

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки

## **ІНДИВІДУАЛЬНЕ ПІДСУМКОВЕ ЗАВДАННЯ**

**з дисципліни**

**Безпека веб-ресурсів**

**Виконав студент(ка):**

Борщ Дмитро

**Група:**

КБ-01

**Перевірила:**

Лаврик Т.В.

**Суми 2023**

## Результати проведення тестування на проникнення

Ваш цільовий ресурс:

### Частина 1. Збір інформації (розвідка)

1.1 Які утиліти Ви використали для збору інформації про цільовий ресурс та команди?

Утиліта 1. host

Команда	Результат
host bktbntu.com.ua	bktbntu.com.ua has address 185.68.16.103 bktbntu.com.ua has IPv6 address 2a00:7a60:0:1067::1 bktbntu.com.ua mail is handled by 15 mx15.ukraine.com.ua. bktbntu.com.ua mail is handled by 20 mx20.ukraine.com.ua.
host -a bktbntu.com.ua	Trying "bktbntu.com.ua" Using domain server: Name: 8.8.8.8 Address: 8.8.8.8#53 Aliases:  ;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 54715 ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0  ;; QUESTION SECTION: ;bktbntu.com.ua. IN ANY  ;; ANSWER SECTION: bktbntu.com.ua. 900 IN A 185.68.16.103  Received 48 bytes from 8.8.8.8#53 in 60 ms

## Утиліта 2. DMitry

Команда	Результат
dmitry -iwse bktbntu.com.ua	<pre> Deepmagic Information Gathering Tool "There be some deep magic going on"  HostIP:185.68.16.103 HostName:bktbntu.com.ua  Gathered Inet-whois information for 185.68.16.103 -----  inetnum:          185.68.16.0 - 185.68.16.255 netname:          HUPROXY descr:            Hosting Ukraine Proxies country:          UA admin-c:          HU2012-RIPE tech-c:           HU2012-RIPE status:           ASSIGNED PA mnt-by:           HOSTINGUKRAINE-MNT mnt-lower:        HOSTINGUKRAINE-MNT mnt-routes:       HOSTINGUKRAINE-MNT created:          2015-10-29T18:10:49Z last-modified:    2015-10-29T18:10:49Z source:           RIPE  role:             Hosting Ukraine Ltd. Netmaster org:              ORG-HUL6-RIPE address:          Hosting Ukraine LTD address:          PO Box 65 phone:            +380443927433 address:          04112, Kiev, Ukraine admin-c:          IR1628-RIPE abuse-mailbox:    network@abuse.team nic-hdl:          HU2012-RIPE mnt-by:           HOSTINGUKRAINE-MNT created:          2013-04-18T07:53:53Z last-modified:    2018-08-13T08:44:09Z source:           RIPE # Filtered  % Information related to '185.68.16.0/22AS200000'  route:            185.68.16.0/22 descr:            DX-DC network origin:           AS200000 mnt-by:           HOSTINGUKRAINE-MNT created:          2014-09-08T18:25:48Z last-modified:    2014-09-08T18:25:48Z source:           RIPE  % This query was served by the RIPE Database Query Service version 1.106 (SHETLAND)  Gathered Inic-whois information for bktbntu.com.ua -----  domain:           bktbntu.com.ua dom-public:       NO mnt-by:           ua.ukraine nserver:          ns118.inhostedns.com nserver:          ns218.inhostedns.net nserver:          ns318.inhostedns.org status:           ok created:          2014-12-30 14:07:04+02 </pre>

	<pre> modified:      2023-02-14 22:00:40+02 expires:       2023-12-30 14:07:04+02 source:        UAEPP  % Registrar: % % The following disclaimer was provided by the domain name % registrar % ===== % Предоставленная информация является неполной и может содержать % ошиi7wU0к^00u0i70и, % связанные с особенностями механизмов кеширования информации, % несинхронного обновления реестров и т.п., поэтому не является % достов0i7wU0к^00u0i70и, 0рно 0xwUй00xwU 0`0b00 *** stack smashing detected ***: terminated Aborted </pre>
--	---

