

Mitbringsel aus dem Alltag

Star Wars in der niedersächsischen Provinz

Alexander Neumann
RedTeam Pentesting GmbH
kontakt@redteam-pentesting.de
<https://www.redteam-pentesting.de>

17. Januar 2023

Unser Alltag

Das tun, was man normalerweise nicht darf! Fast alles ist erlaubt!

Beispiel: Netzwerk-Penetrationstest

- ★ Telefonanlage von Auerswald (COMpact 5500R) gefunden
- ★ Bietet Passwort-Vergessen-Funktion
- ★ Normaler Weg: Kunde kontaktiert Hersteller, bekommt Passwort

Erste Schritte

- ★ Firmware heruntergeladen
- ★ Entpackt, basiert auf Linux
- ★ Programm webserver gefunden
- ★ ⇒ Ghidra

Ghidra

File Edit Analysis Graph Navigation Search Select Tools Window Help

Listing: webservr

```

// segment_3.1
// Loadable segment [0x0000 - 0x3Bee03]
// ras:00008000-ras:00008153

assume spr = 0x0 (Default)
Elf32_Ehdr_00008000

00008000 7f 45 4c      Elf32_Ehdr
           46 01 01
           01 00 00 ...

00008000 7f          db          7fh

00008001 45 4c 46      ds          "ELF"
00008004 01          1h          28h
00008005 01          db          1h
00008006 01          db          1h
00008007 00          db          0h
00008008 00          db          0h
00008009 00 00 00 00 db[7]
           00 00

00008010 02 00        dw          2h
00008012 28 00        dw          28h
00008014 01 00 00 00 ddw         1h
00008018 00 ef 00 00 ddw         entry
0000801c 34 00 00 00 ddw         Elf32_Phdr_ARRAY_000080...
00008020 ac 4a 39 00 ddw         Elf32_Shdr_ARRAY__elfs...
00008024 02 00 00 05 ddw         5000002h
00008028 34 00        dw          34h
0000802a 20 00        dw          20h
0000802c 09 00        dw          9h
0000802e 28 00        dw          28h
00008030 14 00        dw          14h
00008032 1c 00        dw          1c

00008034 01 00 00      Elf32_Ph...
           70 2c dd
           37 00 2c ...

// .interp
// SHF_PROGBITS [0x0154 - 0x0166]

