

Advanced web fuzzing today

Коновалов Никита
@worlak2

Обо мне

- Начинающий IT специалист в сфере информационной безопасности
- Студент РГУПС
- Проходил удаленную стажировку в компании Digital Security по направлениям : "Уязвимости в системах мониторинга", "Социальная инженерия", "Безопасность внутренней сети и уязвимые протоколы", "Продвинутый фазинг"
- В свободное время решаю задачи на root-me, pentestit lab, участвую в task-base ctf, провожу аудит сайтов на предмет уязвимостей
- Планирую выступить на workshop zeronights 2017 с уязвимостями в системе мониторинга cacti

Содержание

Что такое **fuzzing**

Существующие веб-сканеры их преимущества и недостатки

Проблемы web fuzzing

Подходы к fuzzing сегодня

Наша **разработка** для продвинутого тестирования web app

Принцип работы

Fuzzing



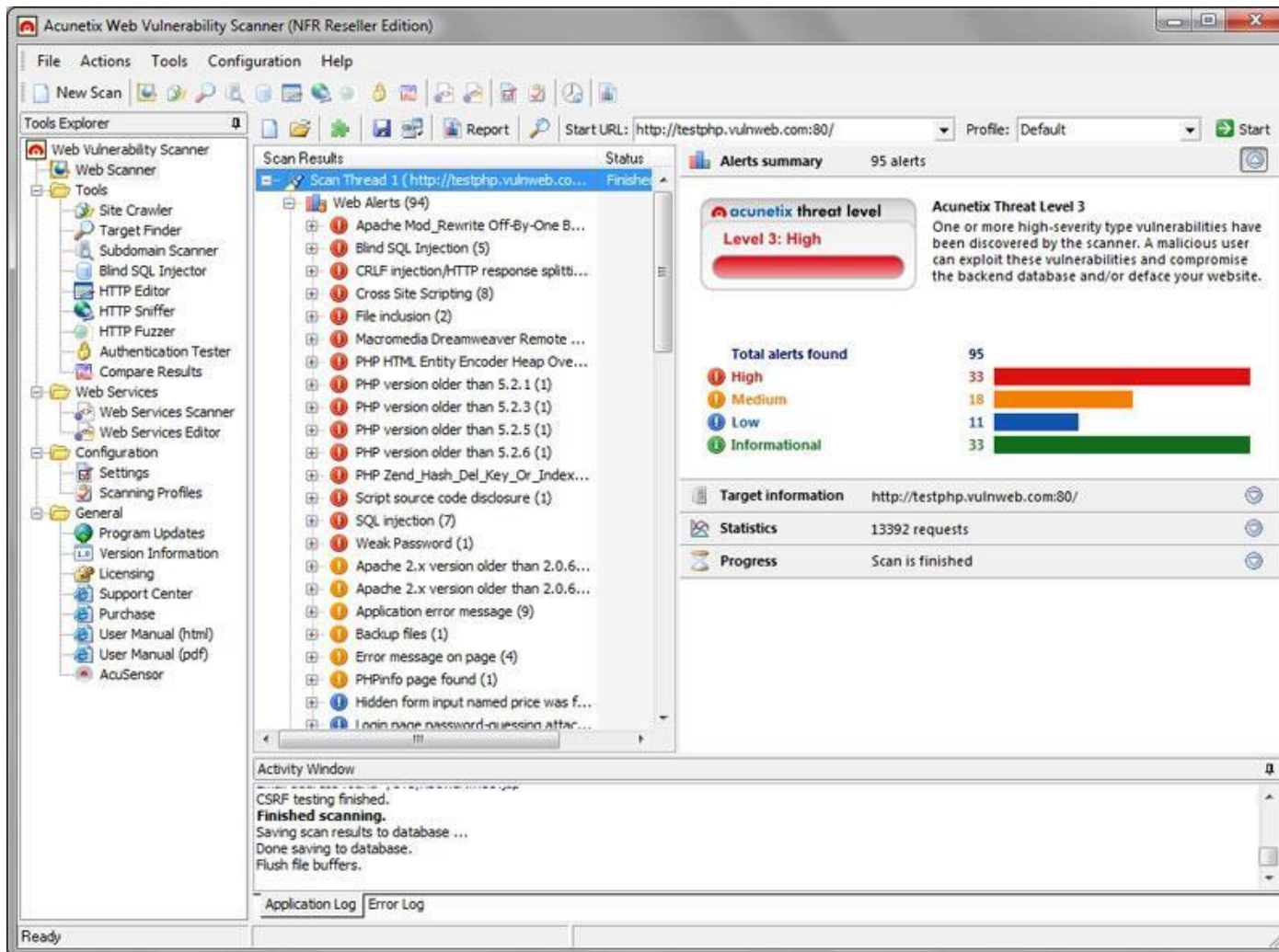
Fuzzing

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	a' waitfor delay '0:0:10'--
Load ...	1 waitfor delay '0:0:10'--
Remove	declare @q nvarchar (200) select @q = 0x770061006900740066006F0072002000640065006...
Clear	declare @s varchar(200) select @s = 0x77616974666F722064656C61792027303A303A3130...
	declare @q nvarchar (200) 0x730065006c006500630074002000400040007600650072007300...
	declare @s varchar (200) select @s = 0x73656c6563742040407665727369666e exec(@s)
	a'
	-
Add	Enter a new item
Add from list ...	

Веб-сканеры



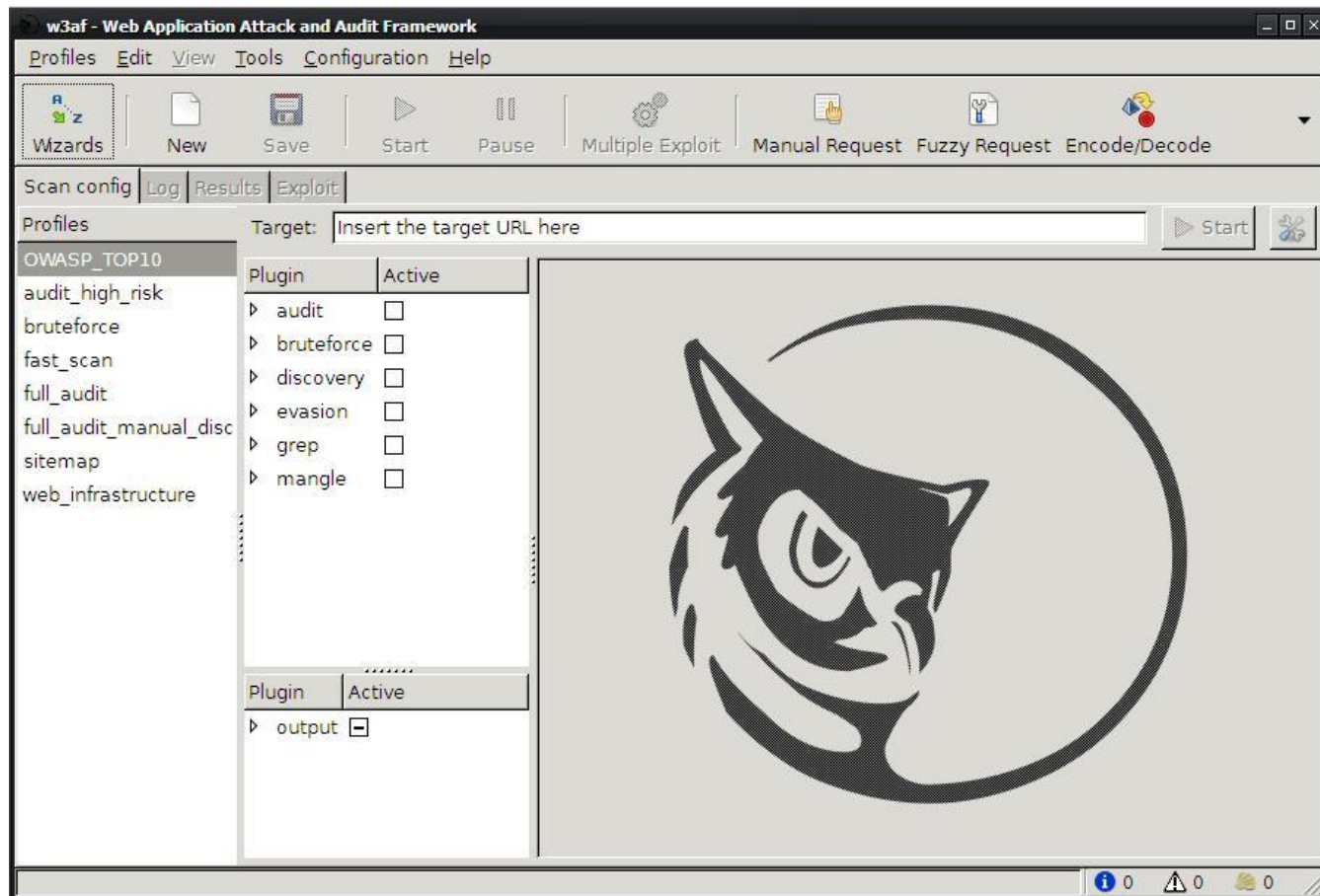
Acunetix – платный веб сканер определяет ошибки конфигурации сервера и приложения.

