

Installeer alvast volgende:

- Wireshark
- Ghidra

Eten: <https://haldis.zeus.gent/order/uh438a5e>

Voor windows:

- 7zip
- WSL (windows subsystem for linux)

Wifi: Zeus Event

ww: eventisdemax1408



Intro hacking en CTF

gehakt

Wat is een CTF

Capture the flag

```
ZeusCTF{1k_b3n_33n_f14g_H4DJ5D}
```

Jeopardy, Attack/Defence

Challenges

Verschillende categorieën

Web	Crypto	Forensics	Reverse	Misc
1	165	100	50	50
150	150	150	100	100
204	150	150	150	165
203	200	200	200	150

Algemene tips

Lees beschrijving en naam van challenge!

Zoeken naar gelijkaardige oude challenges

Kijk eens op de website van de maker van de challenge (tools, blogposts)

Encodings

binary

hexadecimal (hex)

base64

128	64	32	16	8	4	2	1
1	0	0	1	1	0	1	1

0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	10
1011	11
1100	12
1101	13
1110	14
1111	15

0
1
2
3
4
5
6
7
8
9
A
B
C
D
E
F

Encodings - Base 64

encoderen van 6 bits

Index	Binary	Char	Index	Binary	Char	Index	Binary	Char	Index	Binary	Char
0	000000	A	16	010000	Q	32	100000	g	48	110000	w
1	000001	B	17	010001	R	33	100001	h	49	110001	x
2	000010	C	18	010010	S	34	100010	i	50	110010	y
3	000011	D	19	010011	T	35	100011	j	51	110011	z
4	000100	E	20	010100	U	36	100100	k	52	110100	0
5	000101	F	21	010101	V	37	100101	l	53	110101	1
6	000110	G	22	010110	W	38	100110	m	54	110110	2
7	000111	H	23	010111	X	39	100111	n	55	110111	3
8	001000	I	24	011000	Y	40	101000	o	56	111000	4
9	001001	J	25	011001	Z	41	101001	p	57	111001	5
10	001010	K	26	011010	a	42	101010	q	58	111010	6
11	001011	L	27	011011	b	43	101011	r	59	111011	7
12	001100	M	28	011100	c	44	101100	s	60	111100	8
13	001101	N	29	011101	d	45	101101	t	61	111101	9
14	001110	O	30	011110	e	46	101110	u	62	111110	+
15	001111	P	31	011111	f	47	101111	v	63	111111	/
<i>padding</i>		=									



Sophie Alpert
@sophiebits



> aGkgdHdpd...

me: I have no idea what this is

> aGkgdHdpdHRlcg==

me: oh it's base 64

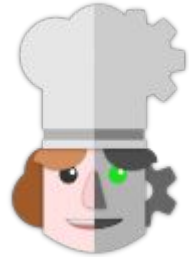
Algemene tools

Cyberchef | encodings

pwntools | Python library voor CTFs

cURL / wget | requests

netcat (nc) | connectie met een server



curl://



PWNTOOLS

Wi wa web - developer console

F12

Ctrl + Shift + i

Rechts klik > inspect element



The screenshot shows the Network tab in Chrome DevTools. The top bar includes 'Inspector', 'Console', 'Debugger', 'Network', 'Style Editor', 'Performance', and 'Disable Cache'. The 'Network' tab is active, showing a list of requests. The table has columns for Status, Method, Domain, File, Initiator, Type, Transferred, and Size. The requests are sorted by size, with the largest being a 480.2 KB HTML document. The status bar at the bottom indicates 58 requests, 18.75 MB / 5.48 MB transferred, and a finish time of 16.75 s.

