



CERT-IS Seminar

designed By. 스마일게이트

INDEX

01. Network

- Protocol
- TCP/IP
- Proxy/VPN
- Tor

02. Socket Prog.

- Server/Client
- Proxy/Tor
- Custom Protocol

03. Web Basic

- APM
- HTTP / Parsing
- Session
- Login Page - 설명

04. Hack 4 Newbie

- OWASP 10
- XSS / CSRF
- SQL injection

0x03

Web Basic

```
root@sakuya-Izayoi:/home/sakuya# apt-get install php apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
php is already the newest version (1:7.2+60ubuntu1).
apache2 is already the newest version (2.4.29-1ubuntu4.11).
0 upgraded, 0 newly installed, 0 to remove and 71 not upgraded.
```

apt-get install php apache2 libapache2-mod-php

03 HTTP

APM

vi /var/www/html/index.php

rm /var/www/html/index.ht*

브라우저 켜고 IP입력

URL 맨뒤에 /?user=이름 입력

```
<?php
    echo "HELLO! {"$_GET['user']}!";
?>
```

← → ↻ 🌐 192.168.0.4/?user=sakuya

HELLO! sakuya!

변수앞에 무조건 \$ 붙여야함

php 파일로 동작하게 하고 싶으면
<?php 로 시작해야함.

문자열끼리 붙이고 싶을땐 .을 사용함

이외에는 C와 비슷함

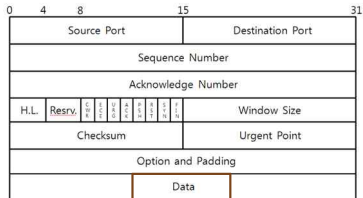
```
<?php
    $age = 0x20;
    $name = "SomeOne";
    print($age.$name."\n");
?>
```

HTTP도 프로토콜의 일종

Hyper Text Transfer Protocol

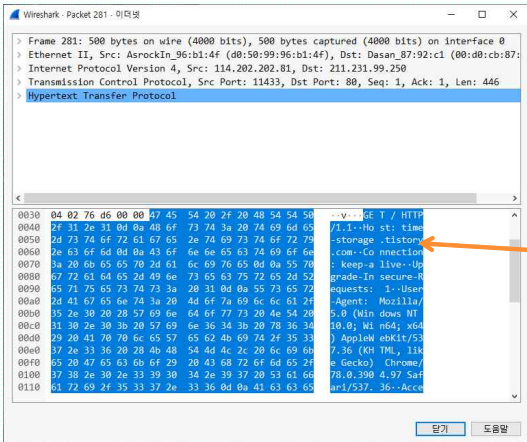
TCP의 Data 부분에서 확인가능함.

[TCP 전송 프레임 구조 특성]

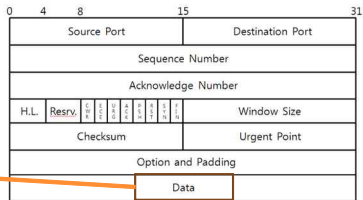


[TCP 구조]

03 HTTP



[TCP 전송 프레임 구조 특성]



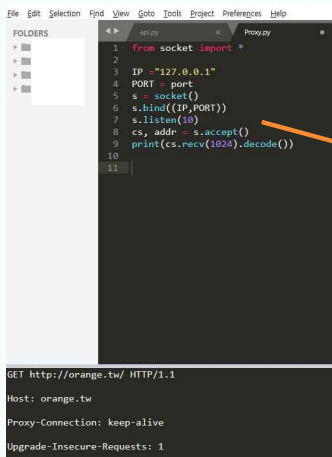
[TCP 구조]

프록시로 직접 확인해보자

```
from socket import *  
  
IP = "127.0.0.1"  
PORT = port  
s = socket()  
s.bind((IP, PORT))  
s.listen(10)  
cs, addr = s.accept()  
print(cs.recv(1024).decode())
```

서버 프로그램 코드와 차이없음

프록시로 직접 확인해보자

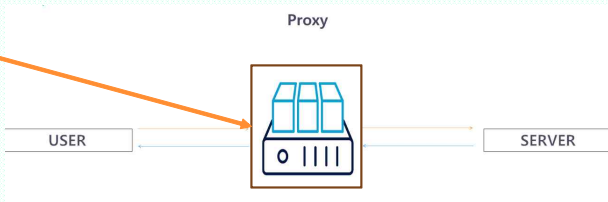


The screenshot shows a code editor with a file named `Proxy.py` containing the following Python code:

```
1 from socket import *
2
3 IP = "127.0.0.1"
4 PORT = port
5 s = socket()
6 s.bind((IP,PORT))
7 s.listen(10)
8 cs, addr = s.accept()
9 print(cs.recv(1024).decode())
10
11
```

