

# Open Redirect & Worm Exploits: A Practical Study

Samuele Aversa

# Indice

Disclaimer.....	1
Fastfood Hacking .....	2
Robots.txt.....	3
Potenziale sfruttamento.....	4
Impatti.....	5
Download malware.....	6
Sintomi.....	7
Conclusioni.....	8

# DISCLAIMER

Tutti i test relativi alla vulnerabilità Open Redirect e all'infezione da worm sono stati eseguiti esclusivamente in ambienti virtuali isolati. L'obiettivo del sito utilizzato per il progetto è puramente didattico e concettuale: si tratta di una piattaforma basic creata per dimostrare come avverrebbe l'exploit in un contesto reale, senza impattare alcun sistema in produzione o pubblico.

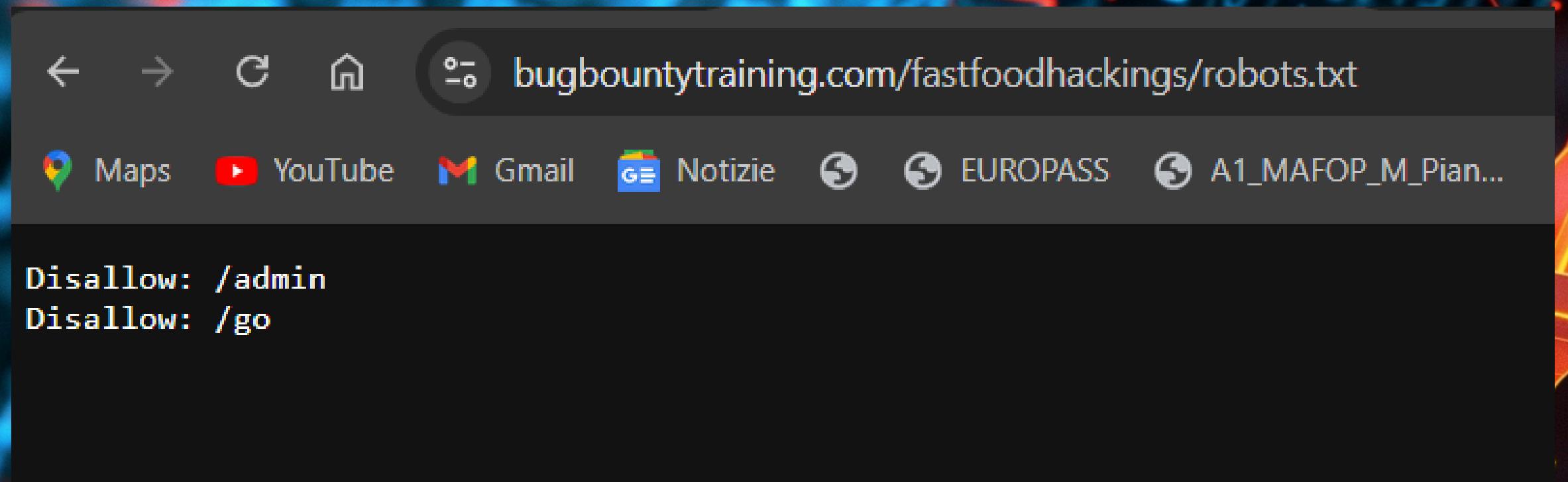
Il worm descritto nel progetto è stato scritto in Python, un linguaggio scelto per la sua semplicità e per facilitare la comprensione del funzionamento base del malware. Tuttavia, va sottolineato che un worm più sofisticato, scritto in Shell, potrebbe bypassare con maggiore facilità i WAF (Web Application Firewall) e altri sistemi di protezione implementati. Questo progetto si concentra su spiegazioni concettuali e non mira a fornire una guida operativa per attacchi informatici, bensì a sensibilizzare sul tema della sicurezza informatica.

