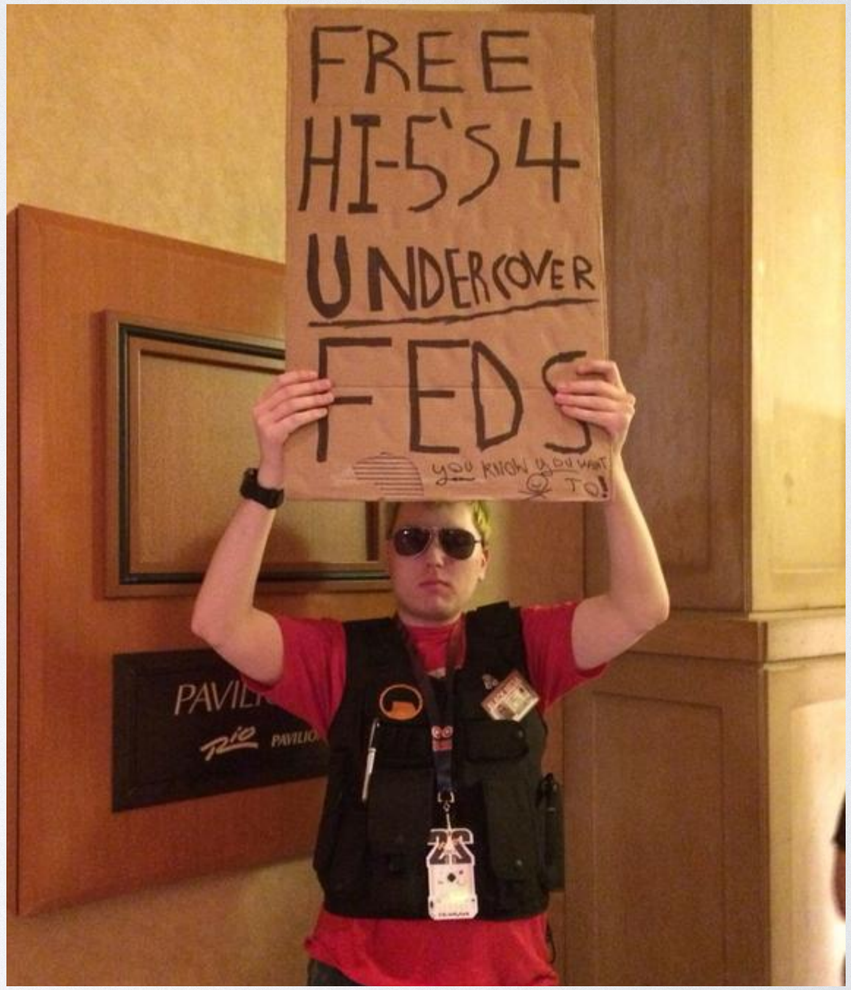
HACKER JEOPARDY

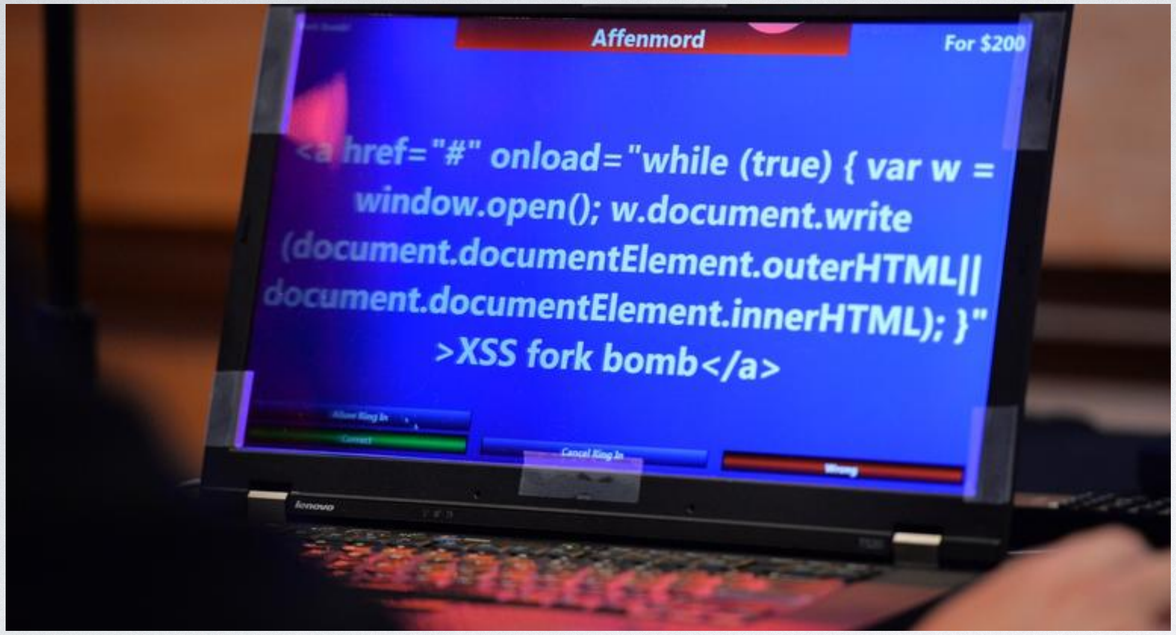
Time to have fun!

