Remotely Owning ‘Secure’ Parking Systems

José A. Guasch
José A. Guasch (Madrid - Spain)

- Tiger Team Technical Coordinator from Grupo SIA
- Security By Default Editor
- Rooted CON staff
DISCLAIMER
<table>
<thead>
<tr>
<th></th>
<th>Basics, patience, go deeper</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced skills</td>
<td>X</td>
</tr>
<tr>
<td>Basics, patience, go deeper</td>
<td>✓</td>
</tr>
</tbody>
</table>
## DISCLAIMER

<table>
<thead>
<tr>
<th>Advanced technical skills</th>
<th>Basics, patience, go deeper</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCADA, High tech engineering, sensors, PLC, zigbee,…</td>
<td>Web vulnerabilities</td>
</tr>
</tbody>
</table>
**DISCLAIMER**

<table>
<thead>
<tr>
<th>Advanced technical skills</th>
<th>Basics, patience, go deeper</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCADA, High tech engineering, sensors, PLC, zigbee,…</td>
<td>Web vulnerabilities</td>
</tr>
<tr>
<td>hacking tools</td>
<td>browser + os tools</td>
</tr>
</tbody>
</table>
## DISCLAIMER

<table>
<thead>
<tr>
<th>Advanced technical skills</th>
<th>Basics, patience, go deeper</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCADA, High tech engineering, sensors, PLC, zigbee,…</td>
<td>Web vulnerabilities</td>
</tr>
<tr>
<td>hacking tools</td>
<td>browser + os tools</td>
</tr>
<tr>
<td>isolated bugs</td>
<td>common vulnerabilities for every product lines of the vendor</td>
</tr>
</tbody>
</table>
BemroseBooth Paragon has secured an exclusive 3 year contract with NCP to supply tickets and ticket advertising

BemroseBooth Paragon has secured an exclusive 3 year contract with NCP to supply tickets and ticket advertising. BemroseBooth has been NCP’s exclusive supplier of

15/05 MobileNOW! to Launch Mobile Payments in Eight New Jersey City, Union
15/05 BemroseBooth Paragon has secured an exclusive 3 year contract with NCP to supply tickets and ticket advertising
16/05 Salt Lake City to Launch ParkLCS: New, Improved Mobile Parking App and Merchant Program
13/05 MBS: Traffic gets a new distributor in Poland
12/05 Substantial benefits with Nedap’s SENDIT RCI Calculator

JOBS
13/05 Senior Traffic Designer (Melbourne, AU)
13/05 Traffic Manager (Sydney, AU)
13/05 Operations Intern (Cranwei, US)
13/05 Senior Accounts Payable Coordinator (Harmitou, AU)
13/05 Head of Automotive Partnerships (London, UK)
13/05 UI Designer (London, UK)
13/05 Contract Manager (Milan Romnes, UK)
13/05 Assistant and Security Manager (Red Cross, UK)

TENDERS
15/05 SE-Stockholm: Parking meters
15/05 FR-Lyon: Car park management services
13/05 CH-Lausanne: Control, safety or signaling equ...
13/05 ES-Alhendiala: Underground car park constr...
13/05 IT-R magistrate: Car park management serv...
12/05 DE-Berlin: Construction work
12/03 CZ-Prague: Parking services
12/03 CZ-České Budějovice: Construction work
“When connecting [XXXX] server to the Internet, it can be accessed from any computer in the world, with the same interface and functionality.”

– The vendor <3
why parkings?
why parkings?

- Complex architecture
why parkings?

- Complex architecture
- Money everywhere
why parkings?

- Complex architecture
- Money everywhere
why parkings?

- Complex architecture
- Money everywhere
- Web based
why parkings?

- Complex architecture
- Money everywhere
- Web based
- **Connected to the Internet**
why parkings?

