

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

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

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-03/msg00489.html>

---

- *From:* "Russ McRee" <[holisticinfosec@xxxxxxxx](mailto:holisticinfosec@xxxxxxxx)>
  - *Date:* Wed, 26 Mar 2008 13:30:39 -0700
- 

<http://www.nosec.org/web/files/demon.exe>

<http://www.virustotal.com/analysis/0bfb9d08a2dfe0ad413d08491d0a82a3>

[http://www.nosec.org/web/files/pdf\\_poc.exe](http://www.nosec.org/web/files/pdf_poc.exe)

<http://www.virustotal.com/analysis/d619319b2c4a7c5bb3a81adf25bf6559>

<http://www.nosec.org/web/files/zps.exe>

<http://www.virustotal.com/analysis/26d6e7ff7aa79d20331906543a73d458>

On Wed, Mar 26, 2008 at 10:54 AM, josh <[mastahflank@xxxxxxxx](mailto:mastahflank@xxxxxxxx)> wrote:

Not me, although I did looked at it. I thought great, kiddies are going to love this

Sent from my BlackBerry(R) smartphone with SprintSpeed

-----Original Message-----

From: davidrook <[david.rook@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:david.rook@xxxxxxxxxxxxxxxxxxxxxxxx)>

Date: Wed, 26 Mar 2008 17:23:03

To: Razi Shaban <[razishaban@xxxxxxxx](mailto:razishaban@xxxxxxxx)>

Cc: full-disclosure@xxxxxxxxxxxxxxxxxxxx, webappsec@xxxxxxxxxxxxxxxxxxxx

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

I wonder how many readers of this list now have a backdoor on their machine.....

Razi Shaban wrote:

    Hmm...  
    Backdoors eh?

    Nice try.

    --  
    razi

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

On 3/26/08, A. Ramos <aramosf@xxxxxxxx> wrote:

Take a look over:

<http://www.virustotal.com/analysis/0603d534b0128bf81ec57a8ab00e145c>

2008/3/26 <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.  
>  
> And supports:  
> \* HTTPS support  
> \* Pre-Login  
> \* Proxy  
> \* Specify any HTTP headers(User-agent, Cookie, Referer  
and so on)

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

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

- > \* 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!!!
- >
- >
- >
- > \_\_\_\_\_
- >
- > 2008t^4û €ç
- > \*( ×üó™@ö SCEôAE,,-‡“e>>

Re: [Full-disclosure] Pangolin v1.2.590 – The best SQLinjector 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/>  
>

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

---

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/>

—  
David Rook | david.rook@xxxxxxxxxxxxxxxxxxxxxx  
Information Security Analyst

Realex Payments  
Enabling thousands of businesses to sell online.

Realex Payments, Dublin, [www.realexpayments.com](http://www.realexpayments.com)  
Castlecourt, Monkstown Farm, Monkstown, Co Dublin, Ireland  
Tel: +353 (0)1 2808 559 Fax: +353 (0)1 2808 538

Realex Payments, London, [www.realexpayments.co.uk](http://www.realexpayments.co.uk)  
1 Hammersmith Grove, London W6 0NB, England  
Tel: +44 (0)203 178 5370 Fax: +44 (0)207 691 7264

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

Pay and Shop Limited, trading as Realex Payments has its registered office at Castlecourt, Monkstown Farm, Monkstown, Co Dublin, Ireland and is registered in Ireland, company number 324929.

This mail and any documents attached are classified as confidential and are intended for use by the addressee(s) only unless otherwise indicated. If you are not an intended recipient of this email, you must not use, disclose, copy, distribute or retain this message or any part of it. If you have received this email in error, please notify us immediately and delete all copies of this email from your computer system(s).

--

---

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/>

--

Russ McRee, GCIH, GCFA, CISSP  
425-518-6998 cell  
holisticinfosec.org  
blog.holisticinfosec.org

---

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