AWVS11提取规则文件

cymady / 2017-04-21 07:38:39 / 浏览数 26116 安全工具 工具 顶(0) 踩(0)

在这里给大家分享一个获取AWVS规则文件的思路。 目前我提取的是17年4月份的扫描规则。 后面如果规则更新，可以自行提取
官网: https://www.acunetix.com/vulnerability-scanner/wvs-demo-requested/
这是我提取复制进去可以直接用的
首先说一下为什么要提权规则文件。
扫描器的规则文件是扫描时用到的漏洞测试方法，用以验证漏洞是否存在，审核漏洞的效果也依赖于此规则是否完善。
所以一般在扫描器可以更新规则的情况下，有人也只更新规则文件，不更新扫描器的核心版本， 可以保证扫描效果即可。
而核心版本升级包可能会更新一些系统组件， 例如修复BUG， 增加功能， 优化性能等, 与验证漏洞关系不大。
话不多说，开始正题。
我这里的环境是将 版本11的扫描规则替换到 版本10.5中。
看下替换规则前的 10.5 的扫描规则。
安装完AWVS 11后， 找到脚本所在目录。
C:\Program Files (x86)\Acunetix 11 Trial\11.0.171101535\data\Scripts
替换到下面目录即可。替换前请自行备份。
C:\ProgramData\Acunetix WVS 10\Data\Scripts
11 与 10.5 的扫描规则对比：
测试下来有3个脚本因为缺少对应 xml 漏洞描述文件，所以执行完有报错。 我选择覆盖时忽略这三个文件。 其他照常, 执行完后没有报错。
Remote_File_inclustion_XSS.script
XSS.script
Javascript_AST_Parse.script 这个规则文件用旧版和新版都会报错，自己考虑要不要覆盖。
执行一次扫描看看：
扫靶机。
替换规则前的扫描结果：
High 90 Medium 58 low 9 info 24
对比替换后的扫描结果
High 88 Medium 55 low 9 info 34
有一些同学很暴力的替换了整个data 目录, 这种情况版本信息会正常显示11， 但我不保证没有问题哈。
C:\ProgramData\Acunetix WVS 10\Data\General
版本信息在C:\ProgramData\Acunetix WVS 10\Data\General\branding.xml。
因为我们替换规则没有替换这个文件， 所以启动后版本没有变化。
想替换的话，文件在这里。
[attachment=4944][attachment=4945]

branding.rar (0.0 MB) 下载附件
Scripts.zip (1.1 MB) 下载附件

上一篇：SQL注入过最新版本安全狗-201... 下一篇：老司机奇淫渗透测试让网站给自己发管...

1. 32 条回复

bigcow 2017-04-21 08:27:03

我一直很想知道wvs的插件是怎么编写的，要是有源码就好了，这些插件有些还是写的很好的，比方延迟盲注。

0 回复Ta


浪漫的大核桃 2017-04-21 08:29:13

楼主能不能。。规范一下帖子格式。。。里面有[size=font-size:14.0pt,14.0pt] 看着很吃力啊

0 回复Ta


cymady 2017-04-21 08:30:34

我用chrome 编辑了一段话， 重发就这样了， 正在重新编辑。

0 回复Ta


浊公子 2017-04-21 08:38:04

0 回复Ta

 浪漫的大核桃 2017-04-21 08:45:16

我感觉AWVS
新版可能更侧重于往SaaS那个方向发展，并且传统的基于爬虫的扫描器可能上升空间有限了。。因为漏洞的类型十几年来了基本都没有怎么变过.....