- Complex architecture
- Money everywhere
- Web based
- Connected to the Internet
- Remote management allowed, recommended, by default (support)
and.....
and.....
how?
PMS models evolution

Company 1 has a park solution **Model A**

Company 1 + Company 2

2008

Model B.1

Model B.2
controlling lane

- **Main functions:** ticket dispensing, ticket verifying and card reading
- It’s a Personal Computer! (Pentium)
- Connected to the **network**.
- **Intercom:** TCP/IP based module with speaker and microphone (Optional)
- Barrier has modes: Auto, Manual, Test…
pay stations

- Main functions: *collect da money!*
- Computer: Industrial PC
- Display: 15” TFT (resolution 1024x768, 400cd/m²), Integrated Touch Screen Panel
- Intercom: TCP/IP based module with speaker and microphone (Optional)
- Connected to the **network**
- Pay with Cards, Coins and Bank notes
Cashiers

- **Main functions:** *one computer to rule them all*
- Another PC, and also connected to the Internet
main app

- **Main functions:** one webapp to rule them all
- **Operating System:** Debian Linux based
- **Web Server:** Apache Server
- **Database System:** PostgreSQL
- **Virtual PBX:** Asterisk Server (for intercom solutions)
- **Network:** Standard TCP/IP
  - Ticket history, including license plate (option) details
  - Video surveillance with IP camera’s (option)
  - White list solution allowing entrance and exit with registered license plates
TESTING
MODEL A
THIS IS MY LOGIN
THIS IS MY SERVER INFORMATION

PHP Version 4.1.0

System Linux 2.4.17-1 #1 SMP Mon Dec 17 18:26:08 GMT 2001 i866 unknown
Build Date Sep 20 2002

Configure Command

Configure

Variable | Value
---|---
PWD | /dev/null
DBROOT | /dev/null
HOSTNAME | /dev/null
CONSOLE | /dev/null
LD_LIBRARY_PATH | /dev/null
splash | silent
MAIL | 0x31f
PRELEVEL | N
REDIRECT | /dev/null
MACHTYPE | 386-suse-linux
LINES | 48
ORACLE_HOME | /dev/null
SHLLVL | 2
COLUMNS | 128
SHELL | /bin/bash
HOSTTYPE | i386
OSTYPE | linux
HOME | /
TERM | linux
PATH | /bin:/bin:/usr/bin:
RUNLEVEL | 3
INIT_VERSION | sysvinit-2.82
DAEMON | /usr/bin/httpd
### Index of /main app path

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td>13-Sep-2005 08:15</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>changelog</td>
<td>13-Jul-2005 13:01</td>
<td>38k</td>
<td></td>
</tr>
<tr>
<td>conf/</td>
<td>13-Sep-2005 08:12</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>docs/</td>
<td>30-Jun-2004 14:36</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>excel.php</td>
<td>28-Jun-2005 11:31</td>
<td>5k</td>
<td></td>
</tr>
<tr>
<td>export.php</td>
<td>13-Apr-2005 16:42</td>
<td>8k</td>
<td></td>
</tr>
<tr>
<td>handkasse.php</td>
<td>16-Feb-2004 10:09</td>
<td>1k</td>
<td></td>
</tr>
<tr>
<td>images/</td>
<td>16-Feb-2004 10:09</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>includes/</td>
<td>13-Sep-2005 09:25</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>release.sh</td>
<td>07-Nov-2004 20:47</td>
<td>1k</td>
<td></td>
</tr>
<tr>
<td>scripts/</td>
<td>06-Jun-2005 11:41</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>statview.php</td>
<td>16-Feb-2004 10:09</td>
<td>4k</td>
<td></td>
</tr>
</tbody>
</table>
HERE ARE MY

- Predictable folders found on web server, and **browsable**
HERE ARE MY **BACKUPS**

- Predictable folders found on web server, and **browsable**

**DBYYYY-MM-DD.tgz** = PostgreSQL database dump
daily database dump

1. download the DB*.tgz file

2. Searching users and passwords inside the dump...

   pg_restore X.tgz | grep -i -A20 "Copy appusers" | awk -F\t '{print $1":"$11}'