```

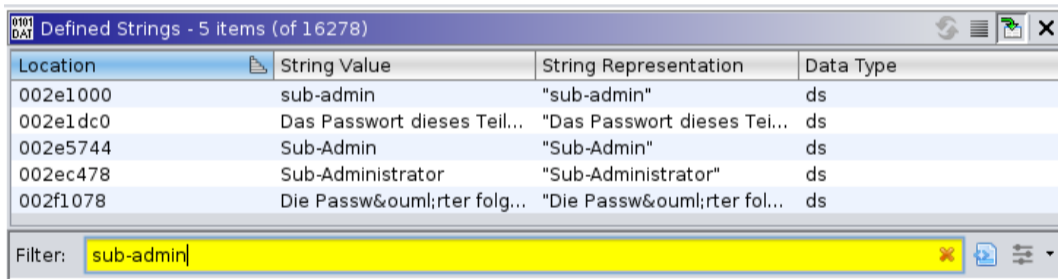
Defined Strings - 16276 items

Location	String Value	String Representa...	Data Type
.shstrtab:00000000...	.shstrtab	".shstrtab"	ds
.shstrtab:00000000...	.interp	".interp"	ds
.shstrtab:00000000...	.note.ABI-tag	".note.ABI-tag"	ds
.shstrtab:00000000...	.note.gnu.build-id	".note.gnu.build-id"	ds
.shstrtab:00000000...	.hash	".hash"	ds
.shstrtab:00000000...	.dysym	".dysym"	ds
.shstrtab:00000000...	.dynstr	".dynstr"	ds
.shstrtab:00000000...	.gnu.version	".gnu.version"	ds
.shstrtab:00000000...	.gnu.version_r	".gnu.version_r"	ds
.shstrtab:00000000...	.rel.dyn	".rel.dyn"	ds
.shstrtab:00000000f...	.rel.plt	".rel.plt"	ds
.shstrtab:00000000...	.init	".init"	ds
.shstrtab:00000000...	.text	".text"	ds
.shstrtab:00000000...	.fini	".fini"	ds
.shstrtab:00000000...	.rodata	".rodata"	ds
.shstrtab:00000000...	.ARM.extab	".ARM.extab"	ds
.shstrtab:00000000...	.ARM.exidx	".ARM.exidx"	ds
.shstrtab:00000000...	.tbss	".tbss"	ds
.shstrtab:00000000...	.init_array	".init_array"	ds
.shstrtab:00000000...	.fini_array	".fini_array"	ds
.shstrtab:00000000...	.jcr	".jcr"	ds
.shstrtab:00000000...	.data.rel.ro	".data.rel.ro"	ds
.shstrtab:00000000...	.dynamic	".dynamic"	ds
.shstrtab:00000000...	.got	".got"	ds
.shstrtab:00000000...	.data	".data"	ds
.shstrtab:00000000...	.bss	".bss"	ds
.shstrtab:00000000f...	.ARM.attributes	".ARM.attributes"	ds
00008001	ELF	".ELF"	ds
00008154	/lib/ld-linux.so.3	".lib/ld-linux.so.3"	ds
00008194	GNU	".GNU"	ds
0000ade5	libcgi.so.0	".libcgi.so.0"	ds
0000ad72	__gmon_start__	".__gmon_start__"	ds
0000ae01	_Jv_RegisterClasses	"._Jv_RegisterClasses..."	ds
0000ae15	.fini	".fini"	ds
0000ae1b	FCGX_VFPriNF	".FCGX_VFPriNF"	ds
0000ae29	FCGX_FFush	".FCGX_FFush"	ds

Decompile: FUN_0001bccc x Defined Strings x

0001bccc FUN_0001bccc stmbd spl.{r4 r5 r6 r7 r8 r9 r...

Ghidra - Strings



0101
D.A.T Defined Strings - 5 items (of 16278)

Location	String Value	String Representation	Data Type
002e1000	sub-admin	"sub-admin"	ds
002e1dc0	Das Passwort dieses Teil...	"Das Passwort dieses Tei..."	ds
002e5744	Sub-Admin	"Sub-Admin"	ds
002ec478	Sub-Administrator	"Sub-Administrator"	ds
002f1078	Die Passwörter folg...	"Die Passwörter fol..."	ds

Filter: sub-admin

Ghidra - Vergleich Admin-Benutzer



```
C:\Decompile: web_getAccessLevel - (webserver)
549 LAB_0001568c:
550     puVar4 = (undefined4 *)strcmp((char *)username, "sub-admin");
551     if (puVar4 == (undefined4 *)0x0) {
552         local_5be = 0;
553         local_5c4 = puVar4;
554         local_5e0 = (undefined4 *)
555             FUN_001b4444(param_1[2], &local_5c4, &local_5be, "WHERE isSubAdmin=1");
556     if (local_5e0 == (undefined4 *)0x0) {
557         puVar4 = (undefined4 *) (uint)local_5be;
558         if (puVar4 == (undefined4 *)0x0) {
559             local_5ec = local_5c4;
560             local_5e0 = puVar4;
561         }
562         else {
563             local_5ec = local_5c4;
```