### Утиліта 3. Recon-NG

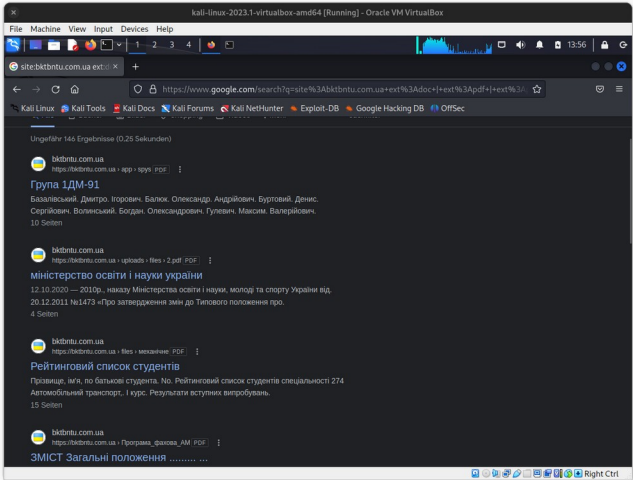
Команда	Результат
recon-ng	<pre> ----- BKTbNTU.COM.UA ----- </pre>
marketplace install hackertarget	<pre> [*] Country: None [*] Host: bktbntu.com.ua [*] Ip_Address: 185.68.16.103 </pre>
modules load recon/domains-hosts/hack ertarget	<pre> [*] Latitude: None [*] Longitude: None [*] Notes: None [*] Region: None </pre>
options set SOURCE bktbntu.com.ua	<pre> [*] ----- [*] Country: None [*] Host: www.bktbntu.com.ua [*] Ip_Address: 185.68.16.103 </pre>
run	<pre> [*] Latitude: None [*] Longitude: None [*] Notes: None [*] Region: None [*] -----  ----- SUMMARY ----- [*] 2 total (2 new) hosts found. </pre>

### Що було виявлено ?

Інформацію від DNS провайдера, на якому зареєстрований домен, про власника сайту, підмережу в якій він знаходиться, а ще те, що існує ще один судбомен, який скоріш за все просто реверсивний проксі на основний.

1.2 Яку інформацію виявлено за допомогою операторів пошуку та запитів із бази GHDB?

Що було виявлено ?

Пошуковий запит	Результат
site:bktbntu.com.ua ext:doc   ext:pdf   ext:ppt	<div></div> <p>Ми змогли знайти велику кількість інформації що зберігається у вигляді документів. Наприклад, як видно на скриншоті, склад якоїсь групи.</p>

**Висновок до частини 1.**

Загалом вдалося дізнатися інформацію про IP адреси хостів та адреси поштових серверів, яку нам надав DNS провайдер. Також інформацію про хостинг провайдера.

Також за допомогою пошукових запитів google було знайдено масу документів. Повний їх аналіз потребує додаткового часу, але з того, що ми бачимо, що списки груп опубліковані у вільному доступі, так само деяка інформація з обмеженим доступом може бути незахищена на даному ресурсі.

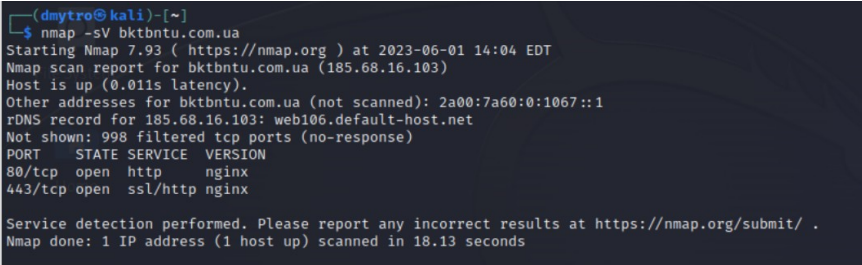
## Частина 2. Сканування

### Сканування портів

2.1 Як утиліту Ви використали для сканування портів цільового ресурсу?

