

Auf der Suche nach dem verlorenen Internet

Vasilij Schneidermann

Januar 2020

Outline

- 1 Intro
- 2 Kurze Einführung in Gopher
- 3 Einmal das Internet durchsuchen
- 4 Wer lauscht auf Port 70?
- 5 Was gibt es im Gopherspace?
- 6 Outro

Abschnitt 1

Intro

- Vasilij Schneidermann, 27
- Cyber Security Consultant bei der msg systems ag
- mail@vasilij.de
- <https://github.com/wasamasa>
- <http://brause.cc/>
- <http://emacsninja.com/>

- Das moderne Web ist eine Zumutung:
 - Tracking
 - Dark Patterns
 - Website Obesity
 - Paywalls

Antibeispiele

1 / 4

Choose Password

Your email @ Domain other ▾

☒ I do not accept the Terms & Conditions

Next Cancel Reset

Your password requires at least 10 characters.
Your password should have at least 1 Capital letter.
Your password must have at least 1 Numeral.
Your password needs at least 1 letter of your email.
Your password can have at least 1 cyrillic character.

The form is a white card on a blue background. It contains a progress indicator '1 / 4'. The password field is a single line. The email field is split into three parts: 'Your email', '@', and 'Domain', followed by a dropdown menu labeled 'other'. There is a checkbox with a checkmark and the text 'I do not accept the Terms & Conditions'. At the bottom are three buttons: 'Next', 'Cancel', and 'Reset'. Below the form, there are five lines of password requirements in a lighter blue font.

Abbildung: <https://userinyerface.com/>

Antibeispiele

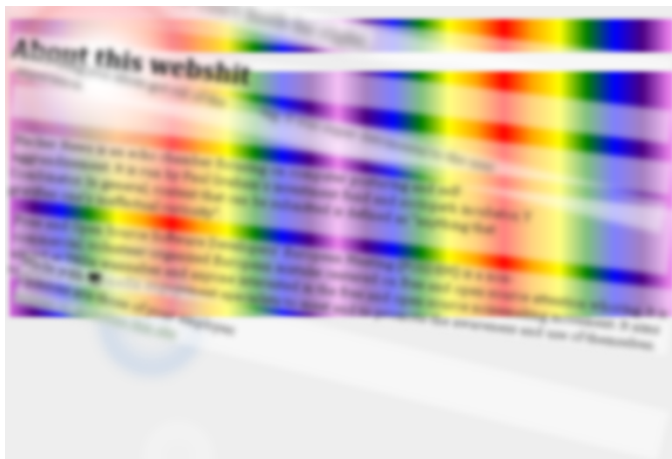


Abbildung: <http://n-gate.com/about/>

Antibeispiele

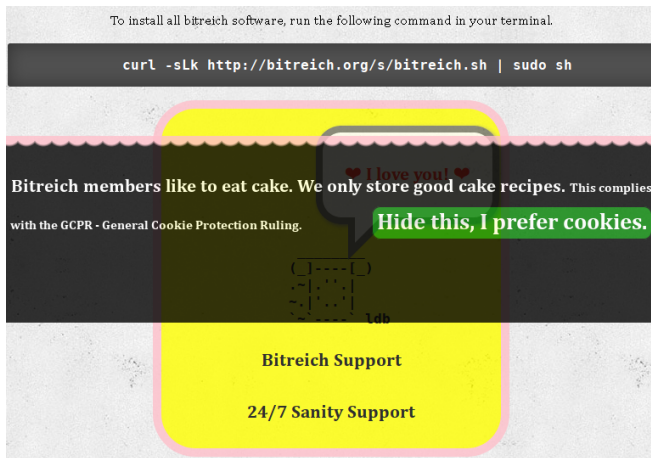
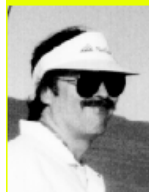


Abbildung: <http://bitreich.org/>

Larry Wall's *Very Own* Home Page



Howdy, world! This website is under construction.



(Did you ever see a website that *wasn't* under construction?)



