

培养未来网络力量

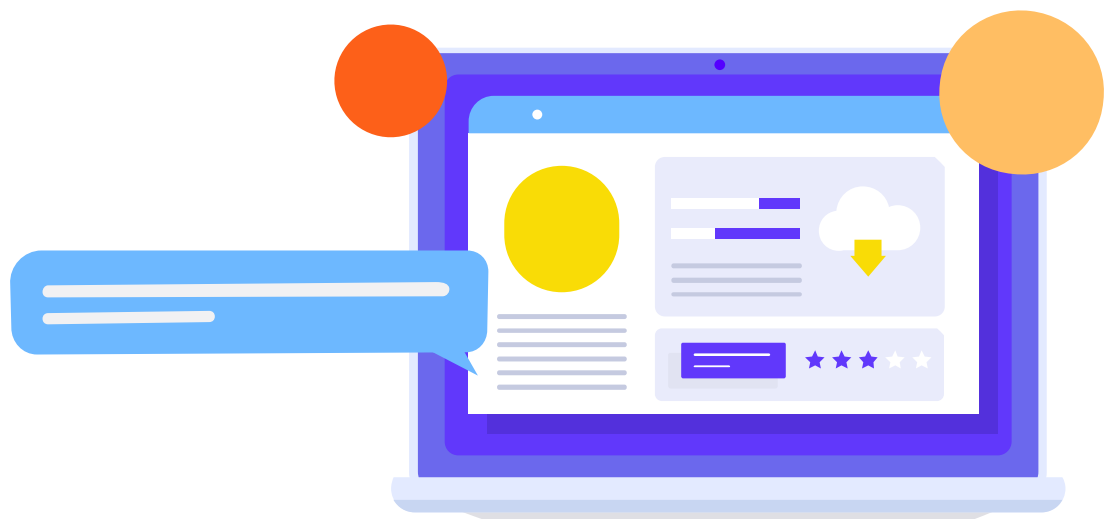
自动化漏洞挖掘之awvs

讲师：跃琪



目录

- 01. awvs介绍
- 02. awvs破解与安装
- 03. awvs批量进行扫描



/01

awvs介绍

- 漏洞扫描

漏洞扫描是指基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用漏洞的一种安全检测（渗透攻击）行为。

- 漏洞扫描工具

网络上公布的付费的、免费的漏洞扫描工具、脚本多种多样，有针对某类漏洞的、有针对某类CMS的、有针对操作系统的、也有针对web服务的、也有针对某类框架的，很是杂乱常见的有如下的：

- ✓ 针对某类漏洞的：sql注入（sqlmap）、weblogic（weblogicscan）
- ✓ 针对某类CMS的：wordpress（wpscan）、dedecms（dedecmscan）
- ✓ 针对系统应用层：nessus
- ✓ 针对某类框架的：Struts2（Struts2漏洞检查工具）、springboot（SB-Actuator）
- ✓ 针对web服务的：burpsuite、xray（被动扫描）、awvs（主动扫描）

- 什么是AWVS

Acunetix Web Vulnerability Scanner (简称AWVS) 是一款知名的网络漏洞扫描工具，它通过网络爬虫测试你的网站安全，检测流行安全漏洞。

