|  |  |
| --- | --- |
| Describe | Vulnerability |
| Services | 21,80 |
| Port | FTP, HTTP |
| Versions | 4.4.0 |
| Severity | high |
| Cve id | 2016-5195 |
| Cvss score | 9/10 |
| Remediations | 1. Command Injection Vulnerability in busque.php:  Vulnerability: The busque.php script accepts user input via the buscar parameter without proper validation, allowing attackers to execute arbitrary system commands.  Remediation:  Input Validation: Implement strict input validation to ensure only expected data is processed. Reject or sanitize any input that deviates from the expected format.  Use Parameterized Queries: When interacting with the system or databases, use parameterized queries or prepared statements to prevent injection attacks.  Least Privilege Principle: Run web applications with the minimum necessary privileges to limit the potential impact of a successful attack.  2. Exposure of Sensitive Information in Backup Files:  Vulnerability: A .backup file containing sensitive information, such as database credentials, is stored in a web-accessible directory, allowing unauthorized users to retrieve it.  Remediation:  Secure Backup Storage: Store backup files outside of the web root directory to prevent direct web access.  Access Controls: Implement proper access controls to restrict access to sensitive files and directories.  Regular Audits: Conduct periodic audits to identify and remove or secure any sensitive files inadvertently placed in public directories.  3. Use of Default or Reused Credentials:  Vulnerability: The application uses default or easily guessable credentials (username: jangow01, password: abygurl69), facilitating unauthorized access.  Remediation:  Enforce Strong Password Policies: Require users to create complex passwords that include a mix of uppercase and lowercase letters, numbers, and special characters.  Unique Credentials: Ensure that default credentials are changed upon deployment and avoid credential reuse across different systems.  Multi-Factor Authentication (MFA): Implement MFA to add an additional layer of security beyond just usernames and passwords.  4. Vulnerable Kernel Allowing Privilege Escalation:  Vulnerability: The system runs a kernel version susceptible to known privilege escalation exploits, such as Dirty COW (CVE-2016-5195).  Remediation:  Regular System Updates: Keep the operating system and kernel up to date with the latest security patches to protect against known vulnerabilities.  Vulnerability Scanning: Regularly scan systems for known vulnerabilities and address them promptly.  Access Controls: Limit user privileges to the minimum necessary to perform their tasks, reducing the potential impact of a compromised account. |
| POC | Step 1  First I found our ip in terminal    After getting my ip, I find victim’s ip.    As we see I get victim ip add  After that I do nmap. Nmap can scan networks to identify live hosts, open ports, running services, operating system, and potential vulnerability    Step 2  As we see to ports are open so, lets see the website    Here is a website lets find some clues in it    After gathering some information I found this  I don’t know the meaning of “buscar” I do google for knowing the meaning of ‘buscar’    The meaning of buscar is ‘to look’ lets try to do something there  Step 3    After doing pwd (present working directory) I get the part of website now I try to do collect more information  After gathering some information I found some sensitive information    Now I do copy and save this to my terminal like this      Now I try to more information from website    After entering html I found one more directory .backup    As we see I get one more username and password in website now I save this also like first one    Step 4  After getting 2 of them username and password I didn’t get anything new so I try to login with FTP    I get ftp login with the help of 2ND one    After getting login so first I found the version of jangow    I get the version of jangow 4.4.0 so now I find exploit with the help of Metasploit    From in this exploit I get perfect one    So I mirror the exploit and use in ftp for gaining access  Step 5    For gaining access firsts I login again with FTP and put exploit like this I done    Like this I done  Step 5  After putting exploit in ftp now I try to do gaining root access while login with user then super-user like this I done    After exploiting ./crack I get root access      Like this I get root access of jangow |
| Reference | https://medium.com/@Thecyberphreak/jangow-1-0-1-walkthrough-7ad06ff4ad2f |

CSV :-[..\Jangow01.csv](../Jangow01.csv)