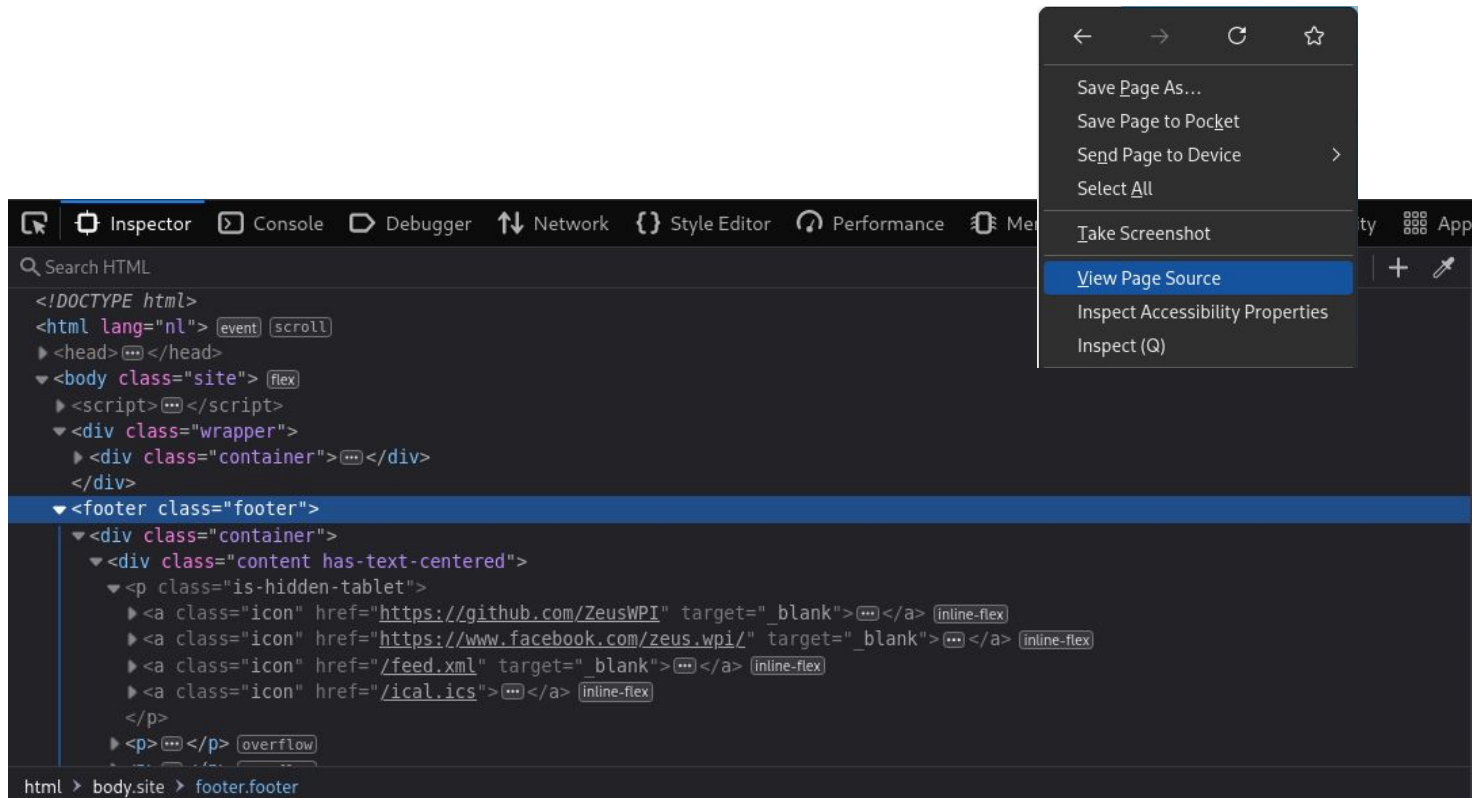
Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	POST	docs.google...	leave?Id=1VjHW_z845vZ7B1WV38EC2dz13uVf	1389170559-e...	json	4.18 kB	0 B
200	GET	docs.google...	edit	document	html	93.81 kB	480.2 ...
200	POST	play.google.com	log?hasfast=true&auth=SAPISIDHASH+45eecc12925907473e...	2925907473e...	Blocked By uBl...		
200	POST	play.google.com	log?hasfast=true&auth=SAPISIDHASH+45eecc12925907473e...	2925907473e...	Blocked By uBl...		
200	GET	docs.google...	4182427246-editor_css_tr.css	stylesheet	css	292.71 kB	2.41 ...
200	GET	docs.google...	1389170559-editor_js_prod_integrated_core.js	script	js	733.55 kB	2.18 ...
200	GET	docs.google...	2925907473-editor_js_prod_integrated_app.js	1389170559-e...	js	1.67 MB	4.86 ...
200	GET	www.gstatic...	rs=AA2YrTVzRfmQmjUw-Brv7g8jTycwfhCO	edit:127 (scrip)	js	80.99 kB	222.9 ...
200	GET	www.gstatic...	rs=AA2YrTVzRfmQmjUw-Brv7g8jTycwfhCO	edit:127 (styles...	css	1.49 kB	1.66 kB
200	GET	docs.google...	4038526571-editor_js_prod_integrated_docs.js	1389170559-e...	js	288.84 kB	862.0 ...
200	GET	docs.google...	488338067-editor_js_prod_integrated_tertiary.js	1389170559-e...	js	314.99 kB	941.2 ...
200	GET	docs.google...	702096908-viewer_core.js	13f6c321-3b33...	js	383.59 kB	1.10 ...
200	GET	docs.google...	2349356900-viewer_css_tr.css	13f6c321-3b33...	css	66.85 kB	457.1 ...
200	GET	docs.google...	631758307-autolayout_map_binary_prof_autol...	13f6c321-3b33...	js	184.85 kB	2.09 ...
200	GET	fonts.gstatic...	font?kit=XRXT3ISEjEpMwU7T2CbzdA6k5e&v=	font	html	67.68 kB	67.02 ...
200	GET	fonts.gstatic...	font?kit=XRXT3ISEjEpMwU7T2CbzdA6k5e&v=	font	html	67.68 kB	67.02 ...
200	GET	fonts.gstatic...	font?kit=XRXT3ISEjEpMwU7T2CbzdBoC6sk&v=	font	html	71.82 kB	71.16 ...
200	GET	fonts.gstatic...	font?kit=XRXT3ISEjEpMwU7T2CbzdBoC6sk&v=	font	html	71.82 kB	71.16 ...
200	GET	fonts.gstatic...	font?kit=XRXT3ISEjEpMwU7T2CbzdV2T8nCO6&v=	font	html	67.92 kB	67.26 ...
200	GET	fonts.gstatic...	font?kit=XRXT3ISEjEpMwU7T2CbzdV2T8nCO6&v=	font	html	67.92 kB	67.26 ...
200	GET	fonts.gstatic...	font?kit=XRXT3ISEjEpMwU7T2CbzdV2T8nCO6&v=	font	html	69.37 kB	68.55 ...
200	GET	fonts.gstatic...	font?kit=XRXT3ISEjEpMwU7T2CbzdV2T8nCO6&v=	font	html	69.37 kB	68.55 ...
200	GET	fonts.gstatic...	font?kit=XRXT3ISEjEpMwU7T2CbzdV2T8nCO6&v=	font	html	8.53 kB	7.87 kB
200	GET	fonts.gstatic...	font?kit=XRXT3ISEjEpMwU7T2CbzdV2T8nCO6&v=	font	html	8.53 kB	7.87 kB
200	OPTI...	peoplestack...	GetExperimentFlags	xhr	html	605 B	0 B
200	OPTI...	peoplestack...	GetExperimentFlags	xhr	html	605 B	0 B
200	OPTI...	peoplestack...	Autocomplete	xhr	html	582 B	0 B
200	GET	docs.google...	2911084315-editor_js_prod_integrated_compan	1389170559-e...	js	34.01 kB	102.6 ...
200	GET	apis.google...	cb=gapi.loaded_0	rs=AA2YrTVzRf...	js	42.06 kB	121.4 ...
200	GET	docs.google...	2507450768-editor_js_prod_integrated_addons	1389170559-e...	js	11.20 kB	26.43 ...
200	GET	docs.google...	701118052-editor_js_prod_integrated_explore	1389170559-e...	js	55.10 kB	182.5 ...
200	GET	docs.google...	3087927840-editor_js_prod_integrated_organiz	1389170559-e...	js	17.96 kB	51.13 ...
200	GET	docs.google...	clientmodel?Id=1VjHW_z845vZ7B1WV38EC2dz	subdocument	html	4.01 kB	1.30 kB
200	GET	apis.google...	cb=gapi.loaded_1	rs=AA2YrTVzRf...	js	72.01 kB	206.6 ...
200	GET	docs.google...	1557726609-editor_js_prod_integrated_emojida	1389170559-e...	js	50.13 kB	301.7 ...
200	GET	docs.google...	4266794499-editor_js_prod_integrated_approva	1389170559-e...	js	7.62 kB	17.98 ...
200	GET	clients6.goo...	proxy.html?usegapi=1&js=mm/_fcs/abc-static/	subdocument	html	1.38 kB	382 B
200	OPTI...	espresso-pa...	prewarm?key=Alza5yBtKq7d4M21P0DCEXU	xhr	html	687 B	0 B
200	GET	docs.google...	3780292722-editor_js_prod_integrated_peopleh	1389170559-e...	js	9.65 kB	23.31 ...
200	GET	apis.google...	cb=gapi.loaded_2	rs=AA2YrTVzRf...	js	16.11 kB	43.85 ...
200	GET	apis.google...	cb=gapi.loaded_3	rs=AA2YrTVzRf...	js	948 B	62 B
200	GET	www.gstatic...	lazy.min.js	cb=gapi.loaded	js	37.66 kB	108.3 ...
200	GET	contacts.goo...	27origen=https://docs.google.com/fusegapi=1&	subdocument	html	13.62 kB	43.40 ...
200	GET	apis.google...	googleapis.proxy.p?load=startup	script	js	7.98 kB	18.39 ...
200	GET	apis.google...	cb=gapi.loaded_07le=scs	script	js	28.97 kB	79.58 ...
200	GET	fonts.google...	css2?family=Google+Sans+Text:wght@400:500	stylesheet	css	1.28 kB	5.51 kB
200	GET	contacts.goo...	m=...b_tp	script	js	67.68 kB	190.0 ...
200	GET	contacts.goo...	m=ws9Tic-n73qwfGkRikb.e5qfLcLZT63.UUjw	m=...b_tp:344 (...)	js	228.81 kB	849.7 ...
200	GET	contacts.goo...	m=mb51tf	m=...b_tp:344 (...)	js	1.69 kB	1.46 kB
200	GET	apis.google...	api.js	m=ws9Tic-n73...	js	7.97 kB	18.37 ...

