sgonçalves

Command Injection - OWASP Multilidae II

1. Para testar esta vulnerabilidade navegue OWASP 2013 > Injection (Other) > Command Injection > DNS Loockup
2. Este é um sistema de DNS Lookup, que consulta as informações de domínios que inserirmos neste campo. Para testar, digite o dominio google.com.br e clique em Loockup DNS.
3. Verifique os dados trazidos pela ferramenta. Mas, onde está a vulnerabilidade? Verifique se você consegue concatenar comandos nesta página. Para concatenar comandos, utilize &.
4. Conseguiu concatenar, correto? Agora, vamos utilizar a criatividade para testar!
5. Teste comandos como:
    a. id
    b. whoami
    c. ls -la
    d. pwd
    e. cat /etc/passwd
    f. cat /etc/shadow
    g. uname -a
    h. ps -ef

6. Bacana! Conseguimos verificar que existe a vulnerabilidade, e também exploramos nosso alvo. Mas, e se pudéssemos fazer tudo isso de forma automática? Nós podemos! Utilizando o commix

7. Todas as informações do commix podemos encontrar em sua documentação oficial, no site: https://tools.kali.org/exploitation-tools/commix

8. Para explorar mais da ferramenta OWASP BWA, vamos acessar a aplicação Damn Vulnerable Web App. Para isso, na home do seu servidor WEB OWASP clique em DVWA.

9. Logue-se com as credenciais: admin admin

10. Navegue até a opção "Command Execution" para explorar a vulnerabilidade

11. Vamos capturar algumas informações importantes desta página utilizando o OWASP ZAP. Precisaremos capturar:

    a. URL

    b. Informações do Cookie como:

        i. Nível de segurança

        ii. PHPSESSID

    c. String POST request

12. Feito isso execute o seguinte comando:

```
sudo commix -u http://<IP-OWASP>/dvwa/vulnerabilities/exec/
--cookie='PHPSESSID=de2ke4i8nu288m075sad4kdn52; security=low'
--data='ip=127.0.0.1&submit=submit'
```

13. Você irá ser questionado do seguinte: Do you want a Pseudo-Terminal shell? Responda com yes. Temos acesso ao servidor da aplicação! Teste executando todos os comandos executados anteriormente.
14. Podemos unir o ataque XSS a este!
15. **Solução:** Este problema é considerado muito grave. Por conta disso, temos