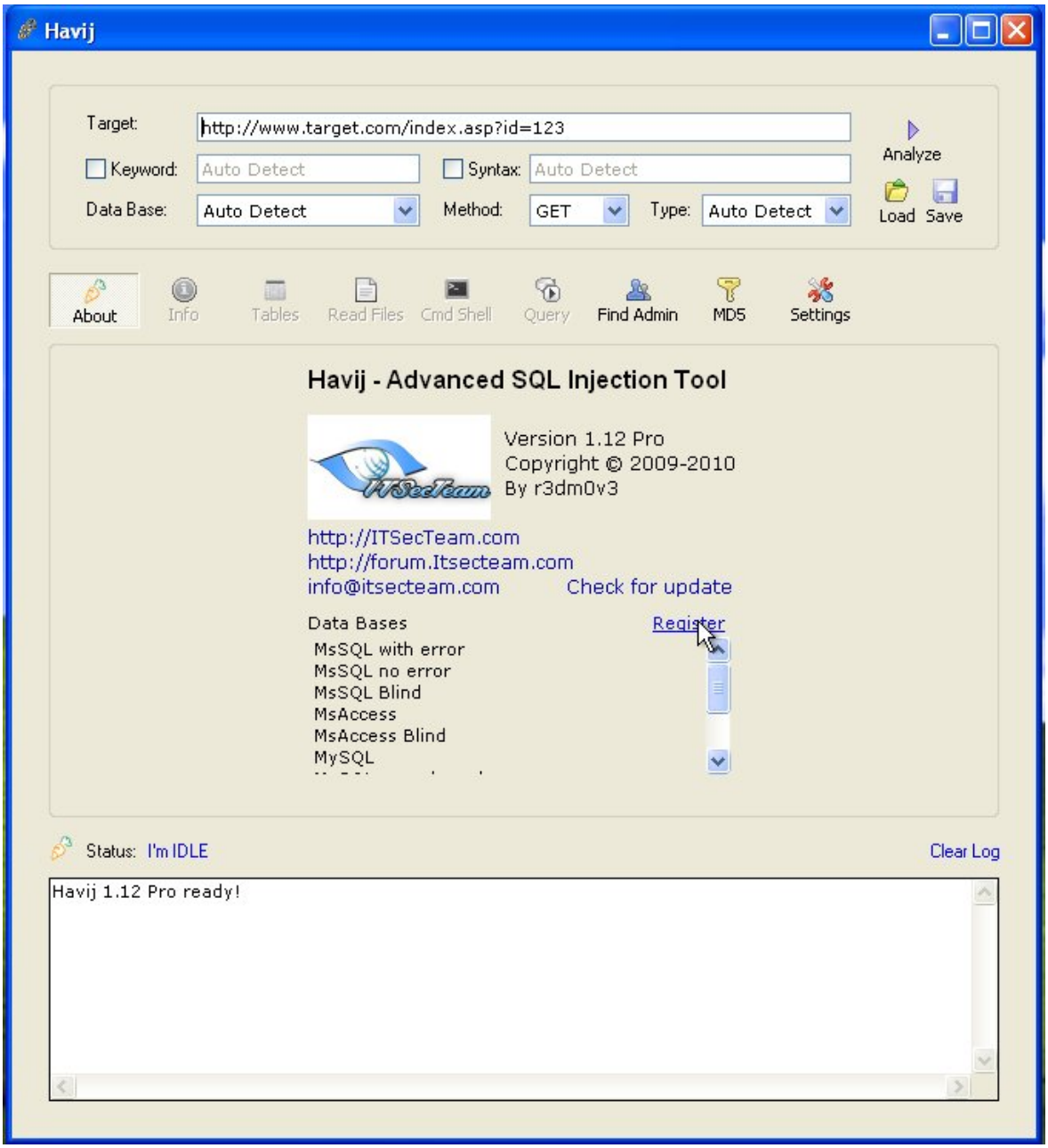
مراحل بالا برای تمام نسخه های برنامه یکسان است.

ITSecTeam
IT Security Research & Penetration Testing Team

رجیستر کردن برنامه

برای رجیستر کردن برنامه شما ابتدا باید یک مجوز خریداری کنید برای جزئیات خرید به آدرس info@itsecteam.com ایمیل بزنید. پس از دریافت مجوز مراحل زیر را در نسخه ی حرفه ای برنامه دنبال کنید تا برنامه را رجیستر کنید.

1- به اینترنت وصل شوید.
2- در قسمت About برنامه بر روی Register کلیک کنید.

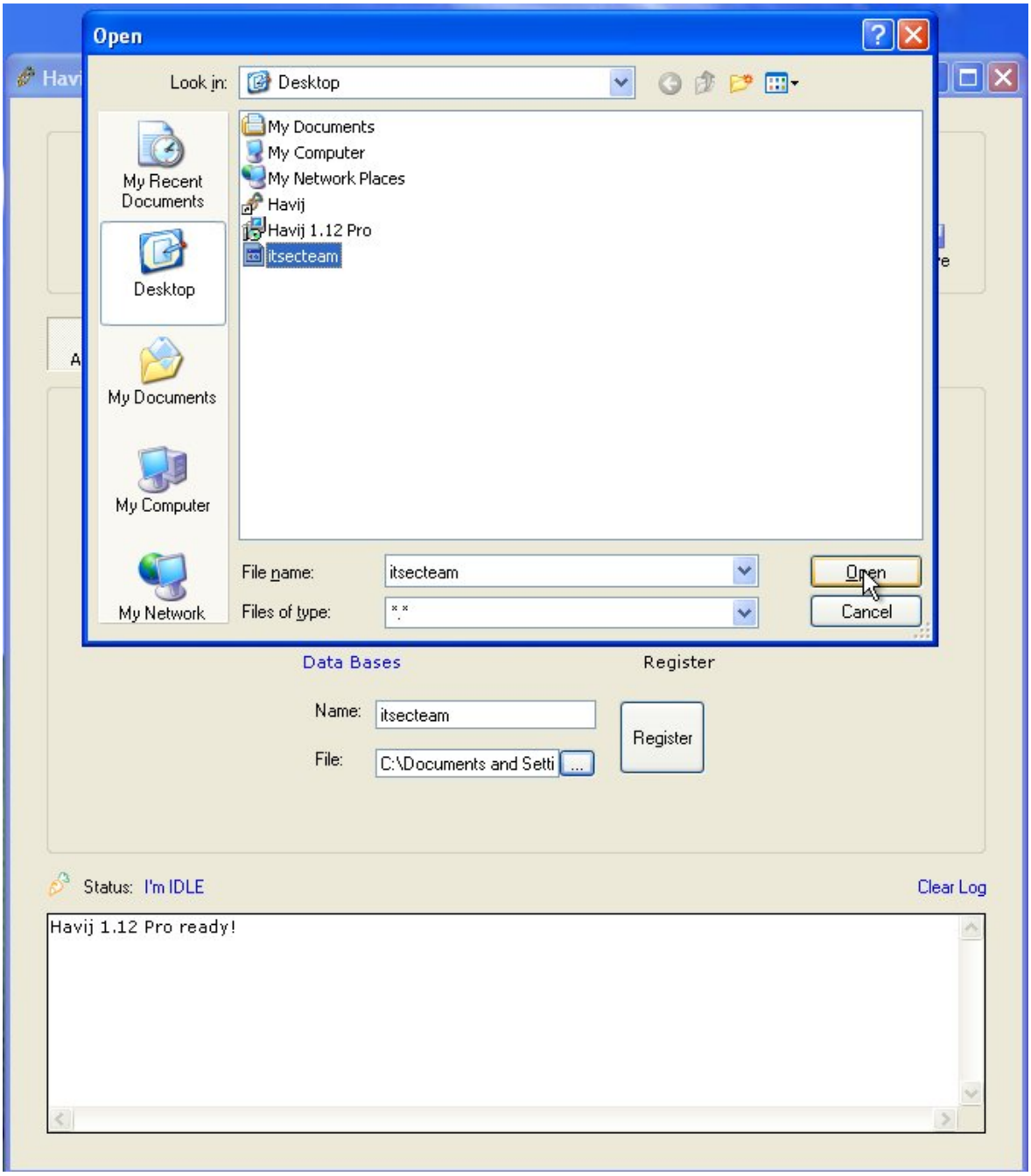


3- در قسمت Name نامی را که در مجوز ثبت شده است وارد کنید. (حروف کوچیک یا بزرگ تاثیری ندارد)

ITSecTeam
IT Security Research & Penetration Testing Team

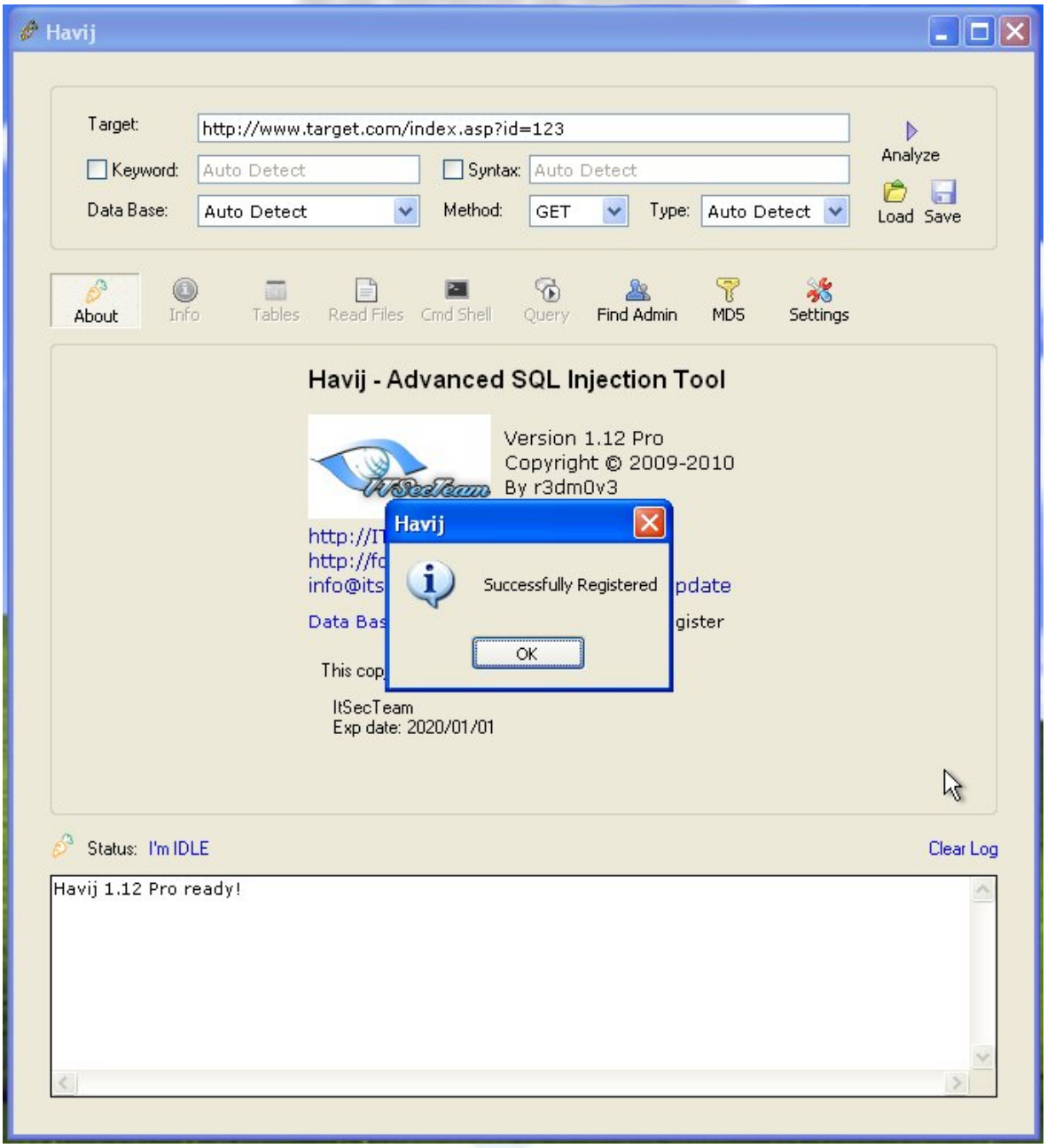
4- در قسمت File آدرس فایل مجوز را وارد کنید.