by Alessandro Tanasi (@jekil)

HACKER JEOPARDY??

- Una competizione basata su **quiz** di **cyber security**.
- Si gioca a **squadre** o **singolarmente**.
- La risposta corretta viene **premiata**, la risposta errata viene **punita**.
- Le domande sono *"di nicchia"*.
- **Google** o la vostra $entità suprema di fiducia non vi aiuteranno.




Affenmord
For $200
<a href="#" onload="while (true) { var w =
window.open(); w.document.write
(document.documentElement.outerHTML||
document.documentElement.innerHTML); }"
>XSS fork bomb


DEFCON DEFCON

REGOLE

- Formate squadre da **6 persone**, con i vostri vicini di tavolo.
- Scegliete il **nome** del team.
- Farò 10 domande a risposta multipla.
- Si risponde per **alzata di mano**.
- Il team che risponde **correttamente** vince uno shot di quello **buono**.
- Il team che **sbaglia** la risposta prende uno shot di quello **pessimo**.

Il digestivo è offerto volentieri, ma nessuno è obbligato a bere! Ci sono alternative **analcoliche**!


Bondage
Error Codes
$100
$200
$300
$400
HACKER
JEOPARDY IS GO!

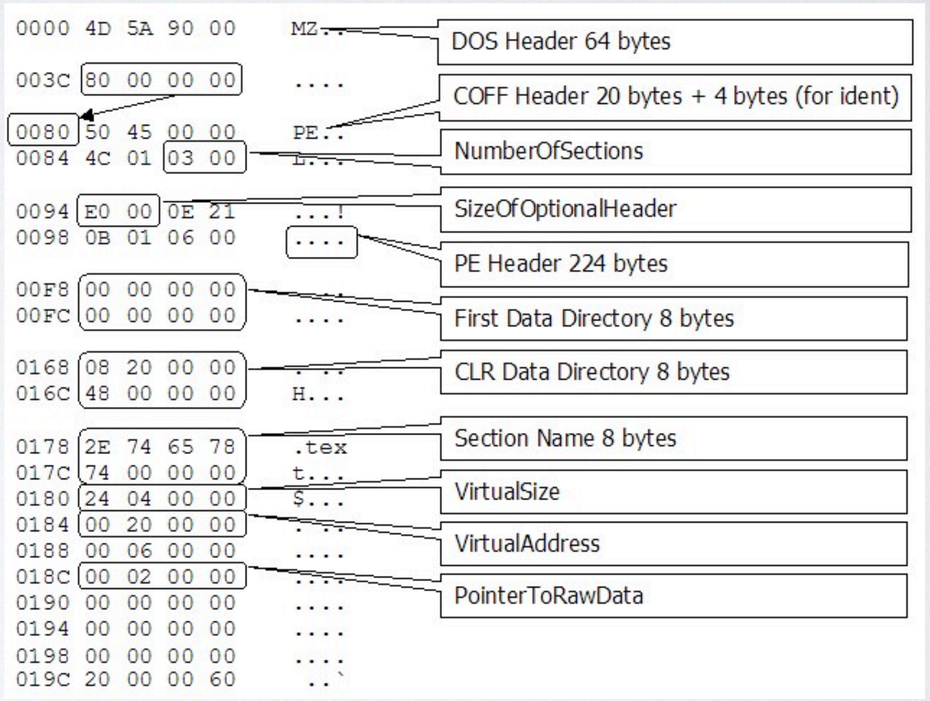
I FILE ESEGUIBILI IN DOS POSSONO ESSERE RICONOSCIUTI DAI PRIMI CARATTERI (MAGIC NUMBER), QUALI?

1. WIN
2. .EXE
3. MZ
4. AX

Domanda #1: Reversing

DOS MZ EXECUTABLE

- Il formato di file "DOS MZ executable" è usato per i file eseguibili (**.exe**) in DOS.
- Il **magic number** è una stringa presente all'inizio del file che indica quale è il suo formato (tipo).
- I file .exe possono essere identificati dalla stringa "**MZ**" (in esadecimale: 4D 5A) all'inizio del file.



