METASCAN

Контроль защищенности Внешнего периметра

https://metascan.ru
https://github.com/vulnspace/

METASCAN
by vulnspace

- Главная
- Мои сайты
- Профили сканера
- Инфраструктура
- Порты
- Уязвимости
- Галерея
- Разведка
- Граф
- Расписание
- История проверок
- Dorks
- Мой аккаунт

Мои сайты

Поиск

demo / 8
6 455 322 169

vulnweb / 3
24 3 23 60 4

Subnets / 1

Создать новую группу

Запустить проверку | Остановить проверку | Переместить

Все хосты | Все порты | Все уязвимости | Отчеты за период

1/12	Статус	Цель	IP адрес	Дата добавления	Последняя завершенная проверка	Статус последнего сканирования
demo						
		bwapp.hakhub.net	221.150.96.204	1 февраля 2024 г.	13.09.2024, 10:45	Cancelled
		nmap.org	50.116.1.184	12 марта 2024 г.	05.09.2024, 20:57	Cancelled
		www.vulnweb.com	44.228.249.3	9 июля 2024 г.	30.08.2024, 16:46	Cancelled
		rest.vulnweb.com	35.81.188.86	9 июля 2024 г.	13.09.2024, 11:13	Cancelled
		www.nmap.org	50.116.1.184	28 сентября 2024 г.	—	Cancelled
		issues.nmap.org	50.116.1.184	28 сентября 2024 г.	—	Cancelled
		svn.nmap.org	50.116.1.184	28 сентября 2024 г.	30.08.2024, 20:26	Cancelled
		echo.nmap.org	45.33.32.156	28 сентября 2024 г.	30.08.2024, 16:52	Cancelled
vulnweb						
		testaspnet.vulnweb.com	44.238.29.244	1 февраля 2024 г.	13.09.2024, 10:44	Finished
		vulnweb.com	44.228.249.3	12 марта 2024 г.	30.08.2024, 16:46	Finished
		testphp.vulnweb.com	44.228.249.3	15 августа 2024 г.	01.10.2024, 12:22	Finished
Subnets						
☑		44.238.29.0/22	—	3 октября 2024 г.	—	—

Успешно
Сканирование успешно запущено

Название профиля

Regular

Сканирование портов

Выбрать регион сканирования | Используемые IP адреса

Россия

Проверять TCP порты

0-65535

Проверять UDP порты

53,88,111,123,138,139,161,445,500,514,623,1028,1433,1645,1646,1701,1812,1813,2000,204

Список разрешенных протоколов

http,https

Список нежелательных протоколов

ssh,ms-wbt-server,telnet,snmp,ipmi,memcached,vnc,mysql,postgresql,amqp,mqtt,rsync,

Ограничение RPS

5

Скорость сканирования портов для подсети

15000

Скорость сканирования портов для хоста

500

Logins file

Загрузить файл

txt

Passwords file

Загрузить файл

txt

HTTP заголовок

Инвентаризация

- [x] Найти поддомены

Поиск системных уязвимостей

- [x] Искать уязвимости по версиям ПО
- [x] Использовать скрипты
- [x] Подобрать пароли

Поиск веб-уязвимостей

- [x] Проверить HTTP заголовки
- [x] Веб уязвимости на основе шаблонов

Критичность уязвимостей для движка шаблонов

medium,high,critical

- [ ] Использовать приватные шаблоны

Перечислить названия приватных шаблонов

template1,template2,template3

- [x] Найти веб-технологии
- [x] Делать скриншоты страниц
- [x] Найти скрытые файлы и папки

Отображать коды ответа

200

- [ ] Рекурсивный перебор каталогов
- [x] Проверить наличие WAF
- [x] Искать уязвимости в Wordpress

WPScan токен

WPScan токен

- [x] Искать уязвимости в Magento

Использовать User-Agent

'vulnspace'

Сканер веб-уязвимостей

- [x] Включить сканер веб-уязвимостей

Настройки обхода сайта

- [x] Включить краулер Katana
- [x] Включить статический анализ js файлов

Максимальный уровень вложенности директорий при обходе сайта краулером

3

Исключить коды ответа

404,403,500,501,502,503,504

Не атаковать URL оканчивающиеся на следующие расширения

3ds,7z,aac,accdb,aiff,apk,arj,avi,bin,bmp,bz2,cab,com,css,cur,dae,dat,dbf,dll,dmg,doc,d