توجه: هر دوی این مشخصات بعد از خرید مجوز برای شما ارسال خواهند شد.



5- حالا بر روی Register کلیک کنید و منتظر بمانید تا مراحل اعتبارسنجی مجوز به اتمام برسد. در صورت صحیح بودن مشخصات پیغام زیر نمایش داده می شود.

ITSecTeam



توجه: در صورتی که از برنامه های دیواره ی آتش (Firewall) استفاده می کنید، مطمئن شوید که برنامه ی هویج اجازه ی دسترسی به اینترنت را داشته باشد. در صورت بروز مشکل دیوار آتش خود را غیر فعال کرده و دوباره مراحل را تکرار کنید.

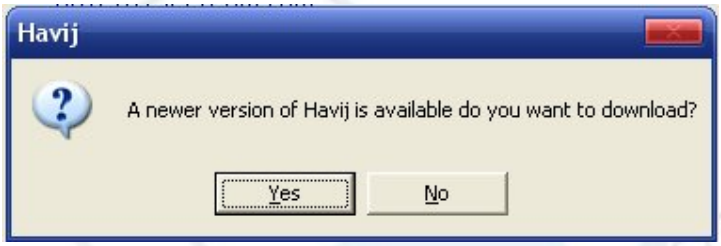
توجه: اگر از یک مجوز در دو سیستم همزمان استفاده شود، مجوز باطل خواهد شد!

ITSecTeam
IT Security Research & Penetration Testing Team

بررسی وجود ورژن جدید

در قسمت About برنامه بر روی Check for update کلیک کنید تا برنامه به صورت خودکار بررسی کند آیا ورژن جدید تری منتشر شده است یا نه. در صورتی که ورژن جدیدتر وجود نداشته باشد، پیغام زیر نمایش داده می شود.

اما در صورت وجود ورژن جدیدتر پیغام زیر نمایش داده می شود



اگر مایلید تا ورژن جدید برنامه را دانلود کنید بر روی Yes کلیک کنید.

ITSecTeam
IT Security Research & Penetration Testing Team

شروع به کار

شروع سریع استفاده از هویج

هویج به گونه ای طراحی شده تا برای استفاده از آن به دانش فنی زیادی احتیاج نباشد در عین حال تنظیمات زیادی برای افراد حرفه ای دارد. برای شروع کار با هویج تنها به آدرس یک صفحه ی آسیب پذیر به SQL Injection احتیاج دارید.

چگونه یک سایت آسیب پذیر به SQL Injection پیدا کنیم؟ برای اینکار می توانید از برنامه های جستجوی آسیب پذیری و ابزارهای نوشته شده برای اینکار و Google استفاده کنید. در ضمن لازم نیست تا از آسیب پذیر بودن صفحه مطمئن باشید زیرا هویج این کار را انجام می دهد.

آدرس صفحه ی آسیب پذیر را در قسمت Targetوارد کنید و Analyze را کلیک کنید و منتظر نتیجه بمانید. هویج تمام کارها را به صورت اتوماتیک انجام می دهد و در صورت موفق شدن و با توجه به سایت مورد هدف امکاناتی از قبیل دریافت اطلاعات، مشاهده ی دیتابیس و اطلاعات آنها، خواندن فایلها و حتی اجرای دستورات بر روی سیستم هدف را در اختیار شما قرار می دهد.

چرا باید آدرس صفحه ی ورودی به شکل http://www.target.com/index.asp**?id=123** باشد؟ بدلیل آنکه صفحه ی آسیب پذیر حداقل باید یک ورودی داشته باشد تا برنامه بتواند عمل تزریق (Injection) را در آن انجام دهد.

www.ITSecTeam.com

Havij

Target: http://www.[redacted]

Keyword: Auto Detect Syntax: Auto Detect

Data Base: Auto Detect Method: GET Type: Auto Detect

Analyze Load Save

About Info Tables Read Files Cmd Shell Query Find Admin MD5 Settings

Havij - Advanced SQL Injection Tool

Version 1.12 Pro
Copyright © 2009-2010
By r3dm0v3

http://ITSecTeam.com
http://forum.Itsecteam.com
info@itsecteam.com Check for update

Data Bases Register

MsSQL with error
MsSQL no error
MsSQL Blind
MsAccess
MsAccess Blind
MySQL

Status: I'm IDLE Clear Log

```
Selected Column Count is 1
Tying to find string column for MySQL
Tying to find string column for MsSQL no error
Valid String Column is 1
DB Server: MsSQL no error
Target Vulnerable :D
DB Name: [redacted]
Injection Syntax: -999.9 UNION ALL SELECT %String_Col%--
```

ITSecTeam
IT Security Research & Penetration Testing Team

ذخیره و بازیابی اهداف

برای سهولت استفاده از برنامه و سرعت بخشیدن به روند تزریق در اهداف خود می توانید در هر مرحله از تزریق، تمام کار انجام شده را ذخیره کنید تا بعدا بتوانید ادامه ی کار را دنبال کنید و نیازی به تکرار آن از اول نداشته باشید.

برای ذخیره ی پروژه بعد از انجام تزریق بر روی Save در زیر Analyze کلیک کرده و یک فایل برای ذخیره سازی انتخاب کنید.

برای بازخوانی مجدد کافی است تا از گزینه ی Load استفاده کنید تا کل پروژه در همان مرحله که قبلا ذخیره کرده بودید بازخوانی شود و بتوانید کار را ادامه دهید.

دریافت اطلاعات (Info)

پعد از اینکه عمل Analyze بر روی هدف مورد نظر به اتمام رسید در صورت موفق بودن تزریق گزینه ی Info در بالای برنامه فعال می شود. با استفاده از این گزینه می توانید اطلاعاتی مانند ورژن سرور دیتابیس سایت آسیب پذیر، نام کاربری، نام دیتابیس و ... را مشاهده کنید. برای اینکار بر روی Info کلیک کرده تا صفحه ی مورد نظر نمایش داده شود سپس بر روی Get کلیک کنید تا اطلاعات دریافت شوند. با استفاده از گزینه ی Saveمی توانید اطلاعات بدست آمده را ذخیره کنید.

forum.ITSecTeam.com

ITSecTeam

Havij

Target: http://www[redacted]

Keyword: Auto Detect Syntax: Auto Detect

Data Base: Auto Detect Method: GET Type: Auto Detect

Analyze Load Save

About Info Tables Read Files Cmd Shell Query Find Admin MD5 Settings

Get Stop Save

Target:	http://www.[redacted]
Host IP:	[redacted]
Web Server:	Microsoft-IIS/6.0
Powered-by:	ASP.NET
Powered-by:	PHP/5.2.6
DB Server:	MsSQL no error
Current User:	dbo
Sql Version:	Microsoft SQL Server 2005 - 9.00.4053.00 (Intel X86) May 26 2009 14::
Current DB:	[redacted]
System User:	sa
Server Name:	C37807-130780
Data Bases:	master
	tempdb
	model
	msdb
	ReportServer

Status: I'm IDLE Clear Log

```
Data Base Found: master
Data Base Found: tempdb
Data Base Found: model
Data Base Found: msdb
Data Base Found: ReportServer
Data Base Found: ReportServerTempDB
Data Base Found: [redacted]
Data Base Found: [redacted]
```

ITSecTeam
IT Security Research & Penetration Testing Team

استخراج اطلاعات جداول و دیتابیس ها

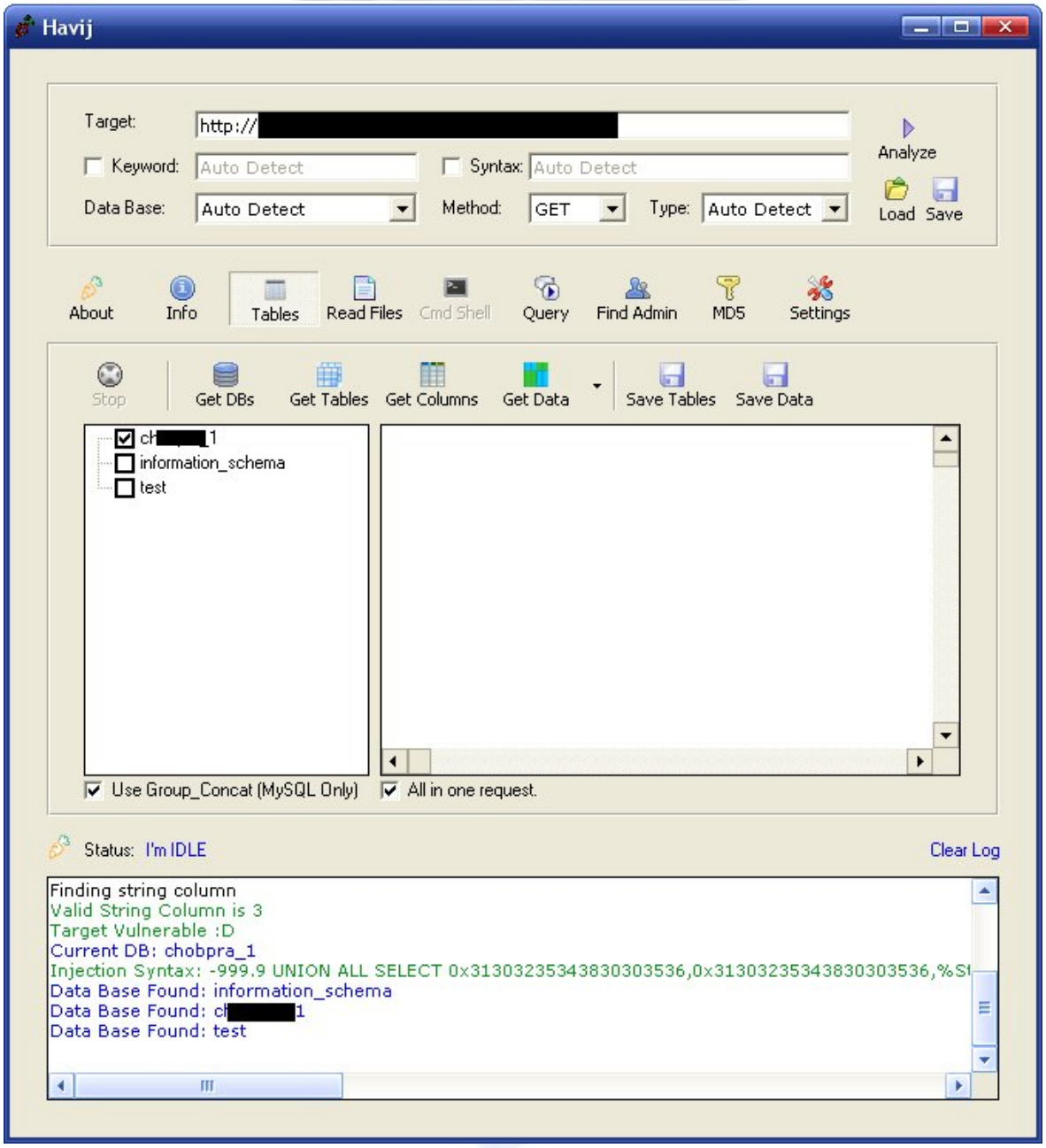
استخراج اطلاعات

با استفاده از منوی Tables در بالای برنامه شما می توانید اطلاعات جداول و ستون های دیتابیس سایت هدف را بدست آورید. برای اینکار بر روی منوی Tables کلیک کنید تا صفحه ی مربوطه نمایش داده شود. در پنجره ی سمت چپ دیتابیس ها و جداول آنها نمایش داده می شود و در پنجره ی سمت راست اطلاعات جداول نمایش داده می شود. پس از تزریق در سایت هدف دیتابیس پیش فرض سایت در پنجره ی سمت راست انتخاب می شود. برای دریافت سایر دیتابیس ها بر روی Get DBs کلیک کنید.