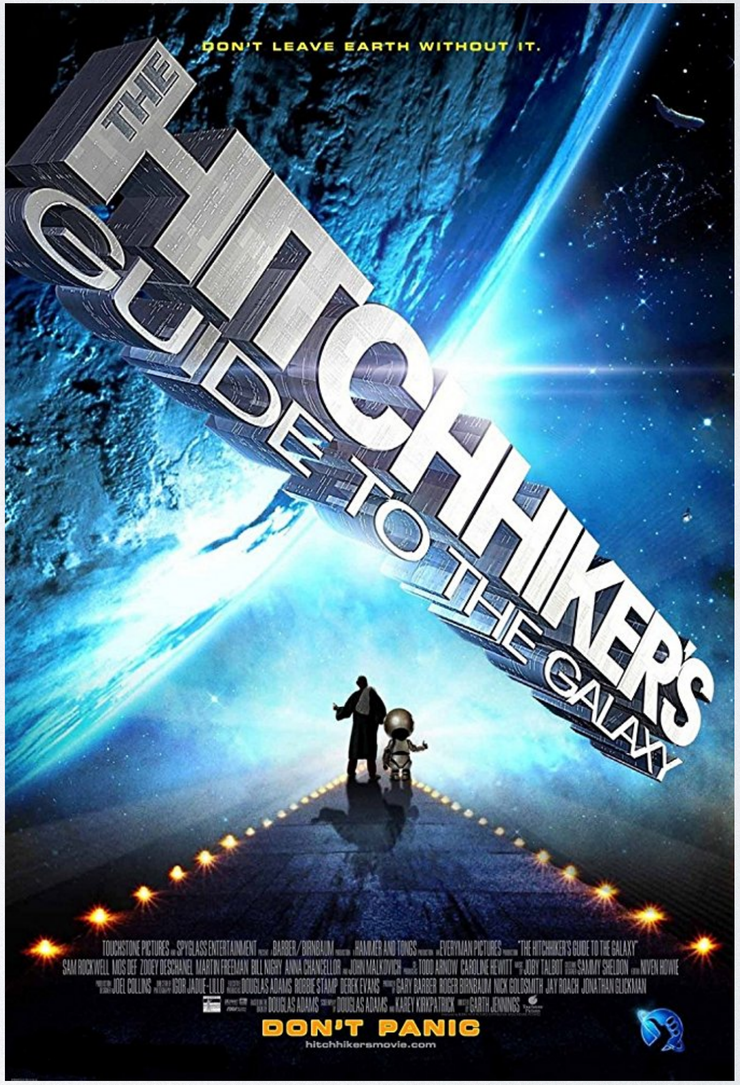
https://en.wikipedia.org/wiki/File_format#Magic_number
https://www.garykessler.net/library/file_sigs.html
https://en.wikipedia.org/wiki/DOS_MZ_executable

COSA E' SEMPRE NECESSARIO AVERE QUANDO SI VIAGGIA NELLO SPAZIO?

1. La mappa della galassia.
2. Un ricetrasmettitore.
3. Una navicella spaziale.
4. Un asciugamano.

GUIDA GALATTICA PER AUTOSTOPPISTI

- L'importanza dell'**asciugamano** è stata sancita nel **1978** in "The Hitchhiker's Guide to the Galaxy".
- *"A towel, it says, is about the most massively useful thing an interstellar hitchhiker can have. Partly it has great practical value"*.
- Il **25 maggio** è il "towel day".



https://en.wikipedia.org/wiki/Towel_Day
https://en.wikipedia.org/wiki/Technology_in_The_Hitchhiker%27s_Guide_to_the_Galaxy#Towels
https://en.wikipedia.org/wiki/The_Hitchhiker%27s_Guide_to_the_Galaxy

QUALE DELLE SEGUENTI RFC NON ESISTE?

1. Standard for the transmission of IP datagrams on Avian Carriers.
2. Customs Enforcement on IPv6 Broadcast.
3. IP over Avian Carriers with Quality of Service.
4. Wrongful Termination of Internet Protocol (IP) Packets.

Domanda #3: Networking

APRIL FOOLS' DAY REQUEST FOR COMMENTS

- Una Request for Comments (**RFC**) è una **specifica** creata dalla comunità scientifica per definire il funzionamento di una tecnologia.
- Dal 1989, ogni 1 aprile, vengono pubblicate delle RFC **Pesce d'Aprile**.
- Queste sono comunque tecnicamente **valide** e presentano soluzioni funzionanti!
- IPv6 **non prevede** il traffico broadcast, solo unicast e multicast.