3. Full list of users and their plaintext passwords
i’m the admin, trust me...

<table>
<thead>
<tr>
<th>File</th>
<th>Operation</th>
<th>Basic Data</th>
<th>Tariff Data</th>
<th>Configuration</th>
<th>Reports</th>
<th>Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• System Diagram</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Event Protocol</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Difference Counting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Means Of Payment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Season Cards</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Ticket Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Uhrzeit</td>
<td>Gerät</td>
<td>Ereignis</td>
<td>Ticket</td>
<td>Bestätigung</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------</td>
<td>--------------</td>
<td>----------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06.09.2013 21:19</td>
<td>Exit</td>
<td>302 Durchfahrt</td>
<td>138029073</td>
<td>ok</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06.09.2013 21:17</td>
<td>Exit</td>
<td>302 Durchfahrt</td>
<td>138029072</td>
<td>ok</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06.09.2013 21:16</td>
<td>Exit</td>
<td>302 Durchfahrt</td>
<td>138029071</td>
<td>ok</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06.09.2013 21:13</td>
<td>Exit</td>
<td>302 Durchfahrt</td>
<td>138029070</td>
<td>ok</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06.09.2013 21:12</td>
<td>Exit</td>
<td>302 Durchfahrt</td>
<td>138029069</td>
<td>ok</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06.09.2013 21:11</td>
<td>Exit</td>
<td>302 Durchfahrt</td>
<td>138029068</td>
<td>ok</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06.09.2013 21:10</td>
<td>Exit</td>
<td>302 Durchfahrt</td>
<td>138029067</td>
<td>ok</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06.09.2013 21:09</td>
<td>Exit</td>
<td>302 Durchfahrt</td>
<td>138029066</td>
<td>ok</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06.09.2013 21:08</td>
<td>Exit</td>
<td>302 Durchfahrt</td>
<td>138029065</td>
<td>ok</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06.09.2013 21:07</td>
<td>Exit</td>
<td>302 Durchfahrt</td>
<td>138029064</td>
<td>ok</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
black magic! witchcraft!
i can help you with the surveillance
MODEL A - Summary

- **info php** - environment information
- directory listing enable at the web server (/backup...)
- Access to backups information
  - sensitive info
  - clients tickets and season cards
  - users/pwds
- no user/password policy (minchars, user=pass,...)
MODEL A - Summary

- **info.php** - environment information
- Directory listing enabled at the web server (/backup...)
- Access to backups information
  - Sensitive info
  - Clients' tickets and season cards
  - Users/passwords
- No user/password policy (minchars, user=pass,...)
TESTING
MODEL B
THIS IS MY LOGIN
backup folder?
backup folder?

Forbidden

You don't have permission to access /backup/ on this server.

Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny16 with Suhoisn-Patch mod_ssl/2.2.9 OpenSSL/0.9.8g Server at Port 80

oh :(
direct access to **backup** files?
direct access to backup files?

Not Found

The requested URL /backup/DB2013-08-07.tgz was not found on this server.

Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny9 with Suhosin-Patch mod_ssl/2.2.9 OpenSSL/0.9.8g Server at Port 443

oh :(
environment information?

<table>
<thead>
<tr>
<th>PHP Version 5.2.6-1+lenny16</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System</strong></td>
</tr>
<tr>
<td><strong>Build Date</strong></td>
</tr>
<tr>
<td><strong>Server API</strong></td>
</tr>
<tr>
<td><strong>Virtual Directory Support</strong></td>
</tr>
<tr>
<td><strong>Configuration File (php.ini) Path</strong></td>
</tr>
<tr>
<td><strong>Loaded Configuration File</strong></td>
</tr>
<tr>
<td><strong>Scan this dir for additional .ini files</strong></td>
</tr>
<tr>
<td><strong>PHP API</strong></td>
</tr>
<tr>
<td><strong>PHP Extension</strong></td>
</tr>
<tr>
<td><strong>Zend Extension</strong></td>
</tr>
<tr>
<td><strong>Debug Build</strong></td>
</tr>
<tr>
<td><strong>Thread Safety</strong></td>
</tr>
<tr>
<td><strong>Zend Memory Manager</strong></td>
</tr>
<tr>
<td><strong>IPv6 Support</strong></td>
</tr>
<tr>
<td><strong>Registered PHP Streams</strong></td>
</tr>
<tr>
<td><strong>Registered Stream Socket Transports</strong></td>
</tr>
</tbody>
</table>

yay! always....
and the login?
and the login?

admin:admin ?
and the login?

admin:admin ?
and the login?

admin:admin ?