Плюсы:

Определяет уязвимости сервера и указывает версии приложений и аддонов.

Минусы:

Ограниченный словарь
отсутствие умного
определения ошибок



W3af – бесплатный
сканер веб уязвимостей

Плюсы:

Отлично определяет
простые ошибки

Быстрая работа

Минусы:

Не определит
уязвимость при
наличии web application
firewall



Burp suite – это платформа для проведения аудита безопасности веб-приложений

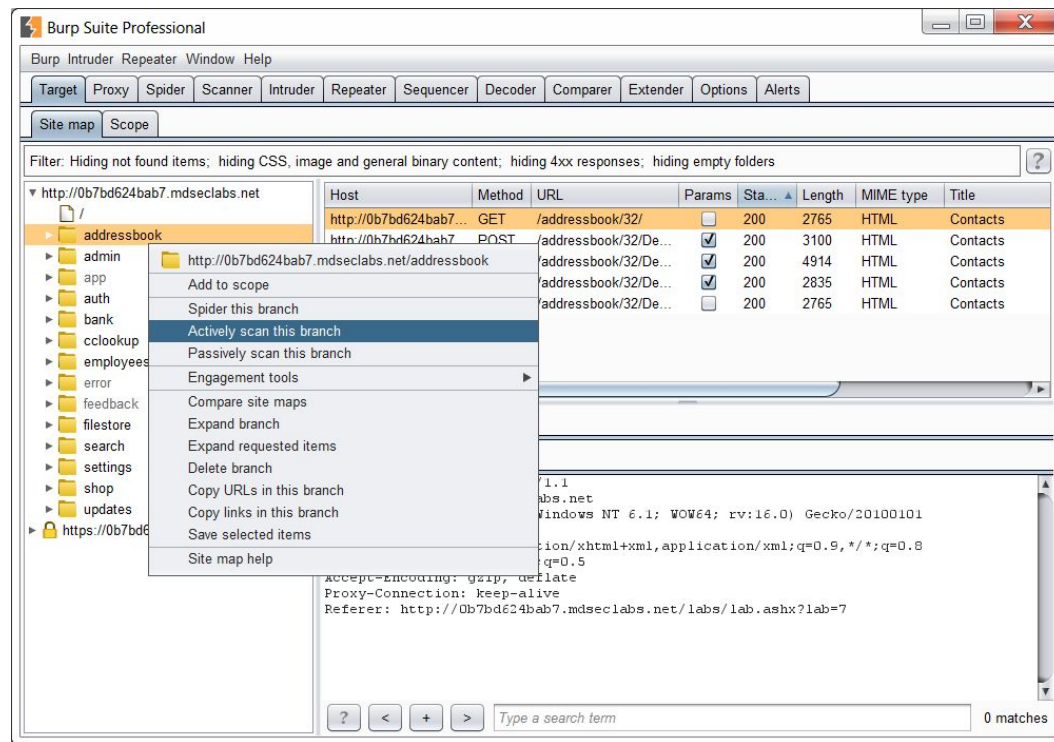
Плюсы

Intruder

Repeater

Минусы

В бесплатной версии недоступен сканер



Проблемы web fuzzing

Медленная работа



False positive из-за возвращения полезных нагрузок в ответе



Отсутствие специфических encode

« " »

%22 - url encode

%2522 - double url encode

\x22 - js encode

" - html encode

\u0022 - unicode

\u0122 - unicode 2

%C4%A2- unicode 2 utf-8

...

