鹰眼网站安全智能监控系统

产品白皮书

产品部 2016
360 企业安全集团
电话：86-10-82778244
传真：86-10-82779255
网址：http://b.360.cn
邮件：support@.360.cn

目录

1. 引言

随着电子信息化的高度普及，越来越多的企业开始建立自己的网站，通过网站对外发布信息，以及业务建设等。网站已经成为政企对外的一面镜子，折射出自身的形象，更是很多企业经济来源的主要基础。但是这面镜子在来自互联网的攻击面前却十分脆弱，很多企业由于自身官网被黑客入侵导致蒙受巨额经济损失，并严重影响了企业自身形象，造成用户流失、经济损失等一系列恶劣影响。

根据 360 网站安全检测平台数据，企业网站被黑客入侵情况十分严重，据统计，企业网站被黑客挂后门程序的比率高达 38.5%，也就是说 100 个企业网站中就有约 40 个被黑客植入了后门程序，可随意进行篡改、挂马和拖库。

现阶段，大多数企业网站本身安全隐患极多，很容易被黑客攻击。而黑客利用漏洞入侵企业网站则成为了一种越来越主流的攻击模式。企业网站存在大量的漏洞主要是有以下几个原因：

- **外包建站，代码质量差，缺乏后期持续的技术维护**

很多企业由于自身没有网站研发团队，将企业网站外包给建站公司制作，市面上很多建站公司开发水平参差不齐，更重要的是普遍的建站公司开发网站只考虑功能性，而不考虑安全性，在满足了企业网站的功能后便交付使用，此类网站很容易被通用的漏洞扫描程序检测出安全问题，从而进一步利用漏洞进行黑客入侵行为。由于是外包开发，当出现安全问题之后很难及时的修复安全漏洞，导致黑客可以长期控制企业网站服务器，将企业网站服务器变为黑客手里的“肉鸡”或者“跳板”，对企业自身的形象造成长期的恶意影响。

- **开源程序建站，缺乏安全运维意识**

目前市面上已经有许多开源的建站系统可供企业选择，常见的有 Dedecms，Discuz，phpcms 等。由于这些建站系统均是开源产品，意味着黑客可以通过研究这些开源建站系统的源代码来挖掘漏洞。当黑客挖掘到一个开源建站程序的漏洞时，通过结合搜索引擎技术，批量搜索同样使用这套程序的网站，实现批量入侵。一般来说，系统开发商发现有黑客利用漏洞进行入侵行为后会尽快开发响应的补丁来告知用户，但是很多企业网站缺少专业的运维人员或者站长缺少安全运维意识，没有及时安装补丁或者根本不关注厂商官网发布的补丁更新信息，导致存在漏洞的企业网站长期暴露在互联网上，成为黑客攻击的目标之一。

- **企业网站开发人员缺乏安全编程意识**

由于人的因素不可控，导致很多企业网站在开发过程中就引入了安全漏洞，这些漏洞在测试环节缺乏有效的安全测试，上线后可以被漏洞扫描器检测，引发后续一系列的黑客攻击。网站开发人员不了解安全编程的同时也不了解黑客攻击，此类安全隐患在不借助第三方防御机制的帮助下很难被发现和修复。

黑客入侵企业网站后，有可能会为企业带来巨大的损失。

- **核心资料外泄**

黑客一旦通过企业网站将木马植入企业员工电脑中就很容易进行内部渗透，继而取得更高权限，进行窃取企业核心资料等侵害行为。企业商业机密一旦外泄，将会给企业带来不可估量的巨大损失。

- **在线交易等风险带来的直接财产损失**

有电子商务业务的企业网站一旦被攻破，涉及财务的模块，企业收款账号等很可能被篡改，给企业带来直接的财产损失。

- **网站被篡改、挂马导致被安全软件拦截，损失商誉、名誉**

企业网站一旦被挂马、篡改等，就会被安全软件、安全浏览器拦截并提示风险网站，这样会对企业的商誉带来无形的损失。对政府部门也会造成名誉上的损失。

2. 用户所面临的问题

面对上述的种种威胁，企业也加强了对 Web 应用的安全建设。Web 漏洞扫描器作为主要的 Web 应用安全产品之一，其主要作用是事前预防，从根源发现漏洞、及时修补，预防威胁。但随着企业网站的逐渐扩大，用户使用的增多，一些问题也逐渐显现出来。传统的 Web 漏洞扫描器基于主动的蜘蛛爬虫技术，这就需要用户充分了解自己有哪些网站，同时爬虫的爬行深度、覆盖完整性、性能等问题也日益凸显。主要体现在如下几个方面：

2.1. 配置工作量大，易产生遗漏

传统的 Web 漏洞扫描器利用蜘蛛爬虫获取检测目标，这就需要事先搜集并录入完整的域名清单，而在实际的工作中网站运维人员并不能完整的知晓自己有哪些根域名、子域名、IP、业务系统等，同时对于日后新增的业务也无法及时的录入，形成空窗期或永久遗漏。

2.2. 无法扫描“孤岛”页面，扫描不彻底

传统的 Web 漏洞扫描器基于主动爬虫获取扫描地址列表，而受限于爬行深度和性能的影响，爬虫往往会设置一定的深度和数量范围，超过范围的页面将得不到扫描，故针对页面较多的网站传统扫描器存在天然的缺陷。同时，一些在网站上需要用户进行一系列操作才能触发的链接，也是传统爬虫无法爬取到的，即便是使用 Web2.0 蜘蛛，在这点上依然存在大量遗漏。

所谓“孤岛”页面，即在上述条件之外，还存在一些链接在公开网页中没有任何入口，是爬虫无法获取到的，如管理员后台、内部测试地址、备份文件、内部业务接口、移动 APP 后台等，上述“孤岛”地址中若存在漏洞传统扫描器几乎无法发现。

