# Michał Budnik – Sprawozdanie 5

# 1. Raport

W ramach rozwiązania listy zadań zmodyfikowany został program serwera napisany w Perlu.

## Charakterystyka skryptu

W kodzie należy podać nazwę hosta oraz port serwera. Te informacje są wymagane do połączenia się przez przeglądarkę. Początkowo, po otrzymaniu jakiegokolwiek żądania skrypt znajduje plik ‘index.html’ w katalogu, w którym się aktualnie znajduje. Warto również zauważyć, że w konsoli, w której jest uruchamiany zostaje wyświetlana informacja na tematu adresu, pod którym można się z nim połączyć.

## Nagłówek żądania

Zadanie 4 wymaga modyfikacji serwera (lub napisanie własnego) w taki sposób, aby ten wyświetlał nagłówek żądania, które otrzymuje. Można w ten sposób w łatwy sposób sprawdzić, jakie dane są przekazywane stronom przez przeglądarkę. W celu połączenia się należy w przeglądarce wpisać DESKTOP-PUEBIU8:4321.

Kod 1: Serwer wyświetlający nagłówek żądania. Istotne linijki są zaznaczone niebieskim kolorem

use HTTP::Daemon;

use HTTP::Status;

use IO::File;

my $d = HTTP::Daemon->new(

LocalAddr => 'DESKTOP-PUEBIU8',

LocalPort => 4321,

)|| die;

print "Please contact me at: <URL:", $d->url, ">\n";

while (my $c = $d->accept) {

while (my $r = $c->get\_request) {

$response = HTTP::Response->new(300,'OK');

$response->content($r->as\_string);

$c->send\_response($response);

}

$c->close;

undef($c);

}

Jak w powyższym przykładzie można zauważyć, że użytkownik otrzymuje informacje dotyczące nagłówka swojego żądania „GET”. Poza tym w nagłówku jest obecnych jeszcze kilka informacji – trzecia linia zawiera informację o rodzaju nawiązywanego połączenia (w tym przypadku keep-alive).

Wynik 1: Nagłówek żądania

GET /index.html HTTP/1.1

Cache-Control: max-age=0

Connection: keep-alive

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Encoding: gzip, deflate

Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7

Host: desktop-puebiu8:4321

User-Agent: Chrome/66.0.3359.181

Upgrade-Insecure-Requests: 1

Kolejne 4 linie pokazują co ma być akceptowane przez przeglądarkę:

- treści,   
- standardy kodowania znaków,   
- akceptowane języki (litera q odpowiada preferencjom użytkownika przeglądarki, np. użytkownik preferuje język polski, potem język angielski w wersji US, a następnie inne odmiany języka angielskiego).

Kolejna linia zawiera pełny adres serwera http, a następna wskazuje na program, przy pomocy którego dokonano zapytania.

Ostatnia linia zawiera informację dla serwera oznaczającą, że klient preferuje szyfrowaną i uwierzytelnioną odpowiedź od serwera.

## Prosty serwis WWW

Serwer został rozszerzony o zmienną $WEBDIR, wskazującą na folder, w którym znajdują się pliki serwisu. Zaimplementowana została również zaawansowana obsługa żądań – serwer potrafi odsyłać do odpowiednich podstron.

Do zbadania połączeń z serwisem został wykorzystany program **HTTPWatch** pozwalający na przejrzenie podstawowych informacji dotyczących wysyłanych oraz otrzymywanych pakietów.

Przy sprawdzeniu nagłówka za pomocą takiego sniffera widać te same informacje, które były opisane w poprzednim podpunkcie.

use HTTP::Daemon;

use HTTP::Status;

use IO::File;

$WEBDIR = 'C:\Users\University\Desktop\4th semester\WWW\Projekt 1';

my $d = HTTP::Daemon->new(

LocalAddr => 'DESKTOP-PUEBIU8',

LocalPort => 4321,

)|| die;

print "Please contact me at: <URL:", $d->url, ">\n";

while (my $c = $d->accept) {

while (my $r = $c->get\_request) {

if ($r->method eq 'GET') {

$file\_s = $r->url;

if($file\_s eq "/"){

$file\_s= "./index.html";

}

$c->send\_file\_response($WEBDIR.$file\_s);

}

else {

$c->send\_error(RC\_FORBIDDEN)

}

}

$c->close;

undef($c);

}

Kod 2: Kod serwera serwisu WWW. Dwie najważniejsze linie zostały wyróżnione kolorem niebieskim

2. Wnioski:

Co może nie wydawać się oczywiste, gdy łączymy się z różnymi stronami, to ilość informacji które wymienia nasza przeglądarka. W samym nagłówku żądania serwer może się dowiedzieć o tym z jakiej dokładnie wersji przeglądarki korzystamy czy jakie mamy preferencje językowe (i prawdopodobnie państwo, z którego pochodzimy), a dodatkowe żądanie ‘DNT: 1’, obsługiwane tylko przez niektóre strony, wydaje się czymś co powinno być standardowym zachowaniem w erze masowego gromadzenia informacji. A o wiele więcej informacji można uzyskać np. za pomocą skryptów oraz procederu o nazwie Cross-Site tracking.

Na podstawie tych wszystkich danych wiążą się o wiele większe zagrożenia, np. *fingerprinting.* Na podstawie łatwych do pozyskania metadanych, takich jak szerokość okna w przeglądarce, pasków, akceptowanych języków (i, jak widać, ich wartości liczbowych), dostępnych czcionek i wielu innych czynników, które razem tworzą unikatowy ślad, tworzy się odcisk użytkownika co pozwala na dość jednoznaczną jego identyfikację. Problemem jest to, że nawet ludzie mający do czynienia z technologią na co dzień nie zawsze wiedzą o tym, ile danych jest gromadzonych na ich temat, nie wspominając o reszcie społeczeństwa.