' or '1'='1 ?
and the login?

admin:admin ? 

' or '1'='1 ?
and the login?

admin:admin ? ✗

' or '1'='1 ? ✗

test:test ?
and the login?

admin:admin ✗

' or '1'='1 ✗

test:test ✓
we are in! more or less...
we are in! more or less...
we are in! more or less...
Manuals for every parking device (cashiers, web application, pay stations...)

We get:

- Network services used by the parking management system
- FTP and Samba default u/p for backup
what we have until now?

- environment information (phpinfo Information disclosure)
- users/passwords for Samba and FTP (default, but accounts not always exist)
- extra services available by the product (not always exposed to internet)
- access with ‘test’ account (VERY restricted)
what we have until now?

- environment information (phpinfo Information disclosure)
- users/passwords for Samba and FTP (default, but accounts not always exist)
- extra services available by the product (not always exposed to internet)
- access with ‘test’ account (VERY restricted)

going back to the restricted access with test account...
wait...how the webapp manage downloads?
wait...how the webapp manage downloads?

https://<host>/<main path>/<main file>.php?
mod=base&page=download&dir=manuals&file=<filename.pdf>
wait...how the webapp manage downloads?

https://<host>/<main path>/<main file>.php?
mod=base&page=download&dir=manuals&file=<filename.pdf>

../../../../etc/passwd
wait...how the webapp manage downloads?

https://<host>/<main path>/<main file>.php?
mod=base&page=download&dir=manuals&file=<filename.pdf>

../../../../etc/passwd
path traversal in ‘download’ module

- System files
  - /etc/passwd - users and their shell
  - /etc/hostname - hostname
  - /etc/hosts - systems on the network
  - /var/log/syslog - important paths and users

- Services files
  - /etc/sshd.conf - SSH server configuration
  - xferlog (proftpd) - important paths and files
  - asterisk.conf - Intercom configuration
  - ...

- application files and scripts
  - <webapp>.php - some paths and vulnerabilities
  - rpc.php - bypassing web-gui
  - modules - some paths and vulnerabilities
  - ...

- application specific log files
  - <webapp>.log - important paths and files
  - ...

path traversal in ‘download’ module

- **System files**
  - `/etc/passwd` - users and their shell
  - `/etc/hostname` - hostname
  - `/etc/hosts` - systems on the network
  - `/var/log/syslog` - important paths and users

- **Services files**
  - `/etc/sshd.conf` - SSH server configuration
  - `xferlog` (proftpd) - important paths and files
  - `asterisk.conf` - Intercom configuration
  - ...

- **application files and scripts**
  - `<webapp>.php` - some paths and vulnerabilities
  - `rpc.php` - bypassing web-gui
  - `modules` - some paths and vulnerabilities
  - ...

- **application specific log files**
  - `<webapp>.log` - important paths and files
  - ...

typical exposed system services (FTP)

asterisk:x:1001:1001::/home/asterisk:/bin/ftp
flashimage:x:1003:1004::/nonexistent:/bin/ftp
pms-acs:x:1002:1002::/home/pms-acs:/bin/ftp
*********:x:1005:1002::/nonexistent:/bin/ftp
typical exposed system services (FTP)

asterisk:x:1001:1001::/home/asterisk:/bin/ftp
flashimage:x:1003:1004::/nonexistent:/bin/ftp
pms-acs:x:1002:1002::/home/pms-acs:/bin/ftp
*********:x:1005:1002::/nonexistent:/bin/ftp

Users with user=password (remembering the manual?)
Users with user=password (remembering the manual?)