Время работы AjaxSpider

20

- [x] Взаимодействие AjaxSpider с элементом не более одного раза

Элементы для взаимодействия AjaxSpider

[x] a	[ ] abbr	[ ] addr	[ ] area	[ ] articl	[ ] aside	[x] butto	[ ] canv	[ ] detai
[ ] div	[ ] foote	[ ] form	[ ] head	[ ] img	[x] input	[ ] label	[ ] li	[ ] nav
[ ] ol	[ ] optio	[ ] p	[ ] radio	[ ] secti	[ ] selec	[ ] span	[ ] sumr	[ ] table
[ ] td	[ ] texta	[ ] th	[ ] tr	[ ] ul	[ ] vidio			

Передать пользовательские элементы для взаимодействия AjaxSpider

element

Идеальное Состояние периметра

Назначение каждого порта на внешнем периметре известно ИБ

(Прошло через согласование связности)

На периметре отсутствуют уязвимости CVSS выше 4.0

Переодичность проверки каждого хоста на внешнем периметре < 24 часов

ВОЗМОЖНОСТИ СКАНЕРА

- Автоматизированная инвентаризация DNS и ASN
- Ежедневный скан портов 0-65535 + udp
- Контроль white\blacklist протоколов
- Баннерный поиск уязвимстей CVE.org + NIST + БДУ
- Поиск уязвимостей сетевого оборудования
- Поиск уязвимостей и ошибок конфигурации системных сервисов
- Подбор слабых паролей
- Поиск уязвимостей в CMS (WP, Bitrix, Magento)
- Поиск утечек файлов (логи, бекапы, архивы, скрипты)
- Краулинг веб-приложений с использованием Selenium
- 60 видов иньекций для веб-уязвимостей
- Сканирование API на основе Swagger\Postman
- Сканирование под учетной записью пользователя

L3-L7 проверки

XSS	Интенсивность	Точность
Cross Site Scripting (Persistent)	DEFAULT	DEFAULT
Cross Site Scripting (Persistent) - Spider	DEFAULT	DEFAULT

Others	Интенсивность	Точность
Remote File Inclusion	DEFAULT	DEFAULT
External Redirect	DEFAULT	DEFAULT
Format String Error	DEFAULT	DEFAULT
CRLF Injection	DEFAULT	DEFAULT
Server Side Include	DEFAULT	DEFAULT
Out of Band XSS	DEFAULT	DEFAULT
Web Cache Deception	DEFAULT	OFF
Server Side Request Forgery	DEFAULT	DEFAULT
Confidential Tokens Search	DEFAULT	DEFAULT
Server Side Code Injection	DEFAULT	DEFAULT
XPath Injection	DEFAULT	DEFAULT
Expression Language Injection	DEFAULT	DEFAULT

SQL Injection	Интенсивность	Точность
SQL Injection	LOW	DEFAULT

Time Based Injections	Интенсивность	Точность
SQL Injection - Hypersonic SQL	DEFAULT	OFF
SQL Injection - PostgreSQL	DEFAULT	OFF
SQL Injection - MsSQL	DEFAULT	OFF
Server Side Template Injection (Blind)	DEFAULT	OFF

Cross Site Scripting (Reflected)	DEFAULT	DEFAULT
Cross Site Scripting (Persistent) - Prime	DEFAULT	DEFAULT
Cross Site Scripting (DOM Based)	DEFAULT	DEFAULT
Path Traversal	DEFAULT	HIGH
HTTP Parameter Pollution	DEFAULT	OFF
Buffer Overflow	DEFAULT	OFF
Integer Overflow Error	DEFAULT	OFF
Parameter Tampering	DEFAULT	OFF
LDAP Injection	DEFAULT	OFF
Bypassing 403	DEFAULT	OFF
Spring4Shell	DEFAULT	OFF
Text4shell (CVE-2022-42889)	DEFAULT	OFF
XSLT Injection	DEFAULT	OFF
Remote OS Command Injection	DEFAULT	DEFAULT
XML External Entity Attack	DEFAULT	DEFAULT
Server Side Template Injection	DEFAULT	DEFAULT
SQL Injection - MySQL	DEFAULT	OFF
SQL Injection - Oracle	DEFAULT	OFF
SQL Injection - SQLite	DEFAULT	OFF
NoSQL Injection - MongoDB	DEFAULT	OFF