Console - Inspector

HTML

Comments

Hidden HTML



The image shows a screenshot of the Chrome DevTools Inspector. The main panel displays the HTML structure of a page, with the following elements visible:

```
<!DOCTYPE html>
<html lang="nl">
  <head>
  <body class="site">
    <script>
    <div class="wrapper">
      <div class="container">
    </div>
    <div class="content has-text-centered">
      <p class="is-hidden-tablet">
        <a class="icon" href="https://github.com/ZeuswPI" target="_blank">
        <a class="icon" href="https://www.facebook.com/zeus.wpi/" target="_blank">
        <a class="icon" href="/feed.xml" target="_blank">
        <a class="icon" href="/ical.ics" target="_blank">
      </p>
    </div>
  </div>
  <div class="footer">
    <div class="container">
      <div class="content has-text-centered">
        <p class="is-hidden-tablet">
          <a class="icon" href="https://github.com/ZeuswPI" target="_blank">
          <a class="icon" href="https://www.facebook.com/zeus.wpi/" target="_blank">
          <a class="icon" href="/feed.xml" target="_blank">
          <a class="icon" href="/ical.ics" target="_blank">
        </p>
      </div>
    </div>
  </div>
</body>
</html>
```

The context menu is open, showing the following options:

- Save Page As...
- Save Page to Pocket
- Send Page to Device
- Select All
- Take Screenshot
- View Page Source** (highlighted)
- Inspect Accessibility Properties
- Inspect (Q)

The breadcrumb at the bottom of the Inspector panel reads: `html > body.site > footer.footer`.

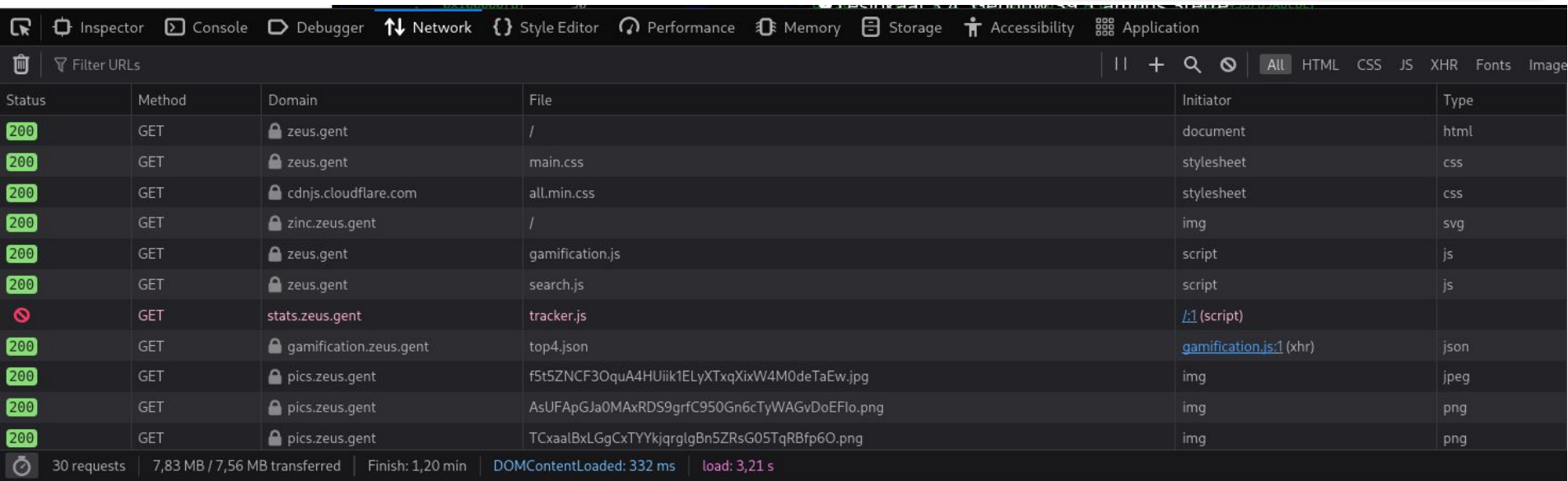
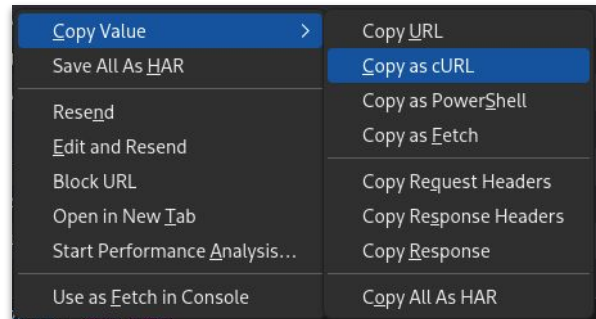
Console - Network

Requests tussen browser en server

images, javascript, json, ...

headers

Copy as cURL



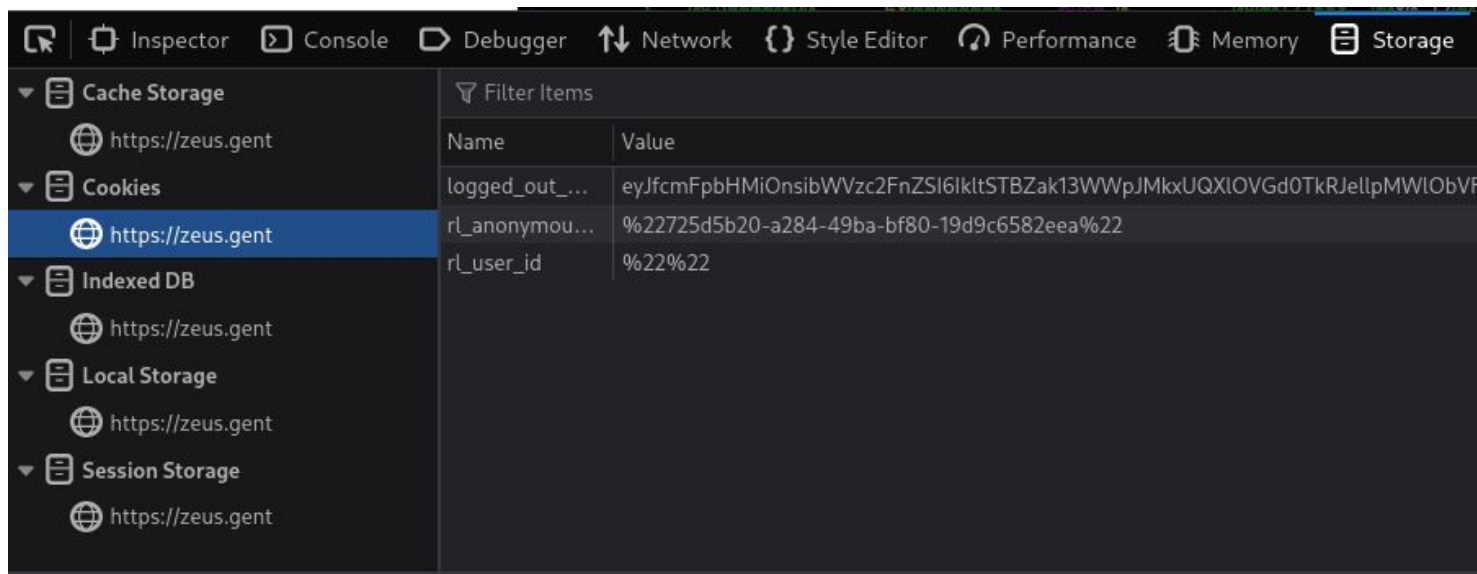
Console - Network - Requests

- Informatie over requests
- Status
- Headers
 - Informatie over request en response
 - Soms nuttig
- Cookies