Il progetto non incoraggia né supporta l'utilizzo di vulnerabilità per fini illegali. Qualsiasi sperimentazione deve essere condotta in ambienti controllati e per scopi di apprendimento o di ricerca.



Fastfood Hacking è un sito concettuale e minimalista, progettato per simulare alcune delle vulnerabilità più comuni in ambito di sicurezza informatica. Il nome richiama l'idea del "fast food": tecniche di hacking che, come i piatti pronti, sono accessibili, rapide da implementare e semplici da comprendere, ma non per questo meno potenti o impattanti a livello didattico.

# LEGENDA

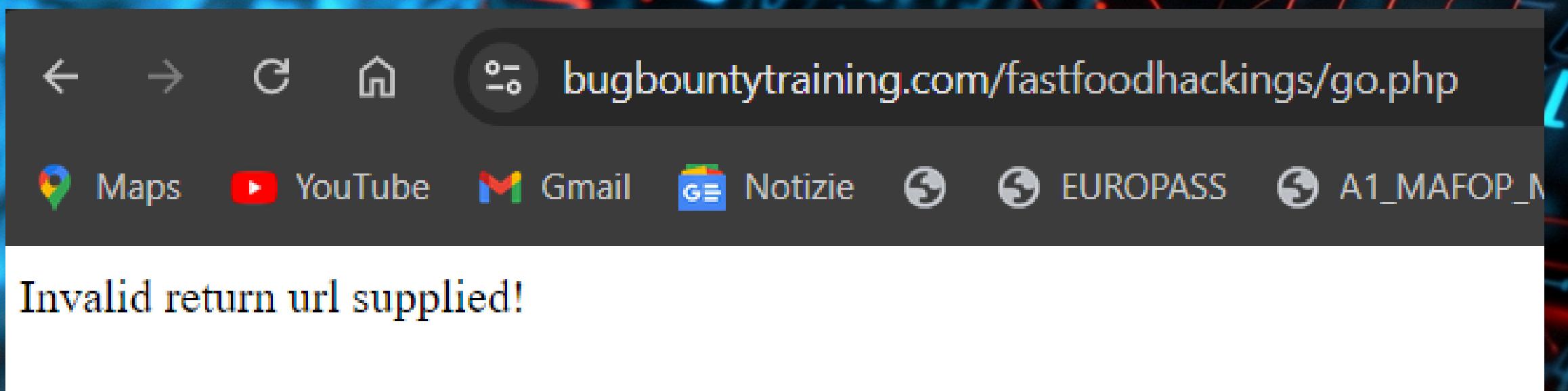


**User-agent:** indica il crawler a cui sono destinate le regole (es. Googlebot per Google).

**Disallow/Allow:** specificano le parti del sito da bloccare all'indicizzazione (Disallow) o da permettere (Allow).

**Il robots.txt è un file di testo semplice utilizzato dai siti web per dare indicazioni ai crawler (anche detti spider), ossia quei programmi automatici che "scansionano" i siti per conto dei motori di ricerca (come Google), su quali pagine o sezioni del sito possono essere esplorate e indicizzate, e quali invece devono essere escluse.**

**Il file robots.txt non è un meccanismo di sicurezza, quindi non impedisce effettivamente l'accesso a determinate pagine. Un utente malintenzionato o un crawler che ignora il file potrebbe comunque visitare e accedere a qualsiasi URL.**