Yes, I'm afraid chartreuse *is* one of my favorite colors.



No, I'm not going to change.

Abbildung: <http://www.wall.org/~larry/>

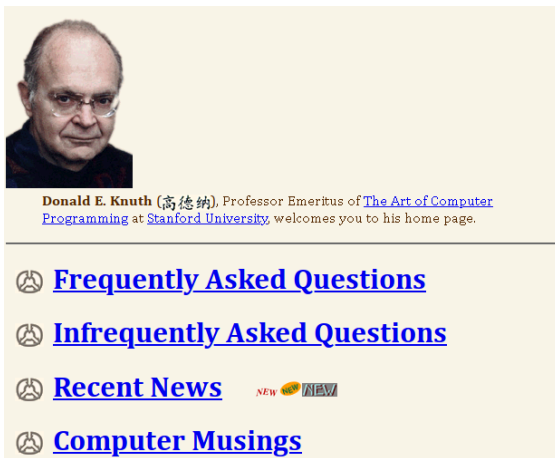


Abbildung: <https://www-cs-faculty.stanford.edu/~knuth/>

**IVAN'S
BODY DISPOSAL**



- no questions asked
- 24/7 service
- unmarked vehicle

ivanbd@crowburger.std

*Welcome to our *new* home page!!!*

KUTTING EDGE KLINIK

==== CYBER TREATMENT - SURGERY - SERVICE - NEW -
REFURBISH =====

~DISCRETE PROCEDURES - QUALIFIED SURGEONS -ALL MAJOR
FORMS OF PAYMENT ACCEPTED~



***** NO \$CASH\$? ASK ABOUT OUR INSTALMENT PLAN!!!



Abbildung: <https://kuttingedgeklinik.neocities.org/>

- Geht es noch schlichter?
- Ja, wenn man auf HTTP, HTML, CSS und JavaScript verzichtet
- Es gibt andere Protokolle als HTTP
- Gopher zum Beispiel
- Nutzt das noch jemand und wofür?

Abschnitt 2

Kurze Einführung in Gopher

- Textuelles Protokoll
- RFC 1436: The Internet Gopher Protocol (Informational)
- RFC 4266: The Gopher URI Scheme (Proposed Standard)
- Es existieren einiges an Lücken im RFC
- Ein "Living" Standard also?

Protokollfunktionsweise

- Client verbindet sich mit Server über TCP auf Port 70
- Client sendet Selektor gefolgt von `\r\n`
- Server antwortet mit einem textuellen Menü oder sendet eine Datei
- Einfachster Client: `echo -ne '\r\n' | nc hostname.tld 70`
- Hierarchische Struktur ähnelt einem Dateisystem

Beispiel einer Gopher-Session

```
$ echo -ne '\r\n' | nc gopher.olfart.eu 70 | head -n5
iWelcome to gopher.olfart.eu  fake      (NULL)  0
i      fake      (NULL)  0
1Blog articels  /blog  gopher.olfart.eu      70
0Has the KSK rolled?  /ksk  gopher.olfart.eu      70
1Other gopher sites  /links  gopher.olfart.eu      70
$ echo -ne '/links\r\n' | nc gopher.olfart.eu 70 | head -n5
iSome links to get you started: fake      (NULL)  0
i      fake      (NULL)  0
1jpmens /          serf.jpmens.net 70
1Pygopherd Home /devel/gopher/pygopherd gopher.quux.org 70
1Quux.Org Mega Server  /          gopher.quux.org 70
```

Aufbau eines Menüs

- Erstes Zeichen symbolisiert die Art des Eintrags
- Tabulator-gretrennte Felder: Text, Selektor, Host, Port

```
iWelcome to gopher.oldfart.eu\tfake\t(NULL)\t0
i\tfake\t(NULL)\t0
1Blog articels\t/blog\tgopher.oldfart.eu\t70
0Has the KSK rolled?\t/ksk\tgopher.oldfart.eu\t70
10ther gopher sites\t/links\tgopher.oldfart.eu\t70
```