Ghidra - Vergleich „Schandelah“?

```
Decompile: web_getAccessLevel - (webserver)
504     puVar4 = input_password;
505 LAB_00015930:
506     if ((uVar9 & (uint)local_5f8) == 0) goto LAB_0001593c;
507 LAB_00015340:
508     iVar10 = strcmp((char *)username,"Schandelah");
509     if (iVar10 == 0) {
510         gen_password(0,&generated_password);
511         if (input_password == (undefined4 *)0x0) {
512             iVar10 = FUN_00121668(*param_1,param_1 + 0x10);
513             if (iVar10 != 0) goto LAB_00015ea8;
514         }
515         else {
516             iVar10 = strcmp((char *)input_password,(char *)&generated_password);
517             if (iVar10 == 0) {
LAB_00015ea8:
```


W Schandelah - Wikipedia x +

de.wikipedia.org/wiki/Schandelah

Nicht angemeldet [Diskussionsseite](#) [Beiträge](#) [Benutzerkonto erstellen](#) [Anmelden](#)

Artikel [Diskussion](#) Lesen [Bearbeiten](#) [Quelltext bearbeiten](#) [Versionsgeschichte](#)

Koordinaten: 52° 15′ 56″ N, 10° 41′ 15″ O

Schandelah

Schandelah ist ein **Dorf** in **Niedersachsen**, 15 km östlich von **Braunschweig** gelegen. Schandelah gehört zur Gemeinde **Cremlingen** im Landkreis **Wolfenbüttel** und hat über 2000 Einwohner, einen Bahnhof, einen Kindergarten, eine Grundschule und einen **Sportverein**.

Inhaltsverzeichnis [Verbergen]

- 1 **Geographie**
 - 1.1 **Geopunkt Jurameer Schandelah**
- 2 **Geschichte**
- 3 **Politik**
 - 3.1 **Ortsrat**

Schandelah

Gemeinde **Cremlingen**



Höhe:	101 m
Einwohner:	2277 (31. Dez. 2017) ^[1]
Eingemeindung:	1. März 1974

Wirtschaft und Infrastruktur [\[Bearbeiten | Quelltext bearbeiten \]](#)

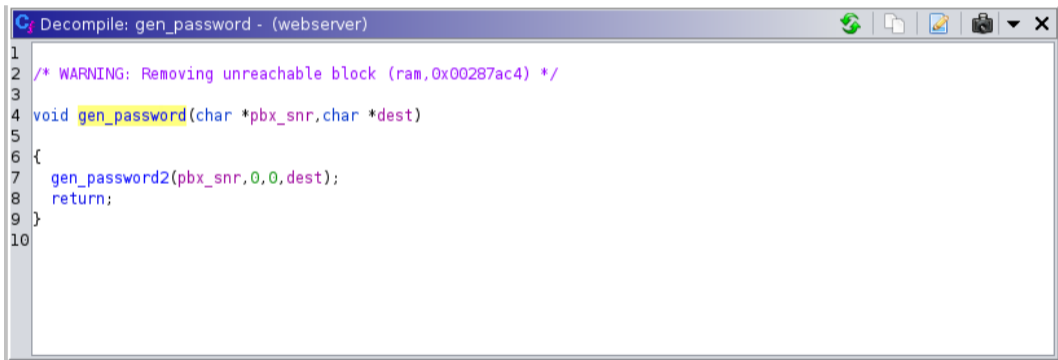
Unternehmen [\[Bearbeiten | Quelltext bearbeiten \]](#)

Die Firma Auerswald GmbH & Co. KG, ein Hersteller von Telekommunikationsanlagen, unterhält am Ort eine Produktionsstätte.

Ghidra - Benutzer „Schandelah“

```
Decompile: web_getAccessLevel - (webserver)
504     puVar4 = input_password;
505 LAB_00015930:
506     if ((uVar9 & (uint)local_5f8) == 0) goto LAB_0001593c;
507 LAB_00015340:
508     iVar10 = strcmp((char *)username,"Schandelah");
509     if (iVar10 == 0) {
510         gen_password(0,&generated_password);
511         if (input_password == (undefined4 *)0x0) {
512             iVar10 = FUN_00121668(*param_1,param_1 + 0x10);
513             if (iVar10 != 0) goto LAB_00015ea8;
514         }
515         else {
516             iVar10 = strcmp((char *)input_password,(char *)&generated_password);
517             if (iVar10 == 0) {
LAB_00015ea8:
```