- FTP Login successful with **pms-acs** account
- Two folders at home folder: **backup** + **pms-acs**
- Inside backup folder: `<hostname>.tgz` + `<hostname>_bin.tgz`
inside the .tgz files (I)

- Partial path to the database dump (current) stored at the system
  - swe/<name of product>/*
    - swe/<name of product>/database/<hostname>.dump

*database dump (plain text of PostgreSQL)*
inside the .tgz files (II)

- `swe/<name of product>/`

- `swe/<name of product>/etc/properties-<hostname>.tgz`

'`etc` + 'home' + 'tftpboot' folders backup

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>apache2</td>
<td>hosts.2009.01.26</td>
</tr>
<tr>
<td>apcupsd</td>
<td>hosts.2009.11.19_11.48</td>
</tr>
<tr>
<td>asterisk</td>
<td>hosts.2009.11.19_11.50</td>
</tr>
<tr>
<td>cups</td>
<td>hosts.2009.11.19_12.36</td>
</tr>
<tr>
<td>debian_version</td>
<td>hosts.2009.11.19_12.38</td>
</tr>
<tr>
<td>default</td>
<td>hosts.2009.11.19_13.00</td>
</tr>
<tr>
<td>exports</td>
<td>hosts.2010.02.10_15.18</td>
</tr>
<tr>
<td>fstab</td>
<td>hosts.allow</td>
</tr>
<tr>
<td>group</td>
<td>hosts.deny</td>
</tr>
<tr>
<td>ha.d</td>
<td>init.d</td>
</tr>
<tr>
<td>host.conf</td>
<td>initmtab</td>
</tr>
<tr>
<td>hostname</td>
<td>isdn</td>
</tr>
<tr>
<td>hosts</td>
<td>issue</td>
</tr>
<tr>
<td>issue</td>
<td>issue.mgetty</td>
</tr>
<tr>
<td>netadm</td>
<td>issue.net</td>
</tr>
<tr>
<td>modprobe</td>
<td>modprobe.d</td>
</tr>
<tr>
<td>default</td>
<td>modules</td>
</tr>
<tr>
<td>init</td>
<td>modutils</td>
</tr>
<tr>
<td>optconfig</td>
<td>motd</td>
</tr>
<tr>
<td>passwd</td>
<td>network</td>
</tr>
<tr>
<td>passwd-old</td>
<td>openvpn</td>
</tr>
<tr>
<td>pcmcia</td>
<td>passwd</td>
</tr>
<tr>
<td>ppp</td>
<td>passwd-</td>
</tr>
<tr>
<td>printcap</td>
<td>printcap</td>
</tr>
</tbody>
</table>
inside the .tgz files (II)

- `swe/<name of product>/`

- `swe/<name of product>/etc/properties-<hostname>.tgz`

  `etc` + `home` + `tftpboot` folders backup
inside the .tgz files (II)

- swe/\<name of product\>/

- swe/\<name of product\>/etc/properties-\<hostname\>.tgz

`etc` + `home` + `tftpboot` folders backup
/etc/shadow file

root:$1$1OchR2Tm$jfXqBluZDSXjDCdY2cK9.1:14173:0:99999:7:::
????????:$1$5rwtf/qk$9eVMajU7xyj7PGPHqPrV/:14173:0:99999:7:::
pms-acs:$1$14z6oJdq$W0bSieC1sQjmqXiycdc4C.:14189:0:99999:7:::
flashimage:$1$hez46n1/$kWLNG9f4ygvBw8xHbK.0g1:14390:0:99999:7:::

cracking...
/etc/shadow file

root:$1$1OchR2Tm$jfXqBluZDSXjDCdY2cK9:1:14173:0:99999:7:::
???????:$1$5rwtf/qk$9eVMajU7xyj7PGPHqpPrV/:14173:0:99999:7:::
pms-acs:$1$14z6oJdq$W0bSieC1sQjmqXiycdc4C:14189:0:99999:7:::
flashimage:$1$hez46n1/$kW1NG9f4ygvBw8xHbK.0g1:14390:0:99999:7:::

cracking... and after 9 seconds...
/etc/shadow file

cracking... and after 9 seconds...

root:parking:14173:0:99999:7:::

????????:parking:14173:0:99999:7:::

flashimage:flashimage:14390:0:99999:7:::
typical exposed system services (SSH)

• Trying SSH Login with root account
  • PermitRootLogin No - root account not allowed to connect directly through SSH
• SSH Login with ??????? account
• su :) -> root
important full paths of files (backups)