Arten von Menüeinträgen

- 0: Text
- 1: Menü
- 3: Fehler
- 7: Suche
- 9: Binary
- I: Bild

- Leere Selektoren sind immer gültig
- Oft spiegeln Selektoren ein Dateisystem wieder
- Dies ist nicht zwangsläufig der Fall, / kann ebenso gut einen Fehler werfen
- Im Zweifelsfall einfach Selektoren wie sie im Menü stehen nutzen

- Suchselektoren verwenden \t als Trenner für den Suchbegriff
- Suchselektor + dynamisch generierte Seite = interaktive Anwendung
- Veronica-2 Suchmaschine: `echo -ne /v2/vs\temail\r\n | nc floodgap.com 70`
- Gästebuch: `echo -ne /guestbook\tHello\r\n | nc dread.life 70`

Gopher-URLs

- `gopher://host.tld:port/type/selector%09query`
- Startseite: `gopher://87.145.6.138`
- Alternativer Port: `gopher://rico.sytes.net:7070`
- Menü: `gopher://richardf.synchro.net/1grp:local`
- Datei: `gopher://gopher.wdj-consulting.com:70/1/retro`
- Suche: `gopher://ratthing.com/7/guestbook.cgi%09Hello`

Kompatibilität mit HTTP

- Ein Gopher-Server kann theoretisch auf HTTP-Requests antworten
- Erste Zeile eines HTTP-Requests: `GET / HTTP/1.1`
- Dies kann als Selektor interpretiert werden
- Umgekehrt gibt es die Möglichkeit auf HTTP-Inhalte zu verlinken
- Typ: `h`, Selektorsyntax: `URL:http://ix.de/`

Abschnitt 3

Einmal das Internet durchsuchen

Gibt es nicht schon Suchmaschinen?

- Tatsächlich, ja
- <https://www.shodan.io/> ist die bekannteste, Fokus auf IoT und ICS
- Besonders geschätzt als Hackerbelustigung (IP-Cams insbesondere)
- Alternativen:
 - <https://www.binaryedge.io/> (Unternehmenstauglich)
 - <https://www.zoomeye.org/> (Chinesisch)
 - <https://fofa.so/> (Chinesischer)
- Aufgrund von APIs besonders interessant

Geht es besser?

- Man kann sich ein spezialisiertes Shodan™ bauen
- Zutaten:
 - Mächtige Internetleitung
 - Immunität vor böser Post
 - Suche nach Servern die auf Port 70 lauschen
 - Herunterladen von Menüs
 - Speichern von Menüs
 - Durchsuchen von Menüs nach interessanten Daten

- Mir wurde des öfteren empfohlen solche Experimente auf dem Chaos Communication Congress zu wagen:
 - Gute Internetanbindung
 - Kurzweilige Veranstaltung
 - Abuse-Briefe gehen ins Leere
 - Viele Spezialisten™ vor Ort
- Alternativ: Einen oder mehr Server mieten, Datenlast geschickt verteilen und koordinieren

Legale Bedenken

- Portscans sind in einer rechtlichen Grauzone
- Gängige Interpretation: Vorbereitung eines Hackversuches
- Teile des Internets reagieren eher angespannt darauf:
<https://github.com/robertdavidgraham/masscan/blob/master/data/exclude.conf>
- Situation zu Banner Grabbing ist eher unklar
- Wenn das Banner "AUTHORIZED ACCESS ONLY" sagt, sollte man vielleicht das System in Ruhe lassen
- Meine Absicht ist eine Erhebung, ähnlich einer Suchmaschine
- Publikation der Daten ist fragwürdig (kein robots.txt-Äquivalent)

- Klassisches `nmap` ist toll, aber zu langsam
- Tools wie `masscan` können mit der richtigen Hardware und Treibern die IPv4-Range innerhalb von 5 Minuten durchsuchen
- Alternatives Tool: `zmap`
- Größter Nachteil: Unpräzise im Vergleich zu `nmap`
- Ich habe von einer Gruppe Spezialisten™ einen Portscan erhalten
- Menge an Hosts: 3154751 (44M IP-Adressen)
- Übungsaufgabe: Eigenes Tool bauen