IP over Avian Carriers

From Wikipedia, the free encyclopedia

A homing pigeon can carry Internet Protocol traffic.

In computer networking, **IP over Avian Carriers** (IPoAC) is a humorously-intended proposal to carry Internet Protocol (IP) traffic by birds such as homing pigeons. IP over Avian Carriers was initially described in **RFC 1149**, a "Request for Comments" (RFC) issued by the Internet Engineering Task Force (IETF) written by D. Waitzman and released on 1 April 1990 (April Fools' Day). It is one of several April 1 RFCs.

Waitzman described an improvement of his protocol in **RFC 2549**, *IP over Avian Carriers with Quality of Service* (1 April 1999).

IPoAC has been successfully implemented, but for only nine packets of data, with a packet loss ratio of 55% (due to user error[1]), and a response time ranging from 3000 seconds to over 6000 seconds. Thus, this technology suffers from poor latency. Nevertheless, for large transfers avian carriers are capable of high average throughput when carrying flash memory devices.

https://en.wikipedia.org/wiki/IPv6
https://en.wikipedia.org/wiki/Request_for_Comments
https://en.wikipedia.org/wiki/April_Fools%27_Day_Request_for_Comments

C'È UNA VULNERABILITÀ?

```c
#include  <stdio.h>
#include  <string.h>
#include  <stdlib.h>

int main (int argc, char **argv)
{
    char buf [100];
    int x = 1 ;
    snprintf ( buf, sizeof buf, argv [1] ) ;
    buf [ sizeof buf -1 ] = 0;
    printf ( "Buffer size is: (%d) \nData input: %s \n" , strlen (buf) , buf ) ;
    printf ( "X equals: %d/ in hex: %#x\nMemory address for x: (%p) \n" , x, x, &x) ;
    return 0 ;
}
```

1. No.
2. Cross Site Scripting.
3. Format String.
4. Integer Overflow.

FORMAT STRING VULNERABILITY

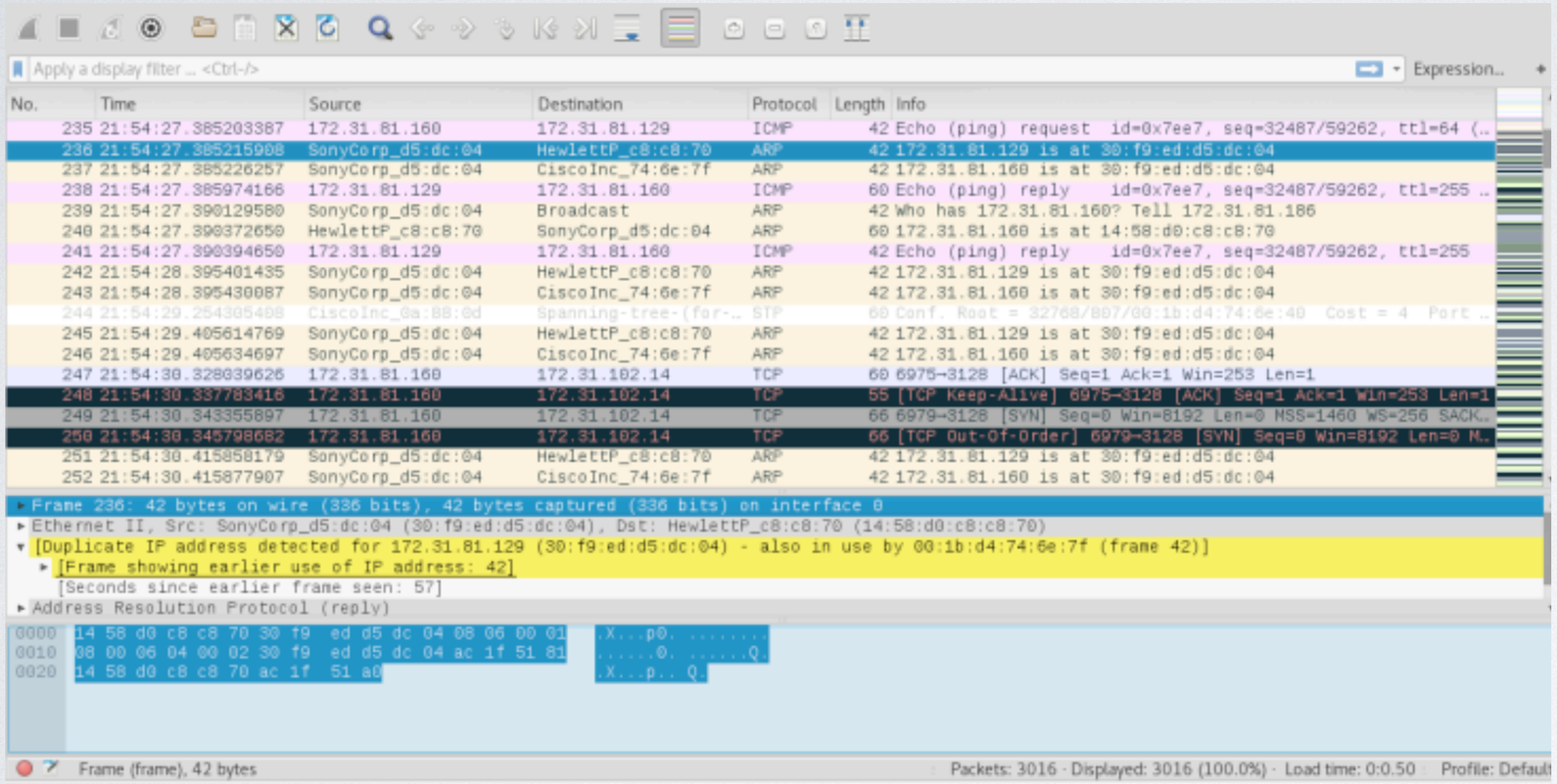
- Una **format string** è una stringa contenente parametri di formato come ad esempio **%i** o **%d**.
- Un errore classico è quello di stampare direttamente una stringa senza **specificare** il formato.
- L'iniezione di format string permette di **leggere** e **scrivere** aree di memoria.

```
% ./fmtme "hello world"
buffer (11): hello world
x is 1/0x1 (@ 0x804745c)
```

```
% ./fmtme "%x %x %x %x"
buffer (15): 1 f31 1031 3133
x is 1/0x1 (@ 0x804745c)
```