توجه: ممکن است کاربر جاری دیتابیس به بعضی از دیتابیس ها دسترسی نداشته باشد!

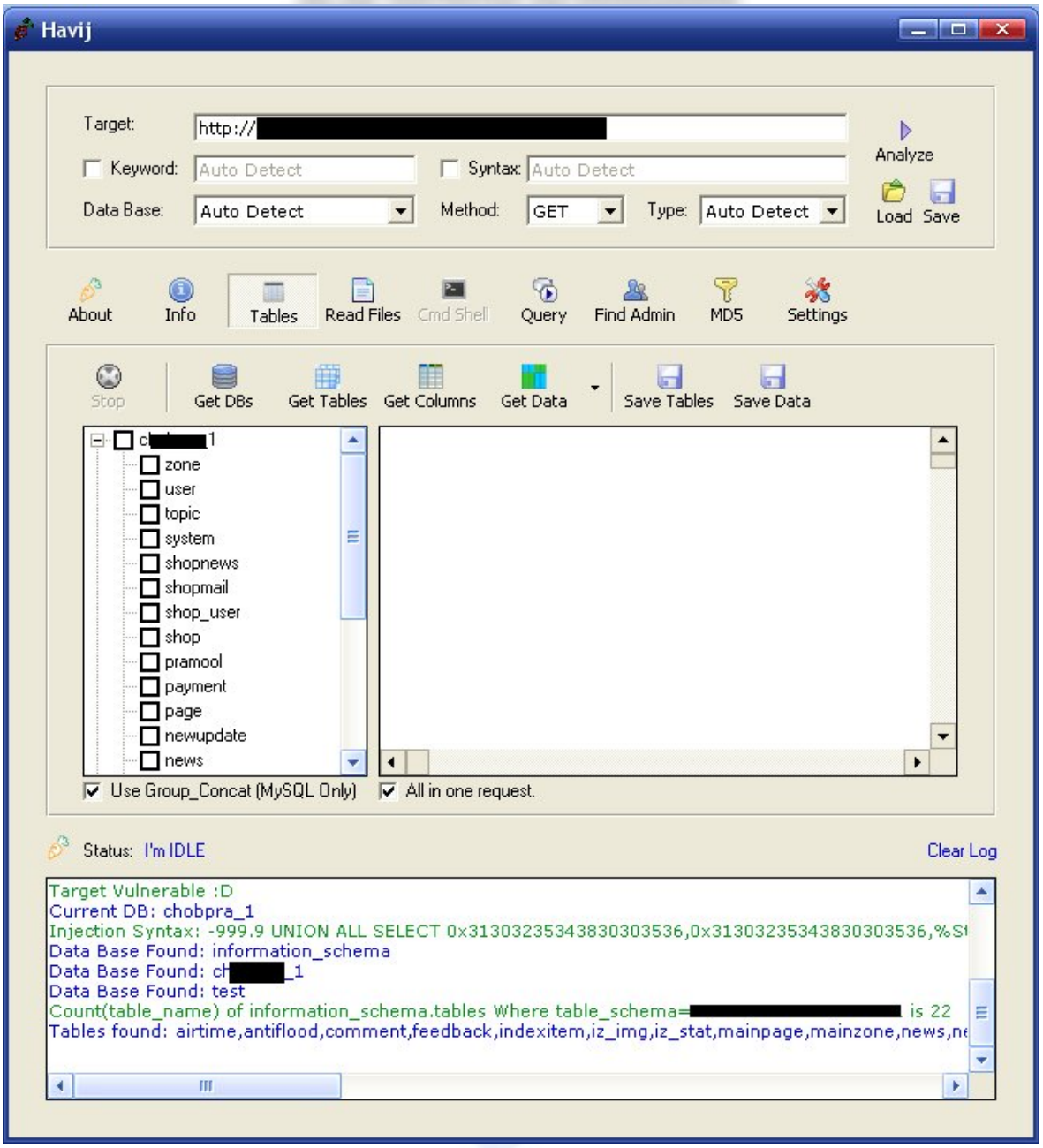
forum.ITSecTeam.com

ITSecTeam



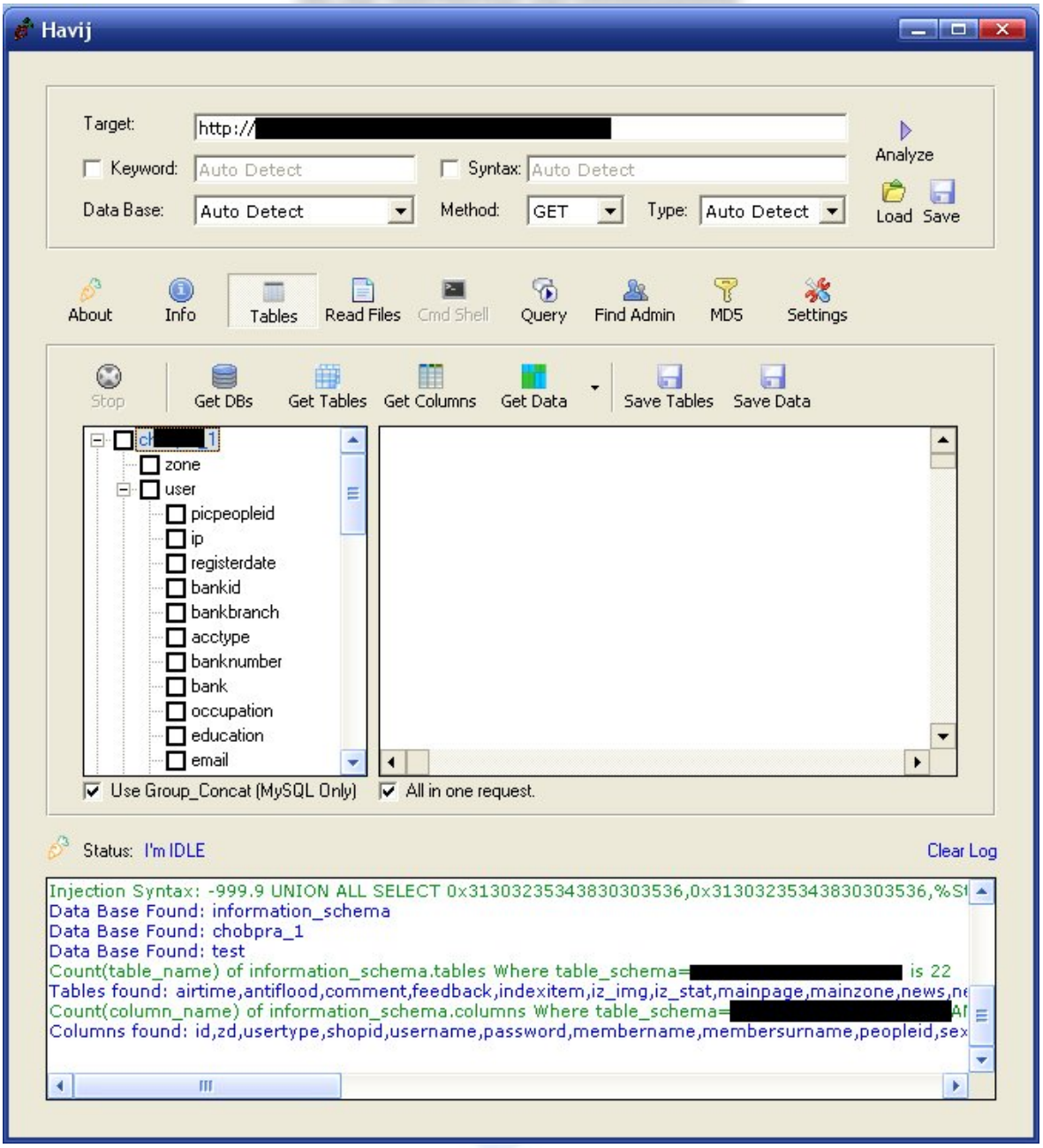
برای مشاهده ی جداول دیتابیس ها دیتابیس مورد نظر خود را از لیست سمت چپ انتخاب کرده (تیک بزنید) و بر روی Get Tables کلیک کنید، جداول در زیر دیتابیس نمایش داده می شوند.

ITSecTeam



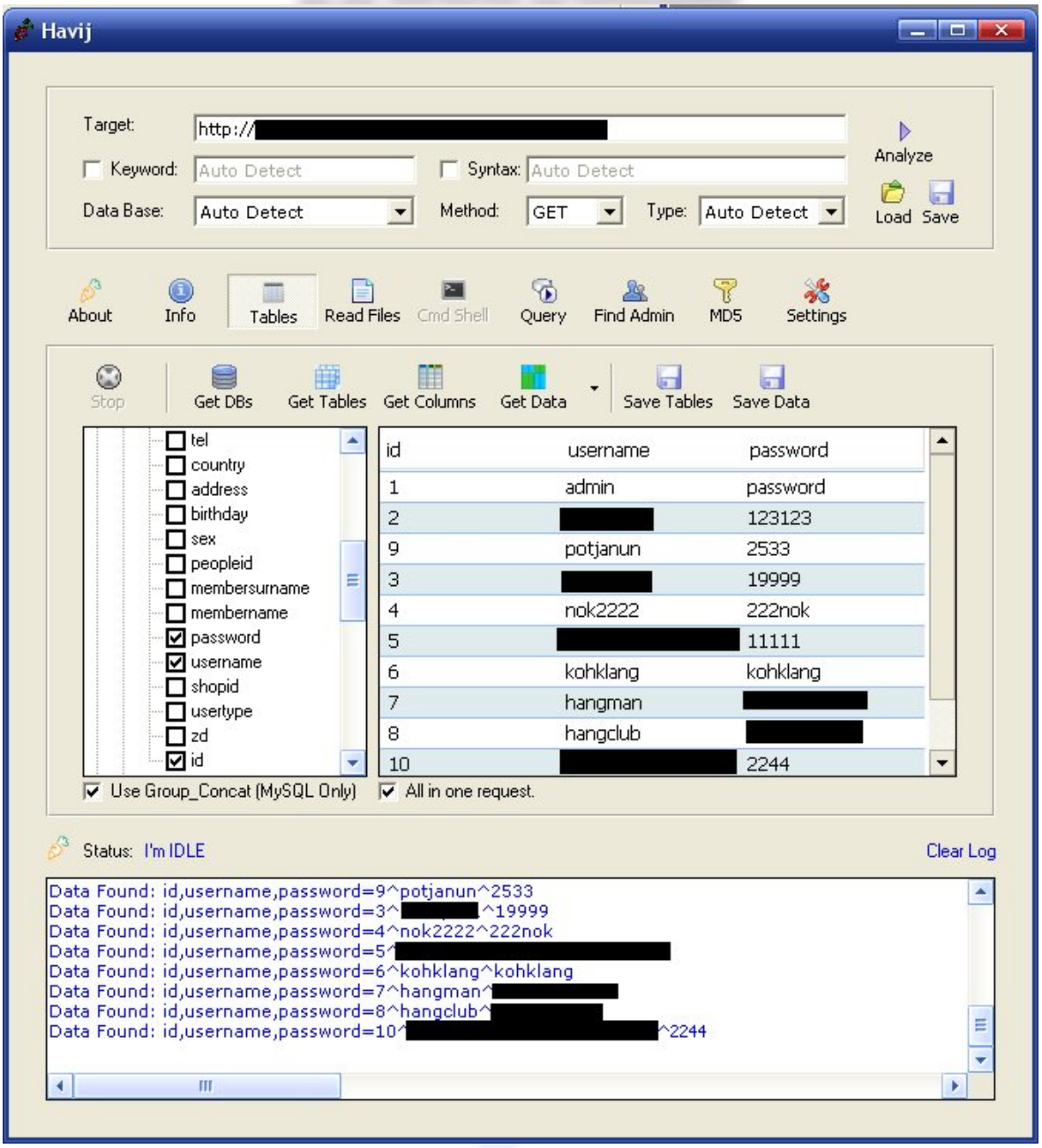
برای دریافت ستون های جداول ابتدا جداول مورد نظر خود را انتخاب کرده و سپس بر روی Get Columns کلیک کنید.