Banner Grabbing

- Idee: An jede IP-Adresse `\r\n` schicken, Antwort in strukturierter Form speichern
- Problem: Naive Herangehensweise dauert länger als die Veranstaltung
- Lösung: Das `zmap`-Projekt bietet unter anderem `zgrab2` an
- Es speichert Banner mit hoher Parallelisierung und anpassbaren Timeouts als JSON
- `zgrab2 banner -p70 -f 70.targets -o 70.banners -t1`
- Mit einer Sekunde Timeout dauert es knapp eine Stunde alle Hosts zu kontaktieren
- Für die wenigen Hosts die nach Gopher aussehen, kann man die Banner mit einem längeren Timeout erneut herunterladen

Aufbewahrung der Daten

- JSON ist strukturiert, aber nicht platzsparend
- Repräsentation von binären Daten ist schwierig (Unicode lässt grüßen)
- zmap bietet ein eigenes binäres Format an, Parsing ist schwierig
- Datenbanken sind eine spannende Option
 - Relationale Datenbanken erlauben mächtige Analyse
 - Key-Value Stores sind sehr einfach, benötigen aber individuelle Werkzeuge
 - NoSQL... Vielleicht ein andermal

- jq ist toll um JSON zu verarbeiten
- DBM ist ein stupider Key-Value Store
- Werkzeug der Wahl: Shell-Einzeiler und kleine Ruby-Skripte (<200SLOC)

Abschnitt 4

Wer lauscht auf Port 70?

Filterung von Bannern

- Nicht alle Services schicken ein Banner zurück
- `jq -c 'select(.data.banner.result.banner and .data.banner.status = "success")' 70.banners > 70.banners.success=`
- 13300 Banner (0,4%) bleiben danach übrig
- Das können aber unmöglich alle Gopher-Services sein?
- Ungeklärte Frage: Was ist mit den restlichen IP-Adressen?
- 200 SLOC Ruby zum Kategorisieren von Bannern in separate Dateien
- nmap hat eine schöne Liste:
<https://svn.nmap.org/nmap/nmap-service-probes>

Aufschlüsselung der Verteilungen

Percent	Count	Filename
49.2%	6543	70.banners.unknown
24.0%	3190	70.banners.http
13.5%	1798	70.banners.ssh
5.2%	694	70.banners.gopher
2.3%	305	70.banners.ftp
1.3%	178	70.banners.imap
1.1%	151	70.banners.smtp
1.1%	142	70.banners.pop3
0.7%	93	70.banners.telnet
0.5%	63	70.banners.vnc
0.4%	50	70.banners.misc
0.4%	48	70.banners.ipcam
0.3%	46	70.banners.mysql

Honeypots

- Ganze 694 Banner sehen nach Gopher aus
- Warum würde jemand E-Mail auf Port 70 betreiben?
- Shodan erlaubt den gesamten Host zu prüfen
- Shodan zeigt für viele dieser Hosts identische Banner auf 30-40 verschiedenen Ports an
- Fun Fact: Shodan hat einen Honeyscore™ von 0 für diese Systeme
- Von Interaktion wird abgeraten

Honeypot

Ports

11	37	81	311	444	554	873	1022	1099	1599
1883	2002	2082	2222	2323	2762	3070	3128	3306	3550
3780	4000	4443	4444	4664	5222	5560	5801	6000	6009
6666	7493	7657	8001	8087	8092	8123	8443	8827	8864
8889	9039	9041	9051	9191	9418	10134	10243	16010	28017

Abbildung: Shodan

HTTP-Server

Server: Boa/0.92o
Server: CompuOffice Webserver/2.0.0.0
Server: EchoLink/2.0 # Radio
Server: Genetic Lifeform and Distributed Open Server 1.4.2
Server: Microsoft-Cassini/1.0.0.0 # MS CRM
Server: RealVNC/E4
Server: RStudio
Server: Symantec Endpoint Protection Manager
Server: VNC Server Enterprise Edition/E4.4.1 (r12183)
Server: WEBrick/1.3.1 (Ruby/1.9.3/2011-10-30)

