Министерство науки и высшего образования Российской Федерации Федеральное государственное бюджетное образовательное учреждение высшего образования «Тульский государственный университет»

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

БАЗОВЫЕ МЕТОДЫ ИССЛЕДОВАНИЯ СТРУКТУРЫ WEB ПРИЛОЖЕНИЙ

отчет о

лабораторной работе №6

по дисциплине ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Выполнила: ст. гр. 230711 Павлова В.С.

Проверил: асс. каф. ИБ Греков М.М.

ЦЕЛЬ РАБОТЫ

Цель: ознакомиться с основными методами анализа структуры WEB приложений, и методами оценки результатов анализа.

ЗАДАНИЕ НА РАБОТУ

- 1. Установить Metasploitable 2 в комплекте с платформой DVWA. Выполнить привязку двух машин (Kali Linux и Metasploitable).
- 2. Зайти через браузер Kali Linux на Metasploitable. Ввести в строку запросов IP-адрес машины, на которую установлен Metasploitable. Выбрать тренировочную площадку DVWA.
- 3. Просканировать площадку DVWA с помощью DirBuster и представить скриншот и отчёт.
- 4. Просканировать DVWA при помощи DirSearch, предоставить скриншот и отчёт.
- 5. Просканировать DVWA в рекурсивном режиме с анализом подкаталогов и предоставить скриншот и отчёт. В качестве дополнительного задания просканировать сайт scanme.org

ХОД РАБОТЫ

1. Привязка Kali и Metasploitable (10.0.2.5) друг к другу (рисунок 1):

S	Metas	ploitak	le [Работает]] - Oracle VM Vi	irtualBox			_		\times
Ф	айл М	ашина	Вид Ввод	д Устройства	Справк	а				
				icmp_seq=31						
				icmp_seq=32						
				icmp_seq=33						
				icmp_seq=34						
				icmp_seq=35						
				icmp_seq=36						
				icmp_seq=37						
				icmp_seq=38						
				icmp_seq=39 icmp_seq=40						
				icmp_seq=40						
				icmp_seq=42						
				icmp_seq=43						
				icmp_seq=13						
				icmp_seq=45						
				icmp_seq=46						
				icmp_seq=47						
				icmp_seq=48						
				icmp seq=49						
				icmp_seq=50						
				icmp_seq=51						
64	bytes	from	10.0.2.6:	icmp_seq=52	ttl=64	time=0.372	ms			
64	bytes	from	10.0.2.6:	icmp_seq=53	ttl=64	time=0.427	ms			
64	bytes	from	10.0.2.6:	icmp_seq=54	tt1=64	time=0.299	ms			

Рисунок 1 – Результат выполнения команды ping

2. Сканирование площадки DVWA с помощью DirBuster показано на рисунке 2. Результат приведен ниже:

Dirs found with	Files found during	Files found with a 200 responce:			
a 200 response:	testing:	/dvwa/login.php			
/dvwa/login/	Files found with a	/dvwa/docs/DVWA-			
/dvwa/docs/	302 responce:	Documentation.pdf			
/	/dvwa/index.php	/dvwa/setup.php			
/icons/	/dvwa/about.php	/dvwa/config/config.inc.php			
/dvwa/external/	/dvwa/security.php	/dvwa/external/phpids/0.6/LICENSE			
	a 200 response: /dvwa/login/ /dvwa/docs/ / /icons/	/dvwa/login/ Files found with a /dvwa/docs/ 302 responce: / /dvwa/index.php /icons/ /dvwa/about.php			

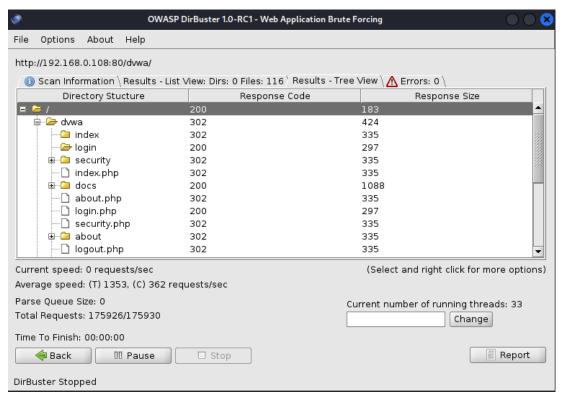


Рисунок 2 – Результат сканирования DVWA с помощью DirBuster

3. Сканирование площадки DVWA с помощью DirSearch (рисунок 3).

```
File Actions Edit View Help

[12:38:40] 403 - 2938 - /.htaccessBAK
[12:38:40] 403 - 2938 - /.htaccessOLD
[12:38:40] 403 - 2938 - /.htaccessOLD
[12:38:40] 403 - 2938 - /.htam

[12:38:40] 403 - 2858 - /.htm

[12:38:40] 403 - 2858 - /.htm

[12:38:40] 403 - 2958 - /.html

[12:38:40] 403 - 2958 - /.html

[12:38:40] 403 - 2958 - /.html

[12:38:40] 403 - 2928 - /.httr-oauth
[12:38:40] 403 - 2918 - /.htpasswds
[12:38:40] 403 - 2918 - /.htpasswds
[12:38:40] 200 - 111KB - /doc/
[12:38:49] 200 - 111KB - /doc/
[12:38:49] 302 - 08 - /dwa/ → login.php
[12:38:56] 200 - 49KB - /phpinfo.php
[12:38:56] 200 - 49KB - /phpinfo.php
[12:38:56] 200 - 49KB - /phpinfo.php
[12:38:56] 200 - 4KB - /phpinfo.php
[12:38:56] 200 - 4KB - /phpMyAdmin/index.php
[12:38:56] 200 - 4KB - /phpMyAdmin/index.php
[12:38:58] 403 - 2958 - /server-status/
[12:39:01] 301 - 3088 - /test → http://10.0.2.5/test/
[12:39:01] 301 - 3088 - /test → http://10.0.2.5/tikiwiki/

Task Completed

[**Coot® nix2twix**)-[**]
```

Рисунок 3 – Результат сканирования DVWA с помощью DirSearch

4. На рисунке 4 приведен результат сканирования площадки DVWA в рекурсивном режиме с анализом подкаталогов:

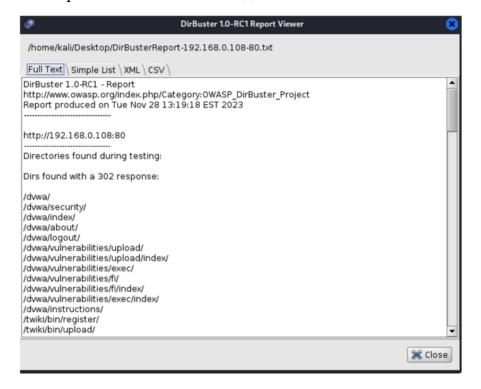


Рисунок 4 – Результат сканирования в рекурсивном режиме

ВЫВОД

В ходе выполнения данной лабораторной работы я ознакомилась с основными методами анализа структуры WEB приложений, и методами оценки результатов анализа.