Below the code editor, a terminal window displays the output of the script:

```
GET http://orange.tw/ HTTP/1.1
Host: orange.tw
Proxy-Connection: keep-alive
Upgrade-Insecure-Requests: 1
```



이 짓을 매일 할수 없다

Fiddler 검색 -> 설치

이외에도 paros, burp suite 등이 있음

Telerik Fiddler

The free web debugging proxy
for any browser, system or platform

Download now

03 HTTP

HTTP / Parsing

Progress Telerik Fiddler Web Debugger

File Edit Rules Tools View Help

WinConfig Replay X Go Stream Decode

Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff MSDN Search...

Statistics Inspectors AutoResponder Composer FiddlerOrchestra Beta FiddlerScript Log Filters Timeline

Headers TextView SyntaxView WebForms HexView Auth Cookies Raw JSON XML

| # | Result | Protocol | Host | URL |
|---|--------|----------|------------------|--------------------------|
| 1 | 200 | HTTPS | www.fiddler2.com | /UpdateCheck.aspx?ts=... |
| 2 | 200 | HTTP | orange.tw | / |

주요받은놈들

보낸 데이터

Find... (press Ctrl+Enter to highlight all)

View in Notepad

Transformer Headers TextView SyntaxView ImageView HexView Webview Auth Caching Cookies Raw JSON XML

HTTP/1.1 200 OK
Date: Sat, 16 Nov 2019 01:50:26 GMT
Server: Apache/2.4.7
X-Powered-By: PHP/5.6.9-1ubuntu4.27
Content-Length: 24
Keep-Alive: Timeout=5, Max=100
Connection: Keep-Alive
Content-Type: text/plain
114.202.202.81
Korea, Republic of

받은 데이터

보낼/받을 데이터 수정하기

프록시 끄기/켜기(F12)

Capturing All Processes 12 http://orange.tw/

```
GET http://orange.tw/?a=1 HTTP/1.1  
Host: orange.tw  
Cookie : Chocochip=1
```

요청방법(메소드)

서버에 변수 전달방법

GET: URL로 넘김

POST: HTTP 의 Body를 사용하여 넘김

```
GET http://orange.tw/?a=1 HTTP/1.1  
Host: orange.tw  
Cookie : Chocochip=1
```

`https://test.com/?a=b&c=d&e=f..`

요청하는 파일 / GET 변수

해당 경로에 있는 파일을 요청하며,
GET 방식으로 인자를 전달 할 수 있다.

```
char *a = "b";  
char *c = "d";  
char *e = "f";
```

?를 기준으로 앞부분은 파일 / 뒷부분은 변수
변수끼리 구분은 &로 한다

POST http://orange.tw/ HTTP/1.1

Host: orange.tw

Cookie : Chocochip=1

Content-Length:21

id=sakuya&pass=sakuya

요청방법(메소드)

POST: HTTP 의 Body를 사용하여 넘김

GET http://orange.tw/?id=sakuya&pw=sakuya

Host: orange.tw

Cookie : Chocochip=1

```
POST http://orange.tw/ HTTP/1.1
Host: orange.tw
Cookie : Chocochip=1
Content-Length:21

id=sakuya&pass=sakuya
```

요청방법(메소드)
GET : 4096자 언저리 까지 가능
POST: 제한없음

```
GET http://orange.tw/?id=sakuya&pw=sakuya
Host: orange.tw
Cookie : Chocochip=1
```


Session은 간단히 말하면 '연결된 상태'

TCP는 연결을 지향하는 프로토콜이고
UDP는 연결을 지향하지 않는 프로토콜임.
강 설계를 그렇게 했음

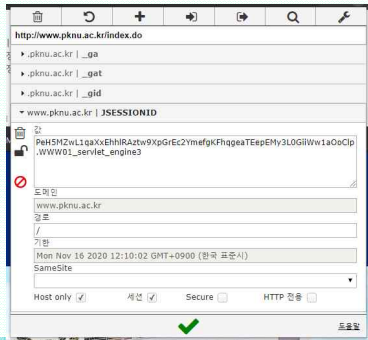
ip.addr == 175.117.252.187 && tcp.port == 4444