Embedded Web Services

```
Server: alphapd/2.1.8 # IPCam
Server: AVR_Small_Webserver
Server: axhttpd/1.5.3 # router
Server: BlueIris-HTTP/1.1 # IPCam
Server: DVR Webcam daemon 1.1 / NES Technology., Inc.
Server: Ethernut 4.6.3.0
Server: Henry/1.1 # telephony
Server: mxhttpd/2.19-MX Apr 11 2019 # IPCam
Server: thhttpd/2.04 10aug98
Server: TibetSystem Server 2.0 # DVR
```

Telnet

Authentication required

This is an unrestricted telnet server.\r\nPlease do not user for
↪ production purposes\r\n

Telnet Disabled.

Error: Must authenticate before using this service.

Andere Kuriositäten

```
Asterisk Call Manager/2.8.0 # telephony  
# ODYSSEY_E receiver ready # gps  
Crestron Terminal Protocol Console Opened # home automation  
Welcome to the TeamSpeak 3 ServerQuery interface  
WinAQMS Data Server V2.3.71 # medical  
<aafMessage><aafInitRequest> # medical
```

Römer geht nach Hause

```
YOUR CONNECTION ATTEMPT HAS BEEN LOGGED AND SECURITY TEAM HAS  
↪ BEEN ALERTED  
CONNECTION ATTEMPT HAS BEEN LOGGED *** GO OUT, YOU STUPID N****R!  
YOUR CONNECTION ATTEMPT HAS BEEN LOGGED. GO AWAY. # portsentry
```

Hollywood lässt grüßen

- Siemens BAU Task Diagnostics Delta (50) SnapShots
- Shodan zeigt einen offenen UDP-Port für ein "Siemens BACnet Field Panel"
- <https://en.wikipedia.org/wiki/BACnet>

BACnet was designed to allow communication of building automation and control systems for applications such as heating, ventilating, and air-conditioning control (HVAC), lighting control, access control, and fire detection systems and their associated equipment.

Hollywood lässt grüßen



Abbildung: Hackers (1995)

Abschnitt 5

Was gibt es im Gopherspace?

Bekannte Server

- Debian bietet Pygopherd und Gophernicus zur Installation an
- Viele Menschen bauen ihre eigenen Server
- Manche Services bieten nebenbei noch Gopher an
- Fingerprinting ist auf viele Weisen möglich:
 - Menüeinträge
 - Fehlermeldungen
 - Erwähnt im Bannertext
 - Hosting vom eigenen Quellcode
 - Leute anschreiben

Pygopherd

Welcome to Pygopherd! You can place your documents in /var/gopher for future use. You can remove the gophermap file there to get rid of this message, or you can edit it to use other things. (You'll need to do at least one of these two things in order to get your own data to show up!)

Some links to get you started:

[Pygopherd Home](#)

[Quux.Org Mega Server](#)

[The Gopher Project](#)

[Traditional UMN Home Gopher](#)

[Hello World](#)

Welcome to the world of Gopher and enjoy!

Pygopherd

```
$ ./bannersearch.rb banners '~pygopherd' | wc -l
63 # self-advertising
$ ./bannersearch.rb banners type:i selector:fake 'host:(NULL)' |
↪ wc -l
170 # revealing info line
$ ./bannersearch.rb banners 'Welcome to Pygopherd!' | wc -l
30 # uncustomized
```

Gophernicus

Welcome to Gophernicus!

[...]

