UNIS XScan-G 系列漏洞扫描系统用户 FAQ

用户 FAQ

目 录

1 软件类 FAQ

如何查看当前系统版本号?

登录系统，点击页面右上角的“  ”按钮，则会显示系统的版本信息，包括扫描引擎的版本和规则库的版本以及更新日期。

扫描策略是否可以实时更新?

系统在可以访问互联网的情况下，可以访问在线更新服务器，进行在线更新，如果有新版本，系统将会根据用户自己的设置显示是否提醒可升级版本。

在线升级启用后为什么没有进行升级?

请分别检查以下内容：

- 确认授权未过期。
- 确认已配置 DNS 及网关。
- 确认默认的升级地址没有被更改。

授权过期会有什么影响，如何解决?

授权过期后用户将无法进行升级操作，正式版本不影响漏扫的正常使用，试用版本需要重新导入授权才能正常使用。如需升级版本，联系紫光恒越技术有限公司重新导入授权。

2 业务功能类 FAQ

为什么配置了管理地址IP，PC却Ping不通?

在同网段中，PC 的 IP 地址与配置管理 IP 地址必须同属这一网段；在不同网段中，需要在漏洞扫描设备上添加相应的路由，确保与 PC 连通。

忘记管理口IP了怎么办?

漏扫管理口有两个 IP 地址，用户设置 IP 和内置固定 IP。用户设置 IP 可以修改，用户可以根据网络环境设置 IP 地址；内置固定 IP 是系统默认的，不能修改，用于配置漏扫网络。

系统默认内置固定 IP 是 192.168.0.1，可以通过 PC 或笔记本直连访问漏扫页面，修改其网络配置。

系统有哪些内置账户?

系统内置账户包括 admin\audit\scan\security 四个账户，对应的角色分别为系统管理员、审计管理员、扫描管理员、安全管理员，以下密码为默认密码，建议修改，避免安全隐患。

系统管理员：admin 密码：admin。

安全管理员: security 密码：security。

审计员：audit 密码：audit。

操作员：scan 密码：scan。

为何网络中真实存在的主机，扫描结果却显示不在线？

检查是否为跨网段扫描，中间可能有防火墙、IPS 等设置将漏扫发送的数据包丢弃。建议修改网络设备配置，漏扫发送的数据包都设置为放行。

在什么情况下，漏扫扫描Windows系统时能获得更多的信息？

请分别检查以下内容：

- 目标是否关闭了防火墙,关闭防火墙能获得更多信息。
- 需要猜测到具有管理员权限操作的用户口令。
- 能扫描本地漏洞的前提是：
  - 在服务列表中开启“可远程访问注册表”服务-Remote Registry。
  - Windows 2000/2003/2008 的帐号配置方面需要配置一个具有脆弱帐号的 Administrator 权限帐号。此时还需要在本地安全策略-安全选项中,开启匿名 SID 转换。
  - Windows XP/7/8 同样需要配置一个具有脆弱帐号的 Administrator 权限帐号。

同时，需要做以下两个配置：

- 在本地安全设置中，进入安全选项>网络访问>本地账户的共享和安全模式，设置为经典模式。
- 在本地安全设置中，进入本地策略>用户权利指派，在拒绝网络用户访问这台计算机的列表中删除 Guest 帐号。

系统漏扫如何进行深度扫描？

系统漏扫要进行深度扫描，需要新建任务时设置目标认证信息，在填写完〈扫描目标〉后，会自动出现认证设置，认证设置支持 SMB、SSH、TELNET 三种协议的认证，通过认证设置可以提高扫描精确度与深度，支持【导入认证】与【手动添加】两种设置方式。【导入认证】提供认证模板下载，根据模板格式填写相应的信息即可导入；〈手动添加〉通过下拉菜单选择目标地址，输入端口、用户名、密码等信息，完成添加认证。

导致漏扫产品扫描速度慢的原因有哪些？

大致有以下几方面原因：

- 有防火墙。
- 端口扫描范围设置过大。
- 扫描策略多。
- 主机并发数和扫描进程数量大。

目标主机或网站为什么不能被扫描？

目标主机或网站可以正常访问，但是不能被扫描。

请检查以下内容：

- 确认产品可扫描 IP 数是否充足，IP 列表是否有该主机或网站的记录。
- 确认任务所属用户的可扫描 IP 地址和 URL 地址是否有限制。

暂停后继续扫描该任务的起始时间如何计算?

