

Re: [Full-disclosure] Pangolin v1.2.590 – The best SQL injector you've ever seen

# Re: [Full-disclosure] Pangolin v1.2.590 – The best SQL injector you've ever seen

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-03/msg00478.html>

---

- *From:* "Razi Shaban" <[razishaban@xxxxxxxx](mailto:razishaban@xxxxxxxx)>
  - *Date:* Wed, 26 Mar 2008 19:01:35 +0200
- 

Hmm...  
Backdoors eh?

Nice try.

--  
razi

On 3/26/08, A. Ramos <[aramosf@xxxxxxxx](mailto:aramosf@xxxxxxxx)> wrote:

Take a look over:  
<http://www.virustotal.com/analysis/0603d534b0128bf81ec57a8ab00e145c>

2008/3/26 <[zwell@xxxxxxxx](mailto:zwell@xxxxxxxx)>:

>  
>  
>  
> Pangolin is a GUI tool running on Windows to perform as more as possible  
> pen-testing through SQL injection. This version now supports following  
> databases and operations:  
>  
> \* MSSQL : Server informations, Datas, CMD execute, Regedit, Write file,  
> Download file, Read file, File Browser...  
> \* MYSQL : Server informations, Datas, Read file, Write file...  
> \* ORACLE : Server informations, Datas, Accounts cracking...  
> \* PGSQL : Server informations, Datas, Read file...  
> \* DB2 : Server informations, Datas, ...  
> \* INFORMIX : Server informations, Datas, ...  
> \* SQLITE : Server informations, Datas, ...  
> \* ACCESS : Server informations, Datas, ...  
> \* SYBASE : Server informations, Datas, ...  
> etc.

Re: [Full-disclosure] Pangolin v1.2.590 – The best SQL injector you've ever seen

>  
> And supports:  
> \* HTTPS support  
> \* Pre-Login  
> \* Proxy  
> \* Specify any HTTP headers(User-agent, Cookie, Referer and so on)  
> \* Bypass firewall setting  
> \* Auto-analyzing keyword  
> \* Detailed check options  
> \* Injection-points management  
> etc.  
>  
> What's the differences to the others?  
> \* Easy-of-use : What I try to do is making pen-tester more care about  
> result, not the process. All you should do is clicking the buttons.  
> \* Amazing Speed : so many people told you things about brute sql injection,  
> is it really necessary? Forget char-by-char, we can row-by-row(of course,  
> not every injection-point can do this)?  
> \* The exact check method : do you really think automated tools like  
> AWVS,APPSCAN can find all injection-points?  
>  
> So, whatever, just check it out, and then enjoy your feeling ;)  
> More information : <http://www.nosec.org/web/index.php?q=pangolin>  
> Download : [http://seclab.nosec.org/security/pangolin\\_bin.rar](http://seclab.nosec.org/security/pangolin_bin.rar)  
>  
> Declare: Pangolin is designed for security testing by pen-tester when he has  
> been authorized. DO NOT attack any website viciously or accept the  
> consequences!!!  
>  
>  
>  
> \_\_\_\_\_  
>  
> 2008t³4û €ç  
> \*( ×üó™@ö SCEôAE,,-‡“e>>

>  
> Full-Disclosure – We believe in it.  
> Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>  
> Hosted and sponsored by Secunia – <http://secunia.com/>  
>

—  
Alejandro Ramos / Alex — (aramosf@xxxxxxxxxx)  
molling://CISSP/GWAS/CISA  
<http://www.unsec.net>

Re: [Full-disclosure] Pangolin v1.2.590 – The best SQL injector you've ever seen

Re: [Full-disclosure] Pangolin v1.2.590 – The best SQL injector you've ever seen

---

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>

---

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>