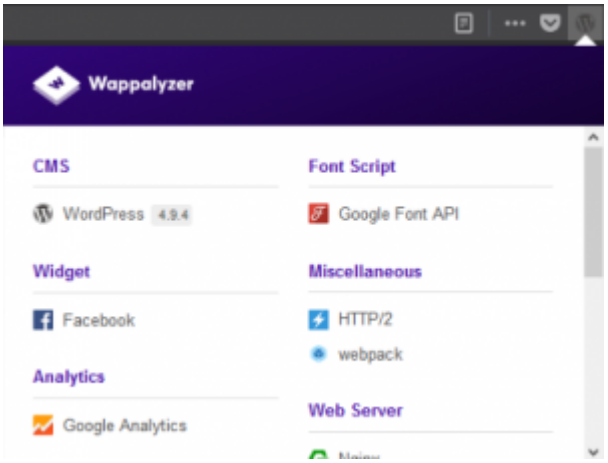
SWRhapsody

记录些收集的wpscan的cheat sheet 和一些对wordpress的攻击方法

散碎的方法

wordpress版本的识别，我一般使用 Wapplayzer，firefox上可以找到插件



用户枚举，nmap有个脚本

```
nmap -sV --script http-wordpress-enum --script-args limit=25

PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack
| http-wordpress-enum:
| Username found: admin
| Username found: testadmin
| Username found: fred
| Username found: alice
| Username found: bob
|_Search stopped at ID #25. Increase the upper limit if necessary with 'http-wordpress-enum.li
```

Cheat Sheet

更新数据（记得周期性更新）

```
wpscan --update
```

最基本的扫描

```
wpscan --url https://XXX.XXX.XXX
```

用户枚举

```
wpscan --url https://127.0.0.1 -e u
wpscan --url https://127.0.0.1 -e u[1-25]
```

枚举结果样例，在输出的最下面

```
[+] Enumerating usernames ...
[+] Identified the following 2 user/s:
    +----+--------+--------+
    | Id | Login  | Name   |
    +----+--------+--------+
    | 1  | admin  | Core   |
    | 2  | backup | backup |
    +----+--------+--------+
```

对用户密码进行爆破

```
wpscan --url https://127.0.0.1 -w PASSOWRD_FILE -U USER_NAME
wpscan --url https://127.0.0.1 -w PASSOWRD_FILE --usernames USER_NAME_FILE
```

爆破结果样例

```
  Brute Forcing 'admin' Time: 00:00:30 <==== > (102 / 113) 90.26%  ETA: 00:00:03
  +----+-------+------+----------+
  | Id | Login | Name | Password |
  +----+-------+------+----------+
  |    | admin |      | princess |
  +----+-------+------+----------+
```

参考

[1] https://hackertarget.com/attacking-wordpress/

分类: CHEAT SHEET PENETRATION TEST

SWRhapsody

0 条评论

发表评论

名称 *

电子邮件 *

网站

在想些什么?

发表评论

近期文章

- 携程Apollo YAML 反序列化
- CVE-2020-5410
- CodeQL部分源码简读
- 服务器与网关的不一致
- CodeQL 部分使用记录

SWRhapsody

文章归档

2020年8月

2020年6月

2020年5月

2020年3月

2020年1月

2019年12月

2019年11月

2019年8月

2019年7月

2019年5月

2019年4月

2019年1月

2018年11月

2018年10月

2018年9月

2018年4月

2018年3月

2018年2月

2018年1月

分类目录

Article Collection

Cheat Sheet

SWRhapsody

Exploit

HackTheBox

Penetration Test

Uncategorized

相关文章

PENETRATION TEST

服务器与网关的不一致

前言 一次渗透测试时遇到的，官方认为不是漏洞。 Code 遇到了大约这 阅读更多…

CHEAT SHEET

CodeQL 部分使用记录

前言 CodeQL 是一个代码分析引擎，主要原理是通过对代码进行构建并 阅读更多…

CHEAT SHEET

Tcpdump Cheat Sheet

SWRhapsody

ABOUT

Hestia |由ThemeIsle开发