

#SMDCyberChallenge
#MissionCyberChallenge

Disassembly of section .init:

00000000002000 <.init>:

```
2000: f3 0f 1e fa  
2004: 48 83 ec 08  
2008: 48 8b 05 a9 6f 00 00  
200f: 48 85 c0  
2012: 74 02  
2014: ff d0  
2016: 48 83 c4 08  
201a: c3
```

```
endbr64  
sub $0x8,%rsp  
mov 0x6fa9(%rip),%rax  
test %rax,%rax  
je 2016 <__cxa_finalize@plt -0x37a >  
call *%rax  
add $0x5,%rsp  
ret
```

Disassembly of section .plt:

00000000002020 <.plt>:

```
2020: ff 35 b2 6d 05 00  
2026: 41 52 ff 43 6d 00  
202d: 01 00 00 00  
2030: 00 00 00 00  
2034: 00 00 00 00  
2039: 00 00 00 00  
203f: 00 00 00 00  
2040: 00 00 00 00  
2044: 00 00 00 00  
2049: 00 00 00 00  
204f: 00 00 00 00  
2056: 00 00 00 00  
2054: 68 00 00 00  
2059: 00 00 00 00  
205f: 00 00 00 00
```

```
endbr64  
Target Protection  
sub $0x8,%rsp  
mov 0x6fa9(%rip),%rax  
test %rax,%rax  
je 2016 <__cxa_finalize@plt -0x37a >  
call *%rax  
add $0x5,%rsp  
ret
```

```
endbr64  
Target Protection  
sub $0x8,%rsp  
mov 0x6fa9(%rip),%rax  
test %rax,%rax  
je 2016 <__cxa_finalize@plt -0x37a >  
call *%rax  
add $0x5,%rsp  
ret
```

SFIDE

// MISSIONE CYBER CHALLENGE

Partecipa alla prima Cyber Challenge
dello Stato Maggiore Difesa
e metti in gioco il tuo talento



CHE SFIDE TI ASPETTANO?

Le principali aree tematiche su cui verteranno le sfide della Cyberchallenge potranno essere:

- **Cryptography & Steganography** - decifrare messaggi segreti trasmessi in rete. Scoprire dati nascosti in immagini o file compressi;
- **Forensic** - investigare su file modificati o cancellati da dispositivi digitali (es. chiavette USB, immagini digitali);
- **Reverse Engineering & Binary Exploitation** - analizzare e capire il funzionamento interno di software e programmi sconosciuti, per trovarne il comportamento nascosto o i punti deboli;
- **Segnali e sorveglianza** - intercettare e interpretare segnali (radio, video, ecc.) per scoprire messaggi nascosti, anche in ambienti isolati (air-gap);
- **Sicurezza dei siti web** - attaccare e difendere siti web con vulnerabilità comuni (es. falle nei moduli di ricerca, nei caricamenti di file o nelle comunicazioni);
- **Attacchi avanzati ai sistemi** - simulare scenari complessi con attacchi combinati per entrare nei sistemi sfruttando errori di configurazione e vulnerabilità multiple;
- **Tecnologie emergenti (Web3)** - esplorare e violare contratti digitali su blockchain per mostrare i rischi nelle nuove piattaforme decentralizzate.

[Qui esempi di sfide per esercitazione](#)