0 回复Ta

 紫霞仙子 2017-04-21 08:59:26

想想我之前还自己写规则，折腾了那么久

0 回复Ta

 三十九度风 2017-04-21 09:00:55

让我来试试水

0 回复Ta


cymady 2017-04-21 09:02:34

https://www.acunetix.com/blog/docs/creating-custom-vulnerability-checks/

下载官方的插件编辑工具 ， 可以看到官方插件的扫描/处理逻辑， 如果是自己写扫描器， 也可以参考借鉴。
用这个工具也可以自定义 插件放到AWVS里。

0 回复Ta


独自等待 2017-04-21 09:31:29

我还以为你已经提供了明文的特征呢。

0 回复Ta


风之传说 2017-04-21 11:59:19

首先得有10.5.。。。。我表示我的版本还是10.0 没有data目录。

0 回复Ta


hades 2017-04-24 02:27:29

10.5 网上应该有不少滴

0 回复Ta


finger 2017-04-24 05:16:34

测试失败，什么都扫不出来了。。

0 回复Ta


finger 2017-04-24 06:14:53

反复测试了 好几遍 还是很不正常

0 回复Ta


cymady 2017-04-26 11:00:30

贴一下报错看看。

0 回复Ta


0x 2017-04-26 16:30:12

楼主能否发下AWVS的漏洞测试网站

0 回复Ta


liumazai 2017-04-27 06:27:03

非常感谢

0 回复Ta


cover 2017-04-27 15:40:04

wvs 强在爬虫，虽然是全爬

0 回复Ta


酷帥王子 2017-04-28 01:53:51

我安装的是10.5的，但是没有data目录呀

0 回复Ta


酷帥王子 2017-04-28 02:45:28

找到了谢谢了，原来在2003服务器下会在一个很深的目录藏着而且用搜索搜不到的呢，还好在卸载的时候无意间看到那个目录了

0 回复Ta


hades 2017-04-28 03:04:26

C:\Documents and Settings\All Users\Application Data\Acunetix WVS 10\Data\Scripts

0 回复Ta


酷帥王子 2017-04-28 03:05:48

扫描出现一大堆错误，不知道为何，请楼主来解决

0 回复Ta


酷帥王子 2017-04-28 03:08:42

还有这个错误

0 回复Ta


any3ite 2017-05-02 07:53:33

11 的 pro 包 52 已经有了， 至于什么时候去 C 掉 并且放出来 看 52站长了。

0 回复Ta


jax777 2017-05-04 07:29:33

师傅 这个插件在我试了下awvs11，看不见官方的扫描处理逻辑了。师傅用的什么版本

0 回复Ta


cymady 2017-05-04 11:02:10

- http://testphp.vulnweb.com
- http://testasp.vulnweb.com
- http://testaspnet.vulnweb.com
- http://testhtml5.vulnweb.com

文中所测的网站是第一个。 http://testphp.vulnweb.com

0 回复Ta

cymady 2017-05-04 11:04:57

你确定你只覆盖了C:\ProgramData\Acunetix WVS 10\Data\Scripts　目录么， 不要整个Data全部覆盖。
如果是自己提取规则， 注意不要覆盖 以下三个文件， 因为新版的缺少漏洞描述，无法显示。
Remote_File_inclustion_XSS.script
XSS.script
Javascript_AST_Parse.script

0 回复Ta

cymady 2017-05-04 11:05:11

哥， 你这个不是错误。
这是漏洞汇总信息

0 回复Ta


cymady 2017-05-04 11:05:37

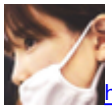
看不见官方处理逻辑是啥意思？
有报错的话贴一下图

0 回复Ta


jax777 2017-05-08 00:43:43

怎么穿不上去图片？
具体情况是哪个插件打开awvs11里的脚本时，显示跟普通记事本一样，都是显示了一些不可见字符，看不到逻辑

0 回复Ta


hades 2017-05-08 06:00:44

https://xianzhi.aliyun.com/forum/read/560.html 图片发帖攻略在此   有问题私信我联系方式

0 回复Ta


bma 2017-05-19 01:02:24

关键是脚本能搞出明文来不？

0 回复Ta


yexusky 2017-06-22 06:48:57

给力 强大 谢谢分享哦

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板