The screenshot shows the 'Network' tab in a browser's developer console. The selected request is a GET to 'https://zeus.gent/'. The status is 200 (OK) with a question mark icon. The version is HTTP/2, and 5,80 kB of data was transferred. The request priority is 'Highest' and the DNS resolution is 'System'. Below this, the 'Response Headers' (450 B) and 'Request Headers' (826 B) are expanded. The response headers include content-encoding: gzip, content-type: text/html, date: Wed, 21 Feb 2024 16:17:32 GMT, etag: W/"65d5e871-447c", last-modified: Wed, 21 Feb 2024 12:11:29 GMT, permissions-policy: interest-cohort=(), referrer-policy: same-origin, strict-transport-security: max-age=31536000; includeSubDomains; preload, x-content-type-options: nosniff, X-Firefox-Spdy: h2, x-frame-options: SAMEORIGIN, and x-xss-protection: 1; mode=block. The request headers include Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8, Accept-Encoding: gzip, deflate, br, Accept-Language: en-US,en;q=0.5, Cache-Control: no-cache, Connection: keep-alive, and a Cookie: rl_user_id=%22%22; logged_out_marketing_header_id=eyJfcmlpMjI0bWVzc2FnZSI6I...

Console - Storage

- Cookies
 - Waarden bekijken (en veranderen)
- Local storage (en varianten)



The screenshot shows the Chrome DevTools Storage panel. The left sidebar is expanded to show the 'Cookies' section for the domain 'https://zeus.gent'. The right pane displays a table of cookies with the following data:

Name	Value
logged_out_...	eyJJcmFpbHMlOnsibWVzc2FnZSI6IkltSTBZak13WWpJMkxUQXlOVGd0TkrJellpMWlObVF
rl_anonymou...	%22725d5b20-a284-49ba-bf80-19d9c6582eea%22
rl_user_id	%22%22

Web - Challenge

onotes - 3 flags

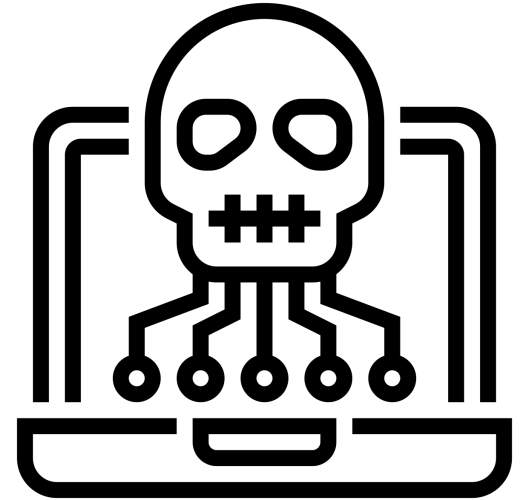
Browser naar IP: <http://10.2.2.175:5000>

Reverse engineering / Binary exploitation

Begrijpen wat een programma doet (met of zonder code)

Bugs vinden

Bugs gebruiken



RE/BE - Strings

zoekt strings in gelijk welke files

idee krijgen van wat het is

flags?

grep

```
👤 ~ /c/r/intro_hacking_ctf/reversing > on git main ?1 strings strings_example
/lib64/ld-linux-x86-64.so.2
*et(
__cxa_finalize
__libc_start_main
puts
printf
libc.so.6
GLIBC_2.2.5
GLIBC_2.34
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH
plopkoek
CTF{1_h4v3_b33n_string3d}
;*3$"
GCC: (GNU) 13.2.0
.B#>M$#=1
LU=/
../sysdeps/x86_64/start.S
/builddir/glibc-2.38/csu
GNU AS 2.41
```

```
👤 ~ /c/repos/intro_hacking_ctf/reversing > on git main ?1 strings strings_example | grep -E '[[[:alpha:]]+{[^}]+}'
CTF{1_h4v3_b33n_string3d}
```

RE/BE - Assembly

Compiler:

Code \Rightarrow binary

binary gelezen als assembly

Makkelijker om te begrijpen

```
#include <stdio.h>

int main() {
    int num = 0;
    char buf[10];

    printf("Name: ");
    scanf("%s", &buf);

    if (num > 0) {
        printf("Ohno\n");
        printf("%d", num);
    }

    printf("Hello %s!", buf);
}
```

```
***** FUNCTION *****
undefined main()
AL:1 <RETURN>
undefined4 Stack[-0xc]:4 local_c

undefined1 Stack[-0x16]:1 local_16
main XREF[4]:

00401136 55          PUSH      RBP
00401137 48 89 e5    MOV      RBP, RSP
0040113a 48 83 ec 10 SUB      RSP, 0x10
0040113e c7 45 fc    MOV      dword ptr [RBP + local_c], 0x0
                00 00 00 00
00401145 bf 04 20    MOV      EDI, s_Add_number:_00402004
                40 00
0040114a b8 00 00    MOV      EAX, 0x0
                00 00
0040114f e8 dc fe    CALL     <EXTERNAL>::printf
                ff ff
00401154 48 8d 45 f2 LEA      RAX=>local_16, [RBP + -0xe]
00401158 48 89 c6    MOV      RSI, RAX
0040115b bf 11 20    MOV      EDI, DAT_00402011
                40 00
00401160 b8 00 00    MOV      EAX, 0x0
                00 00
00401165 e8 d6 fe    CALL     <EXTERNAL>::_isoc99_scanf
                ff ff
0040116a 83 7d fc 00 CMP      dword ptr [RBP + local_c], 0x0
0040116e 7e 23      JLE      LAB_00401193
00401170 bf 14 20    MOV      EDI, DAT_00402014
                40 00
00401175 b8 00 00    MOV      EAX, 0x0
                00 00
0040117a e8 b1 fe    CALL     <EXTERNAL>::printf
                ff ff
0040117f 8b 45 fc    MOV      EAX, dword ptr [RBP + local_c]
00401182 89 c6      MOV      ESI, EAX
00401184 bf 18 20    MOV      EDI, DAT_00402018
```