从11.0版本开始，AWVS就变成了使用浏览器端打开的形式，使用安装时自定义的端口来访问。

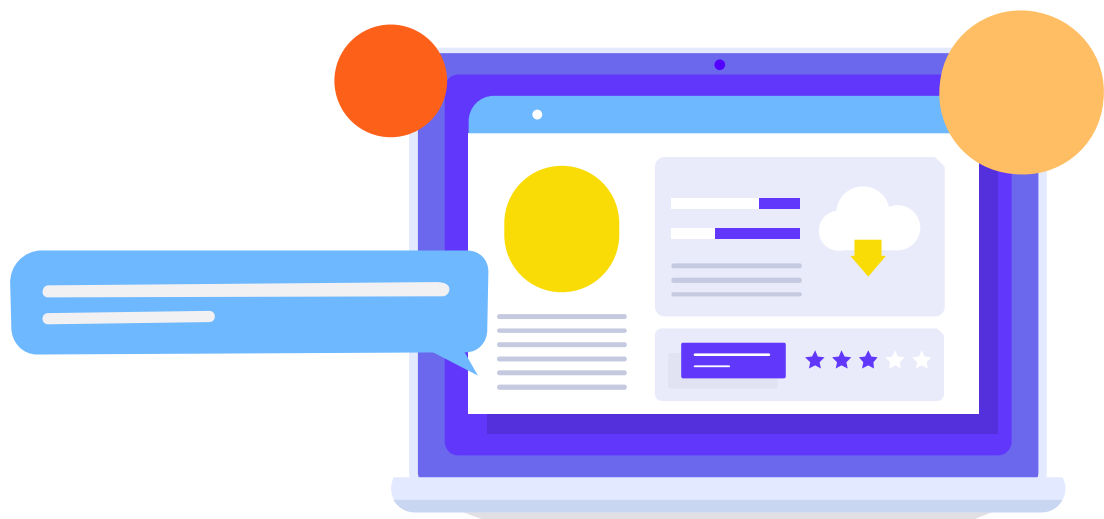
awvs13破解版下载：

链接：https://pan.baidu.com/s/1RCK7L_o42NBpWpb57kWMjw

提取码：yjwa

中文手册：

<https://blog.csdn.net/showgea/article/details/84633703>



/02

awvs的破解与安装

一、安装awvs 13

下载awvs 13

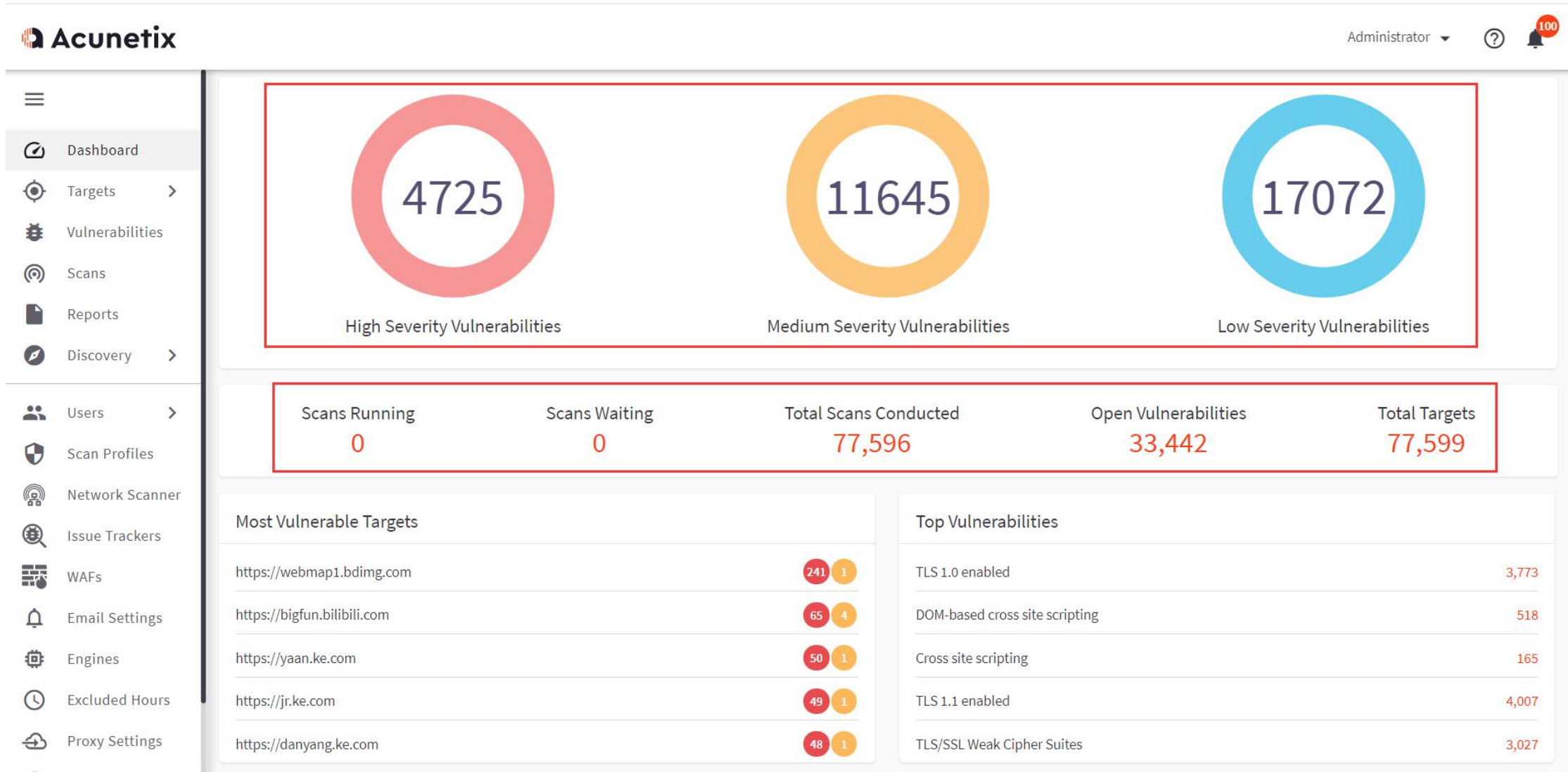
名称	修改日期	类型	大小
破解补丁	2020/2/18 13:54	文件夹	
acunetix_13.0.200205121.exe	2020/2/18 14:06	应用程序	114,472 KB
使用方法.txt	2020/2/18 14:07	文本文档	1 KB