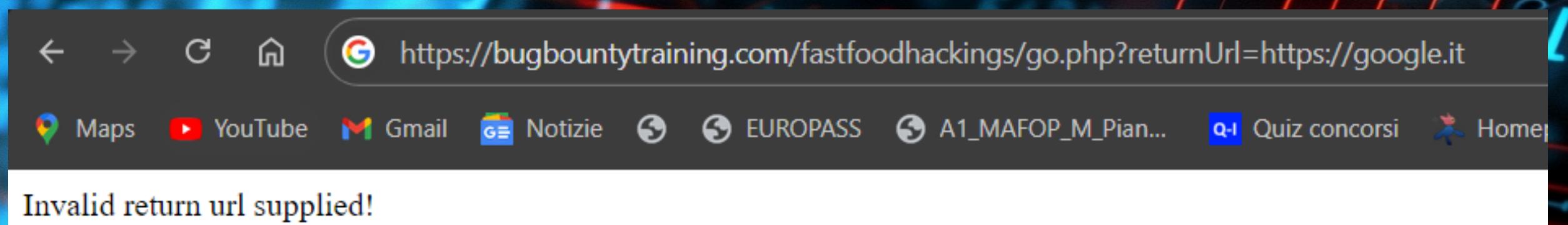


# Potenziale sfruttamento

Nel caso specifico, l'errore "URL invalido" suggerisce che nel file .php manchi un parametro o un set di parametri necessari per completare correttamente la richiesta. Questa situazione potrebbe indicare un potenziale punto di sfruttamento per un attacco Open Redirect.

Gli hacker potrebbero tentare di inviare varie query string per capire quale sia il parametro corretto dell'URL, utilizzando convenzioni di denominazione comuni dei programmatori:

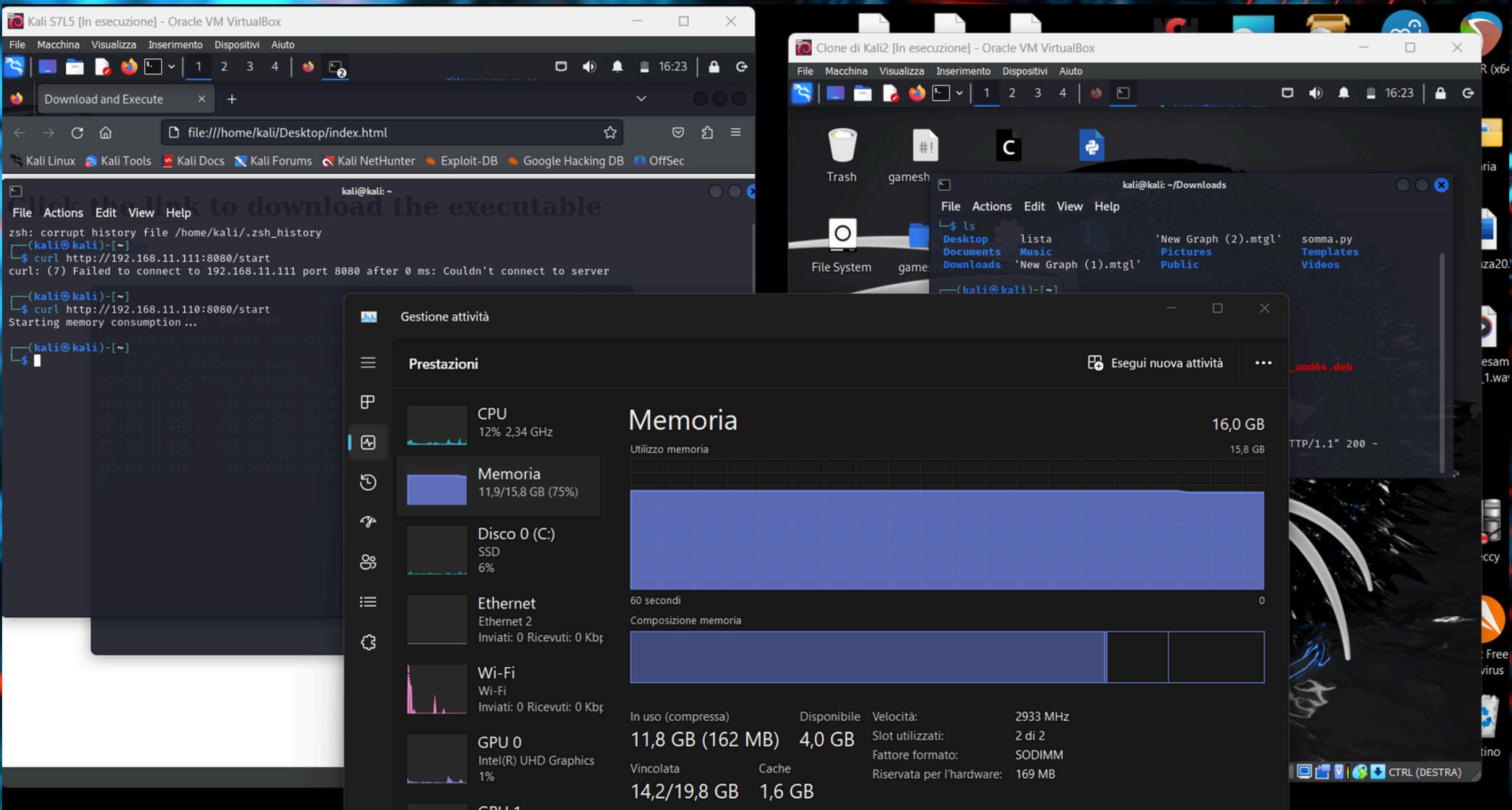
Ad esempio: url=, returnurl, redirect, oppure varianti come reUrl o nomi di variabili con underscore (\_). Inviando questi tentativi attraverso il link con il parametro ?, gli attaccanti potrebbero scoprire come forzare un reindirizzamento verso un sito arbitrario.