ITSecTeam



برای دریافت اطلاعات از داخل جداول ستون هایی را که مایلید اطلاعات آنها استخراج شود انتخاب کنید و بر روی Get Data کلیک کنید.

ITSecTeam

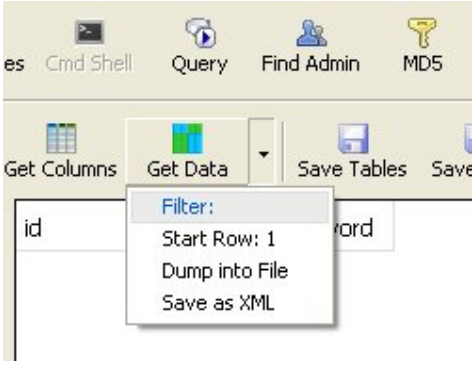


توجه: ممکن است کاربر جاری اجازه ی خواندن اطلاعات را نداشته باشد.

اعمال فیلتر بر روی دریافت اطلاعات

گاهی اوقات است که شما به دنبال اطلاعاتی خاص در دیتابیس هستید در این مواقع می توانید از فیلتر استفاده کنید تا زودتر به نتجیه ی مورد نظر خود برسید.

برای اعمال فیلتر در دریافت اطلاعات بر روی علامت فلش کنار Get Data کلیک کنید تا منوی آن باز شود سپس Filter را انتخاب کنید و شرط مد نظر خود را وارد کنید. حالا Get Data را کلیک کنید تا اطلاعات مطابق شرط شما دریافت شوند.



برای مثال اگر می خواهید رکوردی را که ستون Username آن Admin است دریافت کنید شرط را اینگونه وارد کنید.

Username='admin'

برای از بین بردن فیلتر کافی است به جای فیلتر چیزی وارد نکنید.

شروع دریافت اطلاعات از سطر دلخواه

گزینه ی Get Data به صورت عادی از اولین سطر اطلاعات تا آخرین سطر اطلاعات را دریافت می کند. اگر می خواهید سطر شروع اطلاعات را تغییر دهید و مثلا از دهمین سطر اطلاعات را دریافت کنید بر روی علامت فلش کنار Get Data کلیک کنید تا منوی آن باز شود سپس Start Row را انتخاب کنید و عدد سطر شروع را وارد کنید. حالا Get Data را کلیک کنید تا اطلاعات از آن سطر به بعد دریافت شوند. در هر زمان از دریافت اطلاعات می توانید با کلیک بر روی Stop دریافت را متوقف کنید.

استفاده از Group_Concat

اگر این گزینه که در زیر لیست جداول و ستون ها قرار دارد و فقط برای دیتابیس MySQLکاربرد دارد تیک زده شود برنامه با استفاده از تابع Group_Concat در دیتابیس MySQL تمام جداول و یا ستون ها را یکجا استخراج می کند.

توجه: اگر تعداد جداول یا ستون ها خیلی زیاد باشد ممکن است برنامه قادر نباشد تا همه آنها را با این روش استخراج کند در این صورت پیغام زیر را نمایش می دهد.

ITSecTeam

```
Count(table_name) of information_schema.tables Where table_schema=0x534E4941 is 297
Tables found: CSEurope,Customer_table,Datacentre,EAS_digi_mag,IC_Awards_Categories,I
Can not get all tables by group_concat!
```

در این حالت تیک این گزینه را برداشته و دوباره اطلاعات را استخراج کنید تا با روش معمولی تمام اطلاعات را دریافت کند.

دریافت اطلاعات یک سطر به صورت یکجا

با استفاده از گزینه ی All in one request که در زیر قسمت نمایش اطلاعات قرار گرفته می توانید اطلاعات هر تعداد ستونی که انتخاب کرده اید را یکجا و با یک تزریق دریافت کنید.

توجه: اگر تعداد ستون ها خیلی زیاد باشد ممکن است با این روش نتوانید اطلاعات را استخراج کنید. در این حالت بهتر است تیک این گزینه را ورداشته و به صورت عادی اطلاعات را استخراج نمایید.

ذخیره ی اطلاعات

پس از دریافت اطلاعات برای ذخیره ی جداول در فرمت html می توانید از Save Tables و برای ذخیره ی اطلاعات استخراج شده از Save Data استفاده کنید.

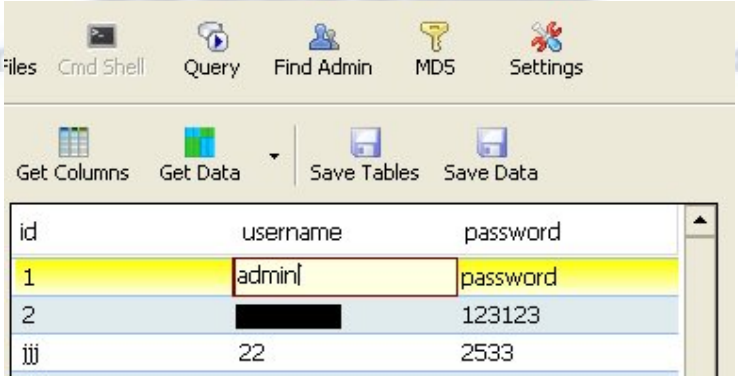
اگر می خواهید تا اطلاعات را با فرمت xml ذخیره کنید بر روی علامت فلش کنار Get Data کلیک کنید تا منوی آن باز شود سپس Save as XML را انتخاب کنید و یک فایل برای ذخیره سازی مشخص کنید سپس Get Data را کلیک کنید تا اطلاعات به جای نمایش در پنجره مستقیما در فایل ذخیره شوند. این گزینه برای دریافت اطلاعات با حجم بالا مناسب است.

اگر می خواهید تا اطلاعات را با فرمت dump همانند دیتابیس MySQL ذخیره کنید بر روی علامت فلش کنار Get Data کلیک کنید تا منوی آن باز شود سپس Dump into File را انتخاب کنید و یک فایل برای ذخیره سازی مشخص کنید سپس Get Data را کلیک کنید تا اطلاعات به جای نمایش در پنجره مستقیما در فایل ذخیره شوند. این گزینه برای دریافت اطلاعات با حجم بالا مناسب است.

تغییر اطلاعات یک سطر

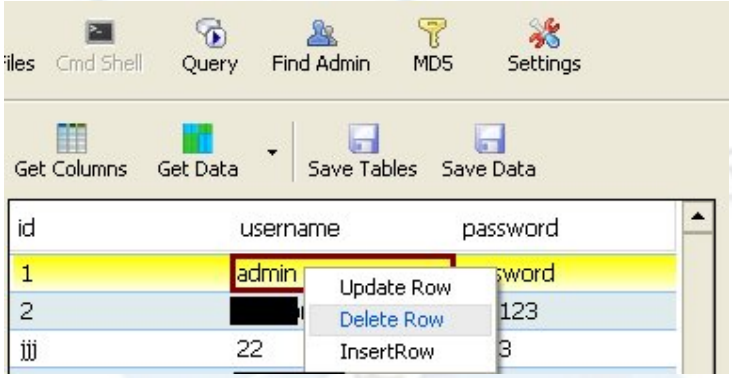
برای اینکه اطلاعاتی را تغییر دهید بر روی آن دوبار کلیک کنید و مقدار جدید را وارد کرده و سپس Enter را فشار دهید.

ITSecTeam



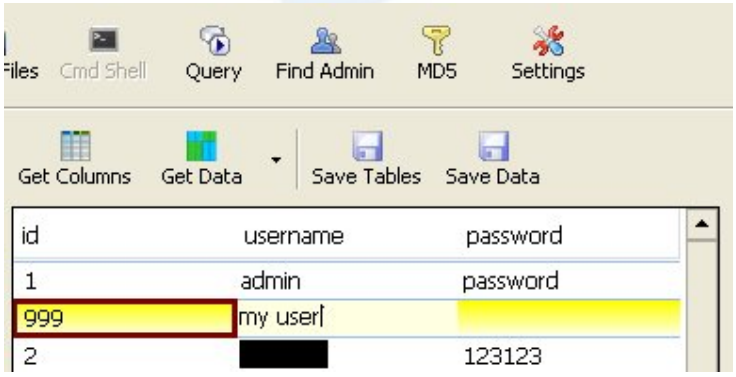
حذف یک سطر

برای حذف یک سطر بر روی آن کلیک راست کرده و گزینه ی Delete Row را انتخاب کنید.



ایجاد یک سطر جدید

برای ایجاد سطر جدید در پنجره ی نمایش اطلاعات کلیک راست کرده و گزینه ی Insert Row را انتخاب کنید و اطلاعات را وارد کرده و Enter را فشار دهید.



ITSecTeam
IT Security Research & Penetration Testing Team

توجه: امکان تغییر، حذف و یا ایجاد اطلاعات جدید در MySQL همراه با PHP وجود ندارد. این امکان برای سایر دیتابیس ها و زبان های برنامه نویسی در جدول زیر نمایش داده شده است.

	SQL Server	MySQL	PostgreSQL	Oracle	MsAccess
ASP	بله	؟	؟	؟	خیر
ASP.NET	بله	؟	؟	؟	خیر
PHP	بله	خیر	بله	؟	خیر
JAVA	؟	خیر	؟	خیر	خیر
ColdFusion	بله	؟	؟	؟	خیر

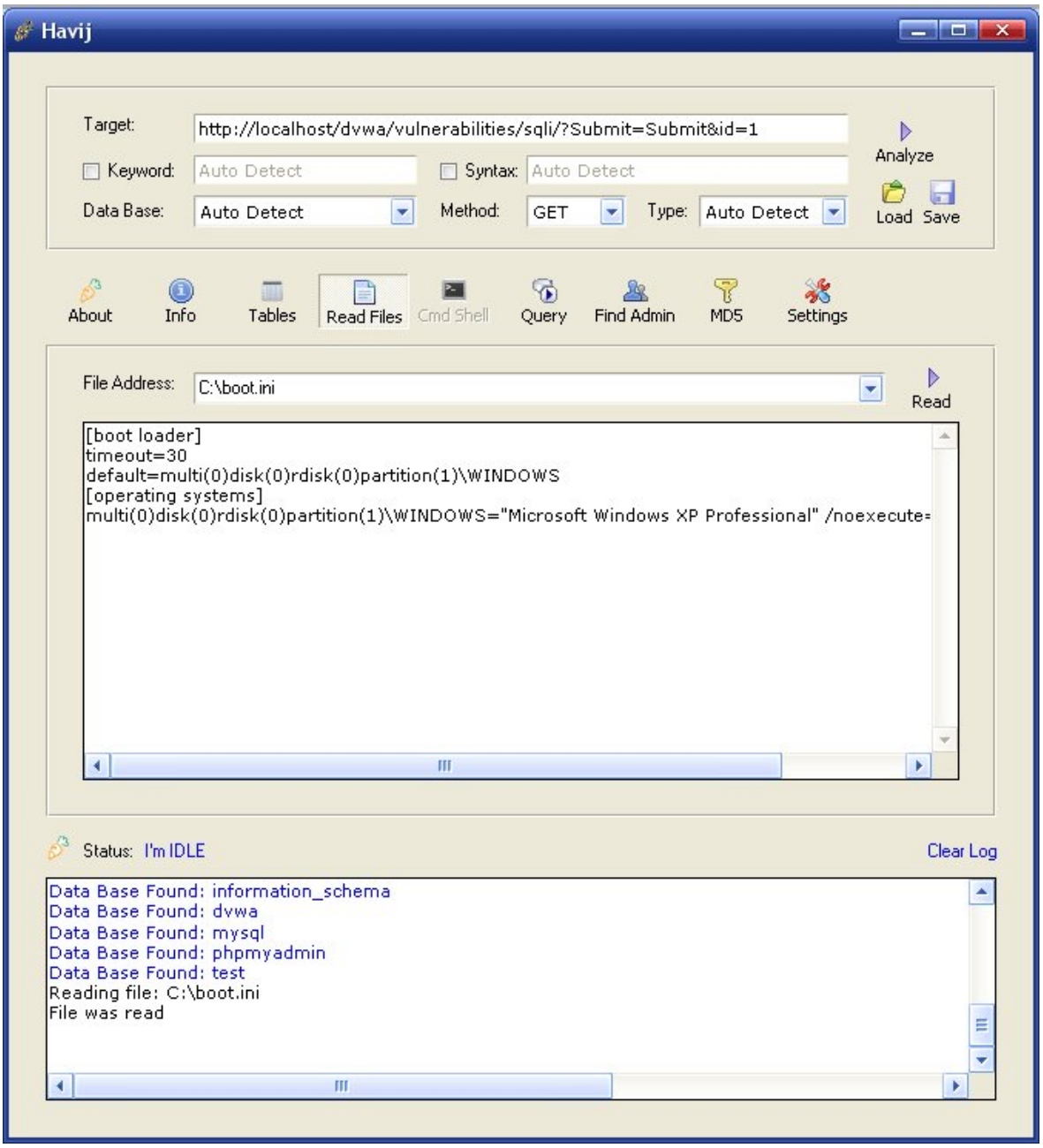
forum.ITSecTeam.com

ITSecTeam
IT Security Research & Penetration Testing Team

خواندن فایل ها

اگر دیتابیس هدف MySQL باشد پس از تزریق منوی Read Files در بالای برنامه فعال می شود و شما می توانید فایل های روی سرور MySQL را بخوانید. کافی است آدرس فایل مورد نظر خود را در Files Address وارد کنید و Read را کلیک کنید.

