UNIVERSITÀ DEGLI STUDI DI SALERNO

DIPARTIMENTO DI INFORMATICA

Corso di Laurea Magistrale in Informatica
Penetration Testing and Ethical Hacking

Penetration Testing Report
Bizness

Relatore:
Prof.
Arcangelo Castiglione

Luca Boffa
Mat. 0522501521

ANNO ACCADEMICO 2023/2024

Indice

1. Executive Summary

Il presente rapporto illustra i risultati del penetration test condotto sull'asset "Bizness" della piattaforma HackTheBox da Luca Boffa. Questo test è stato commissionato nell'ambito del corso di Penetration Testing and Ethical Hacking dell'Università degli Studi di Salerno. L'obiettivo principale del test era valutare la sicurezza dell'asset Bizness, identificando, analizzando, sfruttando e documentando il maggior numero possibile di vulnerabilità presenti.
Il penetration test è stato avviato il 30 giugno 2024 e concluso il 9 luglio 2024. Poiché al pentester non sono state fornite informazioni preliminari, l'approccio adottato è stato di tipo black-box. Durante questo periodo, l'asset Bizness è stato analizzato in modo approfondito utilizzando tecniche sia manuali che automatiche, con l'ausilio di software consolidati nel campo del penetration testing.
Queste tecniche hanno permesso di individuare diverse vulnerabilità. Successivamente, è stato analizzato come un potenziale attaccante potrebbe sfruttare tali vulnerabilità per eludere i sistemi di sicurezza dell'asset e compromettere ulteriori sistemi collegati. È stato quindi determinato il potenziale impatto di queste vulnerabilità sull'asset.
I risultati del test hanno rivelato varie vulnerabilità, alcune delle quali di natura critica, che potrebbero portare alla completa compromissione della macchina Bizness. Questo documento fornirà una descrizione dettagliata di tutte le vulnerabilità identificate e il loro potenziale impatto sull'asset. Inoltre, verranno specificate le possibili mitigazioni per eliminare completamente il rischio e ripristinare la totale sicurezza della macchina. Finché la postura di sicurezza non verrà rafforzata, il rischio di compromissione rimarrà significativo.

2. Engagement Highlights

Considerando quanto affermato in precedenza e il fatto che l'asset Bizness è progettato per essere vulnerabile agli attacchi (vulnerable by design), non ci sono limitazioni tecniche o legali nell'esecuzione del processo di penetration testing, purché si rimanga all'interno dell'environment di Bizness e non si tenti di attaccare altre parti della rete interna di HackTheBox.
Poiché si tratta di un'attività di penetration testing non finanziata esternamente, ma condotta a fini progettuali nel contesto di un corso universitario, il test doveva essere effettuato utilizzando esclusivamente la macchina a disposizione dello studente e solo con strumenti gratuiti o forniti dall'università. Il test doveva essere completato entro il

16/07/24, data dell'esame, entro la quale bisognava verificare e certificare la sicurezza del sistema, individuare le vulnerabilità e suggerire mitigazioni.
La metodologia adottata per condurre il test si basa su un framework generico composto dalle seguenti fasi:

1. Target Scoping
2. Information gathering
3. Target discovery
4. Enumerating target
5. Vulenrability mapping
6. Target Exploitaion
7. Privilage Escalation
8. Manteining access
9. Reporting

Per effettuare il test è stato utilizzato un computer con OS Kali Linux, sul quale erano stati già installati e configurati gran parte dei tool necessari.

Questo documento rappresenta solo la fase 9. Per la descrizione dettagliata di tutte le fasi rimanenti, si rimanda al documento allegato "Penetration Testing Narrative".

3. Vulnerability Report

Le vulnerabilità riscontrate durante il penetration testing derivano principalmente dall'utilizzo di versioni obsolete di alcuni applicativi. Tali versioni vulnerabili possono essere sfruttate da un attaccante per ottenere accesso parziale o completo all'asset, o per raccogliere ulteriori informazioni sul target. In particolare, queste criticità possono consentire l'acquisizione di una shell con privilegi di amministratore, rappresentando così il massimo livello di compromissione poiché offrirebbe all'attaccante il controllo totale del sistema.
Ulteriori debolezze riscontrate sono legate a configurazioni errate o alla mancanza di controlli durante l'implementazione delle Web Application disponibili.

