

Sieci komputerowe - Warsztaty 6 - wyzwanie

Będziemy dodawać nowy wpis na stronie WWW za pomocą **nc**.

Krok 1

Uruchamiamy usługę serwera WWW wyświetlającego prostą stronę do dodawania wpisów używając **systemctl start hydepark**.

```
root@virbian:/home/user# systemctl start hydepark
```

Figure 1: Hyde park

Krok 2

Odpalamy devtools w firefoxie na karcie Network. Wchodzimy na stronę **http://virbian:8080/**. W Devtoolsach możemy podejrzeć komunikację między serwerem a przeglądarką, obejrzeć nagłówki, treść zapytania, odpowiedzi, zaznaczając Raw nawet surowe zapytanie odpowiedź bez parsowania.

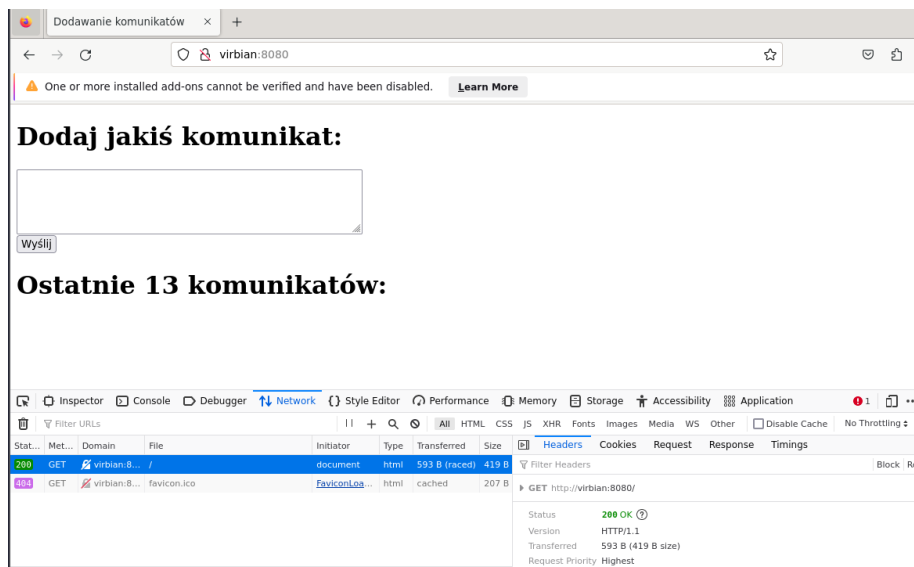
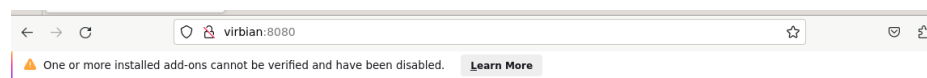


Figure 2: Firefox - devtools

Krok 3

Co się dzieje jak dodaje wpis w formularz na Virbian:8080?

Wysyła się POST do virbian:8080/add z polem content równym mojemu wpisowi. Dostajemy odpowiedź **302 Found**, z polem Location /.



Dodaj jakiś komunikat:

Ostatnie 13 komunikatów:

1. Testowy Komunikat zawierający polskie znaki

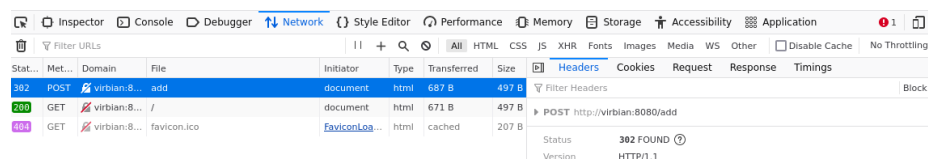


Figure 3: POST

Krok 4

Uruchamiamy program nc w trybie serwera TCP na porcie 8888, używając **nc -l -p 8888 | tee http_request**

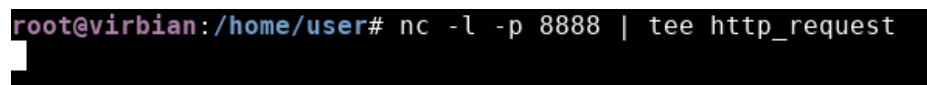


Figure 4: nc

Krok 5

W menu przeglądarki->Settings->Network settings->Connection settings->Manual proxy configuration ustawiamy: - w polu HTTP proxy wartość localhost - w polu Port wartość 8888

The screenshot shows the 'Connection Settings' dialog box with the title 'Configure Proxy Access to the Internet'. There are four radio button options: 'No proxy', 'Auto-detect proxy settings for this network', 'Use system proxy settings', and 'Manual proxy configuration'. The 'Manual proxy configuration' option is selected. Below this, there are three sections: 'HTTP Proxy' with a text field containing 'localhost' and a 'Port' field containing '8888'; 'HTTPS Proxy' with a text field and a 'Port' field containing '0'; and 'SOCKS Host' with a text field and a 'Port' field containing '0'. There is a checkbox 'Also use this proxy for HTTPS' which is unchecked. Below these, there are two radio button options for 'SOCKS': 'SOCKS v4' and 'SOCKS v5', with 'SOCKS v5' selected. At the bottom, there is a radio button option 'Automatic proxy configuration URL' with an empty text field and a 'Reload' button. At the very bottom, there are 'Cancel' and 'OK' buttons.