RE/BE - Ghidra

Reverse engineering tools

Binary => (leesbare) assembly => decompile



```
undefined8 main(void)
{
    undefined local_16 [10];
    uint local_c;

    local_c = 0;
    printf("Name: ");
    __isoc99_scanf(&DAT_0040200b, local_16);
    if (0 < (int)local_c) {
        puts("Ohno");
        printf("%d", (ulong)local_c);
    }
    printf("Hello %s!", local_16);
    return 0;
}
```

```
*****
*                               FUNCTION
*****
undefined main()
AL:1 <RETURN>
undefined4 Stack[-0xc]:4 local_c

undefined1 Stack[-0x16]:1 local_16
main

00401136 55          PUSH     RBP
00401137 48 89 e5    MOV     RBP,RSP
0040113a 48 83 ec 10 SUB     RSP,0x10
0040113e c7 45 fc    MOV     dword ptr [RBP + local_c],0x0
00 00 00 00
00401145 bf 04 20    MOV     EDI,s_Add_number:_00402004
40 00
0040114a b8 00 00    MOV     EAX,0x0
00 00
0040114f e8 dc fe    CALL    <EXTERNAL>::printf
ff ff
00401154 48 8d 45 f2 LEA     RAX=>local_16,[RBP + -0xe]
00401158 48 89 c6    MOV     RSI,RAX
0040115b bf 11 20    MOV     EDI,DAT_00402011
40 00
00401160 b8 00 00    MOV     EAX,0x0
00 00
00401165 e8 d6 fe    CALL    <EXTERNAL>::__isoc99_scanf
ff ff
0040116a 83 7d fc 00 CMP     dword ptr [RBP + local_c],0x0
0040116e 7e 23      JLE     LAB_00401193
00401170 bf 14 20    MOV     EDI,DAT_00402014
40 00
00401175 b8 00 00    MOV     EAX,0x0
00 00
0040117a e8 b1 fe    CALL    <EXTERNAL>::printf
ff ff
0040117f 8b 45 fc    MOV     EAX,dword ptr [RBP + local_c]
00401182 89 c6      MOV     ESI,EAX
00401184 bf 18 20    MOV     EDI,DAT_00402018
```

RE/BE - Stack (overflow)

Opslag van variabelen

In volgorde van uitvoering

scanf schrijft alle output naar buffer

11 chars => overschrijft num

=> num != 0

```
#include <stdio.h>

int main() {
    int num = 0;
    char buf[10];

    printf("Name: ");
    scanf("%s", &buf);

    if (num > 0) {
        printf("Ohno\n");
        printf("%d", num);
    }

    printf("Hello %s!", buf);
}
```

buf[0]

buf[1]

buf[2]

buf[3]

buf[4]

buf[5]

buf[6]

buf[7]

buf[8]

buf[9]

num

Andere tools

- GDB: GNU Project Debugger
- pwntools
 - Veel tools voor binary exploitation
 - integratie met GDB
- Objdump
- Hexedit

RE/BE - Challenge

buf.c - 1 flag

ono.c - 1 flag

<http://10.2.2.175:8000/>

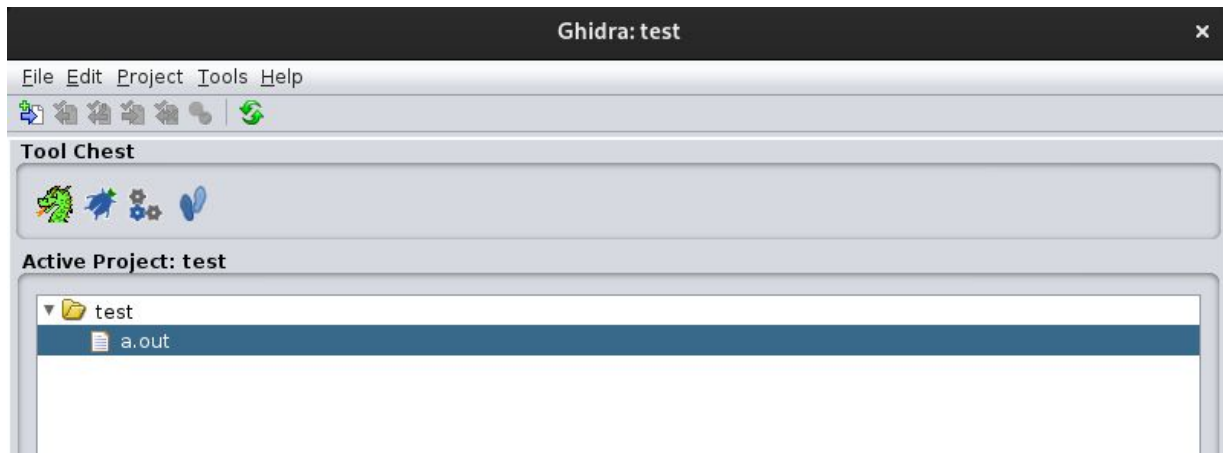
Ghidra:

Maak project

Druk op draak icoon

(~animatie~)

Sleep binary op Ghidra



Mobile

Mostly Android APK's - IOS is very rare

Languages:

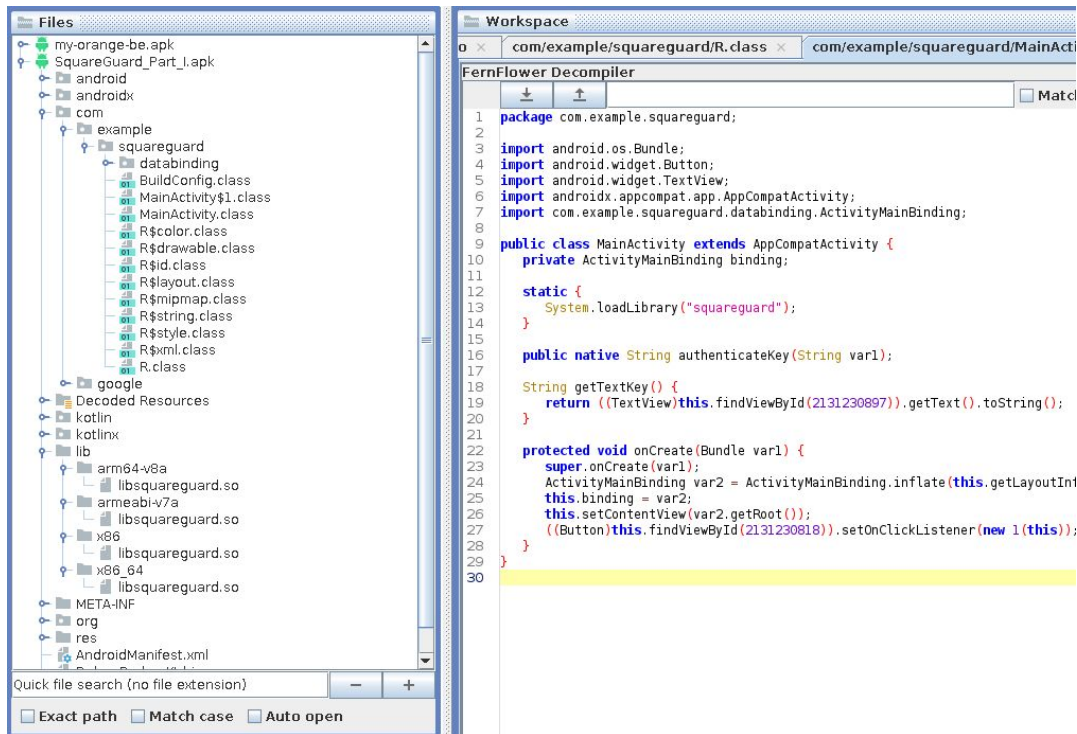
- Java
- Kotlin
- Dart

APKs are just zip files. Use a decompiler on the final files.