In particolare, le configurazioni errate hanno portato all'individuazione delle seguenti vulnerabilità:

- **TLS Version 1.1 Deprecated Protocol - Livello criticità: MEDIUM**
  - Il servizio remoto accetta connessioni crittografate tramite TLS 1.1. TLS 1.1 manca del supporto per le suite di crittografia attuali raccomandate. I cifrari che supportano la crittografia prima del calcolo MAC e le modalità di crittografia autenticate come GCM non possono essere utilizzati con TLS 1.1 A partire dal 31 marzo 2020, gli endpoint che non sono abilitati per TLS 1.2 e versioni successive non funzioneranno più correttamente con i principali browser web e i principali fornitori.
- **Web Application Potentially Vulnerable to Clickjacking - Livello criticità: MEDIUM**
  - Il server Web remoto non imposta un'intestazione di risposta X-Frame-Options o un'intestazione di risposta "frame-ancestors" di Content-Security-Policy in tutte le risposte di contenuto. Ciò potrebbe potenzialmente esporre il sito a un clickjacking o a un attacco di riparazione dell'interfaccia utente, in cui un utente malintenzionato può indurre un utente a fare clic su un'area della pagina vulnerabile che è diversa da quella che l'utente percepisce la pagina. Ciò può comportare l'esecuzione di transazioni fraudolente o dannose da un utente. X-Frame-Options è stato proposto da Microsoft come un modo per mitigare gli attacchi di clickjacking ed è attualmente supportato da tutti i principali fornitori di browser.
- **ICMP Timestamp Request Remote Date Disclosure - Livello criticità: LOW**
  - L'host remoto risponde a una richiesta di timestamp ICMP. Ciò consente a un utente malintenzionato di conoscere la data impostata sulla macchina di destinazione, il che può aiutare un utente malintenzionato remoto non autenticato ad attaccare i protocolli di autenticazione basati sul tempo.
- **TCP Timestamps Information Disclosure - Livello criticità: LOW**
  - L'host remoto implementa timestamp TCP e quindi consente a un utente malintenzionato di conoscere la data impostata sulla macchina di destinazione, il che può aiutare un utente malintenzionato remoto non autenticato ad attaccare i protocolli di autenticazione basati sul tempo.
- **Weak MAC Algorithm(s) Supported (SSH) - Livello criticità: LOW**
  - Il server SSH remoto supporta algoritmi MAC client-to-server deboli.

4. Remediation Report

Il penetration test condotto ha rivelato un livello di sicurezza dell'asset piuttosto basso. Di conseguenza, è fondamentale adottare le seguenti contromisure dettagliate per migliorare la sicurezza complessiva:

- **Sviluppo di un piano di risoluzione delle vulnerabilità**: È cruciale sviluppare un piano strutturato per affrontare tutte le vulnerabilità e debolezze identificate in questo report. Si raccomanda di iniziare dalle vulnerabilità critiche, poiché presentano il rischio più elevato per la sicurezza dell'asset. Successivamente, si dovrebbe procedere con le vulnerabilità ad alta, media e bassa gravità.

- **Aggiornamento continuo degli applicativi**: È cruciale mantenere tutti i software utilizzati costantemente aggiornati. Gli aggiornamenti regolari assicurano che le ultime patch di sicurezza siano applicate, riducendo il rischio di exploit noti. Si consiglia di implementare un sistema di gestione delle patch che notifichi la presenza di eventuali aggiornamenti di sicurezza. Ignorare gli aggiornamenti lascia i sistemi esposti a rischi significativi.

- **Politiche rigorose per password sicure**: Le password deboli sono un vettore di attacco comune. Si raccomanda di implementare politiche di sicurezza che richiedano agli utenti e agli sviluppatori di creare password complesse, che includano una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali. Inoltre, è consigliabile l'implementazione dell'autenticazione a due fattori (2FA) per aggiungere un ulteriore livello di sicurezza agli account ove possibile.

- **Audit di sicurezza regolari**: Pianificare e condurre regolari audit di sicurezza è essenziale per mantenere e migliorare la postura di sicurezza del sistema. Gli audit dovrebbero includere verifiche periodiche delle configurazioni di sicurezza, test di vulnerabilità, e revisione delle politiche di sicurezza. Questi audit dovrebbero essere eseguiti da un team interno o da un consulente di sicurezza esterno per garantire un'analisi obiettiva e approfondita.