暂停后，继续扫描该任务的起始时间仍为任务最初开始执行的时间。

任务设置接收报告的邮箱，为什么收不到扫描报告？

请检查以下内容：

- 确认已配置 SMTP，该邮箱是否开启 SMTP 服务。
- 确认已配置 DNS 及网关。

哪些扫描任务支持导出和报表下载功能？

系统扫描任务、Web 扫描任务和数据库扫描任务支持导出任务和报表下载。

系统运行一段时间后，发现部分系统日志和操作日志不见了，为什么？

在无手动删除的情况下，查看是否超过了保存该日志的时间。

漏洞扫描时被扫描网站应注意什么？

由于漏洞扫描会对目标站点的应用输入点进行各类测试，发送各类有可能导致应用异常的请求，如果目标站点的设备性能不佳，难以承载约十几人同时访问的流量压力，则最好与网站管理员协商在非业务时段进行扫描，或通知扫描人员降低扫描线程。

如果被扫描网站有 Web 应用防火墙等防护措施，监测平台则只能扫描评估目标站点的防护能力，如果需要检测目标站点代码层根源应用漏洞，则还是需要 Web 应用防火墙或抗 DDOS 等设备中开放平台的扫描 IP，允许其所有请求访问网站。

为什么扫描目标添加总是提示已存在？

同一个任务下添加多个扫描目标，扫描目标是根据协议头+IP+端口号来区分的，如 http://192.168.1.118/test 和 http://192.168.1.118/app 会被认为是同一目标，不允许重复添加。

为什么要进行COOKEI录制，如何录制？

扫描一些需要登录后才能继续访问的网站目标时，就需要进行 cookie 录制，因为用 cookie 录制更准确且效率高并能访问到更多的网页。

录制步骤：

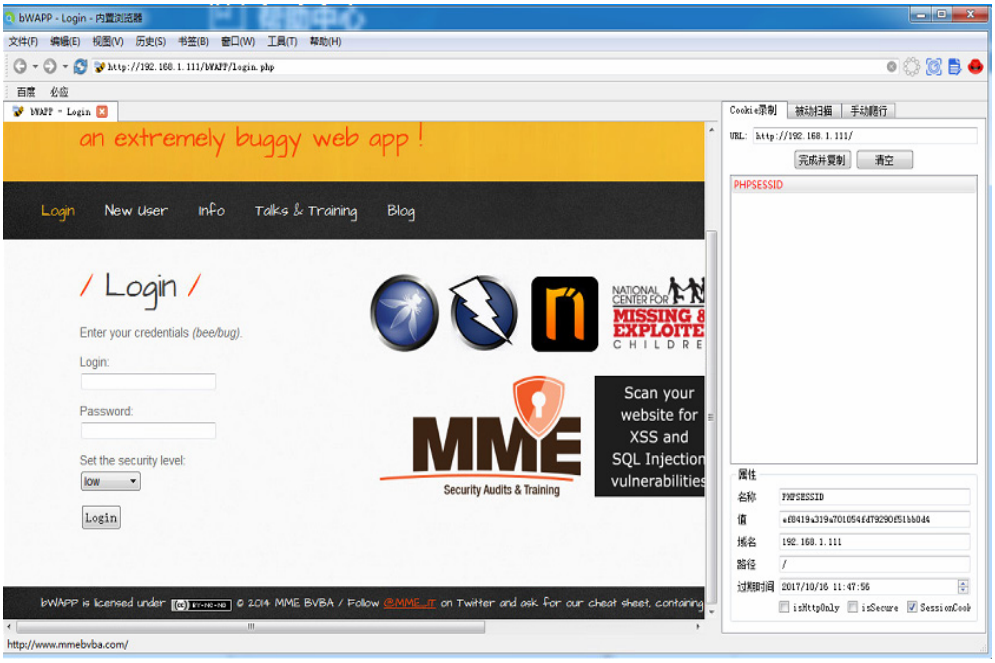
首先需要下载 web 漏扫专用的内置浏览器，如果已经下载并且是最新的内置浏览器则不需要再重复下载。下载步骤：新建一个任务，填写扫描的目标，然后点击