Mobile - Native Libraries

Sometimes native libraries are used \Rightarrow regular reversing techniques



The image displays two windows from an IDE. The left window, titled 'Files', shows a project tree for 'my-orange-be.apk'. Under the 'com' package, there is a sub-package 'squareguard' containing various classes like 'BuildConfig.class', 'MainActivity\$1.class', 'MainActivity.class', 'R\$color.class', 'R\$drawable.class', 'R\$id.class', 'R\$layout.class', 'R\$mipmap.class', 'R\$string.class', 'R\$style.class', 'R\$xml.class', and 'R.class'. Below this, under the 'lib' folder, there are native libraries for different architectures: 'arm64-v8a' (libsquareguard.so), 'armeabi-v7a' (libsquareguard.so), 'x86' (libsquareguard.so), and 'x86_64' (libsquareguard.so). The right window, titled 'Workspace', shows the source code of 'com/example/squareguard/R.class'. The code includes package declarations, imports for Android classes, and the definition of the 'MainActivity' class which extends 'AppCompatActivity'. It features a static block that calls 'System.loadLibrary("squareguard");', a native method 'authenticateKey', and an 'onCreate' method that inflates the layout and sets up a button listener.

```
1 package com.example.squareguard;
2
3 import android.os.Bundle;
4 import android.widget.Button;
5 import android.widget.TextView;
6 import androidx.appcompat.app.AppCompatActivity;
7 import com.example.squareguard.databinding.ActivityMainBinding;
8
9 public class MainActivity extends AppCompatActivity {
10     private ActivityMainBinding binding;
11
12     static {
13         System.loadLibrary("squareguard");
14     }
15
16     public native String authenticateKey(String var1);
17
18     String getTextKey() {
19         return ((TextView)this.findViewById(2131230897)).getText().toString();
20     }
21
22     protected void onCreate(Bundle var1) {
23         super.onCreate(var1);
24         ActivityMainBinding var2 = ActivityMainBinding.inflate(this.getLayoutInflater(), this, true);
25         this.binding = var2;
26         this.setContentViews(var2.getRoot());
27         ((Button)this.findViewById(2131230818)).setOnClickListener(new 1(this));
28     }
29 }
30
```

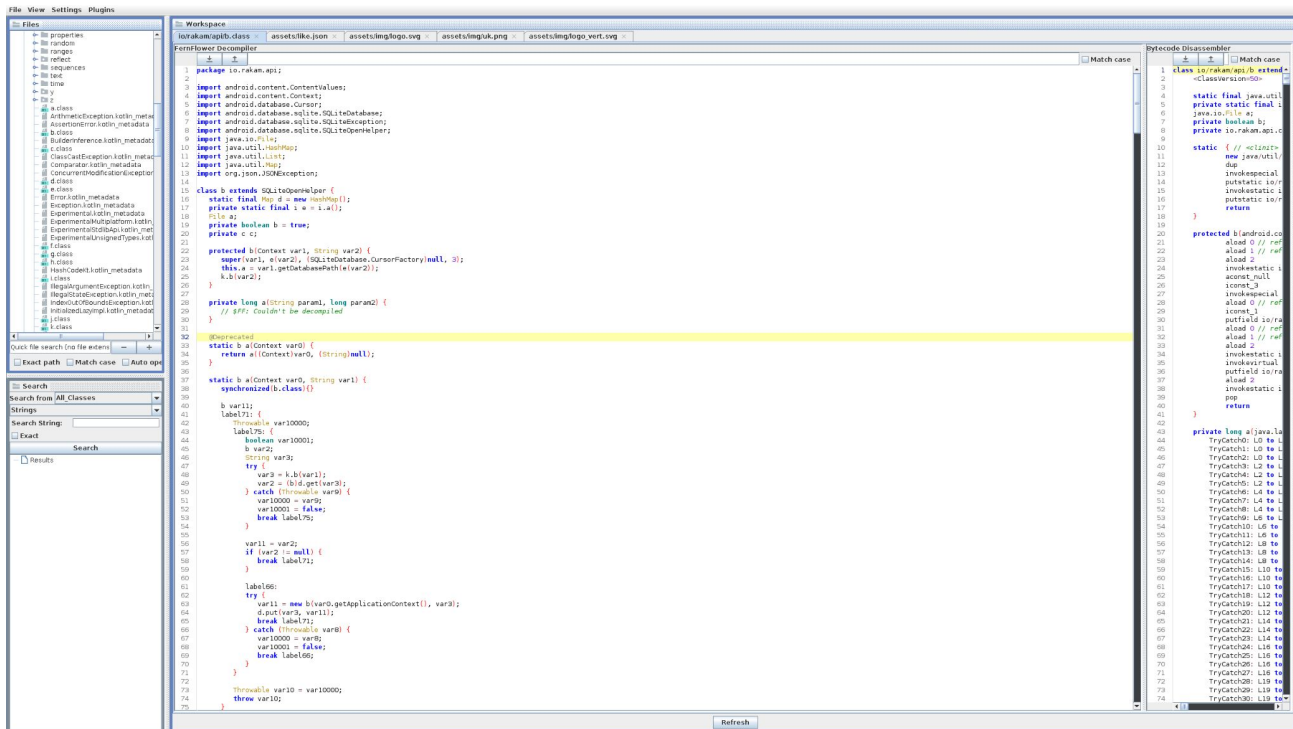
Mobile - Bytecodeviewer

Jar/Apk viewer

Multiple Decompilers

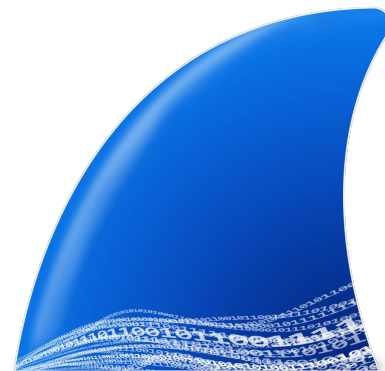
(recompiling)

<https://github.com/Konloch/bytecode-viewer>



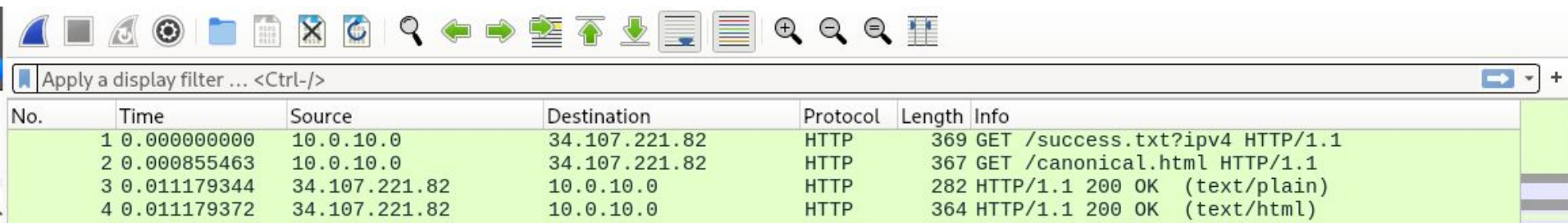
Forensics

- Verstoppen van data in een ander bestand (Steganography)
- Kijken naar inhoud van files (niet alleen interpretatie ervan)
 - metadata in foto's
 - verstopte data in pdf's
- Network traces (wireshark)
 - TCP, UDP, HTTP



Forensics - Wireshark

- pcap bestand
 - bevat de data over een connectie (bv wifi)
 - kan veel protocollen begrijpen: HTTP, TCP, UDP, ...