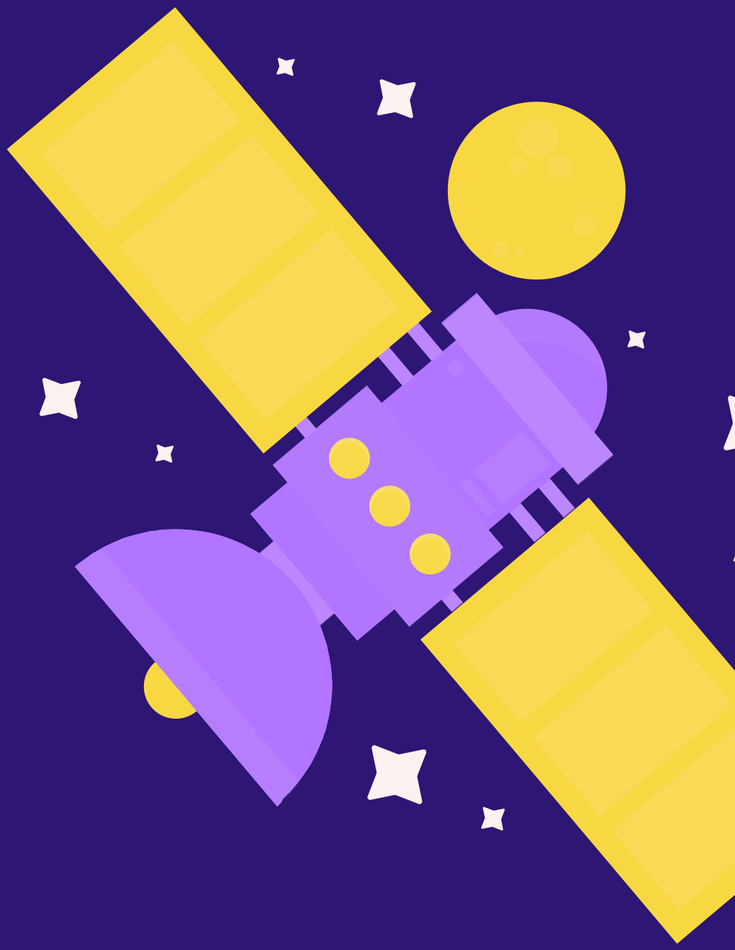
ОТЛИЧИТЕЛЬНЫЕ ОСОБЕННОСТИ

- 28 инструментов для поиска уязвимостей в едином интерфейсе (ZAP, nuclei, dirsearch, hydra, patator, cameradar, Katana, wappalyzer, etc)
- Возможность ежедневно проверять до 2 млн с использованием всех модулей сканирования
- Еженедельные ВКС-встречи с пентестером разбирающим для вас уязвимости и предоставляющим отчеты
- Собственный RND уязвимостей для 1С, Bitrix, R7 Office, Trassir, Quick и другого ПО и протоколов специфичного для отечественного ПО.
- Дашборд отчетности для руководства
- Интеграция с DefectDojo, SecurityVision, Rvision

УВЕДОМЛЕНИЯ

- Об обнаруженных уязвимостях
- Открывшихся портах
- Новых доменах

- Telegram-бот
- Email
- Телефонный звонок



Python wrapper

ВЫ МОЖЕТЕ ДОБАВЛЯТЬ СВОИ ПРОВЕРКИ НА PYTHON, В ВИДЕ ШАБЛОНОВ NUCLEI И ZAP-ADDONS

```python
class Scanner(object):
    name = "scanner_base"
    vuln_type = "default_vuln_type"
    user_options = {}
    Vulnerability_body_fields_to_web_interface = []

    def __init__(self, opts, target, metadata):
        self.metadata = metadata
        self.opts = opts
        self.target = target

    @staticmetod
    def circuit(Metadata):
        '''
        Логика работы сканера.
        Принимает на вход объекты типа Metadata.
        Результатом работы должны быть экземпляры класса CVE.
        '''
        return [Vulnerability(), Vulnerability()]

    def check_start_condition(self):
        '''
        Проверка параметров, которым должен соответствовать Target для запуска сканера
        True, если сканер должен запуститься. В другом случае False.
        '''
        return True

    class ScannerError(Exception):
        def __init__(self, value):
            self.value = value
        def __str__(self):
            return repr(self.value)
```