画红线的下载按钮则就会进入帮助中心页面，再点击下载相应的内置浏览器，一般建议下载

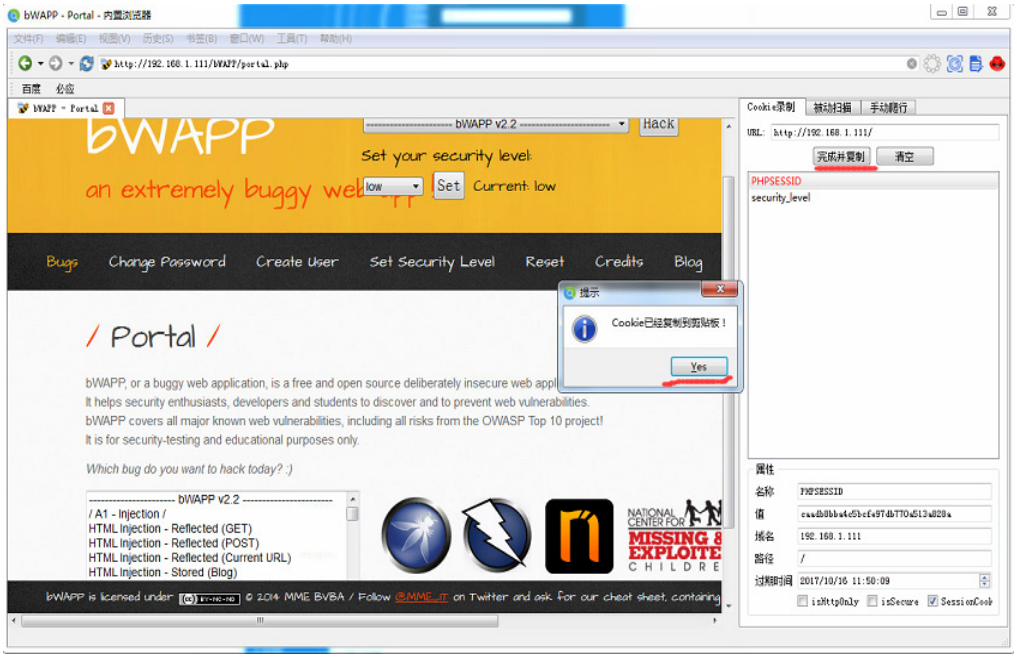
64 位的版本的浏览器。

解压下载的包，双击 LrBrowser.exe 以打开浏览器。

在地址栏输入要录制 cookie 的目标 URL，回车并进行 cookie 录制。



用户登录到目标站点进行扫描录制，点击“完成并复制”按钮。



注意点：“完成并复制”按钮下面的红色条目表示会话 Cookie，在关闭浏览器里此类 Cookie 将会被删除。若使用了 Cookie 录制且存在会话 Cookie，在任务结束前，最好不要关闭浏览器和相关标签页，关闭可能会产生不可预估的结果。