The image shows the Wireshark interface with a network capture table. The table has columns for No., Time, Source, Destination, Protocol, Length, and Info. The first two rows show GET requests from 10.0.10.0 to 34.107.221.82. The last two rows show 200 OK responses from 34.107.221.82 to 10.0.10.0.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.10.0	34.107.221.82	HTTP	369	GET /success.txt?ipv4 HTTP/1.1
2	0.000855463	10.0.10.0	34.107.221.82	HTTP	367	GET /canonical.html HTTP/1.1
3	0.011179344	34.107.221.82	10.0.10.0	HTTP	282	HTTP/1.1 200 OK (text/plain)
4	0.011179372	34.107.221.82	10.0.10.0	HTTP	364	HTTP/1.1 200 OK (text/html)

Forensics - Wireshark

Interpretatie van data

Rauwe data

```
▶ Frame 8: 367 bytes on wire (2936 bits), 367
▶ Ethernet II, Src: Intel_0e:11:ef (3c:6a:a7:
▶ Internet Protocol Version 4, Src: 10.0.10.6
▶ Transmission Control Protocol, Src Port: 37
▼ Hypertext Transfer Protocol
  ▶ GET /canonical.html HTTP/1.1\r\n
    Host: detectportal.firefox.com\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:122.0) Gecko/20100101 Firefox/122.0\r\n
    Accept: */*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Cache-Control: no-cache\r\n
    Pragma: no-cache\r\n
    DNT: 1\r\n
    Connection: keep-alive\r\n
    \r\n
    \[Full request URI: http://detectportal.firefox.com/canonical.html\]
    \[HTTP request 2/2\]
    \[Prev request in frame: 2\]
    \[Response in frame: 10\]
```

```
0000 4c ed fb 35 22 a8 3c 6a a7 0e 11 ef 08 00 45 00 L..5".<j .....E.
0010 01 61 fa b4 40 00 40 06 2b 25 0a 00 0a 00 22 6b .a..@.@. +%...."k
0020 dd 52 92 d4 00 50 49 b3 4c 22 4a 7c ed 70 80 18 .R...PI. L"J}|.p..
0030 01 f5 f6 fa 00 00 01 01 08 0a b8 e7 2c de ba e8 ..... ,...
0040 cd f8 47 45 54 20 2f 63 61 6e 6f 6e 69 63 61 6c ..GET /c anonical
0050 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a .html HT TP/1.1..
0060 48 6f 73 74 3a 20 64 65 74 65 63 74 70 6f 72 74 Host: de tectport
0070 61 6c 2e 66 69 72 65 66 6f 78 2e 63 6f 6d 0d 0a al.firef ox.com.
0080 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 User-Age nt: Mozi
0090 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b 20 4c 69 lla/5.0 (X11; Li
00a0 6e 75 78 20 78 38 36 5f 36 34 3b 20 72 76 3a 31 nux x86_ 64; rv:1
00b0 32 32 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 22.0) Ge cko/2010
00c0 30 31 30 31 20 46 69 72 65 66 6f 78 2f 31 32 32 0101 Fir efox/122
00d0 2e 30 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d .0..Acce pt: */*.
00e0 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 .Accept- Language
00f0 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 35 : en-US, en;q=0.5
0100 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e ..Accept -Encodin
0110 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 g: gzip, deflate
0120 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a ..Cache- Control:
0130 20 6e 6f 2d 63 61 63 68 65 0d 0a 50 72 61 67 6d no-cach e..Pragm
```

Forensics - HTTP

- Communicatie tussen browser en server
 - https = http maar versleuteld
- Request: welk document?
- Response: inhoud document

GET request ↔ HTTP response

```
HTTP      369 GET /success.txt?ipv4 HTTP/1.1
HTTP      282 HTTP/1.1 200 OK (text/plain)
```

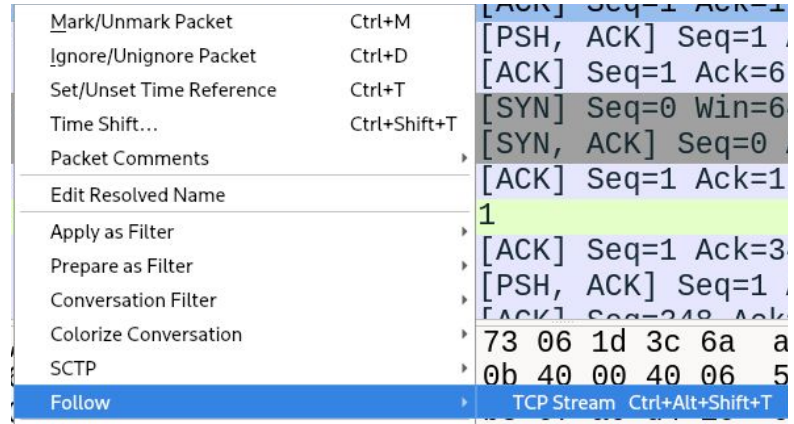
→	11	0.888211434	10.0.10.0	34.107.221.82	HTTP	369 GET /success.txt?ipv4 HTTP/1.1
←	12	0.896326215	34.107.221.82	10.0.10.0	HTTP	282 HTTP/1.1 200 OK (text/plain)

Follow the arrows



Forensics - TCP/UDP

- Data over het netwerk
- Kan anders worden geïnterpreteerd (HTTP loopt over TCP)
- Kan gewoon data zijn
- TCP
 - conversatie
 - beloftes over aflevering
- UDP
 - roepen
 - dingen kunnen verloren gaan



Forensics - File extensies zijn een leugen (sorry windows)

Veel dingen zijn een zip (probeer dingen te openen met 7zip)

- docx, jar, apk

file command

- kijkt naar inhoud om te bepalen welke file het is

```
> file zeus.wpi
zeus.wpi: Zip archive data, at least v2.0 to extract, compression method=deflate
```

Forensics - Challenge

Wireshark - 2 flags

zeus.wpi - 1 flag

<http://10.2.2.175:8000/>

Extracurricular:

Andere protocollen in wireshark (ARP)