- **Formazione continua e sensibilizzazione**: La sicurezza non è solo una questione di tecnologia, ma anche di comportamento umano. È cruciale che gli utenti e gli sviluppatori ricevano formazione continua sulle migliori pratiche di sicurezza. Programmi di sensibilizzazione sulla sicurezza informatica, simulazioni di phishing, e aggiornamenti regolari sulle nuove minacce possono aiutare a mantenere alta la guardia e a promuovere una cultura della sicurezza all'interno dell'organizzazione.

- **Monitoraggio continuo delle reti**: Implementare soluzioni di monitoraggio continuo delle reti per rilevare attività sospette o anomalie che potrebbero indicare un tentativo di intrusione. Strumenti di rilevamento delle intrusioni (IDS) e

di prevenzione delle intrusioni (IPS) possono essere utilizzati per monitorare e rispondere in tempo reale a potenziali minacce.

- **Backup regolari dei dati**: Assicurarsi che vengano effettuati backup regolari e sicuri dei dati critici. I backup devono essere testati periodicamente per garantirne l'integrità e l'affidabilità. Inoltre, i backup dovrebbero essere conservati in una location sicura e separata dal network principale per prevenire la perdita di dati in caso di attacco.
- **Controllo degli accessi rigoroso**: Implementare un sistema di controllo degli accessi basato sui principi del minimo privilegio e della separazione dei compiti. Solo gli utenti autorizzati dovrebbero avere accesso alle risorse critiche, e tali privilegi dovrebbero essere regolarmente rivisti e aggiornati.

5. Findings Summary

L'attività condotta ha individuato diverse vulnerabilità utilizzando tecniche manuali e automatiche. Di seguito è riportato un sommario di queste vulnerabilità, ciascuna classificata secondo i quattro livelli di gravità definiti dal CVSS v3.0:

- **Basso (Low)**: Vulnerabilità con punteggio da 0.1 a 3.9. Indica un impatto limitato sulla riservatezza, integrità e disponibilità del sistema.
- **Medio (Medium)**: Vulnerabilità con punteggio da 4.0 a 6.9. Rappresenta una minaccia significativa che può causare alcuni danni, ma non catastrofici.
- **Alto (High)**: Vulnerabilità con punteggio da 7.0 a 8.9. Indica un alto rischio di compromissione che può avere gravi conseguenze sul sistema e i dati.
- **Critico (Critical)**: Vulnerabilità con punteggio da 9.0 a 10.0. Rappresenta il livello più alto di rischio con impatti molto gravi, che possono compromettere completamente il sistema.

