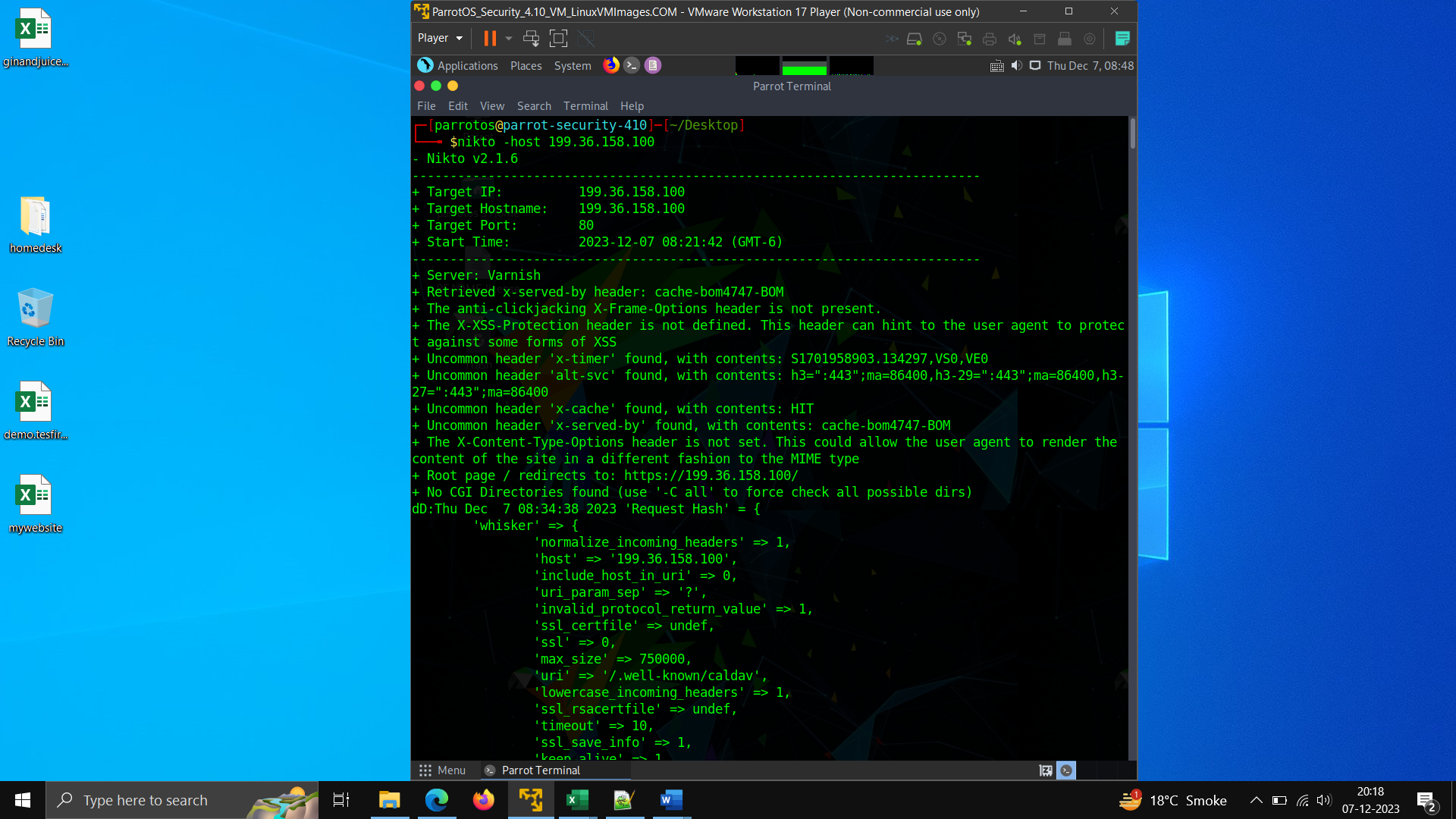
**NIKTO**

**It is used for scanning web vulnerability such as sever information or hidden dir. Access etc.**

**OS USED -PARROT SECURITY**

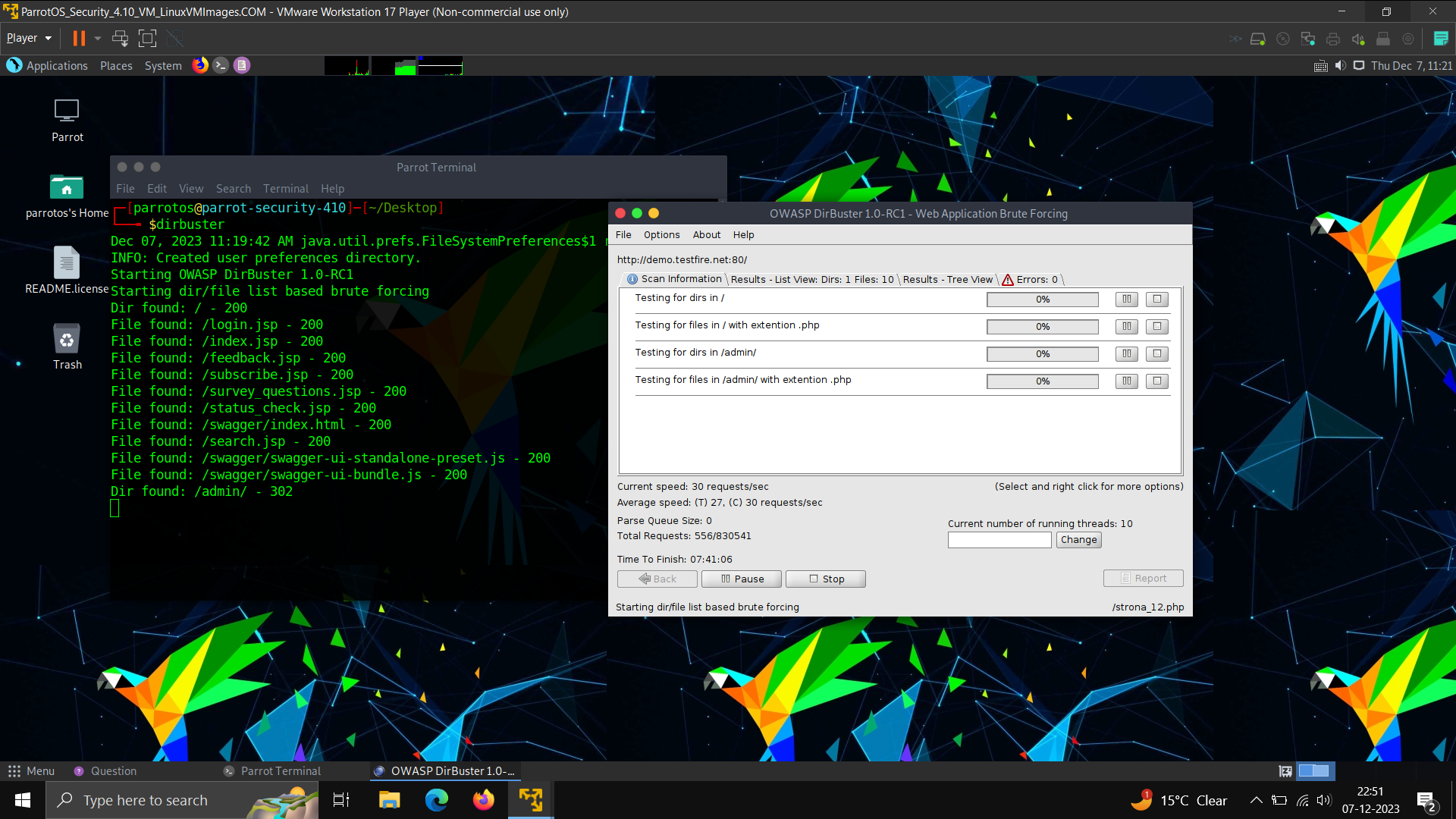
**TARGET IP – 199.36.168.100**

**Command used - NIKTO -host IP address**

**TOTAL VULNERABLITY FOUND -8**

1. **Server name found as Varnish – it can be to exploit the vulnerability in this server**
2. **Anticlicking x-header is not disabled- One** way to protect your web application against clickjacking attacks is to add an anti-clickjacking header to your HTTP responses. If your vulnerability scanner has identified a missing anti-clickjacking header, it means that your website is not currently protected against clickjacking attacks.
3. **The XSS header is not found - The HTTP**X-XSS-Protection**response header is a feature of Internet Explorer, Chrome and Safari that stops pages from loading when they detect reflected cross-site scripting (**[**XSS**](https://developer.mozilla.org/en-US/docs/Glossary/Cross-site_scripting)**) attacks. These protections are largely unnecessary in modern browsers when sites implement a strong**[**Content-Security-Policy**](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy)**that disables the use of inline JavaScript .**
4. **An open redirection vulnerability (open redirect) happens when attackers are able to control where a website or application redirects users. This article shows how bad actors can redirect victims to malicious websites and how you can prevent such vulnerabilities.**
5. **Uncommon header -cache**
6. **uncommon header -xserved-by**
7. Top of Form
8. Bottom of Form

**DIRBUSTER – used for finding all directories/subdomain that can be vulnerable to exploit**



**Ghost\_EYE – used for footprinting like getting information for subdomain, dnslook whoslook – for server duration period and server version ect.**