Утиліта 1. nmap

Що було виявлено ?

nmap -sV bktbntu.com.ua	 <pre>(dmytro@kali)~\$ nmap -sV bktbntu.com.ua Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-01 14:04 EDT Nmap scan report for bktbntu.com.ua (185.68.16.103) Host is up (0.011s latency). Other addresses for bktbntu.com.ua (not scanned): 2a00:7a60:0:1067::1 rDNS record for 185.68.16.103: web106.default-host.net Not shown: 998 filtered tcp ports (no-response) PORT      STATE SERVICE VERSION 80/tcp    open  http    nginx 443/tcp    open  ssl/http nginx  Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 18.13 seconds</pre>
	185.68.16.103
	Операційну сисетму встановити не вдалося

Відкритий порт	Сервіс	Програмне забезпечення та його версія
80	HTTPS	nginx
443	HTTPS	nginx

2.2 Які уразливості вже існують для програмного забезпечення, що виявлено на відкритих портах? (Використати відкриті бази даних вразливостей NVD або CVE).

Програмне забезпечення та його версія	Ідентифікатор уразливості	Опис	Рівень критичності (CVSS*)
Nginx	CVE-2009-3898	Уразливість проходження каталогу в src/http/modules/nginx_http_dav_module.c у nginx (так відомий як Engine X) до 0.7.63 та 0.8.x до 0.8.17 дозволяє віддаленим автентифікованим користувачам створювати або перезаписувати довільні файли через .. (крапка крапка) у HTTP-заголовку призначення для методу WebDAV (1) COPY або (2) MOVE.	4.9
Nginx	CVE-2009-3896	src/http/nginx_http_parse.c у nginx (він же Engine X) від 0.1.0 до 0.4.14, 0.5.x до 0.5.38, 0.6.x до 0.6.39, 0.7.x до 0.7.62 та 0.8.x до 0.8.14 дозволяє віддаленим зловмисникам викликати відмову в обслуговуванні (розіменування NULL-вказівника та збій робочого процесу) через довгий URI.	5.0

