Индивидуальный проект. Этап 4

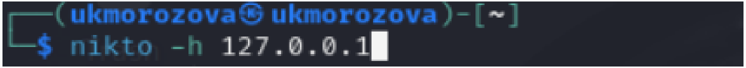
Морозова У.К.

Российский университет дружбы народов, Москва, Россия

Цели и задачи

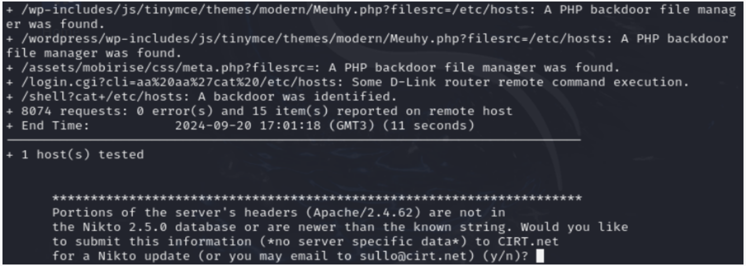
- Использовать nikto для обнаружения уязвимости веб-приложения DVWA.

Запуск nikto



```
┌──(ukmorozova㉿ukmorozova)-[~]
└─$ nikto -h 127.0.0.1
```

Вывод команды



```
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manag
er was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor
file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
+ /shell?cat+/etc/hosts: A backdoor was identified.
+ 8074 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:           2024-09-20 17:01:18 (GMT3) (11 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested


      *********************************************************************
      Portions of the server's headers (Apache/2.4.62) are not in
      the Nikto 2.5.0 database or are newer than the known string. Would you like
      to submit this information (*no server specific data*) to CIRT.net
      for a Nikto update (or you may email to sullo@cirt.net) (y/n)?
```