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|----------|-----------------|-----------------|----------|--------|--|
| 1994 | 2.097953 | 58.120.61.71 | 175.117.252.187 | TCP | 66 | 8554 → 4444 [SYN] Seq=0 Win=64240 Len=... |
| 1995 | 2.098680 | 175.117.252.187 | 58.120.61.71 | TCP | 66 | 4444 → 8554 [SYN, ACK] Seq=0 Ack=1 Win=... |
| 1996 | 2.098742 | 58.120.61.71 | 175.117.252.187 | TCP | 54 | 8554 → 4444 [ACK] Seq=1 Ack=1 Win=2102... |
| 1997 | 2.098802 | 58.120.61.71 | 175.117.252.187 | RTSP | 66 | Continuation |
| 1998 | 2.099293 | 175.117.252.187 | 58.120.61.71 | TCP | 60 | 4444 → 8554 [ACK] Seq=1 Ack=13 Win=642... |
| 1999 | 2.099480 | 58.120.61.71 | 175.117.252.187 | TCP | 54 | 8554 → 4444 [FIN, ACK] Seq=13 Ack=1 Wi... |
| 2000 | 2.104283 | 175.117.252.187 | 58.120.61.71 | TCP | 60 | 4444 → 8554 [FIN, ACK] Seq=1 Ack=14 Wi... |
| 2001 | 2.104396 | 58.120.61.71 | 175.117.252.187 | TCP | 54 | 8554 → 4444 [ACK] Seq=14 Ack=2 Win=210... |

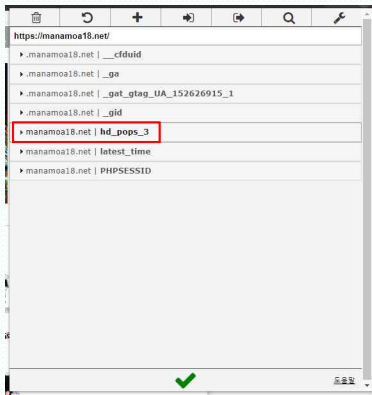
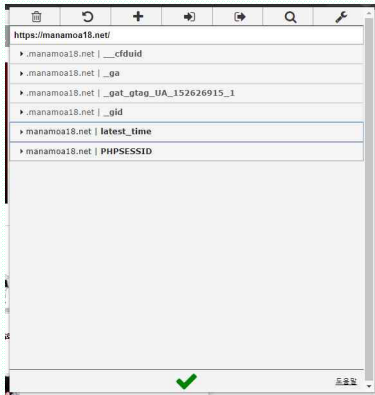
3 hand- shake

근데 HTTP는 TCP위에서 동작함(연결지향)
희안하게 HTTP는 한번 정보를 보내면 그걸로 끝임. 연결 끊음

연결은 하는데 연결을 지속시키지 않음(세션이 없음)
이걸 해결하고자 나온게 '쿠키'



이 쿠키값을 받아서 서버에서 유저별로 서비스를 제공가능



쿠키값을 세팅해주기 위해선 setcookie 함수를 사용함(PHP)

```
<?php
$value = 'something from somewhere';

setcookie("TestCookie", $value);
setcookie("TestCookie", $value, time()+3600); /* expire in 1 hour */
setcookie("TestCookie", $value, time()+3600, "/~rasmus/", "example.com", 1);
?>
```

로그인 페이지를 구현하는 방법

1. 유저 정보를 파일로 저장하고 그것을 읽어와 비교
2. php 스크립트 내에 문자열로 때려박기(하드코딩)
3. DB 서버와 연동하여 비교하기

이후 세션 (쿠키) 만들기

가 과제입니다 ^^

1,2번 중 하나를 선택해서 만들어 오시면 됩니다.

1. 담당조교에게 개인메세지
2. 파일 업로드 후 댓글에 !report 입력



02

Socket Programming

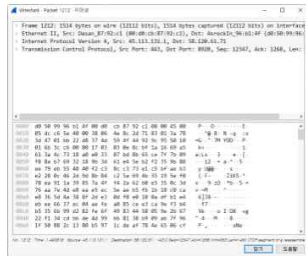
Report

1. 담당조교에게 개인메세지
2. 파일 업로드 후 닷글에 !report 입력
3. 업로드가 성공하면 제출완료라고 알려줌.



Sakuya 오늘 오전 1:56

!report



담당조교 보 오늘 오전 1:56

제출이 완료되었습니다.

```

root@e3f7f778d371:/home/discord/report# ls
Sakuya#5626
root@e3f7f778d371:/home/discord/report# find
.
./Sakuya#5626
./Sakuya#5626/report1.png
root@e3f7f778d371:/home/discord/report#

```

Web Basic

End Of Document