توجه: اگر فایل وجود نداشته باشد و یا کاربر دیتابیس اجازه ی دسترسی به آن را نداشته باشد چیزی نمایش داده نمی شود!



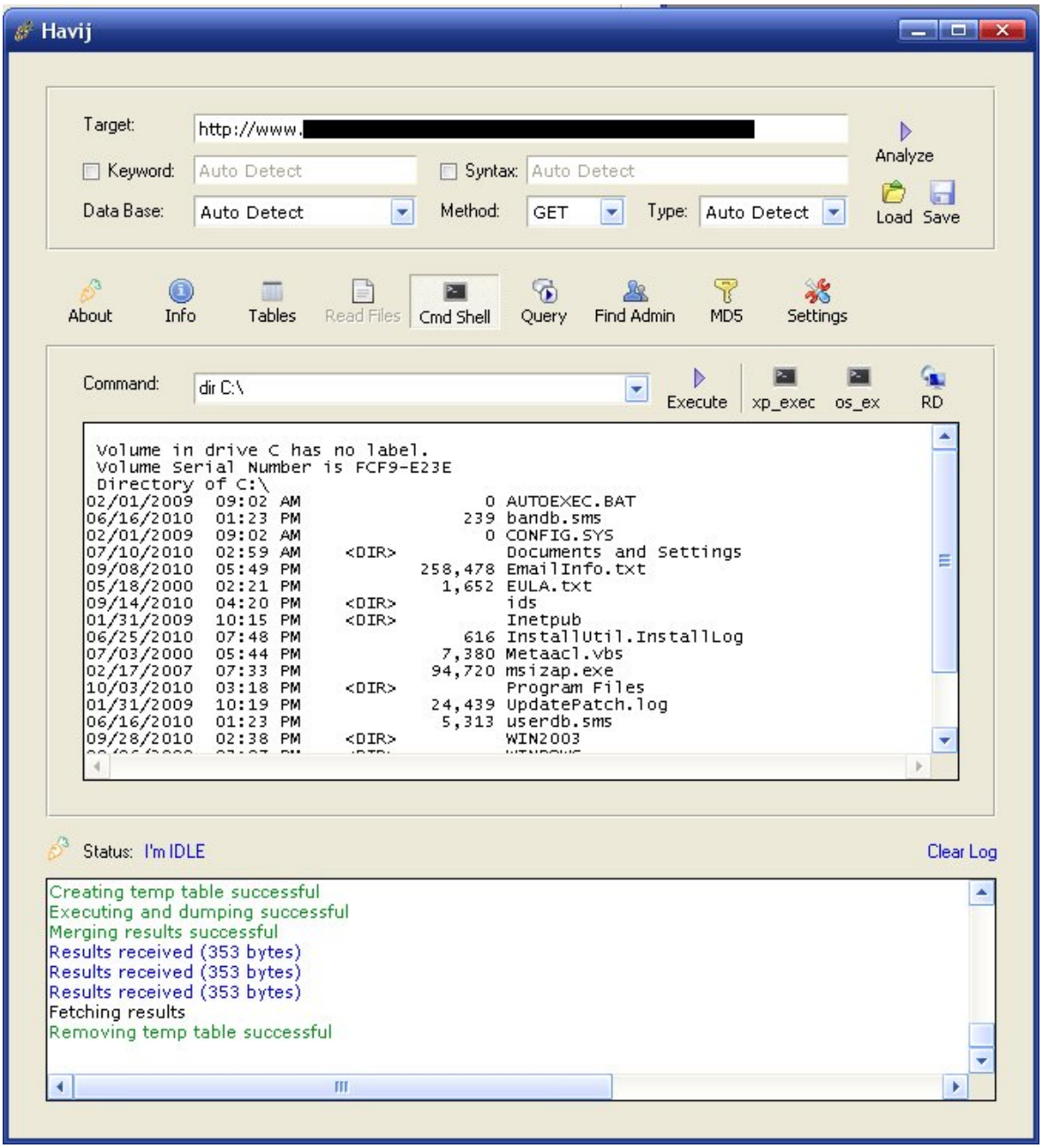
ITSecTeam
IT Security Research & Penetration Testing Team

اجرای دستورات سیستمی بر روی هدف

در صورتی که دیتابیس سایت هدف Microsoft SQL Server باشد گزینه ی CMD Shell در بالای برنامه فعال می شود و شما می توانید دستورات سیستمی بر روی سرور SQL اجرا نمایید.

دستور مورد نظر خود را در Command وارد کنید و Execute را کلیک کنید و منتظر نتیجه بمانید در صورت اجرا شدن دستور نتیجه ی آن در پنجره ی مربوطه نمایش داده می شود.

توجه: برای اجرای دستور کاربر دیتابیس حتما باید اجازه ی کافی برای اجرای دستور را داشته باشد.

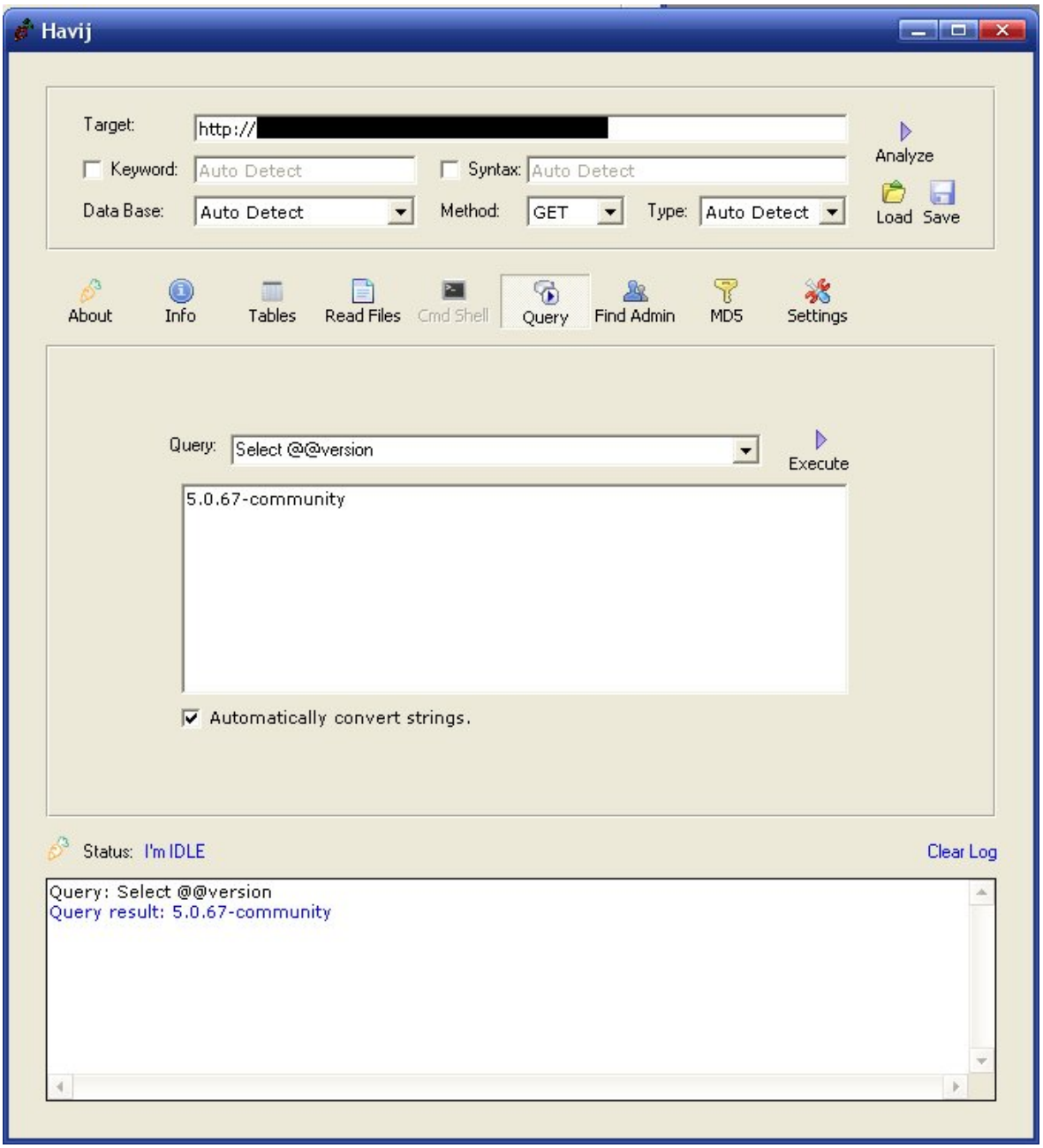


ITSecTeam
IT Security Research & Penetration Testing Team

پرس و جو (Query)

با استفاده از گزینه ی Query در بالای برنامه می توانید جملات SQL دلخواه خود را در هدف اجرا نماید و نتیجه را مشاهده کنید.