文件(F) 编辑(E) 格式(O) 查看(V) 布局(L)

解压附件,

- 1.运行acunetix_13.0.200205121.exe安装。
- 2.复制wvsc.exe到 "C:\Program Files (x86)\Acunetix\13.0.200205121\" 下覆盖同名文件 (安装到其他路径请自行修改)
- 3.复制license_info.json到 "C:\ProgramData\Acunetix\shared\license" 下覆盖同名文件

AWVS介绍



AWVS使用

Acunetix Administrator ? 100

Dashboard

Targets ▾

Add Target

Add Targets

Target Groups

Vulnerabilities

Scans

Reports

Discovery >

Users >

Scan Profiles

Network Scanner

Issue Trackers

WAFs

Email Settings

Add Target

Save Cancel

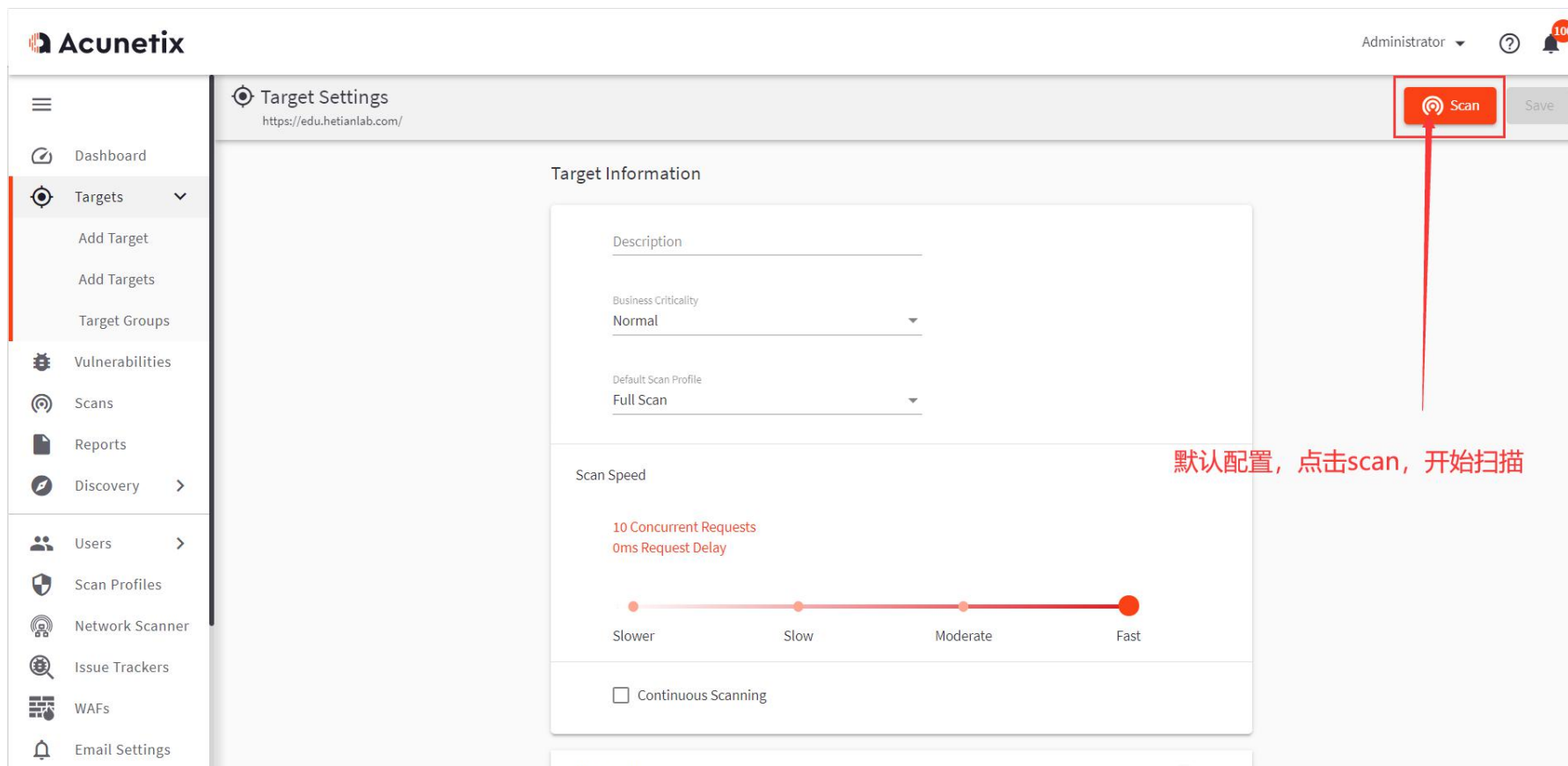
☐ Network Scans only

Address
https://edu.hetianlab.com/

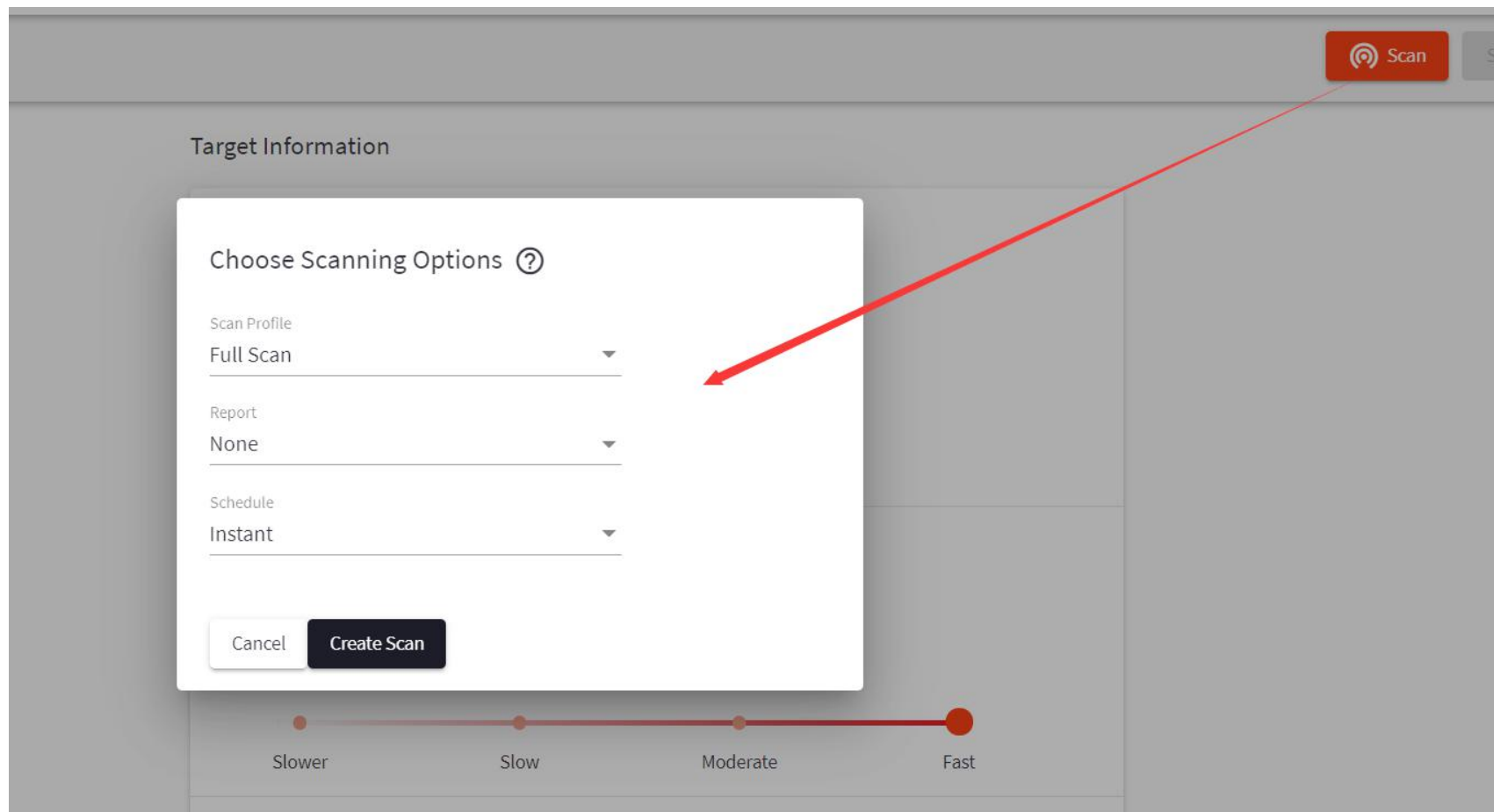
Description

添加要扫描的目标

AWVS使用



AWVS使用



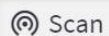
AWVS使用

Acunetix

Administrator



- Dashboard
- Targets
- Vulnerabilities
- Scans
- Reports
- Discovery
- Users
- Scan Profiles
- Network Scanner
- Issue Trackers
- WAFs
- Email Settings
- Engines
- Excluded Hours
- Proxy Settings