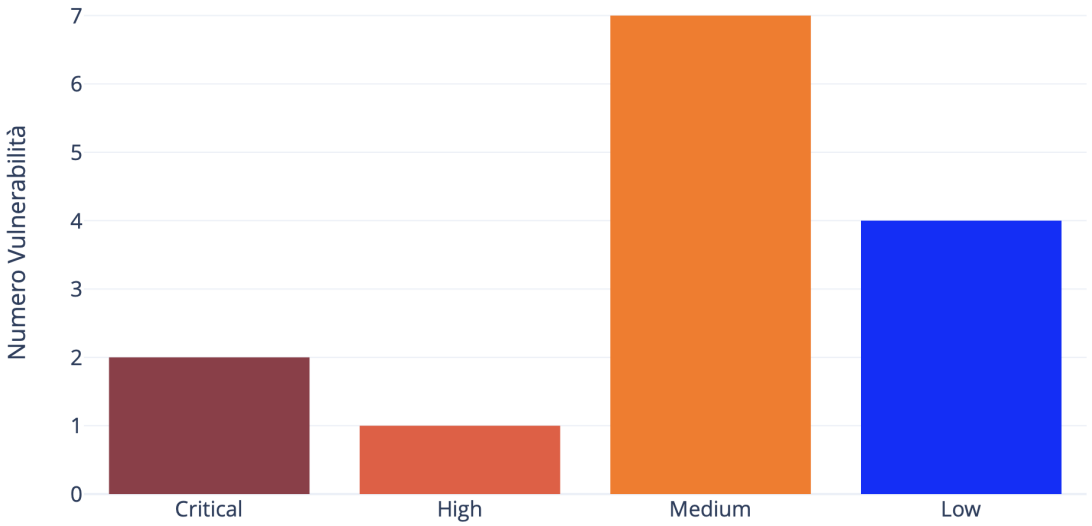

Figura 5.1: Numero di vulnerabilità per gravità

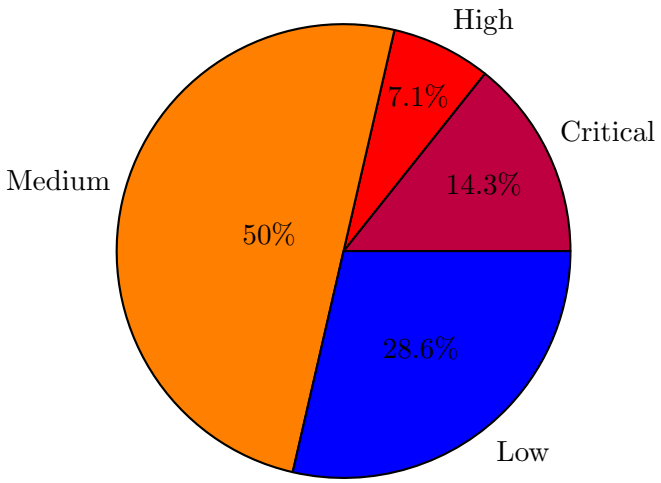

Figura 5.2: Grafico a torta sulle percentuali di vulnerabilità

6. Detailed Summary

6.1 Priorità critica

SN	
Critical (9.8)	
CVE	2023-51467[1]
Descrizione:	La vulnerabilità consente agli aggressori di aggirare i processi di autenticazione, consentendo loro di eseguire in remoto codice arbitrario
Rischi:	Bypass della fase di autenticazione.
Soluzione:	Aggiornare OFBiz ad una versione ancora supportata.
Metodo di detection:	Individuazione manuale.

Tabella 6.1: Dettagli della vulnerabilità sulla CVE-2023-51467

SN	
Critical (9.8)	
CVE	2023-49070[2]
Descrizione:	Pre-auth RCE in Apache Ofbiz versione 18.12.09. È dovuto all'XML-RPC non più mantenuto ancora presente. Questo problema riguarda Apache OFBiz: prima del 18.12.10.
Rischi:	Bypass dell'autenticazione e Remote code execution
Soluzione:	Aggiornare OFBiz alla versione 18.12.10
Metodo di detection:	Individuazione manuale.

Tabella 6.2: Dettagli della vulnerabilità sulla CVE-2023-49070

6.2 Priorità alta

CGI Generic SQL Injection (blind)	
High (8.3)	
CVE	-
Descrizione:	Inviando parametri appositamente realizzati a uno o più script CGI ospitati sul server web remoto, Nessus è stato in grado di ottenere una risposta molto diversa, il che suggerisce che potrebbe essere stato in grado di modificare il comportamento dell'applicazione e accedere direttamente al database sottostante.
Rischi:	Il web server remoto è potenzialmente soggetto ad attacchi SQL injection.
Soluzione:	Modificare gli script CGI interessati in modo che interpretano correttamente agli argomenti.
Metodo di detection:	Individuazione tramite analisi automatica con Nessus.

Tabella 6.3: Dettagli della vulnerabilità CGI Generic SQL Injection (blind)

6.3 Priorità media

SSL Certificate Cannot Be Trusted	
Medium (6.5)	
CVE	-
Descrizione:	Il certificato X.509 del server non può essere considerato attendibile per tre motivi: il vertice della catena di certificati non discende da un'autorità pubblica conosciuta, un certificato della catena non è valido al momento della scansione, o una firma nella catena non è verificabile.
Rischi:	Rende difficile per gli utenti verificare l'autenticità del server, facilitando possibili attacchi man-in-the-middle.
Soluzione:	Acquista o genera un certificato SSL adeguato per questo servizio.
Metodo di detection:	Individuazione tramite analisi automatica con Nessus.