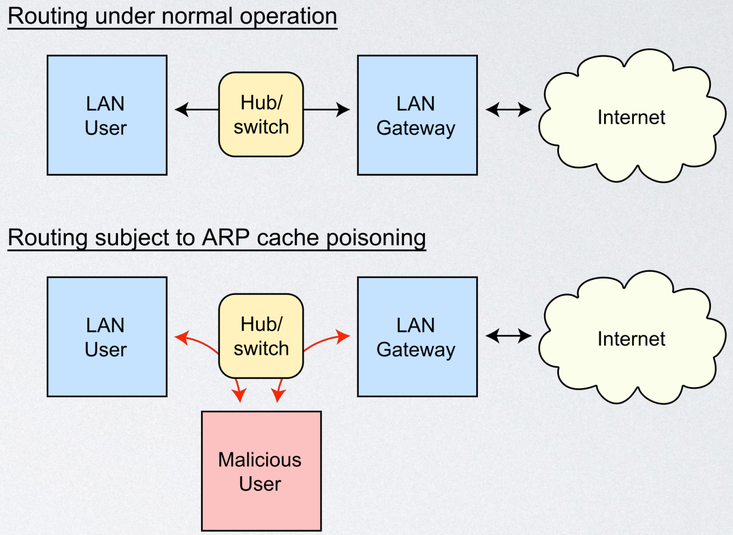
http://www.dsi.unive.it/~focardi/corso-security/lab/lab4-2011.pdf
http://forum.ouah.org/FormatString.PDF

C'È UN ATTACCO IN CORSO?



1. No.
2. VLAN Hopping.
3. DDoS.
4. ARP Spoofing.

- **ARP Spoofing** (o **ARP Poisoning**) è un attacco layer 2 in cui, in una rete switched, si annunciano entry ARP false.
- Perfette di "diventare un altro IP", annunciando la risoluzione ARP.
- Utilizzato in attacchi **Man in The Middle** (MiTM), tipicamente per diventare il gateway di una rete.