Ghidra - Passwort



```
Decompile: gen_password - (webserver)
1
2 /* WARNING: Removing unreachable block (ram,0x00287ac4) */
3
4 void gen_password(char *pbx_snr,char *dest)
5
6 {
7     gen_password2(pbx_snr,0,0,dest);
8     return;
9 }
10
```

Ghidra - Passwort #2

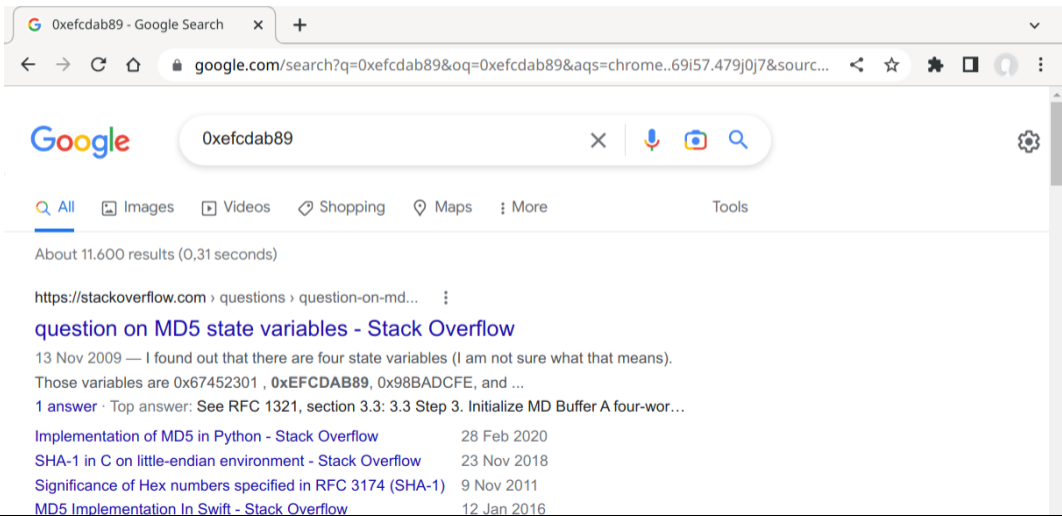
```
Decompile: gen_password2 - (webserver)
1
2 void gen_password2(char *pbx_snr,int include_lang,uint lang_index,char *dest)
3
4 {
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48 local_84 = 0;
49 local_80 = 0;
50 lang = 0;
51 if (pbx_snr == (char *)0x0) {
52     pbx_snr = (char *)&local_84;
53     auer_getPbxSerialNumber(pbx_snr,0x21);
54 }
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74 date_string = current_date_as_string(&local_3c,0x10);
75 __snprintf_chk(&local_c4,0x40,1,0x40,"%s%s%s%s",pbx_snr,"r2d2",date_string,&lang);
76 func_3518(&local_c4,&local_60);
77 auer_strncpy(dest,&local_60,8);
```

Ghidra - Mysteriöse Funktion

C# Decompile: func_3518 - (webserver)

```
1
2 void func_3518(char *data_src, char *data_dest)
3
4 {
5     size_t data_src_len;
6     undefined4 local_94;
7     undefined4 local_90;
8     undefined4 local_8c;
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32 local_2c = __stack_chk_guard;
33 local_90 = 0xefcdab89;
34 local_94 = 0x67452301;
35 local_8c = 0x98badcfe;
36 local_88 = 0x10325476;
37 data_src_len = strlen(data_src);
38 md5_update(&local_94, data_src, data_src_len);
39 md5_finalize(&local_3c, &local_94);
40 *data_dest = "0123456789abcdef"[local_3c >> 4];
41 data_dest[1] = "0123456789abcdef"[local_3c & 0xf];
42 data_dest[2] = "0123456789abcdef"[local_3b >> 4];
43 data_dest[3] = "0123456789abcdef"[local_3b & 0xf];
```