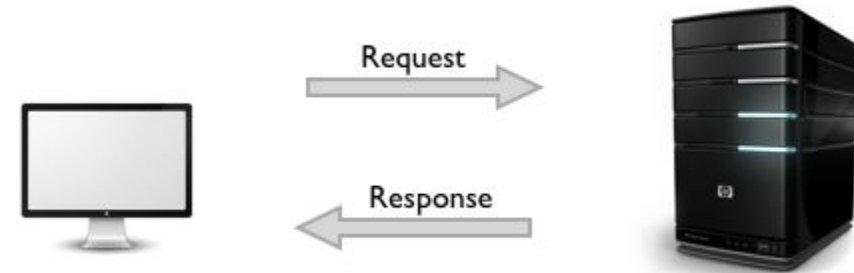
Отсутствие анализа ответа по различным метрикам

Время

Строки

Код страницы

Количество слов



Подходы к web fuzzing сегодня

Анализаторы различных метрик , таких как (время ответа, количество слов, количество заголовков, среднее время ответа, количество конкретных html тегов)



Проверки на различные повторения при специальных символах и выявление закономерностей для дальнейших исследований (Backslash Scanner)

Successful probes

- **Basic fuzz** (`\z`z'z"\`z\'z\'\'`)
 - error: 2 vs 1
 - Content: 17 vs 3
- **String – doublequoted** (`\zz" vs \"`)
 - error: 2 vs 1
 - Content: 16 vs 3
- **Concatenation: "||"** (`z||"z(z"z vs z(z"||"z`)
 - error: 2 vs 1
- **Concatenation: "+"** (`z+"z(z"z vs z(z"+"z`)
 - error: 2 vs 1
 - Content: 16 vs 3
- **Concatenation: "&"** (`z&"z(z"z vs z(z"&"z`)
 - error: 2 vs 1
 - Reflection count: 3 vs 0
- **JavaScript injection** (`" +isFinitee(1) + " vs " +isFinite(1) + "`)
 - error: 2 vs 1
 - Content: 11 vs 3

Наша разработка

[!] Получение стандартного ответа

#	Код	Контент	Строки	Слова	Время	Нагрузка
1	200 (+200)	13493 (-2529)	158 (-78)	924 (-132)	2.109 (+1.031)	title=a%22
2	200 (+200)	13493 (-2529)	158 (-78)	924 (-132)	3.125 (+2.047)	title=a%2522
3	200 (+200)	13493 (-2529)	158 (-78)	924 (-132)	4.172 (+3.094)	title=a%C0%A2
4	200 (+200)	13493 (-2529)	158 (-78)	924 (-132)	1.062 (-0.016)	title=a%21
5	200 (+200)	13493 (-2529)	158 (-78)	924 (-132)	5.188 (+4.11)	title=a%2521
6	200 (+200)	13493 (-2529)	158 (-78)	924 (-132)	6.219 (+5.141)	title=a%C0%A1
7	200 (+200)	16022 (+0)	236 (+0)	1056 (+0)	6.141 (+5.063)	action=search%21
8	200 (+200)	16022 (+0)	236 (+0)	1056 (+0)	6.141 (+5.063)	action=search%2521
9	200 (+200)	16022 (+0)	236 (+0)	1056 (+0)	6.141 (+5.063)	action=search%C0%A1
10	200 (+200)	16022 (+0)	236 (+0)	1056 (+0)	6.141 (+5.063)	action=search%22
11	200 (+200)	16022 (+0)	236 (+0)	1056 (+0)	6.141 (+5.063)	action=search%2522
12	200 (+200)	16022 (+0)	236 (+0)	1056 (+0)	6.125 (+5.047)	action=search%C0%A2