Scan

Full Scan - https://edu.hetianlab.com/

Stop Scan

Pause Scan

Generate Report

Export to

Scan Information

Vulnerabilities

Site Structure

Scan Statistics

Events



Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Activity

In Progress

Overall Progress

89%

Scanning of edu.hetianlab.com started

Jun 30, 2021, 10:53:01 AM

Antivirus not found

Jun 30, 2021, 10:53:01 AM

Scan Duration
1m 10s

Requests
2,603

Average Response Time
17ms

Paths Identified
12

Target Information

Address <https://edu.hetianlab.com/>
Server Engine/2.3.0
Operating System Unknown
Identified Technologies
Responsive Yes

Latest Alerts

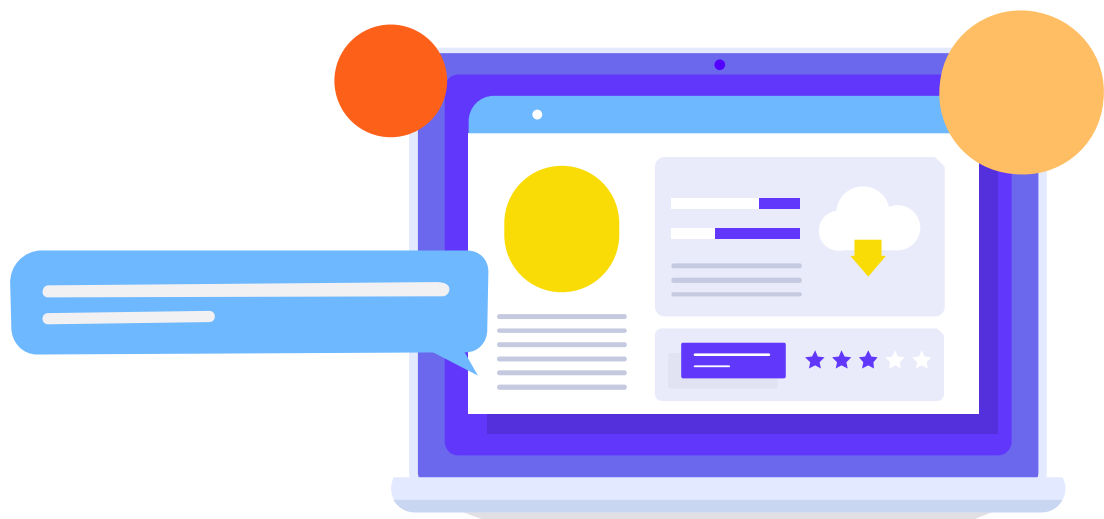
1 3 3 3

Javascript Source map detected Jun 30, 2021, 10:53:21 AM
Clickjacking: X-Frame-Options header Jun 30, 2021, 10:53:15 AM
Content Security Policy (CSP) not implemented Jun 30, 2021, 10:53:15 AM
HTTP Strict Transport Security (HSTS) not implemented Jun 30, 2021, 10:53:15 AM
Insecure Referrer Policy Jun 30, 2021, 10:53:15 AM

AWVS使用

演示目标:

<http://testphp.vulnweb.com/>



/03

awvs批量进行扫描

AWVS接口介绍

The screenshot shows the Acunetix web interface. On the left is a sidebar with navigation links: Dashboard, Targets, Vulnerabilities, Scans, Reports, Discovery, Users, Scan Profiles, Network Scanner, Issue Trackers, WAFs, Email Settings, Engines, Excluded Hours, and Proxy Settings. The main content area is titled 'Profile' and contains several sections:

- Licensed Targets Used:** 50874 (0 deleted)
- Maximum Scanning Engines:** 999999
- Enable Acunetix Online Services:** A button to enable services. Below it, text states: "Acunetix Online Services include **AcuMonitor**, used for the detection of OOB vulnerabilities, and **Malicious Link Detection**."
- API Key:** Displays a long alphanumeric key. To the right of the key are 'Copy' and 'Hide' buttons. Below the key are 'Generate New Api Key' and 'Delete' buttons. A link for 'Acunetix API Documentation' is also present.
- Two Factor Authentication:** Includes a button to 'Enable Two Factor Authentication'.

In the top right corner, the user is logged in as 'Administrator'. A dropdown menu is open, showing 'Profile' and 'Logout' options. A red arrow points from the 'Profile' dropdown to the 'API Key' section.