- /swe/<name of product>/database/<HOSTNAME>.dump - plain text database dump
- /swe/public/ftp/backup/<HOSTNAME>.tgz - whole backup of server (no binaries)
- /swe/public/ftp/backup/<HOSTNAME>_bin.tgz - whole backup of server (with binaries)
- /swe/<name of product>/etc/properties-<HOSTNAME>.tgz - backup of whole ‘etc’ folder
important full paths of files (backups)

- `/swe/<name of product>/database/<HOSTNAME>.dump` - plain text database dump
- `/swe/public/ftp/backup/<HOSTNAME>.tgz` - whole backup of server (no binaries)
- `/swe/public/ftp/backup/<HOSTNAME>_bin.tgz` - whole backup of server (with binaries)
- `/swe/<name of product>/etc/properties-<HOSTNAME>.tgz` - backup of whole ‘etc’ folder

remember **phpinfo**? remember the **path traversal** vulnerability?
now we have the full path of this **yummy** files!
one more thing...
<table>
<thead>
<tr>
<th>Tickets</th>
</tr>
</thead>
<tbody>
<tr>
<td>BBVA</td>
</tr>
<tr>
<td>PUERTO DEPORTIVO</td>
</tr>
<tr>
<td>COMERCIO: 323270520</td>
</tr>
<tr>
<td>TPV: 00574505513</td>
</tr>
<tr>
<td>APLIC.: A0000000031010</td>
</tr>
<tr>
<td>VISA DIEZ</td>
</tr>
<tr>
<td>*************7636</td>
</tr>
<tr>
<td>Tran:00222</td>
</tr>
<tr>
<td>Sec:01</td>
</tr>
<tr>
<td>VENTA</td>
</tr>
</tbody>
</table>
oh my dump!
tickets
oh my dump!

tickets

taking a look to the <hostname>.dump file...

COPY creditcard (i_transno, dt_date, i_deviceid, i_ticketno, cIssuer, cCardno, cBlz, cKtonr, cMerchantno, cAuthcode, cRefcode, cSwitchcardno, dtDateofexp, nValue, dtAccounted, dtInsdate, cIssuer, dtAenddate, cAenduser, cSpur2, iReceiptno) FROM stdin;
SEXTUPLE FACEPALM

A fail of such epic proportions a group facepalm is required
MODEL B - Summary

- info.php
- bad user/password policy in application (minchars, user=pass,...)
- default/test users like test:test
- download manuals
  - user=passwd (backup users)
- exposed services: ftp, ssh (no PermitRootLogin :/ )
- path traversal
  - internal folders
  - app logic
  - system logs (syslog, ftp, application...)
  - system info (passwd, issue, ftp, hostname, network...)
- bad user/password policy in system!
- full access as root in every system
- sensitive information on database dumps
MODEL B - Summary

- info.php
- bad user/password policy in application (minchars, user=pass,...)
- default/test users like test:test
- download manuals
  - user=passwd (backup users)
- exposed services: ftp, ssh (no PermitRootLogin :/ )
- path traversal
  - internal folders
  - app logic
  - system logs (syslog, ftp, application...)
  - system info (passwd, issue, ftp, hostname, network...)
- bad user/password policy in system!
- full access as root in every system
- sensitive information on database dumps
What we can do with this?
<table>
<thead>
<tr>
<th>Dispositivo</th>
<th>Estatus</th>
<th>Ticket</th>
<th>Dispositivo</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENTRADA 1</td>
<td></td>
<td>118569516</td>
<td>ENTRADA 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2290</td>
<td></td>
</tr>
<tr>
<td>SALIDA 1</td>
<td></td>
<td>214743647</td>
<td>CAJERO AUTOMÁTICO</td>
</tr>
<tr>
<td>CAJERO MANUAL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Código</td>
<td>Mensaje</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1097</td>
<td>Por favor espere</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1118</td>
<td>Por favor seleccionar los días de la semana preferidos</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1284</td>
<td>Por Favor introduzca Datos</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1417</td>
<td>Por Favor Seleccionar la Fecha</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3105</td>
<td>¡Contraseña Antigua Disponible, Por Favor Editar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3108</td>
<td>¡Datos incorrectos! Por Favor vuelva a introducir</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5003</td>
<td>Por favor Compruebe Sus Datos</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5009</td>
<td>Por favor Compruebe Sus Datos</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5010</td>
<td>Por favor Seleccione primero los Datos del Display</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5068</td>
<td>Por favor introduzca su Contraseña</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5140</td>
<td>Por favor actualizar los datos</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5451</td>
<td>Sesión inactiva durante demasiado tiempo. Por favor vuelva entrar en el Sistema.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>36002</td>
<td>Por favor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>36011</td>
<td>Por favor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>36052</td>
<td>Por favor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Número</td>
<td>español</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>---------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Por favor</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1097 Por favor espere
1118 Por favor seleccionar los días de la semana preferidos
1284 Por Favor Introduzca Datos
1417 Por Favor Seleccionar la Fecha
3105 ¡Contraseña Antigua Disponible, Por Favor Editar
3108 ¡Datos incorrectos! Por Favor vuelva a introducir
5008 Por favor Compruebe Sus Datos
5009 Por favor Compruebe Sus Datos
5010 Por favor Seleccionando primero los Datos del Display
5068 Por favor introduzca su Contraseña
5140 Por favor actualizar los datos
5451 Sesión inactiva durante demasiado tiempo. Por favor vuelva entrar en el Sistema.
36002 Por favor
36011 Por favor
36052 Por favor
troll mode
troll mode