\*CVSS - Common Vulnerability Scoring System

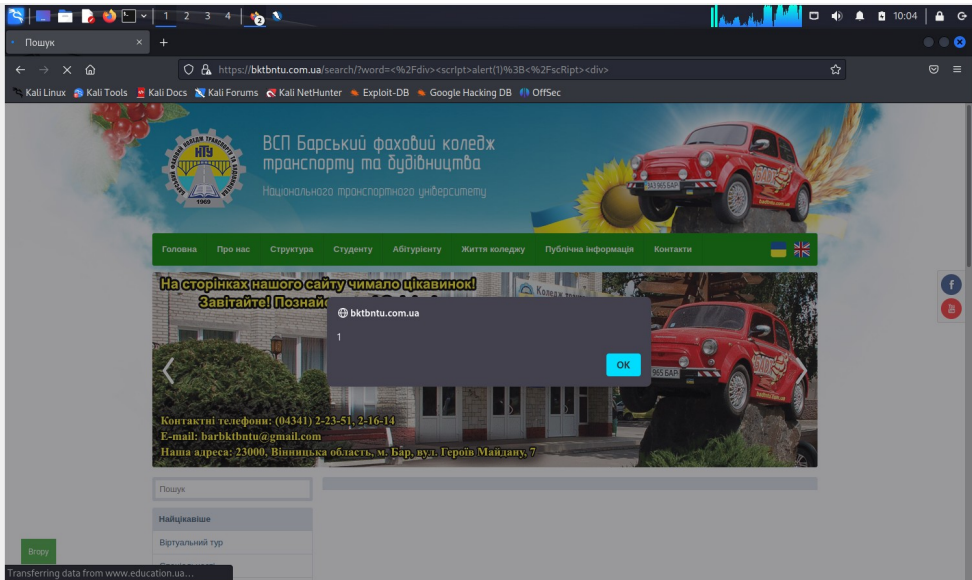


**Сканування вразливостей****2.3 Яку утиліту Ви використали для сканування вразливостей цільового ресурсу?**

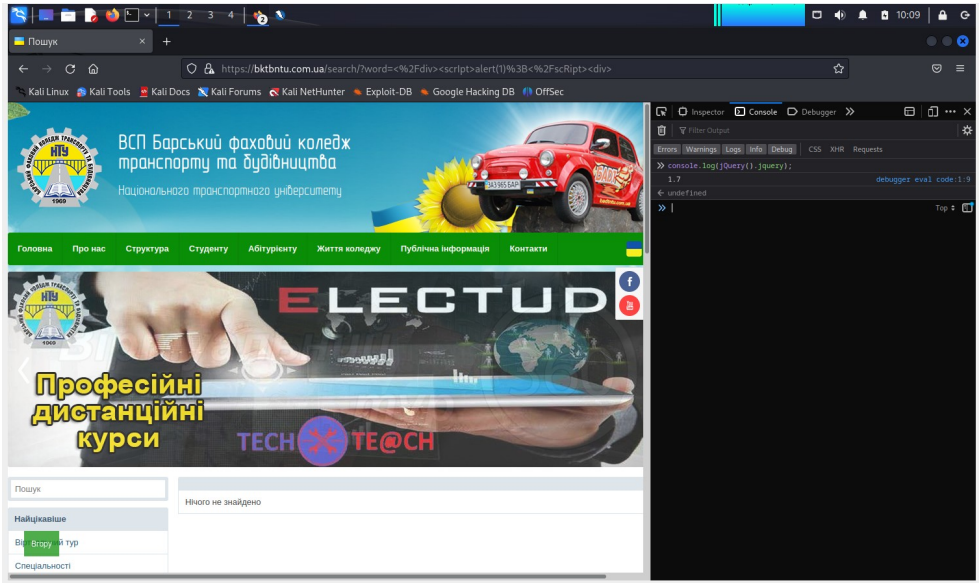
Утиліта 1. OWASP ZAP

*Що було виявлено ?(вказіть як мінімум три виявлені уразливості)*

Уразливість: Cross Site Scripting (Reflected)

Пріоритет	High
URL-адреса	https://bktbntu.com.ua/search/?word=%3C%2Fdiv%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E%3Cdiv%3E
Уразливий параметр	word
Спосіб перевірки	Вбудувати простий JavaScript в пошуковий запит
Скріншот	

## Уразливість: Vulnerable JS Library

Пріоритет	Medium
URL-адреса	<a href="https://bktbntu.com.ua/app/front/js/jquery.js">https://bktbntu.com.ua/app/front/js/jquery.js</a>
Уразливий параметр	
Спосіб перевірки	<p>В консолі розробника перевірити версію активної бібліотеки jQuery. На даний момент актуальна версія jQuery це 3.7.0. Також варто зазначити, що розробники надають спеціальний модуль migrate для того, щоб фактично використовувати нову версію бібліотеки, але не змінюючи при цьому старий код. Навіть такий підхід тут не застосовано.</p>
Скріншот	

## Уразливість: Secure Pages Include Mixed Content

Пріоритет	Low
URL-адреса	https://bktbntu.com.ua/
Уразливий параметр	
Спосіб перевірки	Дослідження вихідного коду сайту
Скріншот	<pre>        &lt;/div&gt;         &lt;div class="copyright"&gt;         &lt;a href="http://www.education.ua" title="Образование в Украине" target="_blank"&gt;&lt;img src="http://www.education.ua/i/logo/education-88x31-ru.gif" width="88" height= "Образование в Украине" border="0"&gt;&lt;/a&gt;</pre>

**Висновок до частини 2.**

Перша вразливість є доволі критичною, бо можна розповсюджувати посилання з вбудованим payload і тим самим виконувати код в браузерах користувачів. Щоб цього уникнути потрібно екранувати пошуковий запит, щоб він не ставав частиною коду веб сторінки.

Друга вразливість не є дуже критичною, оскільки всі CVE пов'язані з нею мають score не більше 4.3 на cvedetails.com. Однак знадобився б ручний аналіз для того, щоб перевірити, чи дійсно ресурс використовує вразливі компоненти jQuery. Щоб убезпечити ресурс потрібно оновити вихідний код до jQuery актуальної версії, або хоча-б використати модуль Migrate.

Третя вразливість не є критичною і пов'язана з тим, що сторінка завантажена за допомогою протоколу https містить контент що завантажується за допомогою http. Така ситуація називається mixed source. Це може свідчити про місконфігурацію ресурсу, але як ми бачимо, джерело контенту на іншому ресурсі, тому ніяк це виправити ми не можемо, окрім як вказати на проблему власнику іншого ресурсу.