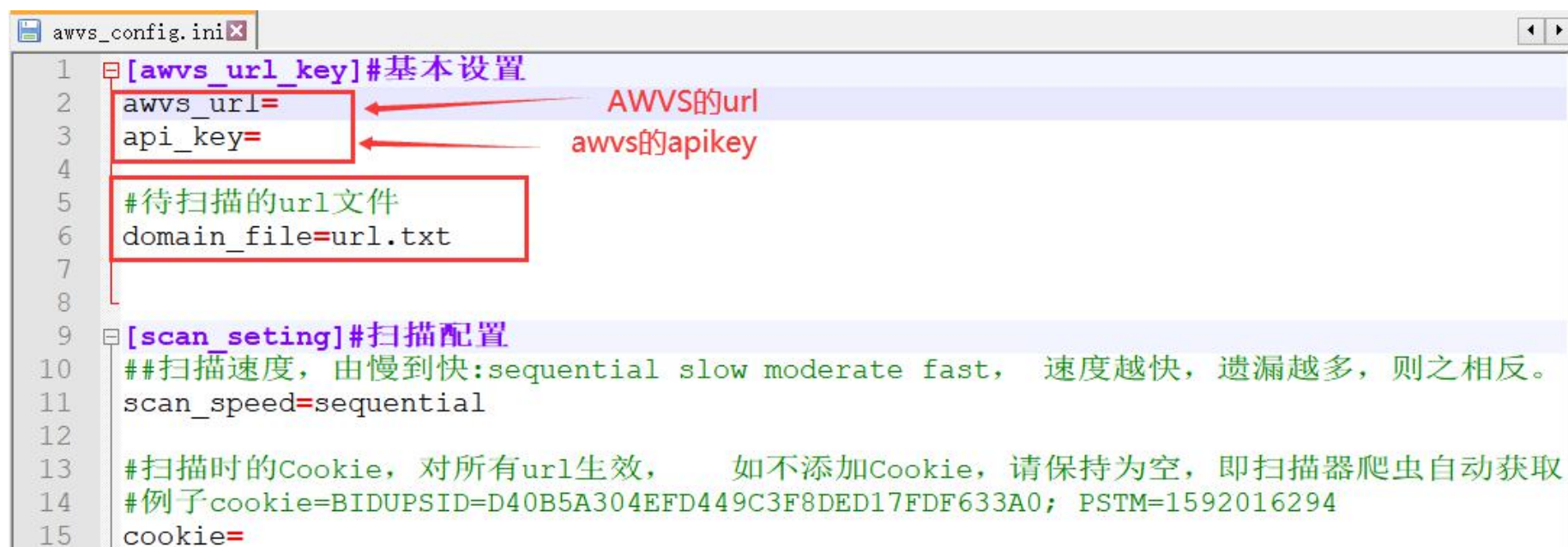
利用awvs简单自动化

awvs批量脚本

场景：遇到大批量的目标时，例如可能一个项目有上千个网站时候，这个时候我们需要利用批量的扫描器来进行操作

https://github.com/test502git/awvs13_batch_py3

1. 添加awvs的api与地址即可，同时扫描数看电脑的配置



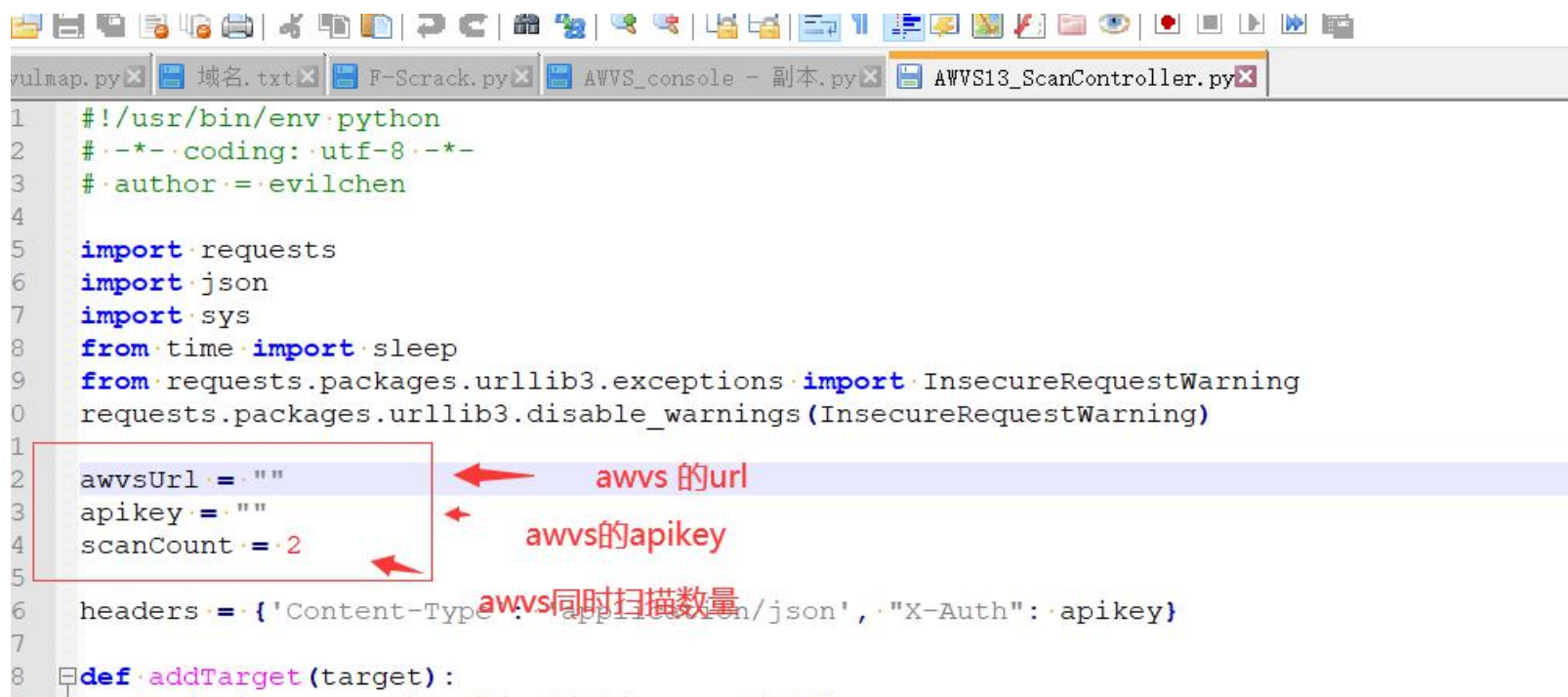
```
1 [awvs_url_key]#基本设置
2 awvs_url=
3 api_key=
4
5 #待扫描的url文件
6 domain_file=url.txt
7
8
9 [scan_seting]#扫描配置
10 ##扫描速度，由慢到快:sequential slow moderate fast， 速度越快，遗漏越多，则之相反。
11 scan_speed=sequential
12
13 #扫描时的Cookie，对所有url生效， 如不添加Cookie，请保持为空，即扫描器爬虫自动获取
14 #例子cookie=BIDUPSID=D40B5A304EFD449C3F8DED17FDF633A0; PSTM=1592016294
15 cookie=
```