Принцип работы

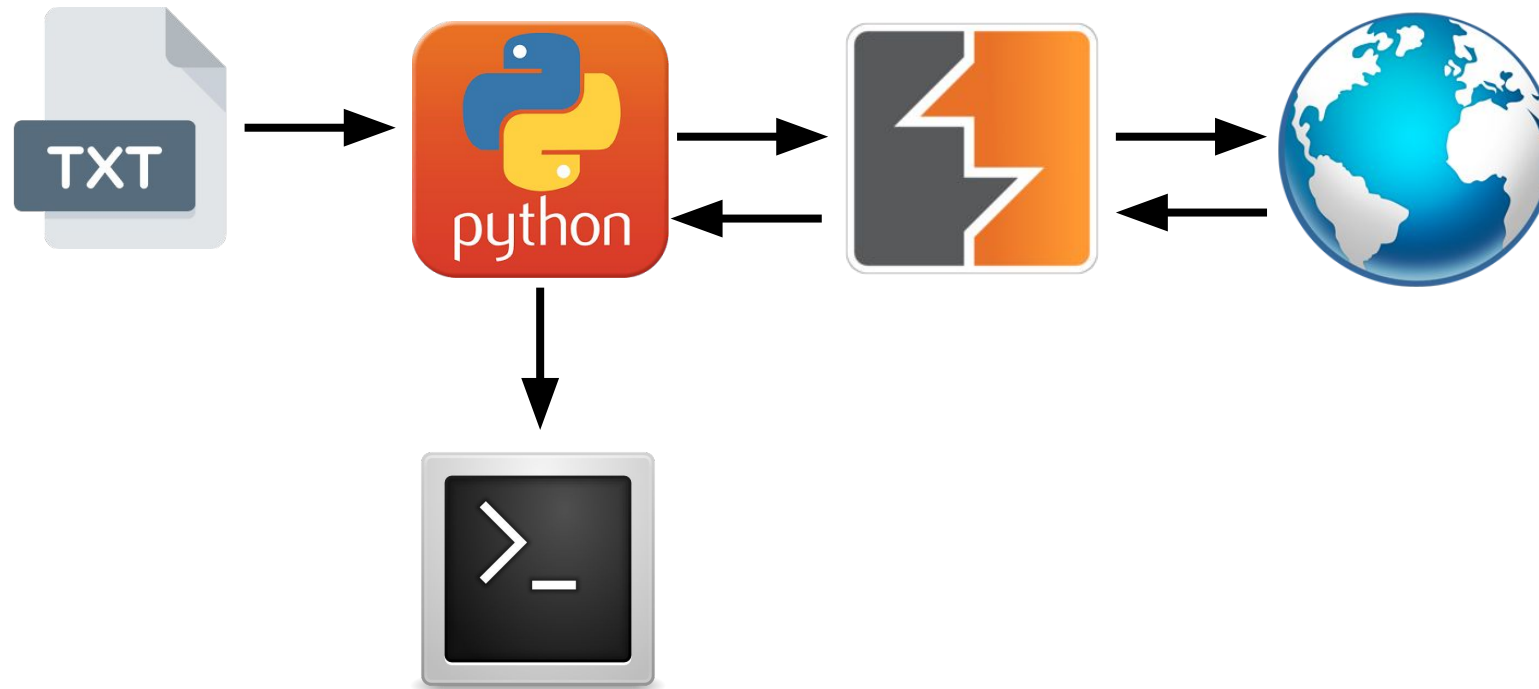
1. Перехватываем стандартный запрос к веб приложению для дальнейшего анализа



2. Передаем тестовый запрос фазеру с заранее заготовленным словарем и ожидаем ответа . По данному ответу мы будем сравнивать метрики



3. Фазер подставляет payload и сравнивает полученный ответ, после чего отображает в консоли отличается ли ответ от обычного или нет, подсвечивая разницу в метриках



В планах на дальнейшую разработку:

Доработать анализ ответов

Добавить правила кодирования payloads

Сохранение в отдельный файл
подозрительных мест и уязвимых
параметров

Работа с парными payloads

Контакты:

Telegram @worlak2

Github <https://github.com/worlak2/>

<https://github.com/Iljala/AdvancedWebFuzzer>

https://vk.com/marko_polo_worlak

Вопросы?