将保存好的录制粘贴到下表对应的项

如何进行手动爬行？

手动扫描是用户通过手动点击浏览器浏览 web 页面，扫描器会把符合项目扫描参数配置的 URL 添加到已扫描到的 URL 列表中。

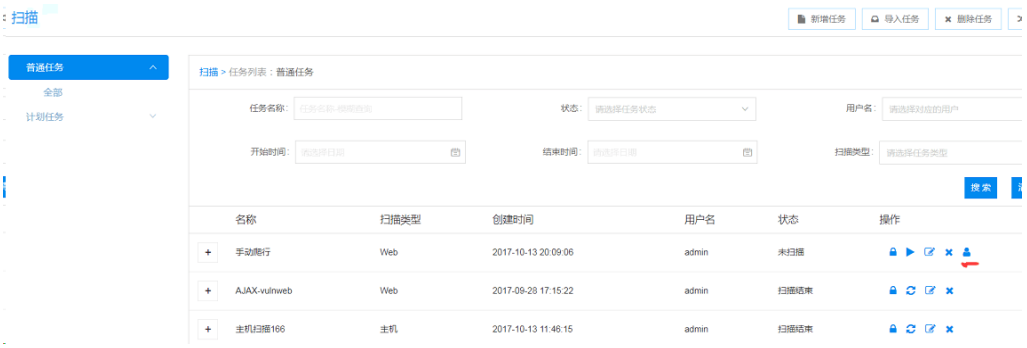
手动爬行步骤：

检查通讯配置，通讯地址是否是当前访问的扫描器 IP 地址，如果不是则需要改成当前访问的扫描器 IP 地址。

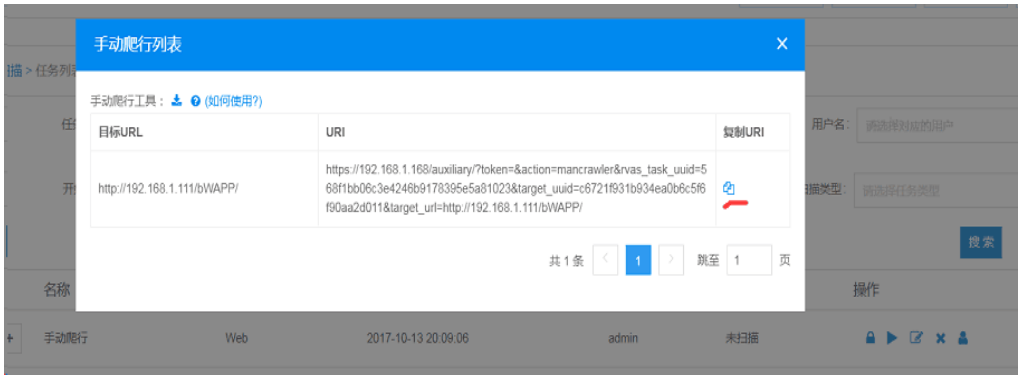
创建扫描任务，执行计划选择“暂不执行”。

输入扫描目标 url，选择扫描类型：“主动扫描”。

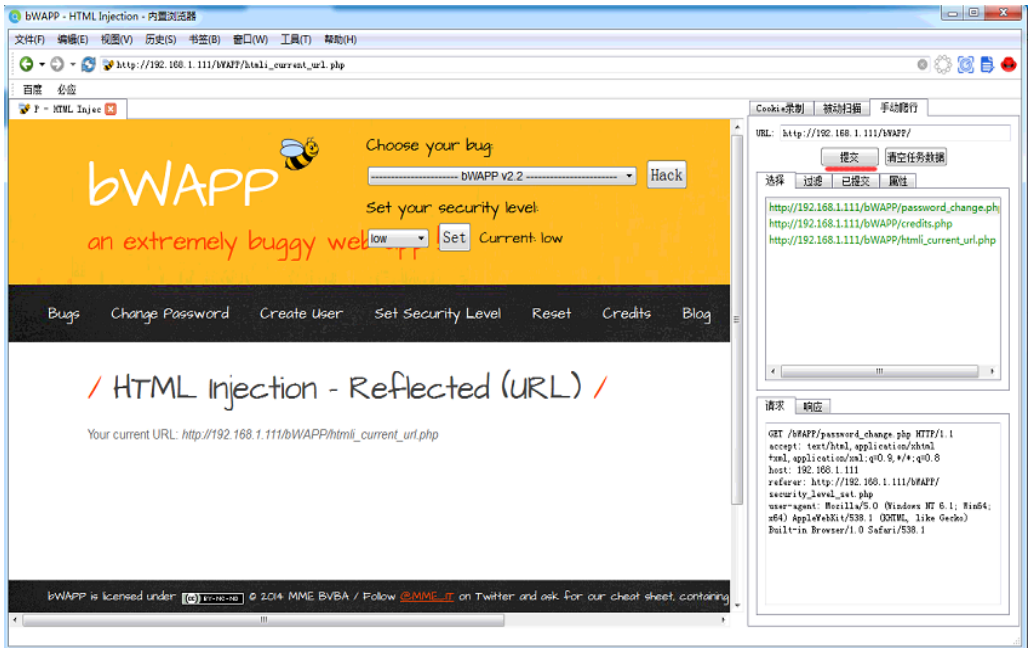
保存后，查看任务列表，点击任务右侧的手动爬行图标。



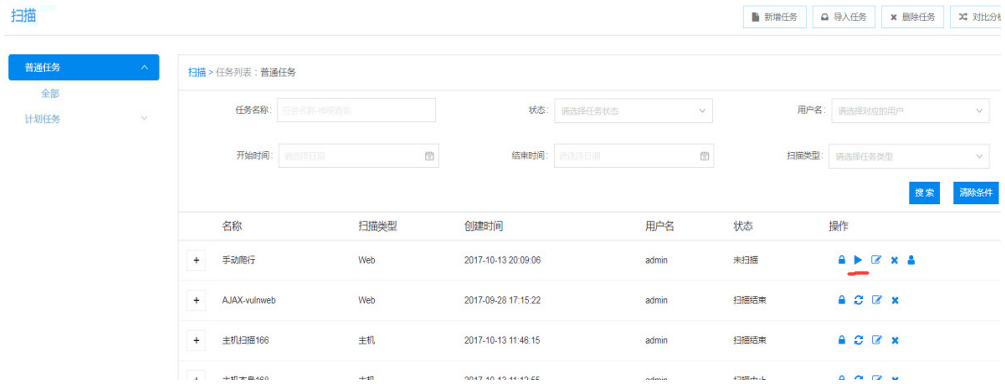
复制 URI 内容到剪贴板（一次只限一条）



将复制好的 URI 内容粘贴到内置浏览器的地址栏，并回车；通过内置浏览器用户进行手动点击想要检测页面的 URL，点击“提交”按钮，扫描器自动保存所有手动爬行的 URL（即保存提交按钮下面的选择下面的 url 链接）



点击运行扫描任务，则开始了手工爬行的扫描任务。



主动扫描与被动扫描的区别？

主动扫描是系统根据输入的目标 url 主动的去探测目标网站存在的 url 并进行扫描；被动扫描则是根据用户想要扫描的网站 url 进行扫描，用户可以自行挑选需要扫描的 url 进行扫描。

创建被动扫描任务或手工爬行任务时需要注意些什么？

同一时刻只准一个相同目标的 url 在进行被动扫描或手工爬行的浏览器上操作。

之前对目标 A 网站进行过被动扫描或手工爬行，现在又对目标 A 网站进行被动扫描或手工爬行任务，则需要确定下之前的扫描是否已经完成，如果完成了可以再对该目标 A 网站进行被动扫描或手工爬行但最好需要按下浏览器上被动扫描或手工爬行的“清空任务数据”，确保之前的扫描对本次扫描没有影响；如果没有完成则不应该对该目标再进行被动扫描或手工爬行任务。