另一个awvs批量脚本

场景：遇到大批量的目标时，例如可能一个项目有上k个网站时候，这个时候我们需要利用批量的扫描器来进行操作

链接：<https://pan.baidu.com/s/1TdJ59rAM4MeooolY9YslQ>
提取码：kuj1

1. 添加awvs的api与地址即可，同时扫描数看电脑的配置



```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
# author: evilchen

import requests
import json
import sys
from time import sleep
from requests.packages.urllib3.exceptions import InsecureRequestWarning
requests.packages.urllib3.disable_warnings(InsecureRequestWarning)

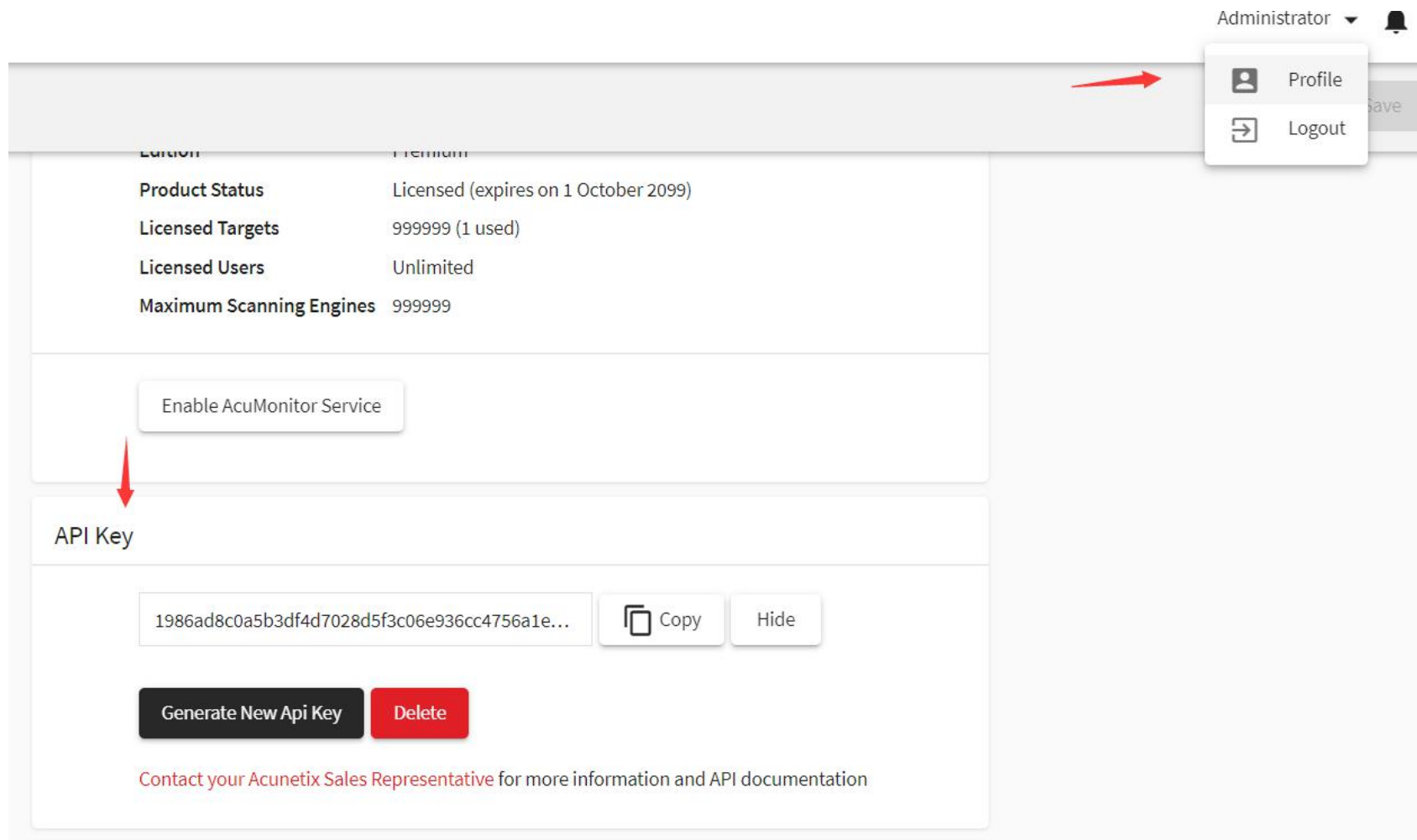
awvsUrl = ""
apikey = ""
scanCount = 2

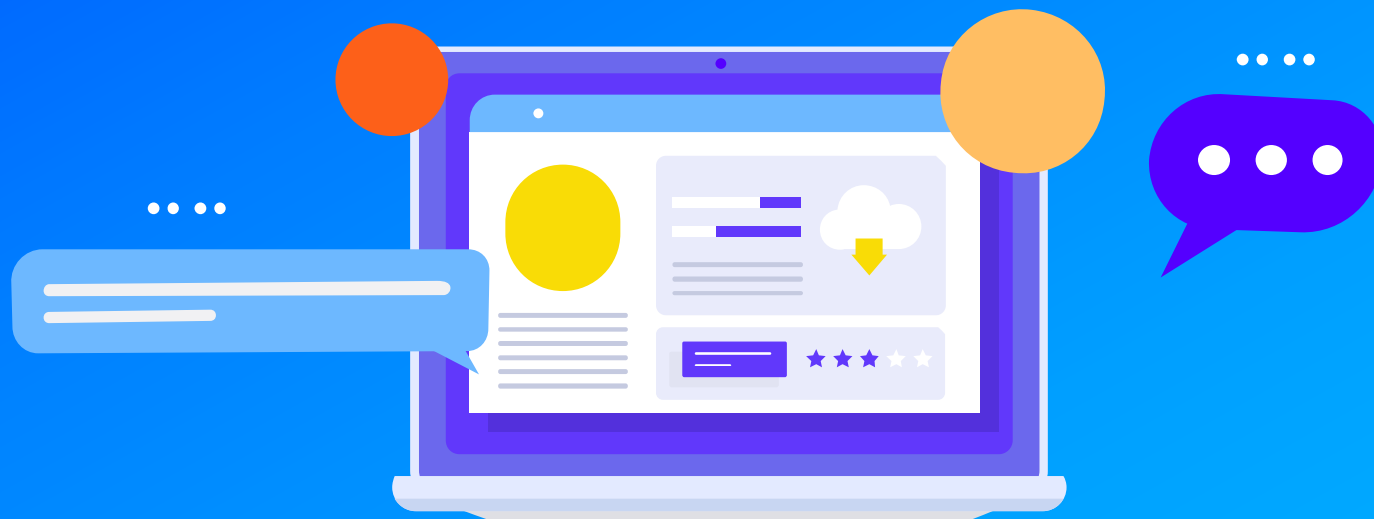
headers = {'Content-Type': 'application/json', 'X-Auth': apikey}

def addTarget(target):
```

The screenshot shows a Python script in a code editor. The script is for interacting with AWVS. It includes imports for requests, json, sys, and time. It also disables InsecureRequestWarning. The configuration variables are: awvsUrl, apikey, and scanCount. The headers are set to {'Content-Type': 'application/json', 'X-Auth': apikey}. The script defines a function addTarget(target). Red arrows point to the configuration variables with labels: awvs的url, awvs的apikey, and awvs同时扫描数量.

1. 添加awvs的api与地址即可，同时扫描数看电脑的配置





感谢聆听

湖南合天智汇信息技术有限公司

www.hetianlab.com