Tabella 6.4: Dettagli della vulnerabilità SSL Certificate Cannot Be Trusted

SSL Self-Signed Certificate	
Medium (6.5)	
CVE	-
Descrizione:	La catena di certificati X.509 di questo servizio non è firmata da un'autorità di certificazione riconosciuta. Se l'host remoto è pubblico e in produzione, questo compromette la sicurezza SSL, permettendo potenziali attacchi man-in-the-middle
Rischi:	Possibili attacchi man-in-the-middle.
Soluzione:	Acquista o genera un certificato SSL adeguato per questo servizio.
Metodo di detection:	Individuazione tramite analisi automatica con Nessus.

Tabella 6.5: Dettagli della vulnerabilità SSL Self-Signed Certificate

TLS Version 1.0 Protocol Detection	
Medium (6.5)	
CVE	2011-3389[3], 2015-0204[4]
Descrizione:	Il servizio remoto accetta connessioni criptate usando TLS 1.0, che presenta diversi difetti di progettazione crittografica. Le versioni moderne di TLS 1.0 mitigano questi problemi, ma le versioni più recenti come TLS 1.2 e 1.3 sono progettate per evitare questi difetti e dovrebbero essere usate quando possibile..
Rischi:	La compromissione della crittografia utilizzata da TLS 1.0 dovuta a difetti di progettazione può indurre attacchi per decrittare o manipolare il traffico
Soluzione:	Abilita il supporto per TLS 1.2 e 1.3 e disabilita il supporto per TLS 1.0.
Metodo di detection:	Individuazione tramite analisi automatica con Nessus e OpenVas.

Tabella 6.6: Dettagli della vulnerabilità TLS Version 1.0 Protocol Detection

TLS Version 1.1 Deprecated Protocol	
Medium (6.5)	
CVE	2011-3389[3], 2015-0204[4]
Descrizione:	Il servizio remoto accetta connessioni criptate usando TLS 1.1. TLS 1.1 non supporta le suite di cifratura attuali e raccomandate. Le cifrature che supportano la crittografia prima del calcolo del MAC e le modalità di crittografia autenticata come GCM non possono essere utilizzate con TLS 1.1.
Rischi:	La compromissione della crittografia utilizzata da TLS 1.0 dovuta a difetti di progettazione può indurre attacchi per decrittare o manipolare il traffico
Soluzione:	Abilita il supporto per TLS 1.2 e 1.3 e disabilita il supporto per TLS 1.0.
Metodo di detection:	Individuazione tramite analisi automatica con Nessus e OpenVas.

Tabella 6.7: Dettagli della vulnerabilità TLS Version 1.1 Deprecated Protocol

JQuery 1.2 < 3.5.0 Multiple XSS	
Medium (6.1)	
CVE	-
Descrizione:	Secondo la versione segnalata nello script, la versione di JQuery ospitata sul server Web remoto è maggiore o uguale a 1.2 e precedente a 3.5.0.
Rischi:	Vulnerabile a cross site scripting.
Soluzione:	Aggiornare JQuery ad una versione più recente
Metodo di detection:	Individuazione tramite analisi automatica con Nessus.

Tabella 6.8: Dettagli della vulnerabilità JQuery 1.2 < 3.5.0 Multiple XSS

SSL/TLS Protocol Initialization Vector Implementation ...(BEAST)	
Medium (5.3)	
CVE	-
Descrizione:	Potrebbe essere possibile ottenere informazioni sensibili dall'host remoto che utilizza servizi abilitati SSL/TLS. Questo può avvenire sfruttando vulnerabilità o configurazioni deboli nei protocolli SSL/TLS, permettendo agli attaccanti di intercettare, decrittare o manipolare i dati trasmessi.
Rischi:	Fuga di informazioni sensibili.
Soluzione:	Configurare i server SSL/TLS per utilizzare solo TLS 1.1 o TLS 1.2 se supportati. Configurare i server SSL/TLS per supportare solo le suite di crittografia che non utilizzano cifrari a blocchi. Applicare le patch se disponibili.
Metodo di detection:	Individuazione tramite analisi automatica con Nessus.

Tabella 6.9: Dettagli della vulnerabilità SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)

Web Application Potentially Vulnerable to Clickjacking	
Medium (4.3)	
CVE	-
Descrizione:	Il server web remoto non imposta l'intestazione di risposta X-Frame-Options né l'intestazione di risposta Content-Security-Policy con la direttiva 'frame-ancestors' in tutte le risposte ai contenuti.
Rischi:	Questo potenzialmente espone il sito a attacchi di clickjacking o UI redress, in cui un attaccante può ingannare un utente affinché clicchi su una parte della pagina vulnerabile diversa da quella percepita dall'utente. Ciò può portare l'utente a compiere transazioni fraudolente o dannose.
Soluzione:	Restituire l'header HTTP X-Content-Type-Options.
Metodo di detection:	Individuazione tramite analisi automatica con Nessus e Nikto.

