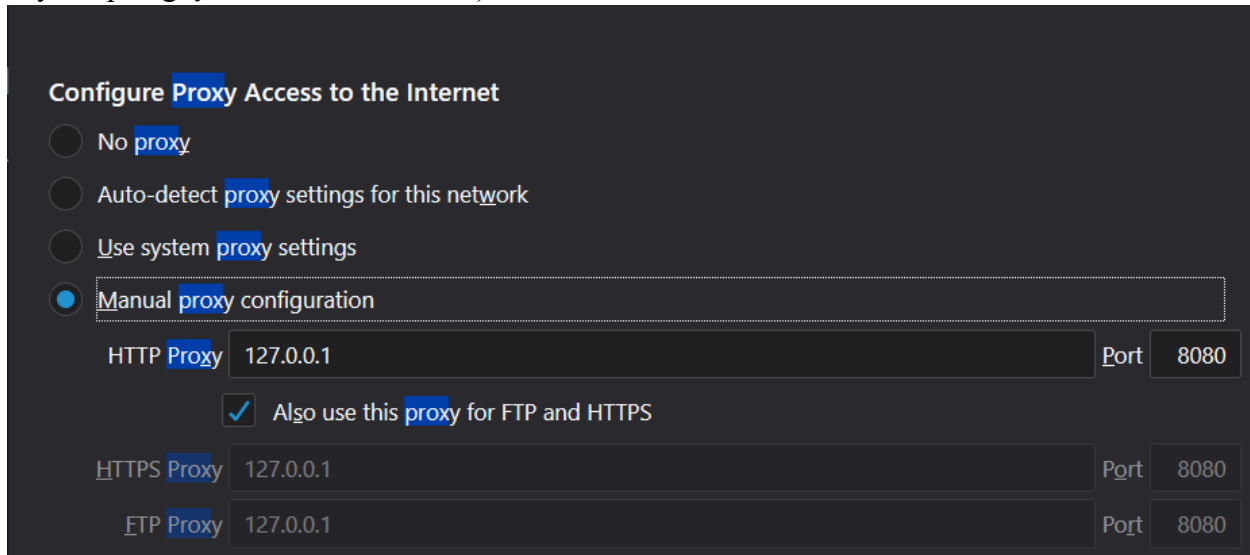


Raport z wykonania zadania 1

Żeby korzystać z Burp'a muszę skonfigurować proxy na swojej przeglądarce (będę używał przeglądarki Mozilla Firefox):



Configure Proxy Access to the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☒ Also use this proxy for FTP and HTTPS

HTTPS Proxy 127.0.0.1 Port 8080

FTP Proxy 127.0.0.1 Port 8080

Dzięki temu mogę przechwytywać wszystkie żądania i je podglądać. W zakładce Proxy -> Intercept mogę włączyć przechwytywanie żądań (intercept on), abym mógł decydować co chcę zrobić (np. zmodyfikować) dla każdego przechwyconego żądania. Na przykład spróbuję skierować żądanie do strony <https://www.ii.uni.wroc.pl/~/> z włączonym interceptem.

Przechwycone żądanie zmodyfikuję:

```
GET /~/ HTTP/1.1
Host: www.ii.uni.wroc.pl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64
Accept: text/html,application/xhtml+xml,application/javascript;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: csrftoken=odyn261Qd3dS9WRDfJlMiYN0muTD1
Upgrade-Insecure-Requests: 1
```

Przed modyfikacją

```
GET /~wzychla/ HTTP/1.1
Host: www.ii.uni.wroc.pl
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: csrftoken=odyn261Qd3dS9WRDfJlMiYN(
Upgrade-Insecure-Requests: 1
```

Po modyfikacji

Zmodyfikowane żądanie wysyłam poprzez przycisk „Forward” nad żądaniem. Otwiera mi się strona Pana Wiktora Zychli, nie strona instytutu informatyki. W zakładce Proxy -> Options mogę zdecydować co chcę zrobić z jakim typem żądań. Poza tym, mogę zmienić ustawienia samej bramki proxy.

Żeby utworzyć żądanie do jakiegoś serwera, mogę użyć zakładki „Repeater”. Spróbuję wysłać żądanie do mojego serwera http o stronę: localhost:8080/example/:

request

```
Pretty Raw \n Actions v
1 GET /example/ HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (Windows NT 10.0;
  Firefox/77.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: text/html
8 Upgrade-Insecure-Requests: 1
9
```

Wysyłam i dostaję odpowiedź:

```
HTTP/1.1 400 Bad Request
Date: Fri, 20 Nov 2020 18:44:48 GMT
Server: Apache/2.4.10 (Debian)
Content-Length: 303
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
```

Czyli serwer odpowiada mi na żądanie (tutaj akurat komunikatem Bad Request).