Generic information:

current time...: Sun Jan 26 18:04:17 CET 2020

your ip address: 87.79.236.180

server uptime..: 632 days

server version.: Gophernicus/1.4

server platform: Debian/6.0 x86_64

description....:

Server configuration:

config file....: /etc/inetd.conf

server hostname: *****

root directory.: /var/gopher

running as user: nobody

output charset.: US-ASCII

output width...: 70 characters

Gophered by Gophernicus/1.4 on Debian/6.0 x86_64

Gophernicus

```
$ ./bannersearch.rb banners '~gophernicus' | wc -l
119 # self-advertising
$ ./bannersearch.rb banners type:i host:null.host port:1 | wc -l
164 # revealing info line
$ ./bannersearch.rb banners 'Welcome to Gophernicus!' | wc -l
15 # (minimal) customization
```

Gophernicus

- Interessante Bannerzeile: "Gophered by Gophernicus/<version> on <OS>"
- Anzahl an Servern mit einer solchen Zeile:
`./bannersearch.rb banners 'Gophered by Gophernicus' on | wc -l # 113`
- Zeit für Popco(r)n

Gophernicus

```
$ ./bannersearch.rb banners 'Gophered by Gophernicus' on | jq -r  
  ↪ '.matches[0].text|split("on ")[1]|split("/") [0]' | sort |  
  ↪ uniq -c | sort -rn
```

Count	OS	Count	OS
27	Debian	3	MacOSX
23	Ubuntu	2	Fedora
20	OpenBSD	1	Peppermint
9	NetBSD	1	Linux
8	FreeBSD	1	Gentoo
6	Raspbian	1	Devuan
5	Slackware	1	CentOS
3	Welcome	1	Arch

- Server mit verräterischem Menüeintrag: "Configure_GoFish"

```
$ ./bannersearch.rb banners '~configure_gofish' | wc -l
```

4

Welcome to the GoFish Gopher Server!

This file is a roadmap of how to add content to your shiny new

↪ gopher

server. Most of the real documentation is in the form of man

↪ pages

which were provided as part of the GoFish package.

For the really impatient:

- 1) Add some files and/or directories to /srv/gopher
- 2) Run ``mkcache -r'`
- 3) Sit back and wait for the hits

Bulletin Board Systems

- Ja, sie existieren noch, wenn auch auf Port 23
- Manche haben ein Gopher-Interface auf Port 70
- Menüeinträge verweisen gerne auf andere BBS-Instanzen (Local, Fidonet)
- "Synchronet Gopher Service" hat Systemeinträge wie "System Statistics", "System Time", "Version Information"

```
$ ./bannersearch.rb banners '~text:~local|fidonet$' | wc -l
```

```
63
```

```
$ ./bannersearch.rb banners '~System Statistics|Version  
↪ Information$' | wc -l
```

```
54
```

Es ist viel zu einfach eigene Server zu bauen

This gopher server is a PDP-11/93 running GOS, my gopher server
↪ for RSX-11M.

This site runs on a Beaglebone Black using a server written in
↪ assembly.

port70 - a Gopher server (RFC-1436) written in Lua

Ungewöhnliche Ports

```
$ ./bannersearch.rb banners '!port:70' '!type:i' | wc -l  
39  
$ ./bannersearch.rb banners '!port:70' '!type:i' | jq -r  
↪ '.matches[].port' | sort | uniq -c | sort -rn | head
```

Count	Port	Count	Port
21	80	3	7006
20	0	3	7005
8	23	3	7003
6	7070	2	9999
4	105	2	2323

ASCII Art

```

      _____
 \ ~~~~~~ / ~ - - ~ ~ - - ~ ~ ~ ~ \
  \ - - - \ _ - ~ | \
    - ~ < _ | \
 / _ - - ~ - - [ " " ] | \
> / ~ \ | - . \ ~ ~ . ~ ~ ~ ~ - ~ - -
 ~ | | | \ % | | ~ . _ ~ - ~ ~ . _
  \ _ // | _ % \ | ~ . ~ - _ ~ \
    \ - - - | \ - - - \ /
      ~ - - / , / - ~ - \ \
        ~ - . _ < \ \ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ## - - ~ /
          | \ \ C F L A G S \ \
          \ ) | \ - - - - ## - - ~ ~ ~ ~ ~ ) |
            ~ - _ / _ / ~ - _ / _ /