OSINT #2



A screenshot of a Google search page. The browser's address bar shows the URL `google.com/search?q=0xefcdab89&oq=0xefcdab89&aqs=chrome..69i57.479j0j7&sourc...`. The search bar contains the text `0xefcdab89`. Below the search bar, the navigation menu includes `All`, `Images`, `Videos`, `Shopping`, `Maps`, `More`, and `Tools`. The search results show approximately 11,600 results found in 0.31 seconds. The top result is a link to a Stack Overflow question titled "question on MD5 state variables - Stack Overflow", dated 13 Nov 2009. The snippet of the question reads: "I found out that there are four state variables (I am not sure what that means). Those variables are 0x67452301, 0xEFCDAB89, 0x98BADCFE, and ...". Below the question, there is a link to "1 answer" and a snippet of the top answer: "See RFC 1321, section 3.3: 3.3 Step 3. Initialize MD Buffer A four-wor...". Below the main result, there are four additional search results, each with a title and a date:

- [Implementation of MD5 in Python - Stack Overflow](#) 28 Feb 2020
- [SHA-1 in C on little-endian environment - Stack Overflow](#) 23 Nov 2018
- [Significance of Hex numbers specified in RFC 3174 \(SHA-1\)](#) 9 Nov 2011
- [MD5 Implementation In Swift - Stack Overflow](#) 12 Jan 2016

Ghidra - Passwort #2

```
Decompile: gen_password2 - (webserver)
60 lang = 0;
61 if (pbx_snr == (char *)0x0) {
62     pbx_snr = (char *)&local_84;
63     auer_getPbxSerialNumber(pbx_snr,0x21);
64 }
65 if (include_lang != 0) {
66     if (lang_index < 0x12) {
67         __strcpy_chk(&lang,(&language_table)[lang_index],8);
68     }
69     else {
70         lang = 0x2e612e6e;
71         local_28 = local_28 & 0xfffff00;
72     }
73 }
74 date_string = current_date_as_string(&local_3c,0x10);
75 __snprintf_chk(&local_c4,0x40,1,0x40,"%s%s%s",pbx_snr,"r2d2",date_string,&lang);
76 md5_as_hexstring(&local_c4,&local_60);
77 auer_strncpy(dest,&local_60,8);
78 if (local_24 == __stack_chk_guard) {
79     return;
80 }
81 /* WARNING: Subroutine does not return */
82 stack_chk_fail(dest);
```


Passwort für Benutzer Schandelah ausrechnen:

1. MD5(Seriennummer + r2d2 + Datum)
2. Davon die ersten 7 Zeichen

Problem: Wie bekommt man Seriennummer und Datum?

Einfach das Gerät fragen:

```
$ curl --include https://192.168.1.2/about_state
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8;
[...]

{
  "pbx": "COMpact 5500R",
  "pbxType": 35,
  "pbxId": 0,
  "version": "Version 7.8A - Build 002  ",
  "serial": "1234123412",
  "date": "30.08.2021",
  [...]
}
```



SHODAN

Explore

Downloads

Pricing [↗](#)`http.title:"Auerswald" product:"lighttpd"`

Account

Shodan Report

`http.title:"Auerswald" product:"lighttpd"`**Total: 1,667**

// GENERAL



🌐 Countries

Germany	1,615
Austria	24
Luxembourg	9
Netherlands	7
Belgium	5

- ★ Schwachstelle durch Auerswald in vier Wochen behoben
- ★ Im Gegensatz zu anderen großen Herstellern



**INTERESSIERT?
WERDE EINE*R VON UNS!**

<https://jobs.redteam-pentesting.de>

RedTeam Pentesting GmbH

Alter Posthof 1

52062 Aachen

Deutschland