

2018

Sqlmap 视频课程

Sql注入工具 Sqlmap介绍

—— 课程内容 ——

➤ 1. Sqlmap介绍

➤ 3. Sqlmap下载

➤ 2. Sqlmap环境安装

➤ 4. Sqlmap版本查看

01

Sqlmap介绍

sqlmap是一个开源的渗透测试工具，它可以自动化检测和利用SQL注入缺陷以及接管数据库服务器的过程。它有一个强大的检测引擎，许多适合于终极渗透测试的小众特性和广泛的开关，从数据库指纹、从数据库获取数据到访问底层文件系统和通过带外连接在操作系统上执行命令。

官方网址：<http://sqlmap.org/>

The screenshot displays the sqlmap.org website. The header features the sqlmap logo and the tagline 'Automatic SQL injection and database takeover tool'. A 'View project on GitHub' button is present. The main content area is divided into two columns. The left column, titled 'Introduction()', describes sqlmap as an open-source penetration testing tool and includes a terminal screenshot showing the tool's execution and output. The right column contains download links for '.zip file' and '.tar.gz file', a promotional banner for 'netsparker' (a Web Application Security Scanner), and a 'Tweets by @sqlmap' section.

sqlmap.org

sqlmap®
Automatic SQL injection and database takeover tool

View project on GitHub

; Introduction();--

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
(1.0.5.63#dev)
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 17:43:06

[17:43:06] [INFO] testing connection to the target URL
[17:43:06] [INFO] heuristics detected web page charset 'ascii'
[17:43:06] [INFO] testing if the target URL is stable
[17:43:07] [INFO] target URL is stable
[17:43:07] [INFO] testing if GET parameter 'id' is dynamic
[17:43:07] [INFO] confirming that GET parameter 'id' is dynamic
[17:43:07] [INFO] GET parameter 'id' is dynamic
[17:43:07] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
```

Download .zip file

Download .tar.gz file

Find vulnerabilities in your websites before hackers do

use **netsparker** Web Application Security Scanner

The sqlmap project is sponsored by [Netsparker Web Application Security Scanner](#)

Tweets by @sqlmap

; Features();--

02

Sqlmap环境安装

Python2.x环境下载地址：<https://www.python.org/downloads/release/python-2715/>

The screenshot shows the Python Software Foundation website for the Python 2.7.15 release. The page includes a navigation bar with links to Python, PSF, Docs, PyPI, Jobs, and Community. Below the navigation bar is a search bar and a 'Socialize' button. The main content area features the Python logo and a section for 'Python 2.7.15'. This section includes the release date (2018-05-01) and a note about macOS users. Below the note is a 'Files' section containing a table of download links, operating systems, descriptions, MD5 sums, file sizes, and GPG signatures.

Python 2.7.15

Release Date: 2018-05-01

Python 2.7.15 is a bugfix release in the Python 2.7 series.

Note:

Attention macOS users: as of 2.7.15, all python.org macOS installers ship with a builtin copy of OpenSSL. Additionally, there is a new additional installer variant for macOS 10.9+ that includes a built-in version of Tcl/Tk 8.6. See the installer README for more information.

Files

Version	Operating System	Description	MD5 Sum	File Size	GPG
Gzipped source tarball	Source release		045fb3440219a1f6923fefdabde63342	17496336	SIG
XZ compressed source tarball	Source release		a80ae3cc478460b922242f43a1b4094d	12642436	SIG
macOS 64-bit/32-bit installer	Mac OS X	for Mac OS X 10.6 and later	9ac8c85150147f679f213add1e7d96e	25193631	SIG
macOS 64-bit installer	Mac OS X	for OS X 10.9 and later	223b71346316c3ec7a8dc8bff5476d84	23768240	SIG
Windows debug information files	Windows		4c61ef61d4c51d615cbe751480be01f8	25079974	SIG
Windows debug information files for 64-bit binaries	Windows		680bf74bad3700e6b756a84a56720949	25858214	SIG
Windows help file	Windows		297315472777f28368b052be734ba2ee	6252777	SIG
Windows x86-64 MSI installer	Windows	for AMD64/EM64T/x64	0ffa44a86522f9a37b916b361eebc552	20246528	SIG

03

Sqlmap下载

Sqlmap下载地址: <https://github.com/sqlmapproject/sqlmap/zipball/master>



Automatic SQL injection and database takeover tool



View project on GitHub

Introduction()

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
{1.0.5.63#dev}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 17:43:06

[17:43:06] [INFO] testing connection to the target URL
[17:43:06] [INFO] heuristics detected web page charset 'ascii'
[17:43:06] [INFO] testing if the target URL is stable
[17:43:07] [INFO] target URL is stable
[17:43:07] [INFO] testing if GET parameter 'id' is dynamic
[17:43:07] [INFO] confirming that GET parameter 'id' is dynamic
[17:43:07] [INFO] GET parameter 'id' is dynamic
[17:43:07] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
```

Download .zip file

Download .tar.gz file



Find vulnerabilities in your websites before hackers do

use **netsparker** Web Application Security Scanner

The sqlmap project is sponsored by [Netsparker Web Application Security Scanner](#).

04

Sqlmap版本查看

总结

➤ 1. Sqlmap介绍

➤ 2. Sqlmap环境安装

➤ 3. Sqlmap下载

➤ 4. Sqlmap版本查看

谢谢

欢迎关注 后续课程