# Impatti

Un Open Redirect può essere utilizzato per reindirizzare le vittime su siti clonati, sfruttati per attacchi di phishing, oppure su pagine contenenti malware, inducendo l'utente a scaricare software dannosi senza saperlo. Anche se non più tra le vulnerabilità più critiche secondo OWASP, i rischi sono ancora rilevanti, soprattutto se il sito in questione ha un elevato traffico di utenti.

Nel contesto del progetto, possiamo anche esaminare una situazione in cui un attacco tramite Open Redirect porta l'utente a scaricare un worm. Ecco come potrebbe evolversi l'attacco e i sintomi che si manifestano sul sistema compromesso.



Dopo il reindirizzamento, l'utente viene portato su un sito malevolo che imita una pagina legittima o utilizza inganni per indurlo a scaricare un file. Se l'utente esegue il download, il worm si installa silenziosamente sul sistema, replicandosi e diffondendosi attraverso la rete o via e-mail.

CPU: 3%

Processes: 18

Memory: 49% (2.6 GiB / 5.3 GiB) Swap: 0% (0 bytes / 1024 MiB)

Task	PID	RSS	▲	CPU
python virus.py	4301	1.4 GiB	1%	

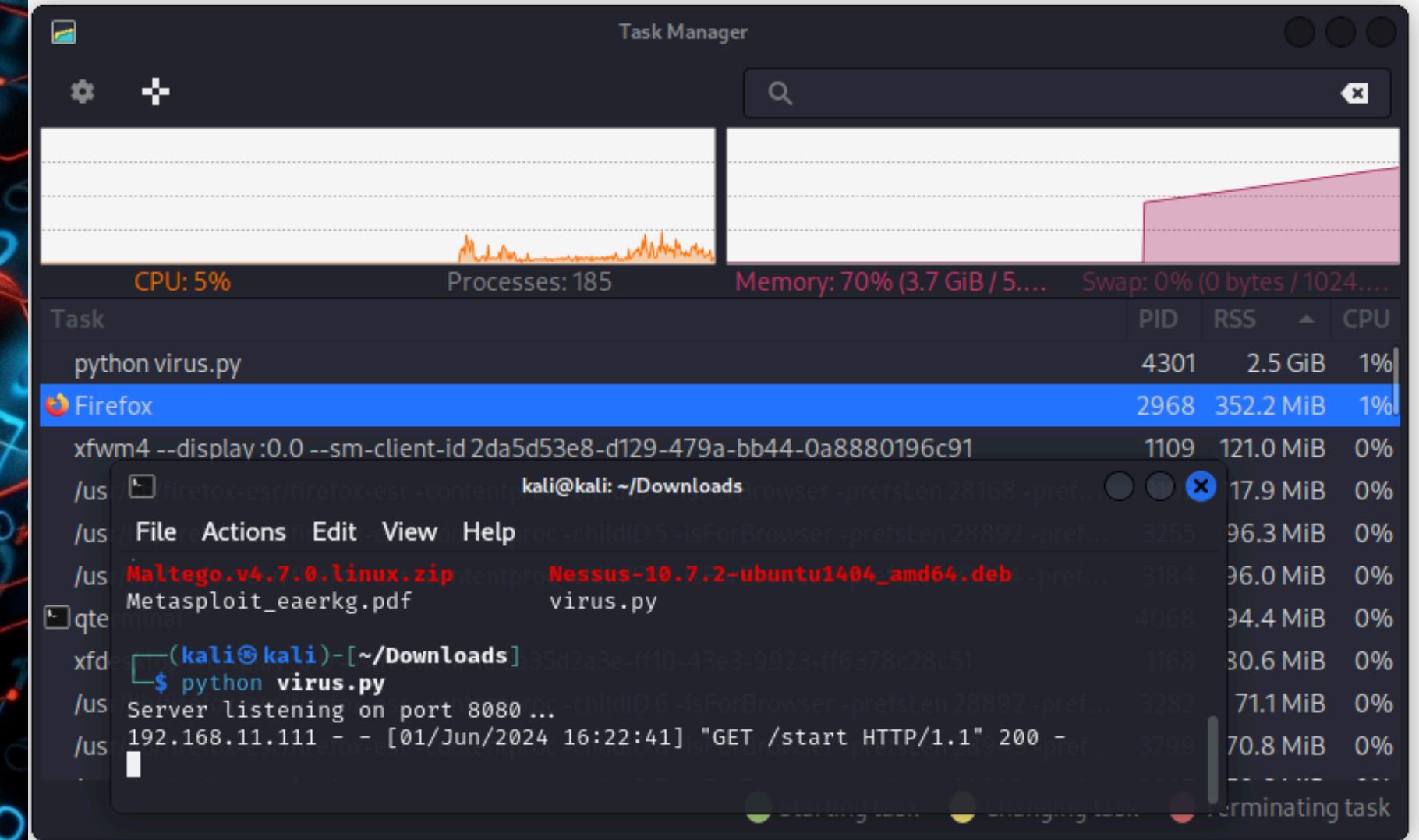
# Sintomi

**Una volta insediato, il worm inizia a consumare risorse di sistema. Ecco i sintomi tipici:**

- **Rallentamento della RAM:** l'uso eccessivo di memoria provoca un calo delle prestazioni, con programmi più lenti ad aprirsi.
  - **Processi sconosciuti:** nel task manager appaiono processi non riconosciuti o simili a quelli legittimi.
  - **Aumento del traffico di rete:** il worm si diffonde inviando dati ad altri computer, causando rallentamenti della connessione o picchi di attività.
  - **Crash improvvisi:** l'eccessivo uso di risorse può portare a crash o blocchi del sistema.

**Click the link to download the executable**

[Download Executable](#)



# CONCLUSIONI

Se non rilevato e rimosso in tempo, il worm potrebbe compromettere l'intera rete, diffondendosi su altri dispositivi, e potrebbe lasciare il sistema vulnerabile ad ulteriori attacchi, come l'installazione di backdoor o la sottrazione di dati personali.

Questo scenario illustra i gravi rischi connessi a vulnerabilità come l'Open Redirect, che, se sfruttate, possono condurre a infezioni come i worm, con conseguenze dannose per le prestazioni del sistema e la sicurezza degli utenti.