```

ASCII Art

```
/-----\
| Welcome to eyeblea.ch, the Melbourne home of the |
|           Gopher and IRC revival!           |
\-----/

\
  \
    ,_---~~~~~_---.
  ,,,,*^-----`~*g*\",
/ _/_/ /' ^./ / \ ^@q f
[ @f | @)) | | @)) 1 0 _/
\~/ \~_---/ _ \_---/ \
|           _1__1_ I
}           [_____] I
]           | | | |
]           ~ ~
|-----|
```

ASCII Art

```

  -----
|  _ _ | | | / _ _ | / / | | | _ \
| | _ | | | | | | | ' / | | | | ) |
| _ | | | | | | _ _ | . \ | | | | _ /
| _ |   \ _ _ / \ _ _ | | \ \ _ _ / | |

```

S O L U T I O N S

Suchfelder

```
$ ./bannersearch.rb banners type:7 | jq -r '.matches[].text' |  
↪ sort | uniq
```

ASCII banner generator

Ask the Magic 8 Ball

Convert an HTML page to gopher

Create a new account

JPG to ASCII convertor (input: URL ending in .jpg)

PDF viewer (input: URL ending in .pdf)

WEATHER FORECAST

Spiele

ShadowGate multi user dungeon is a large text-based Role Playing

↪ game derived from the Dungeons and Dragons [...]

Welcome to the Mare Tranquillitatis People's Circumlunar

↪ Zaibatsu, an ideologically decriminalized world [...]

You wake up slowly from a dream about angry bees. Your phone

↪ vibrates noisily next to your bed [...]

You are at a dead end of a dirt road. The road goes to the east.

Choose Your Own Adventure (anonradio)

Play: Klondike (Turn One)

60 MORE Gopher Solitaire Games!

Phlogs

Die einen haben Weblogs (AKA Blogs), die anderen Phlogs...

```
$ ./bannersearch.rb banners '~phlog' type:10 | wc -l  
98
```

```
$ ./bannersearch.rb banners '~phlog' type:10 | jq -r  
↪ '.matches[].text' | shuf | head
```

Link Phlog

Phlog Roll

Phlog

My Phlog

Phlog

My phlog

microphlog

Beastie Boy - phlog about Unix/BSD, Emacs, Lisp and interesting

↪ things

Ferment Phlog

Kara and Michael\'s Phlog

- Leider sagt der Standard nichts über Encodings
- Viele Services verwenden ASCII oder UTF-8
- Es gibt eine handvoll Seiten aus Russland und Taiwan mit unbekannten Encodings
- Manche kündigen das Encoding des folgenden Textes auf Englisch an
- i18n bleibt ein ungelöstes Problem

Kaputte Links

- Der Standard sieht Menüeinträge nur mit Hosts vor
- Menüeinträge auf den eigenen Server können veralten
- Kein Äquivalent zu relativen/absoluten Links
- Host kann händisch korrigiert werden

Zutritt verboten!

- Protokoll sieht keinerlei Authentisierung vor
- Man könnte theoretisch etwas mit Suchen und CGI bauen...
- Ganze zwei Seiten zeigen "Forbidden!" an

Zutritt verboten!

*** AUTHORIZED ACCESS ONLY ***

This is a private Gopher server. Please log out immediately if
↳ you
have not been explicitly given permission to this server.

This is a Gopher server maintained by Astr0 for the

↪ hackerfraternity

You've reached the first checkpoint in this this hacker

↪ challenge.

Writeups for CTF events and related challenges

Welcome to the Security Diary

flag{do_you_know_gopher?}

The Final Exam Payload

Anderer interessanter Kram

If you came from the Sysadmin Wanted ad, look here
Welcome to the p70.us URL shortening service!
Gopherddit -> simple gopher interface to Reddit by gluon
Leafly is the world's largest cannabis information resource [...]
Welcome to the home of SCC, Simple C Compiler.
Einwohnergemeinde Zermatt
taz.de Die Tageszeitung
Welcome to Devuan

Abschnitt 6

Outro

Mögliche nächste Schritte

- Besseres Fingerprinting
- Suche und CGI
- Sicherheitslücken entdecken und CVEs einreichen
- Suchmaschinenbau
- Mehr Statistiken
- Visualisierungen
- ...

Fragen?