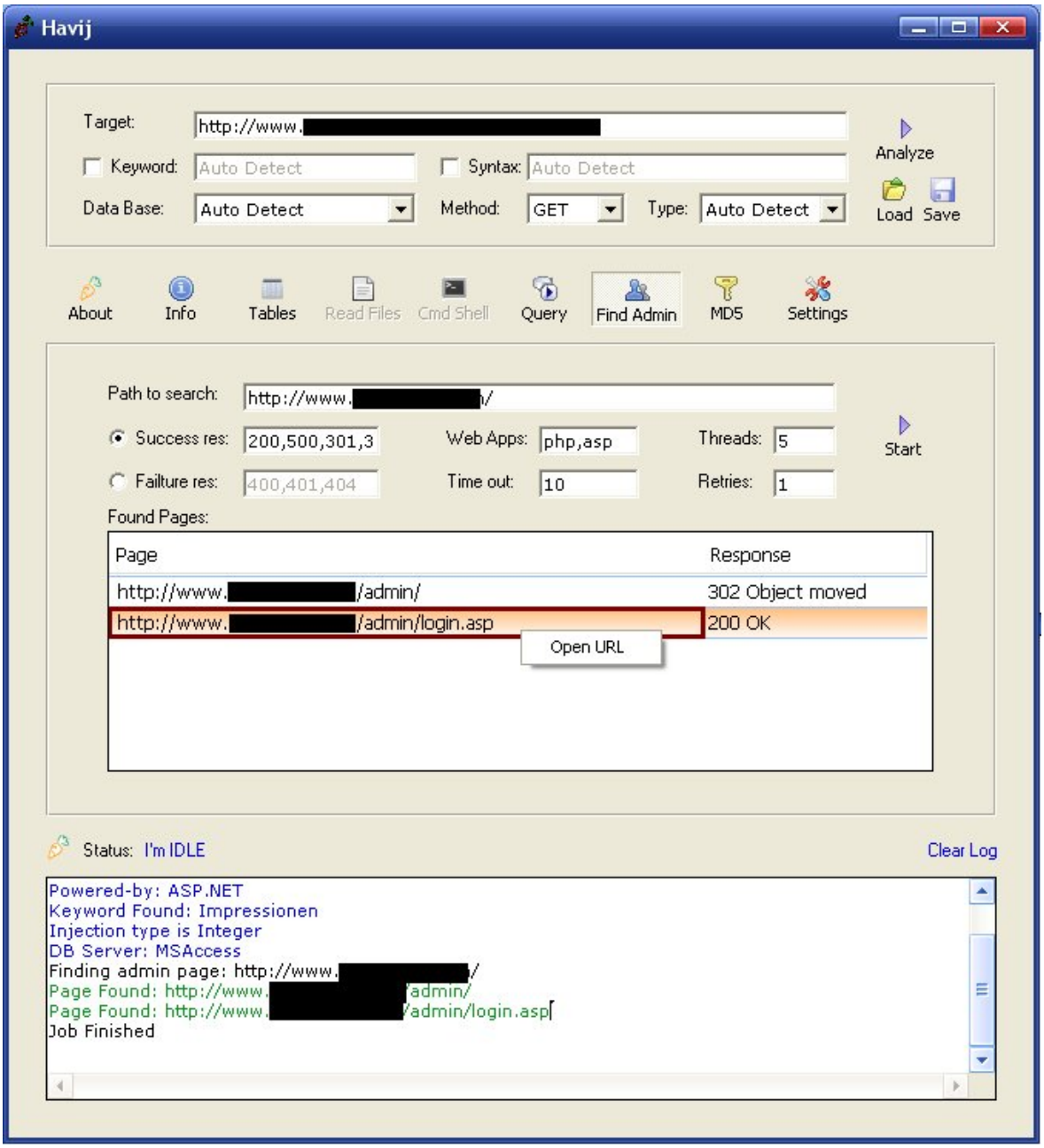
توجه: جملات SQL شما نباید بیشتر از یک سطر بازگردانند!



ITSecTeam
IT Security Research & Penetration Testing Team

پیدا کردن صفحه ی ورود مدیر

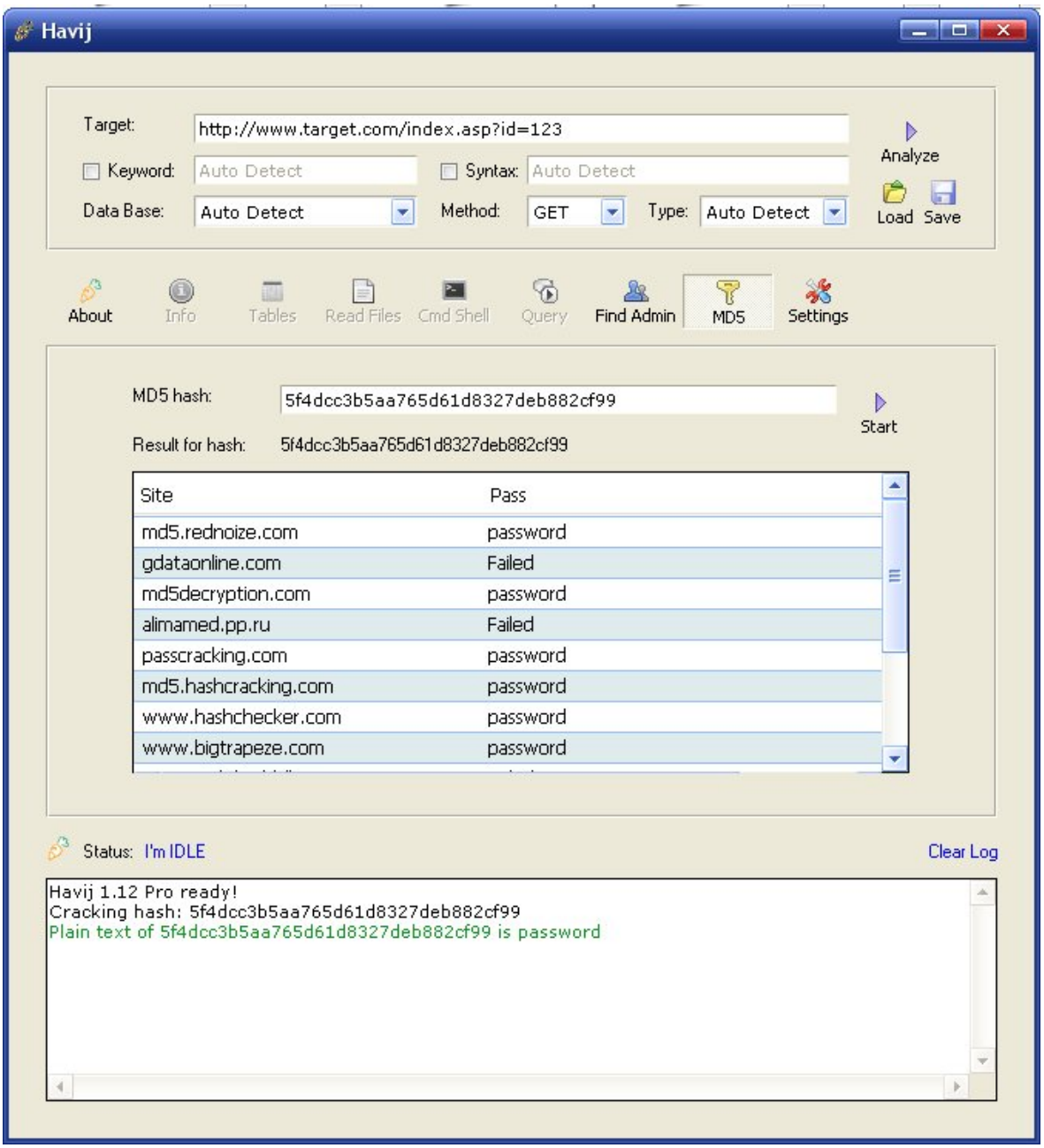
با استفاده از Find Admin در بالای برنامه می توانید آدرس صفحه ی ورود (Login) کاربران سایت را پیدا کنید. برای این کار در صفحه ی مربوطه آدرس سایتی را که می خواهید صفحه ورود آن را پیدا کنید در قسمت Path to Search وارد کنید و Start را کلیک کنید. صفحات پیدا شده در لیست نمایش داده می شوند .با کلیک راست بر روی صفحات پیدا شده و انتخاب گزینه ی Open URL می توانید آنها را در مرور گر خود باز کنید.



ITSecTeam
IT Security Research & Penetration Testing Team

کرک کردن پسوردهای MD5

هویج دارای یک کرکر انلاین MD5 می باشد که می توانید با استفاده از آن پسوردهای MD5 را کرک کنید. در داخل MD5 hash هشی را که می خواهید کرک کنید وارد کنید و Start را کلیک کنید، برنامه به صورت همزمان در چندین سایت کرک آنلاین به دنبال هش می گردد و نتیجه را در لیست نمایش می دهد.



ITSecTeam
IT Security Research & Penetration Testing Team

تزریق به روش دستی

هویج علاوه بر قابلیت تزریق خودکار این امکان را نیز فراهم می کند تا کاربر تنظیمات مربوط به تزریق را به صورت دستی انجام دهد و از امکانات و سرعت برنامه در تزریق برای راحتی کار استفاده کند. در حالت پیش فرض تمامی تنظیمات به صورت تشخیص خودکار (Auto Detect) می باشد. این تنظیمات شامل کلمه ی کلیدی (Keyword)، Syntax، دیتابیس و نوع متغییر (Type) می باشد. شما می توانید یک یا تمامی این تنظیمات را به صورت دستی انجام دهید.

تعیین دیتابیس

اگر شما مطمئن هستید که سرور دیتابیسی که هدف مورد نظرتان استفاده می کند چیست می توانید از داخل لیست Database آن را انتخاب کنید. هویج دیتابیس های زیر را پشتیبانی می کند.

- MsSQL with error: Microsoft SQL Server تزریق با روش استخراج از متن ارور
- MsSQL no error: Microsoft SQL Server تزریق با استفاده از Union
- MsSQL Blind: Microsoft SQL Server با روش تزریق چشم بسته (Blind)
- MySQL unknown ver: MySQL با استفاده از Union
- MySQL Blind: MySQL با روش تزریق چشم بسته (Blind)
- MySQL error based: MySQL با روش استخراج از متن ارور
- Oracle: Oracle با استفاده از Union
- PostgreSQL: PostgreSQL با استفاده از Union
- MsAccess: Microsoft Access با استفاده از Union
- MsAccess Blind: Microsoft Access با روش تزریق چشم بسته (Blind)

تعیین نوع متغییر

نوع متغییر (Type) در تزریق SQL یا عدد (Integer) است و یا رشته (String). منظور از نوع عددی متغییری است که مستقیما توسط سایت هدف در جمله ی SQL استفاده می شود. اما نوع رشته متغییری است که برای استفاده در جمله ی SQL حتما داخل علامت نقل قول ' و یا " (quotation mark) قرار می گیرد. توجه داشته باشید که تمامی تزریق ها داخل همین متغییر صورت می گیرد.

تعیین کلمه ی کلیدی

کلمه ی کلیدی (keyword) کلمه ایست که تفاوت بین حالت صحیح (True) و غلط (False) را در تزریق مشخص می کند. حالت صحیص زمانی است که جمله ی SQL تزریق شده به درستی اجرا می شود و نتیجه ی دلخواه را بر می گرداند ولی در حالت غلط هیچ نتیجه ای

www.ITSecTeam.com

ITSecTeam
IT Security Research & Penetration Testing Team

بازگردانده نمی شود. کلمه ی کلیدی باید یک کلمه یا عبارت از سورس صفحه ای که حالت صحیح را نشان می دهد باشد.

برای پیدا کردن کلمه ی کلیدی می توانید از تزریق های زیر استفاده کنید.

نشان دهنده ی حالت صحیص برای متغییر عددی http://site.com/index.php?id=52 and 1=1

نشان دهنده ی حالت غلط برای متغییر عددی http://site.com/index.php?id=52 and 1=0

و

نشان دهنده ی حالت صحیص برای متغییر رشته ای http://site.com/index.php?id=52′ and ‘x′=′x

نشان دهنده ی حالت غلط برای متغییر رشته ای http://site.com/index.php?id=52′ and ‘x=′y

برای مثال اگر در حالت صحیح عبارت Hello را مشاهده کردید ولی در حالت غلط این عبارت وجود نداشت کلمه ی Hello کلمه ی کلیدی مناسب برای استفاده است.

تعیین Syntax

در برخی از سایت ها به علت خاص بودن هدف و پیچیدگی جملات SQL استفاده شده برنامه موفق به تزریق خودکار نمی شود. در این شرایط اگر شما به صورت دستی می توانید هدف را اینجکت کنید و اطلاعات را استخراج نمایید می توانید باز هم از هویج بهره بگیرید.

برای مثال فرض کنید شما در سایتی با در خواست زیر عمل تزریق را انجام می دهید و موفق به مشاهده ی نسخه ی دیتابیس می شوید.

http://site.com/index.php?id=-52 union all select 1,2,@@version,3—

برای تنظیم دستی در هویج آدرس زیر را در قسمت Target وارد کنید.

http://site.com/index.php?id=52

بر روی Syntax کلیک کنید تا تیک زده شود سپس در کادر روبرو مقدار زیر را وارد کنید:

-52 union all select 1,2,%String_Col%,3—

توجه کنید که به جای @@version که در صفحه برگردانده می شود مقدار %String_Col% را جایگزین کردیم.

توجه: %String_Col% دقیقا باید به همین صورت نوشته شود!

www.ITSecTeam.com

ITSecTeam
IT Security Research & Penetration Testing Team

حالا بر روی Analyze کلیک کنید تا تزریق شروع شود.