- open/close barrier gates (*Ignore Presence?*)
troll mode

- open/close barrier gates (Ignore Presence?)
- close the parking even empty
troll mode

- open/close barrier gates *(Ignore Presence?)*
- close the parking even empty
- my license plate -> always allowed
troll mode

- open/close barrier gates (**Ignore Presence?**)  
- close the parking even empty  
- my license plate -> always allowed  
- change voice messages at entrance and exit, as well as the devices string
troll mode

- open/close barrier gates (*Ignore Presence?*)
- close the parking even empty
- my license plate -> always allowed
- change voice messages at entrance and exit, as well as the devices string
- Print custom tickets, with ascii images like…
troll mode

- open/close barrier gates *(Ignore Presence?)*
- close the parking even empty
- my license plate -> always allowed
- change voice messages at entrance and exit, as well as the devices string
- Print custom tickets, with ascii images like…
- Display movies at Pay Stations LCD
crook mode
crook mode

- plant malware on cashier and pay stations devices (POS)
crook mode

- plant malware on cashier and pay stations devices (**POS**)  
- steal credit card information from dumps
crook mode

- plant malware on cashier and pay stations devices (POS)
- steal credit card information from dumps
- fake messages on devices regarding payments
crook mode

- plant malware on cashier and pay stations devices (POS)
- steal credit card information from dumps
- fake messages on devices regarding payments
- manually open pay stations and coin boxes
crook mode

- plant malware on cashier and pay stations devices (POS)
- steal credit card information from dumps
- fake messages on devices regarding payments
- manually open pay stations and coin boxes
- season cards reselling
License No: [redacted]
Contract: Shortterm Parking
Access Profile: Shortterm Parking - AP
Card Type: Shortterm ticket
Card Status: Present

Entry Time: 20/09/2013 11:17
Exit Time: 20/09/2013 12:05

Images
20/09/2013 11:17:36

[Image of a person driving a vehicle]
spy mode

- access cameras
- clients presence and habits
- warning when license plate/customers detected
conclusions

- Be careful what you expose on the Internet
- Harden!
- Avoid defaults!
- Restrict!
<table>
<thead>
<tr>
<th>IP</th>
<th>Port</th>
<th>Host</th>
<th>Hostname</th>
<th>Country</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>101.54.4</td>
<td>443</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>109.2.29</td>
<td>443</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>109.rev.afr.net</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>123.33</td>
<td>80</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>109.232</td>
<td>443</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>109.232.gdansk.pl</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>123.59.99</td>
<td>8080</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>123.8.134</td>
<td>80</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>110.161.216</td>
<td>443</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>109.rev.afr.net</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>123.16.149.107</td>
<td>443</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>120.146.5.7</td>
<td>443</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>120.146.5.7</td>
<td>443</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>123.27.54</td>
<td>443</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>109.rev.afr.net</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Showing 1 to 15 of 294 entries
THANKS!