Figure 5: Zmiana ustawień

Krok 6

Po zaakceptowaniu ustawień wysyłamy na Virbian:8080 znów jakiś wpis.

Rzeczywiście przeglądarka zachowuje się jakby oczekiwała na odpowiedź a wpis nie zostaje dodany.

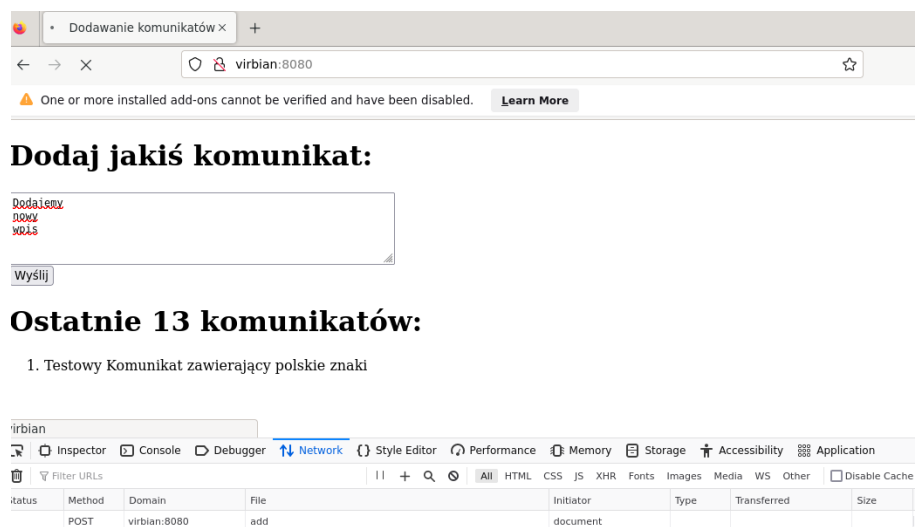


Figure 6: Przeglądarka na oczekiwaniu

Wydaje mi się, że to jest spowodowane tym, że ustawiliśmy proxy w przeglądarce jakko localhost na porcie 8888. A tym proxy jest nasz nasłuchujący serwer TCP poprzez program nc. Przeglądarka oczekuje więc odpowiedzi od serwera TCP a on nie odpowiada.

```
root@virbian:/home/user# nc -l -p 8888 | tee http_request
POST http://virbian:8080/add HTTP/1.1
Host: virbian:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Origin: http://virbian:8080
Connection: keep-alive
Referer: http://virbian:8080/
Upgrade-Insecure-Requests: 1

content=Dodajemy%0D%0Anowy+%0D%0Awpis
```

Figure 7: Podgląd terminala z nc

Krok 7

Przerywamy działanie nc. Widać że automatycznie przeglądarka przestaje czekać na odpowiedź, dostajemy komunikat **The proxy server is refusing connections**.

The proxy server is refusing connections

Firefox is configured to use a proxy server that is refusing connections.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.

Try Again

Figure 8: Przeglądarka po zakończeniu nc

W http_request program nc zapisał oczywiście zapytanie z przeglądarki - POST do add z parametrem content.

```
root@virbian:/home/user# cat http_request
POST http://virbian:8080/add HTTP/1.1
Host: virbian:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Origin: http://virbian:8080
Connection: keep-alive
Referer: http://virbian:8080/
Upgrade-Insecure-Requests: 1
content=Dodajemy%0D%0Anowy+%0D%0Awpisroot@virbian:/home/user#
```

Figure 9: Podgląd http_request

Cofamy ustawienia proxy w przeglądarce.

Krok 8

Wysyłamy zapytanie do serwera WWW poleceniem **nc -q 3 virbian 8080 < http_request**. Odpowiedni komunikat został dodany na stronę.

Krok 9

Modyfikujemy plik `http_request` poprzez zmianę contentu i modyfikację `content-length`.

```
root@virbian:/home/user# cat http_request
POST http://virbian:8080/add HTTP/1.1
Host: virbian:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 61
Origin: http://virbian:8080
Connection: keep-alive
Referer: http://virbian:8080/
Upgrade-Insecure-Requests: 1

content=Dodajemy%0D%0Anowy+%0D%0Awpis a takze go modyfikujemy
```

Figure 10: Zmodyfikowane `http_request`

Wysyłamy na serwer zmieniony `http_request`.

```
root@virbian:/home/user# nc -q 3 virbian 8080 < http_request
HTTP/1.1 302 FOUND
Server: Werkzeug/2.2.2 Python/3.11.2
Date: Tue, 13 May 2025 10:58:36 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 189
Location: /
Connection: close

<!doctype html>
<html lang=en>
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to the target URL: <a href="/">/</a>.
If not, click the link.
```

Figure 11: Odpowiedź po wysłaniu `http_request`

Odpowiedni komunikat znów został dodany na stronę.

Dodaj jakiś komunikat:

A screenshot of a web form. It features a large, empty rectangular text input field. Below the input field, on the left side, is a small button with the text "Wyślij" (Send) in a light blue font. The button has a thin blue border. The input field has a thin blue border and a small blue icon in the bottom right corner.

Ostatnie 13 komunikatów:

1. Dodajemy nowy wpis a także go modyfikujemy
2. Testowy Komunikat zawierający polskie znaki

Figure 12: Przesłany komunikat w przeglądarce

Krok 10

Dezaktywujemy działanie serwera WWW i dezaktywujemy kartę i wyłączamy maszynę.