Crypto in protocollen

Formaat protocollen goed kennen

Checksums

Wifi handshake afluisteren & bruteforce

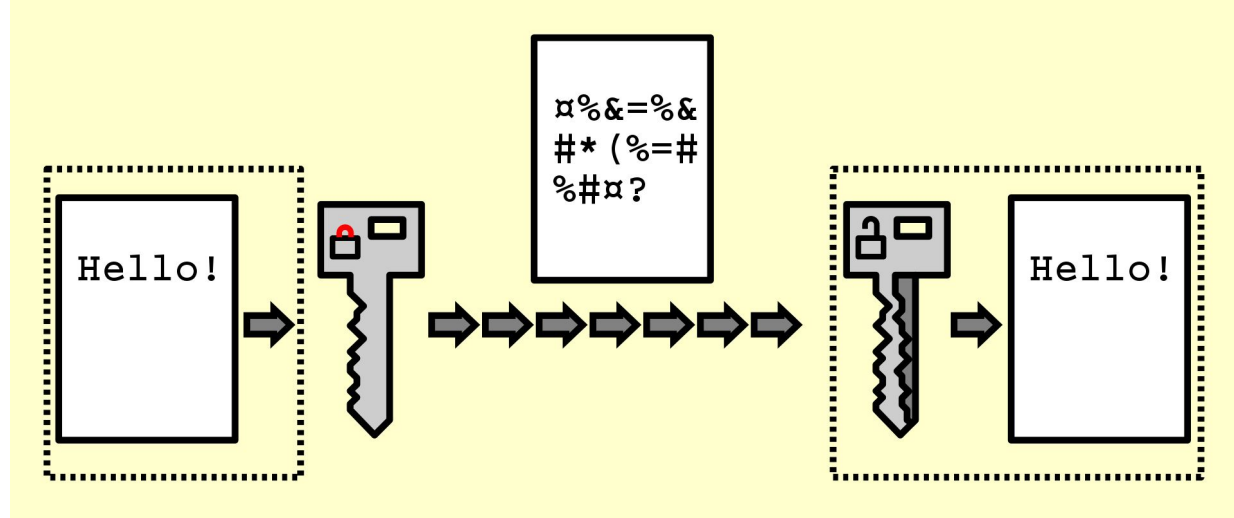
Crypto(graphy)

Versleutelen van informatie

Begrijpen algoritme en fout vinden en gebruiken

- Informatie lekken
- Foute input

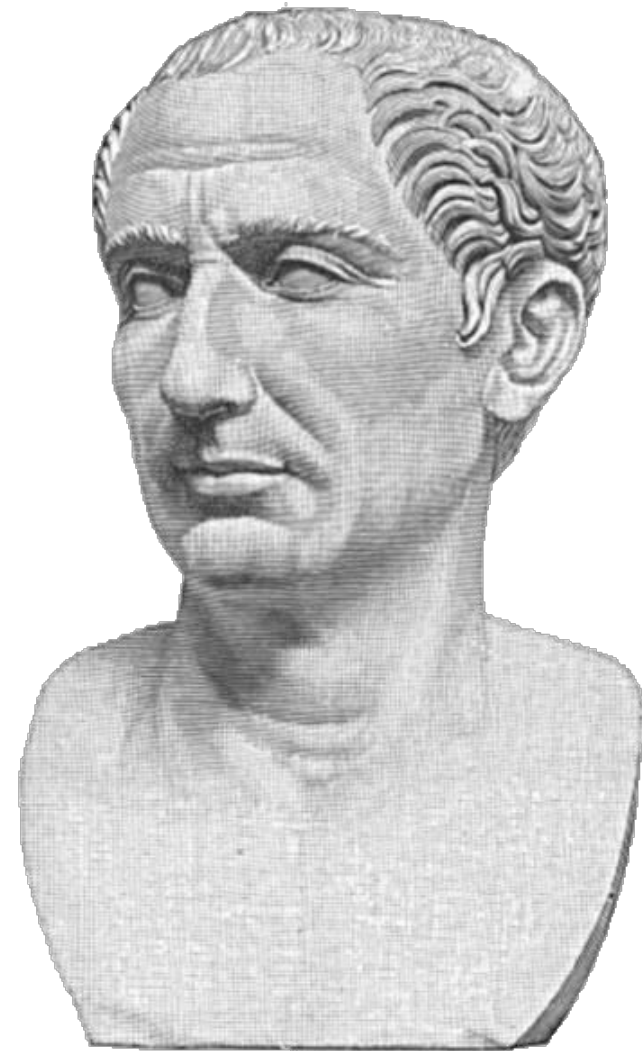
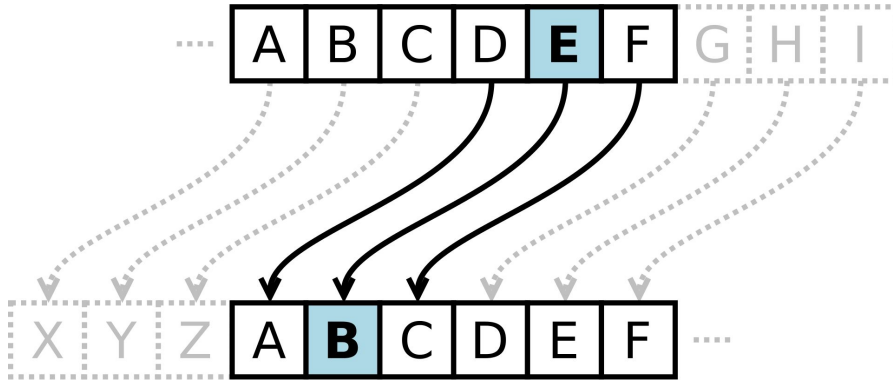
~W~i~s~k~u~n~d~e~



Crypto - Caesar cipher

Elke letter vervangen door de letter x plaatsen verder

Rot13: Caesar cipher met shift = 13



Crypto - XOR \oplus

Exclusieve OR functie = \oplus

Volledig reversibel:

$$\text{Text} \oplus \text{Key} = \text{Encrypted}$$

$$\text{Encrypted} \oplus \text{Key} = \text{Text}$$

$$\text{Text} \oplus \text{Encrypted} = \text{Key}$$

USING EXCLUSIVE OR (XOR) IN CRYPTOGRAPHY			
XOR LOGIC	0 XOR 0 = 0	Same Bits	
	1 XOR 1 = 0	Same Bits	
	1 XOR 0 = 1	Different Bits	
XOR Symbol \oplus	0 XOR 1 = 1	Different Bits	
ENCRYPT			
	0 0 1 1 0 1 0 1	Plaintext	
\oplus	1 1 1 0 0 0 1 1	Secret Key	
	<hr/>		
	= 1 1 0 1 0 1 1 0	Ciphertext	
DECRYPT			
	1 1 0 1 0 1 1 0	Ciphertext	
\oplus	1 1 1 0 0 0 1 1	Secret Key	
	<hr/>		
	= 0 0 1 1 0 1 0 1	Plaintext	

Crypto - XOR \oplus (advanced)

Korte keys = slecht

Key repetition

```
Zeus is the sky and thunder god  
1231231231231231231231231231231231
```

deel input geweten > key lekken?

```
ENCRYPTED  
LONGDATAT  
HATISLONG
```

elke 10de char is newline

Gekende file header (Magic bytes)

Crypto - Challenge

encrypted_flag.txt - 1 flag

flags.txt - 4 flags

Links:

<https://www.dcode.fr/en/>

<https://gchq.github.io/CyberChef/>

<https://github.com/trou/rsbkb>

Andere Categorieën

- OSINT
 - Verzamelen van publieke (open) informatie
- Misc
 - Random challenges
- Programming
 - Programming opdracht (scriptingtalen)
- Hardware
 - Microcontrollers



Next?

Volgende week [zeus CTF](#)

PicoCTF

Writeups lezen

Vragen?

Zeus kelder :D

Nu

cscbe@zeus.ugent.be

