







#	Vulnérabilité	Type	CVSS	Criticité	Localisation	Preuve d'Exploitation
1	Command Injection	Web App	9.8	 <b>CRITICAL</b>	Port 80, paramètre <code>command</code>	<code>curl -X POST -d "command=127.0.0.1; id"</code> → RCE
2	Exposed SSH Private Key	FTP	9.8	 <b>CRITICAL</b>	<code>/alice/files/id_rsa</code> via FTP	Connexion SSH réussie avec clé
3	Hard-coded DB Credentials	Source Code	9.2	 <b>CRITICAL</b>	<code>/opt/evil-web-app/index.js:31-35</code>	<code>jedha:mkiFDUAWqVbSFFk23nK</code>
4	Supervisord No Auth	Service	9.3	 <b>CRITICAL</b>	Unix HTTP server	"running without authentication"
5	FTP Anonymous Access	Network	7.5	 <b>HIGH</b>	Port 21 vsftpd	<code>ftp anonymous</code> → accès libre
6	Sudo Privilege Escalation	System	8.8	 <b>HIGH</b>	<code>sudo /usr/bin/tee -a *</code>	<code>echo "alice ALL=ALL"   sudo tee</code>
7	SUID Binary Exploitation	System	8.8	 <b>HIGH</b>	<code>/home/bob/find</code>	<code>find . -exec /bin/sh \;</code>
8	SQL Injection Login	Web App	8.2	 <b>HIGH</b>	Login Evil CORP	<code>admin' OR '1'='1' --</code> → error
9	Hard-coded Admin Creds	Multiple	7.8	 <b>HIGH</b>	Code + secret page	<code>evil:VeryStr0ngP4ssw0rd</code>
10	MySQL Root No Password	Database	8.4	 <b>HIGH</b>	MySQL server	<code>mysql -u root</code> → accès direct
11	Weak SSH Configuration	Network	7.2	 <b>HIGH</b>	<code>/etc/ssh/sshd_config</code>	PasswordAuth activé
12	Insecure Cron Jobs	System	7.8	 <b>HIGH</b>	<code>/etc/crontab</code>	Backup auto + reset sudoers
13	Stored XSS Reviews	Web App	6.1	 <b>MEDIUM</b>	Formulaire Evil CORP	<code>&lt;script&gt;alert(1)&lt;/script&gt;</code>
14	SSH Host Keys Exposed	System	6.8	 <b>MEDIUM</b>	<code>/etc/ssh/ssh_host_*_key</code>	Fichiers accessibles root
15	Backup Files Weak Perms	System	6.5	 <b>MEDIUM</b>	<code>/usr/share/*.bak</code>	Fichiers 644 permissions

#	Vulnérabilité	Type	CVSS	Criticité	Localisation	Preuve d'Exploitation
16	Command Injection Logs	Logs	6.2	 MEDIUM	<code>/var/log/jedha-ping-*.log</code>	Historique injections visible
17	SSH X11 Forwarding	Network	5.1	 MEDIUM	<code>X11Forwarding yes</code>	Configuration active
18	User Backup Archive	System	5.8	 MEDIUM	<code>/home-john-backup.tgz</code>	Archive auto créée


## STATISTIQUES FINALES

Criticité	Nombre	Pourcentage	CVSS Moyen
 CRITICAL	4	22%	9.5
 HIGH	8	44%	7.9
 MEDIUM	6	33%	6.1
TOTAL	18	100%	7.6

## CHAÎNE D'ATTAQUE OPTIMALE

Étape	Vulnérabilité	Action	Résultat
1	FTP Anonymous (#5)	<code>ftp anonymous</code>	Accès fichiers
2	SSH Private Key (#2)	Download <code>id_rsa</code>	Clé SSH récupérée
3	SSH Access	<code>ssh -i id_rsa alice@target</code>	Shell alice
4	Sudo Escalation (#6)	<code>sudo tee -a /etc/sudoers</code>	Privilèges root
5	Command Injection (#1)	Via PINGOZAURUS	Contrôle web app
6	Database Access (#3)	Credentials hard-codés	Accès MySQL complet

## RÉSUMÉ EXÉCUTIF

- Objectif initial : 9 vulnérabilités
- Résultat obtenu : 18 vulnérabilités validées
- Taux de réussite : 200% 
- Impact global : Compromission totale du système
- Temps de compromission : < 30 minutes