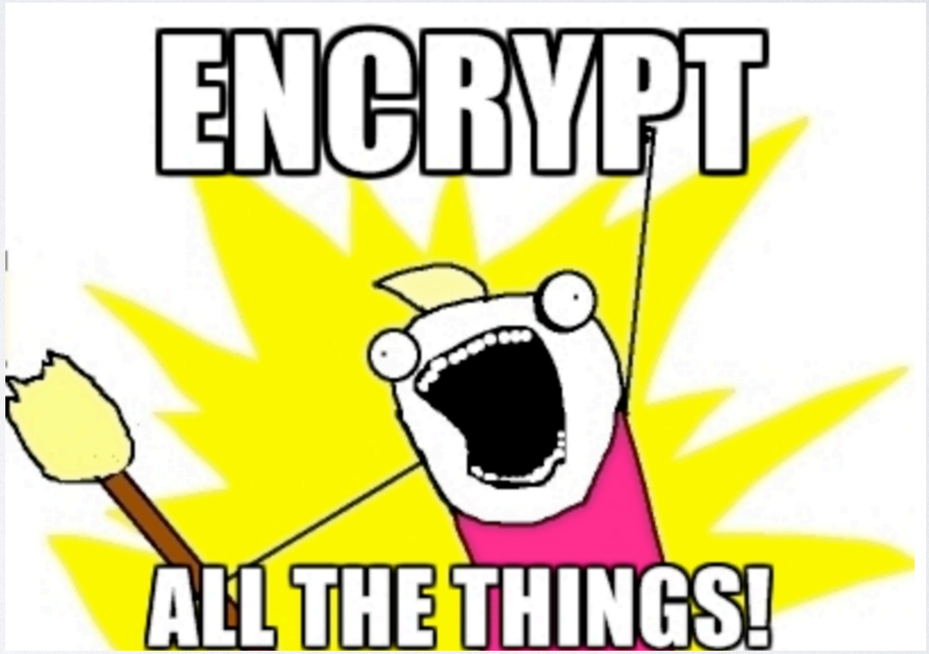
https://en.wikipedia.org/wiki/ARP_spoofing
https://medium.com/secjuice/man-in-the-middle-attack-using-arp-spoofing-fa13af4f4633
https://www.bettercap.org
https://www.ettercap-project.org

PERCHÉ DES È INSICURO?

1. C'è stato un leak del seed.
2. Ha solo 8 bit di controllo.
3. Con 64 bit di chiave ci sono collisioni.
4. La chiave è di 56bit.

DATA ENCRYPTION STANDARD (DES)

- Un **algoritmo** di cifratura scelto come standard dal FIPS per il governo degli USA nel 1976.
- Si basa su un algoritmo a **chiave simmetrica** con chiave a 64 bit (ma solo **56** utili poiché 8 sono di controllo).
- Attualmente DES è considerato **insicuro**, ma è stato creato Triple DES.



https://en.wikipedia.org/wiki/Data_Encryption_Standard
http://www.dia.uniroma3.it/~dispense/merola/critto/tesine/DES.pdf

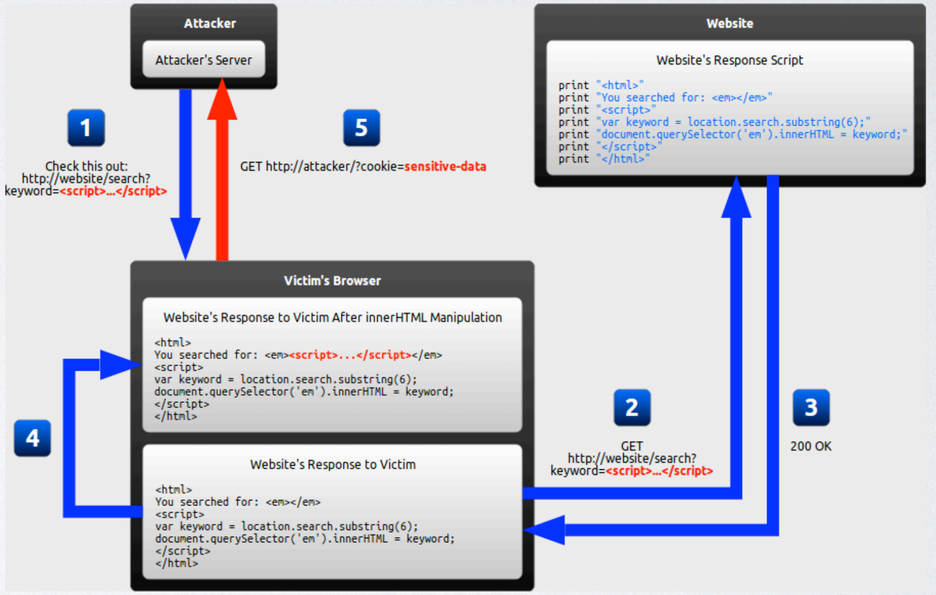
C'È UNA VULNERABILITÀ?

```
<html>
<head>
<title>Custom Dashboard </title>
...
</head>
Main Dashboard for
<script>
        var pos=document.URL.indexOf("context=")+8;
        document.write(document.URL.substring(pos,document.URL.length));
</script>
...
</html>
```

1. DOM XSS.
2. SQL Injection.
3. URL Parameter Overflow.
4. No.

DOM CROSS SITE SCRIPTING

- In un DOM XSS il **payload**, non è riflesso dal web server, ma dal codice **javascript** della pagina.
- La vulnerabilità risiede quindi nel codice **client side**.
- Il testing di questa vulnerabilità è molto complicato (identificazione sink, exploiting).



https://excess-xss.com/
https://www.owasp.org/index.php/DOM_Based_XSS
https://www.scip.ch/en/?labs.20171214

CHI SONO?

