

Индивидуальный проект

Этап 4. Работа с nikto

Крутова Е. Д.

07 сентября 2024

Российский университет дружбы народов, Москва, Россия

Докладчик

- Крутова Екатерина Дмитриевна
- студентка группы НПИбд-01-21
- Российский университет дружбы народов
- 1032216536@pfur.ru
- <https://edkrutova.github.io/ru/>



Целью данной работы является знакомство с веб-сканером nikto.

nikto — базовый сканер безопасности веб-сервера. Он сканирует и обнаруживает уязвимости в веб-приложениях, обычно вызванные неправильной конфигурацией на самом сервере, файлами, установленными по умолчанию, и небезопасными файлами, а также устаревшими серверными приложениями. На Kali Linux nikto предустановлен.

```
(kali@kali)-[~]
$ nikto -h https://www.rudn.ru/
- Nikto v2.5.0

+ Target IP:      185.178.208.57
+ Target Hostname: www.rudn.ru
+ Target Port:    443

+ SSL Info:      Subject:  /CN=*.rudn.ru
                  Ciphers: TLS_AES_128_GCM_SHA256
                  Issuer:   /C=BE/O=GlobalSign nv-sa/CN=GlobalSign GCC R3 DV TLS CA 2020
+ Start Time:    2024-10-05 15:46:34 (GMT-4)

+ Server: ddos-guard
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie __ddg8_ created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie __ddg8_ created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie __ddg9_ created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie __ddg9_ created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: IP address found in the '__ddg9_' cookie. The IP is "46.242.14.227".
+ /: Cookie __ddg10_ created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie __ddg10_ created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie __ddg1_ created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie XSRF-TOKEN created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie XSRF-TOKEN created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie rudnru_session created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /NsQ6QCTI.gif: Uncommon header 'ddg-cache-status' found, with contents: MISS.
```

Рис. 1: Сканирование сайта РУДН

Я воспользовалась веб-сканером nikto для поиска уязвимостей.