تعیین Syntax برای تزریق به روش چشم بسته (Blind)

در تزریق به روش چشم بسته یا همان Blind هیچ کدام از سطر ها ی انتخاب شده توسط جمله ی SQL در صفحه نمایش داده نمی شوند بنابراین این امکان وجود ندارد تا با جملات Union اطلاعاتی از دیتابیس استخراج کنیم. در اکثر مواقع با تزریق های مختلف تنها قادر به مشاهده ی دو حالت مختلف در صفحه ی نمایش داده شده هستیم. یک حالت نشانگر این است که جمله ی SQL صحیص بوده (حداقل یک سطر برگردانده) و حالت دوم نشان دهنده ی غلط بودن جمله ی SQL می باشد. (برای اطلاعات بیشتر قسمت کلمه ی کلیدی مطالعه شود.)

برای مثال فرض کنید که شما با استفاده از تزریق زیر صفحه ی نشان دهنده ی حالت صحیح را مشاهده می کنید:

http://site.com/index.php?id=52 and 1=1

در قسمت Target عبارت زیر را وارد کنید

http://site.com/index.php?id=52

و برای تنظیم دستی syntax این عبارت را وارد کنید

52 and %True_Expression%

توجه: عبارت %True_Expression% دقیقا باید به همین شکل نوشته شود.

در حالتی که نوع متغییر رشته ای است و با تزریق زیر صفحه ی صحیح را مشاهده می کنید:

http://site.com/index.php?id=52’ and ‘x’=’x

در قسمت Target عبارت زیر را وارد کنید:

http://site.com/index.php?id=52

و برای تنظیم دستی Syntax این عبارت را وارد کنید:

52’ and %True_Expression and ‘x’=’x

توجه: اگر Syntax را دستی تنظیم می کنید بهتر است تا کلمه ی کلیدی را نیز دستی وارد کنید (مخصوصا در حالت تزریق چشم بسته)

www.ITSecTeam.com

ITSecTeam
IT Security Research & Penetration Testing Team

تعیین روش (Method)

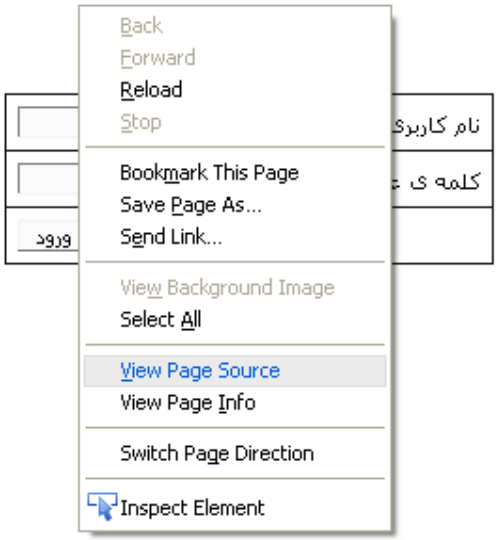
منظور از روش یا همان Method نحوه ی ارسال ورودی ها یا همان تزریق SQL به سایت هدف می باشد. تمام لینک ها در صفحات html از متد GET استفاده می کنند و اغلب فرم ها از متد POST. به طور پیش فرض متد GET انتخاب شده است. اگر در داخل ورودی های یک فرم اینجکشن پیدا کردید باید از متد POST استفاده کنید.

تزریق در فرم ها متد POST

برای مثال اگر در سایتی فرم زیر را مشاهده کردید و مایل بودید تا با استفاده از هویج در آن تزریق SQL انجام دهید می توانید مراحل زیر را دنبال کنید

نام کاربری:	
کلمه ی عبور:	
ورود	

1- متد POST را انتخاب کنید.
2- سپس سورس صفحه ی html را در مرورگر ببینید (کلیک راست در صفحه سپس انتخاب view page source)



3- به دنبال تگ <form> در سورس بگردید

ITSecTeam

```
<body>
<div align="center">
  <center>
  <table border="0" cellpadding="0" cellspacing="0" style="border-collapse: col
    <tr>
      <td width="100%">
      <div align="center">
        <center>
        <form method=post action="index.php">
        <table border="1" cellpadding="6" cellspacing="0" style="border-collaps
          <tr>
            <td width="50%">نام کاربری:</td>
            <td width="50%"><input type="text" name="name" size="20"></td>
          </tr>
          <tr>
            <td width="50%">کلمه ی عبور:</td>
            <td width="50%"><input type="password" name="pass" size="20"></td>
          </tr>
          <tr>
            <td width="100%" colspan="2">
            <p align="left"><input type=submit name=submit value="ورود"></td>
          </tr>
        </table>
        </form>


        </center>
      </div>
      </td>
```

4- در قسمت Target برنامه مقدار action را که در اینجا index.php می باشد بعد از ادرس صفحه وارد کنید:

http://localhost/index.php

5- در قسمت Post Data نام ورودی ها را به شکل زیر وارد کنید:

Pass=&submit=ورود&name=whatever

توجه: تزریق SQL در ورودی آخر (name) صورت می گیرد. در صورتی که می خواهید تزریق در پارامتر Pass انجام شود می توانید این پارامتر را آخر از همه بنویسید و یا به صورت زیر پارامتر تزریق را تعیین نمایید:

Pass=%Inject_Here%&submit=ورود&name=whatever

6- بر روی Analyze کلیک کنید تا تزریق شروع شود.

ITSecTeam
IT Security Research & Penetration Testing Team

تنظیمات

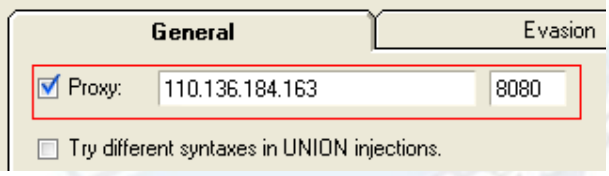
با استفاده از گزینه ی Settings در منوی بالای برنامه شما می توانید بعضی از تنظیمات برنامه را تغییر دهید.

توجه: برای تریتب اثر دادن تنظیمات پس از عمل تزریق (Analyze) و در حین کار حتما باید بر روی Apply کلیک کنید. در غیر اینصورت تنظیمات جدید با تزریق (Analyze) مجدد اعمال خواهند شد.

تنظیمات ساده

تنظیم استفاده از پروکسی

برای تزریق غیر مستقیم به منظور ناشناس ماندن می توانید از پروکسی استفاده کنید. در صفحه ی تنظیمات چک باکس پروکسی را تیک بزنید و آدرس سرور پروکسی و پورت آن را در کادر روبرو بنویسید و Apply را کلیک کنید.

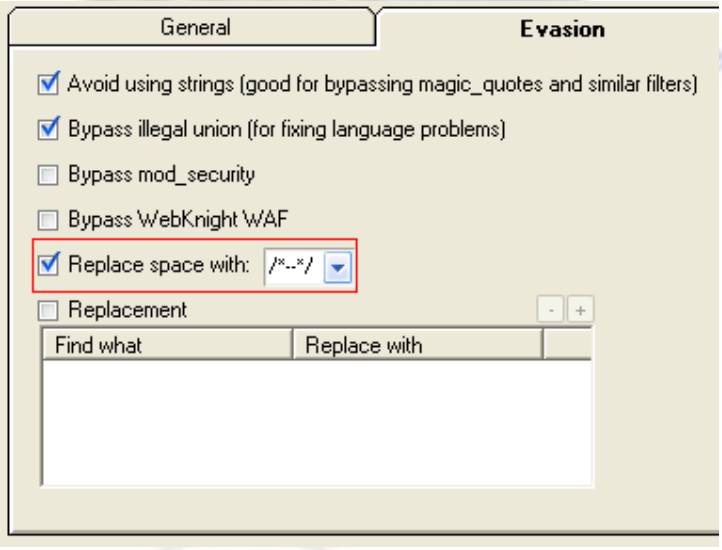


تغییر فاصله (Space) در تزریق

برای اینکه برخی از فیلتر ها که مانع از تزریق به صورت عادی می شوند را دور بزنید می توانید فاصله (Space) را در تزریق ها با کاراکترهایی مانند ...,/**/,+ جایگزین کنید اینکار تغییری در نتیجه ی تزریق ایجاد نمی کند ولی می تواند فیلتر های ضعیف را دور بزند.

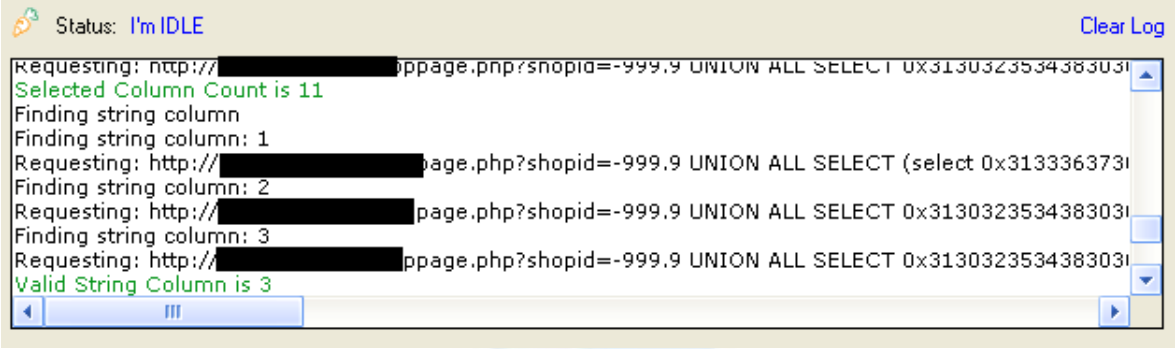
برای اینکار در قسمت تنظیمات بر روی Replace Space with کلیک کنید تا تیک زده شود سپس از داخل لیست کاراکتری را که می خواهید جاگزین فاصله شود انتخاب کنید.

ITSecTeam



نمایش تزریق های انجام شده

هویج این امکان را فراهم می کند تا تمامی تزریق هایی را که انجام می دهد مشاهده کنید و بتوانید خودتان به صورت دستی تزریق ها را انجام دهید. در قسمت تنظیمات گزینه ی Show Requests را تیک بزنید تا تمامی تزریق ها در پنجره ی مربوط به پیغام ها نمایش داده شود.



تزریق در صفحات URL Rewrite

گاهی اوقات صفحات وب سایت ها با استفاده از قابلیت URL Rewriteبدون هیچ پارامتری دیده می شوند. برای تزریق در چنین صفحاتی می توانید محلی را که تزریق باید در آن صورت گیرد با عبارت %Inject_Here% مشخص کنید. برای مثال اگر صفحه ای از سایت به شکل زیر بود:

http://somewhere.com/news/1077/index.html

و مقدار 1077 پارامتر آسیب پذیر باشد، برای تزریق باید آدرس زیر را در Target وارد کنید.

ITSecTeam
IT Security Research & Penetration Testing Team

http://somewhere.com/news/%Inject_Here%/index.html

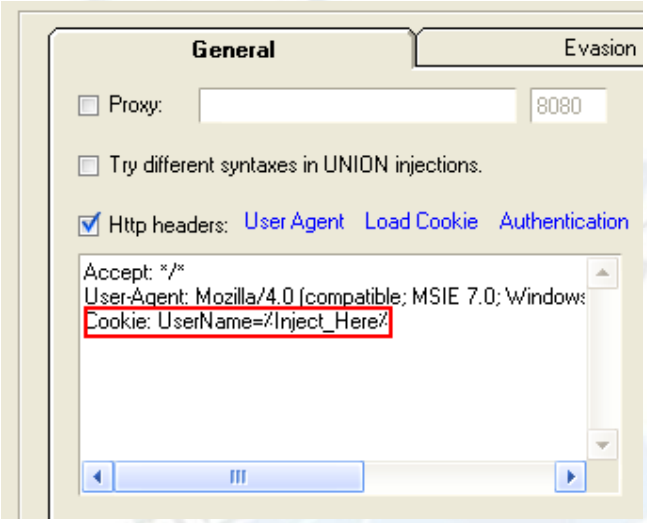
توجه: %Inject_Here% دقیقا باید به همین شکل نوشته شود.

تزریق در کوکی، user-agent و ...