1. L0pht Heavy Industries.
2. Cult of DeathMilk.
3. SubSeven Team.
4. Lizard Squad.

- Famoso **gruppo hacker** tra il 1992 e il 2000 di base a Boston.
- Pionieri sul fronte della **responsible disclosure**.
- Hanno testimoniato al **congresso** su "Weak Computer Security in Government" nel 1998.

https://en.wikipedia.org/wiki/L0pht
https://www.theregister.co.uk/2018/06/18/l0pht_chris_wysopal_interview/

A COSA CORRISPONDE?

```
1   xor ebx, ebx
2   a01:
3   cmp ebx, 10
4   jge z74
5   inc ebx
6   inc ebx
7   jmp a01
8   z74:
```

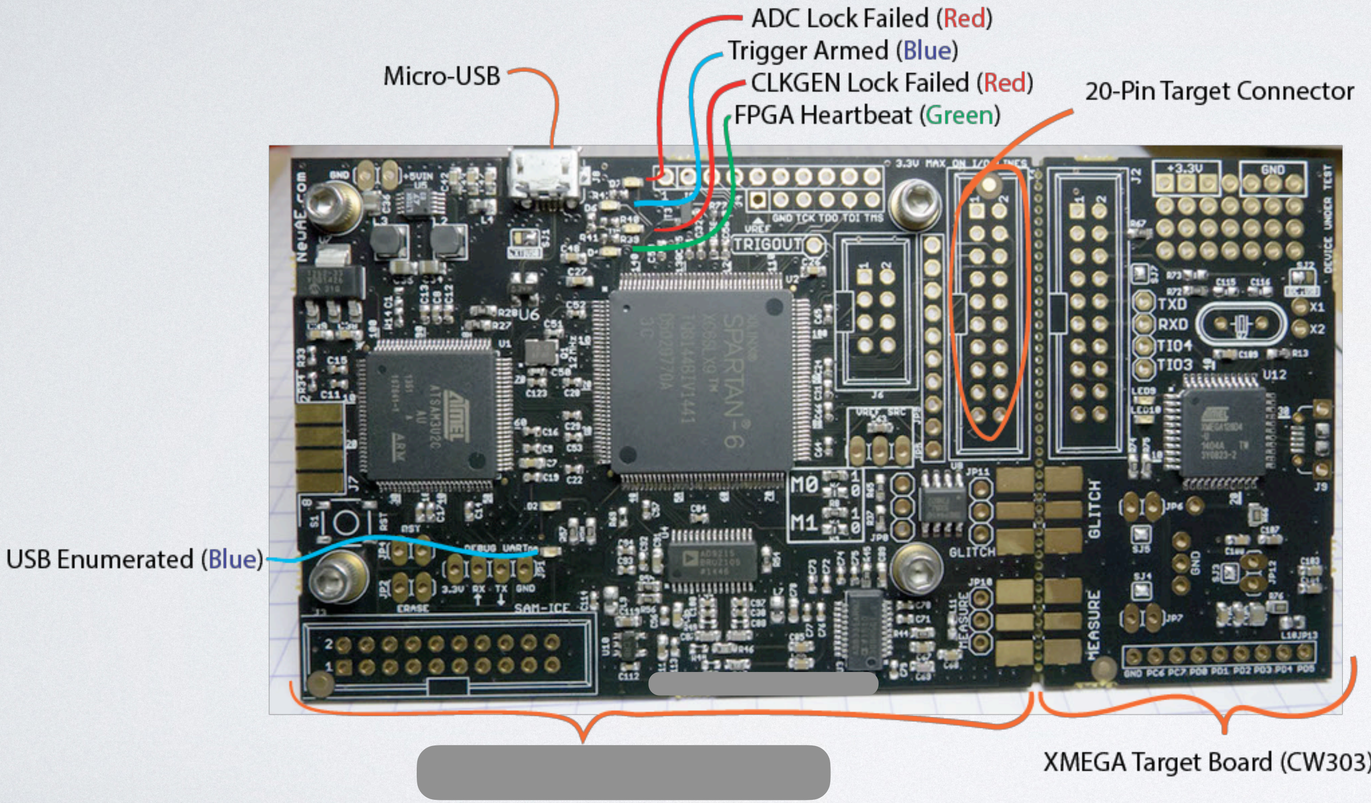
1. L'accensione di un led.
2. Un ciclo for (dettagli?).
3. Una chiamata a funzione (dettagli?).
4. Uno switch…case (dettagli?).