Tabella 6.10: Dettagli della vulnerabilità Web Application Potentially Vulnerable to Clickjacking

6.4 Priorità bassa

ICMP Timestamp Reply Information Disclosure	
Low (2.1)	
CVE	-
Descrizione:	L'host remoto risponde a richieste di timestamp ICMP.
Rischi:	Ciò consente a un utente malintenzionato di conoscere la data impostata sulla macchina di destinazione, il che può aiutare un utente malintenzionato remoto non autenticato ad attaccare i protocolli di autenticazione basati sul tempo.
Soluzione:	Non rispondere a richieste timestamp ICMP
Metodo di detection:	Individuazione tramite analisi automatica con Nessus e OpenVas.

Tabella 6.11: Dettagli della vulnerabilità "ICMP Timestamp Reply Information Disclosure"

TCP Timestamps Information Disclosure	
Low (2.6)	
CVE	-
Descrizione:	L'host remoto risponde a richieste di timestamp TCP.
Rischi:	Ciò consente a un utente malintenzionato di conoscere la data impostata sulla macchina di destinazione, il che può aiutare un utente malintenzionato remoto non autenticato ad attaccare i protocolli di autenticazione basati sul tempo.
Soluzione:	Non rispondere a richieste timestamp TCP
Metodo di detection:	Individuazione tramite analisi automatica con Nessus e OpenVas.

Tabella 6.12: Dettagli della vulnerabilità "TCP Timestamps Information Disclosure"

Weak MAC Algorithm(s) Supported (SSH)	
Low (2.6)	
CVE	1999-0524[5]
Descrizione:	Il server SSH remoto è autorizzato a consentire/supportare algoritmi MAC deboli.
Rischi:	Ciò potrebbe consentire a un aggressore di compromettere l'integrità e l'autenticità dei dati scambiati tramite SSH, mettendo a rischio la confidenzialità delle informazioni e la sicurezza del sistema permettedo accessi non autorizzati.
Soluzione:	Disabilitare gli algoritmi MAC deboli.
Metodo di detection:	Individuazione tramite analisi automatica con OpenVas.

Tabella 6.13: Dettagli della vulnerabilità "ICMP Timestamp Request Remote Date Disclosure"

Password non conformi agli standard di sicurezza	
Low	
CVE	-
Descrizione:	La password utilizzata dall'amministratore è composta da semplici parole di senso compiuto, prive di numeri e caratteri speciali.
Rischi:	Un attaccante potrebbe usare tecniche di password cracking per scoprire la password degli amministratori. Ad esempio con un attacco basato su dizionario, opportunamente configurato, un attaccante riuscirebbe facilmente ad ottenere la password di amministratore.
Soluzione:	Istruire il personale sull'importanza di utilizzare password complesse, aggiungere controlli lato software per obbligare l'utilizzo di password conformi agli standard.
Metodo di detection:	Individuazione tramite analisi manuale.

Tabella 6.14: Dettagli della vulnerabilità "Password non conformi agli standard di sicurezza"

6.5 Appendix

Tali vulnerabilità sono tutte sfruttabili come dimostrato e illustrato passo per passo all'interno del documento di Penetration Testing Narrative.

Riferimenti

[1] NIST. *CVE-2023-51467*. 2023. URL: https://nvd.nist.gov/vuln/detail/CVE-2023-51467.

[2] NIST. *CVE-2023-49070*. 2023. URL: https://nvd.nist.gov/vuln/detail/CVE-2023-49070.

[3] NIST. *CVE-2011-3389*. 2011. URL: https://nvd.nist.gov/vuln/detail/cve-2011-3389.

[4] NIST. *CVE-2015-0204*. 2015. URL: https://nvd.nist.gov/vuln/detail/cve-2015-0204.

[5] NIST. *CVE-1999-0524*. 1999. URL: https://nvd.nist.gov/vuln/detail/CVE-1999-0524.

Elenco delle figure

Elenco delle tabelle