در شرایطی که آسیب پذیری در کوکی، User-Agent و یا سایر هدرهای http وجود داشته باشد همچنان می توانید با استفاده از هویج آن را اکسپلویت کنید.

برای مثال اگر یک آسیب پذیری در یک پارامتر کوکی به نام UserName وجود داشته باشد کافی است تا خط زیر را به به Additional http headers در تنظیمات اضافه کنید.

Cookie: UserName=%Inject_Here%



این عمل برای سایر هدرها هم یکسان است

در حالتی که از %Inject_Here% استفاده شود مقدار 1 در تزریق ها به جای مقدار پیش فرض استفاده می شود شما می توانید این مقدار را در تنظیمات تغییر دهید.

تنظیمات پیشرفته

برای تزریق به احراز هویت نیاز است!

در خیلی از مواقع برای دسترسی به صفحه ی آسیب پذیر لازم است تا حتما در سایت لاگین (login) کنید. هویج اینگونه از اهداف را هم می تواند تزریق کند.

هویج قادر به انجام سه نوع حراز هویت می باشد: 1- احراز هویت به روش Basic 2- احراز هویت به روش Digest 3- احراز هویت به روش http form

ITSecTeam
IT Security Research & Penetration Testing Team

احراز هویت به روش Basic

در صورتی که سایت مورد نظر از این روش برای احراز هویت استفاده کند برنامه به صورت خودکار آن را تشخیص می دهد و از شما نام کاربری و کلمه ی عبور را می پرسد، مانند عکس زیر

کافی است تا اطلاعات مورد نیاز را وارد کنید و بر روی OK کلیک کنید

این کار از طریق تنظیمات و با کلیک بر روی Authentication نیز امکان پذیر است

احراز هویت به روش Digest

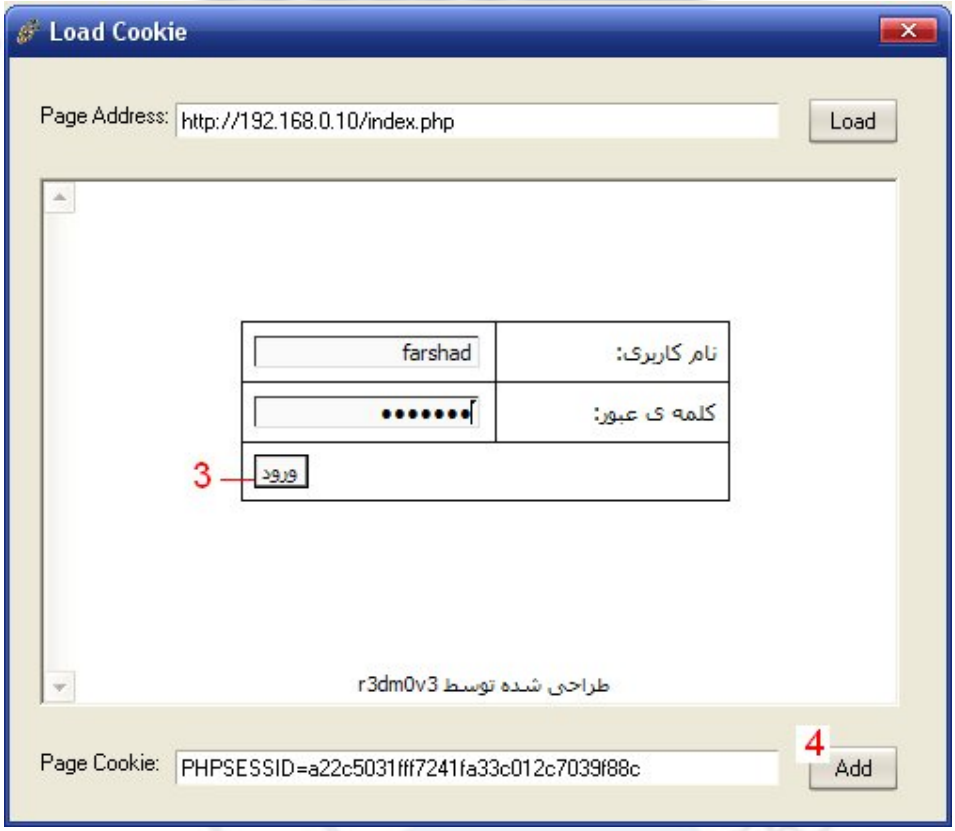
این کار هم مانند روش Basic به صورت خودکار توسط برنامه انجام می شود

احراز هویت به روش HTTP Form

این روش زمانی است که شما باید در داخل سایت نام کاربری و کلمه ی عبور خود را توسط یک فرم وارد کنید.

برای احراز هویت به این روش مراحل زیر را دنبال کنید.

1- ابتدا آدرس لینک آسیب پذیر را در قسمت Target بنویسید.
2- سپس وارد قسمت Settings شوید و گزینه ی Additional http headers را تیک بزنید تا بتوانید بر روی گزینه ی Load Cookie کلیک کنید.
3- در پنجره ی باز شده، سایت همانطور که در مرور گر خود (IE) مشاهده می کنید باز می شود. در سایت لاگین (login) کنید.
4- Add را کلیک کنید.



5- حالا می توانید تزریق را شروع کنید. برای اینکار Analyze را کلیک کنید.

تعیین کاراکترها برای تست در تزریق چشم بسته

هویج در تزریق های چشم بسته (Blind) برای استخراج اطلاعات، تک تک کاراکترها را با روش سعی و خطای دو دویی (باینری) پیدا می کند. محدوده ی کاراکترهای استفاده شده برای سعی و خطا را می توانید در تنظیمات مشخص کنید. کافی است در قسمت Blind injection character ascii set کد اسکی مربوط به کوچکترین و بزرگترین کاراکتر را وارد کنید.

تغییر هدر (Header) ها در تزریق

تزریق هایی که نرم افزار هویج انجام می دهد از طریق پروتکل http ارسال می شوند. این پروتکل هدرهای زیادی دارد که می توانید با اختیار خود آنها تنظیم کنید. یکی از مهم ترین این هدر ها هدر User-Agent است که نشاندهنده ی مرورگر مورد استفاده است.

در قسمت تنظیمات بر روی Additional http headers کلیک کنید تا تیک زده شود سپس در کادر زیر می توانید هدر دلخواه خود را وارد کنید.

برای تنظیم هدر User-Agent بر روی این گزینه کلیک کنید و از لیست هر کدام را می خواهید انتخاب کنید.

ITSecTeam
IT Security Research & Penetration Testing Team

Time out

این گزینه در سربرگ 'General' در تنظیمات مدت زمانی را که هویج برای ارسال و دریافت درخواست ها صرف می کند بر حسب میلی ثانیه مشخص می کند.

مقدار پیش فرض برای تزریق

زمانی که از %Inject_Here% استفاده می کنید می توانید از این گزینه برای مشخص کردن مقدار پیش فرض در تزریق ها استفاده کنید.

برای مثال اگر یک آسیب پذیری در URL زیر وجود داشته باشد

http://site.com/index.html/id/1324

و ورودی آسیب پذیر 1324 باشد، شما آن را با %Inject_Here% جایگزین می کنید.

http://site.com/index.html/id/%Inject_Here%

برای مشخص کردن 1324 به عنوان مقدار پیش فرض می توانید آن را در قسمت Default injection value در تنظیمات وارد کنید.

Avoid using strings

این گزینه اگر تیک داشته باشد برنامه به صورت خودکار تمام رشته ها را تبدیل می کند. این گزینه برای دور زدن فیلتر هایی مانند magic_quotes که علائم نقل قول را بی اثر می کنند مناسب است. توصیه می شود این گزینه را فعال کنید.

Bypass illegal union

این گزینه برای بر طرف کردن مشکل تفاوت زبان جداول و دیتابیس هنگام تزریق با استفاده از union می باشد. توصیه می شود این گزینه را فعال کنید.

Try different syntaxes in union injection

با انتخاب این گزینه در صورتی که تلاش برای پیدا کردن تعداد ستون های جمله ی select به نتیجه نرسد، با حالتهای مختلف مثل استفاده از پرانتز دوباره سعی در پیدا کردن تعداد ستون ها می کند.

www.ITSecTeam.com

ITSecTeam
IT Security Research & Penetration Testing Team

Follow redirections

اگر این گزینه فعال باشد در صورتی که سرور برنامه را به صفحه ی دیگری منتقل کند برنامه در آن صفحه به دنبال نتیجه ی تزریق می گردد.

Column count

در این قسمت می توانید حداقل و حداکثر تعداد ستون هایی را که به هنگام تلاش برای پیدا کردن ستون های جمله select در تزریق به روش union مورد آزمایش قرار می گیرند را وارد کنید.

Do not find columns count in MsSQL with error

این گزینه اگر تیک زده شود در سایت هایی که دیتابیس از نوع MsSQL و تزریق از نوع استخراج از متن ارور می باشد، برنامه تعداد ستون های جمله ی select را پیدا نمی کند. توصیه می شود این گزینه را فعال کنید.

Bypass mod_security

این گزینه برای دور زدن فایروال برنامه های تحت وب mod_security و بسیاری دیگر از فایروال های مشابه استفاده می شود. این گزینه به صورت خودکار توسط برنامه مورد استفاده قرار می گیرد البته شما می توانید به صورت دستی آن را فعال کنید.

Bypass WebKnight

این گزینه برای دور زدن فایروال برنامه های تحت وب AQTRONIX WebKnight و بسیاری دیگر از فایروال های مشابه استفاده می شود. این گزینه به صورت خودکار توسط برنامه مورد استفاده قرار می گیرد البته شما می توانید به صورت دستی آن را فعال کنید.

جایگزینی عبارات دلخواه در تزریق

گاهی اوقات لازم است تا عباراتی را در تزریق ها جایگزین کنید تا از به دام افتادن در فیلترها جلوگیری کنید. در این شرایط می توانید از گزینه ی Replacement استفاده کنید. برای مثال اگر می خواهید در تمام تزریق ها عبارت 'select' با 'SeLeCt' عوض شود، در سربرگ 'evasion' در تنظیمات بر روی Replacement کلیک کنید سپس بر روی '+' کلیک کنید و عبارت زیر را وارد کنید

select::SeLeCt

www.ITSecTeam.com

ITSecTeam
IT Security Research & Penetration Testing Team

این باعث می شود تا عبارت 'SeLeCt' جایگزین 'select' در تمام تزریق ها شود.

Time based method delay

این گزینه مقدار زمان تاخیر را برای حالت تزریق مبتنی بر زمان مشخص می کند در صورتی که گزینه ی Auto انتخاب شود، مناسب ترین و سریعترین زمان به صورت خودکار توسط برنامه انتخاب می شود. در صورت تمایل می توانید مقدار دلخواه خود را بر حسب میلی ثانیه وارد کنید.

Blind table prefix

اگر پیشوند جداول هدف مورد نظر را می دانید می توانید با استفاده از این گزینه آن را مشخص کنید تا در حالت تزریق چشم بسته هویج از پیدا کردن پشوند خودداری کند تا در وقت صرفه جویی شود.

Blind column prefix

اگر پیشوند ستون های هدف مورد نظر را می دانید می توانید با استفاده از این گزینه آن را مشخص کنید تا در حالت تزریق چشم بسته هویج از پیدا کردن پشوند خودداری کند تا در وقت صرفه جویی شود.

Table list for blind guessing

با استفاده از این گزینه می توانید یک لیست از نام جداول را مشخص کنید تا هنگامی که هویج نمی تواند به روش معمول جداول را استخراج کند از آن برای حدس زدن نام جداول استفاده کند. هویج از یک لیست پیش فرض خود استفاده می کند در صورت تمایل می توانید ان را تغییر دهید.

Column list for blind guessing

با استفاده از این گزینه می توانید یک لیست از نام ستون ها را مشخص کنید تا هنگامی که هویج نمی تواند به روش معمول ستون ها را استخراج کند از آن برای حدس زدن نام ستون ها استفاده کند. هویج از یک لیست پیش فرض خود استفاده می کند در صورت تمایل می توانید ان را تغییر دهید.

www.ITSecTeam.com