FOR PATTERN IN ASM

```
1   xor ebx, ebx    ; Reset ebx, for (i = 0;
2   top:            ; Punto di inizio loop.
3   cmp ebx, 10     ; Check i < 10
4   jge end_loop    ; Se i < 10 vai esci.
5                   ; Corpo del loop (codice qui)
6   inc ebx         ; i++
7   inc ebx         ; i++
8   jmp top         ; Ricomincia dal inizio.
9   end_loop:
```

for(i=0;i<10;i+2)

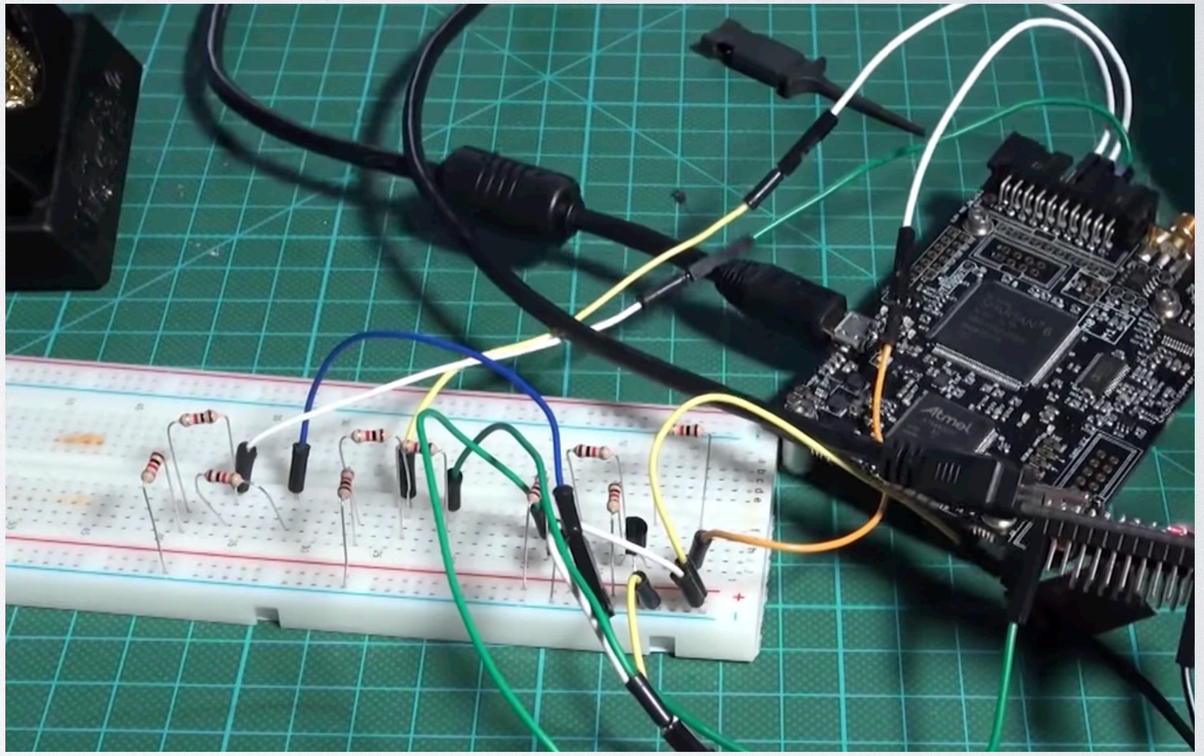
A COSA SERVE? CHE COSA È?



1. Power Analysis - ChipWhisperer.
2. Bluetooth Hacking - Ubertooth.
3. GSM Hacking: SDR / OpenBTS.
4. Embedded PC - Arduino PowerPro.

DIFFERENTIAL POWER ANALYSIS

- Una forma di **side channel attack** basato sullo studio dei **consumi elettrici**.
- L'hardware altera il suo consumo in base alle istruzioni che vengono eseguite all'interno dei **chip**.
- Misurando la differenza di consumo e applicando **modelli statistici** è possibile fare ipotesi sul codice (o i dati) interni ad un chip.



https://en.wikipedia.org/wiki/Power_analysis
https://newae.com/tools/chipwhisperer/
https://www.youtube.com/watch?v=FktI4qSjzaE
https://www.youtube.com/watch?v=bFfyROX7V0s