2.3. 无法及时发现网站漏洞，存在较大时间差

网络安全的本质是攻防对抗。主要体现在技术对抗、成本对抗、时间对抗。传统 Web 漏洞扫描器基于主动爬虫技术，通过定期按序爬取的方式搜集 URL。当有新业务上线时系统毫无感知，更无法做到实时精准扫描，故此在时间对抗中失去先机。期间一旦有漏洞被黑客发现并利用，很容易被攻击进而造成损失。

2.4. 导致网站不稳定或性能变差

传统 Web 漏洞扫描器基于主动的爬虫技术，在爬取时不仅占用大量的网络带宽，而且容易造成 Web 服务器的资源占用过高导致性能变差，对正常的用户访问造成影响。同时频繁的抓取页面会造成某一时刻网站的 PV 值偏高，为站长对网站的准确监控带来一定的烦恼。

3. 产品介绍

3.1. 产品概述

鹰眼网站安全智能监控系统（以下简称：鹰眼 WSIMS）是 360 公司自主研发的新一代 Web 安全监测系统。其通过旁路获取镜像流量，自动解析 URL 并添加到扫描任务中进行漏洞检测；也可手工添加网站 URL 进行针对性检测。除此还可利用域名匹配

和 IP 关联做到对未知站点的发现及检测，无需人工持续跟进，减少人工工作量的同时，极大的提升了网站的整体安全。

3.2. 设计理念

3.2.1. 极简操作，避免遗漏

随着网站数量的增多，安全事故的频繁发生，对网站运维人员的要求也越来越高。鹰眼 WSIMS 利用流量解析技术，可以做到域名自动发现。仅需简单的操作即可实现漏洞扫描、即刻生成结果，并给出详细的修复建议。省去了人工搜集、录入、修复困难的烦恼。站点覆盖范围更广，更大程度的避免了遗漏的可能。

3.2.2. 自动发现，全面监测

网站业务的不断更新迭代，为避免“漏扫”总是需要网站运维人员持续的跟进各种新上线的业务。鹰眼 WSIMS 可以利用域名匹配和 IP 关联发现企业中新上线的业务，让运维人员省去追着业务跑的局面。即使不在该链条下的未知或孤岛页面，也可轻松发现。做到未知站点监控及网站业务的全面检测。

3.2.3. 低干扰，高效率

传统的 Web 漏洞扫描器基于主动的蜘蛛爬虫技术，需要不定期的到目标站点进行链接爬取。而在这过程中相当于一个快速循环访问的过程，对目标服务器的性能及稳定性都会造成一定的影响，因此更无法做到实时检测。鹰眼 WSIMS 凭借自身解析 url 技术，无需到目标服务器中进行爬取，不会对目标服务器造成任何影响。另外，依靠精准的定向检测技术，做到访问即扫描，无需等待，即刻生成结果。在与黑客的时间对抗中提供有力保证。

4. 产品功能

4.1. 域名、IP 管理

鹰眼 WSIMS 可通过流量自动解析 url，利用特殊算法将 url 进行分解，提取出顶级域名作为根节点。一键添加后可全面覆盖所有相关子域，保证了网站的全面检测。同时可以根据需要有选择性的添加子域，为快速有效的检测提供便利条件。IP 管理，利用解析到的 host 信息可提取出 IP 信息，添加扫描后，会根据 IP C 段进行自动关联，将所有 C 段相同的 IP 进行分组，不仅可以有针对性的加入检测，也可以从中发现未知站点。

4.2. 检测策略管理

鹰眼 WSIMS 默认支持 SQL 注入、跨站脚本攻击（XSS）、设计错误、文件包含、代码执行、文件上传、信息泄露、权限许可和访问控制、跨站请求伪造（CSRF）、路径遍历、配置错误等漏洞类型的检测，同时也可根据需要，配置严重等级更高、威胁更大的潜在漏洞的检测策略。为保证用户服务器的可用性及稳定性鹰眼 WSIMS 支持多重检测策略的配置。如 POST 漏洞检测、暴力破解检测、破坏型 SQL 注入检测。

独有的命令执行盲打检测和跨站盲打检测，可依靠 360 或企业自己搭建的回连地址在无任何危害的情况下发现更多的潜在漏洞。如存储型跨站漏洞等等。

4.3. 任务控制管理

鹰眼 WSIMS 可根据网站、带宽等关键因素的负载情况，自动调整扫描策略和强度，避免对网站的业务连续性造成影响。除此还可进行多种任务配置以满足用户的各种实际需求。为避免短期内对同一 url 进行多次扫描而造成的资源浪费，可配置 url 级周期性扫描任务，也可配置域名级的周期性扫描任务，以免因单位时间内检测频率过高而影响网站服务器的稳定性。独有的内网 IP 自动发现、自动识别、自动添加的功能，做到全面检测的同时也节省了人力成本。除此之外还提供了扫描任务手动启停等功能。

4.4. 漏洞信息展示

随着漏洞类型的逐渐增多，漏洞利用的手段也呈多样化发展。普通的安全人员即使知道了漏洞结果，但由于没有专业的经验积累，也是无法做到漏洞的有效验证。鹰眼 WSIMS 依靠 360 独有的攻防研究团队，利用专业的攻防经验深入简出的提供了漏洞的详细信息，即使没有专业的经验积累，也可以轻松的进行漏洞验证，根据详细的解决方案修补漏洞。特别的，鹰眼 WSIMS 提供了一键式漏洞验证功能，直接即可根据返回的结果判断漏洞存在与否。做到漏洞发现、漏洞确认、修补建议的闭环管理。

4.5. 数据报表

为配合网站运维人员下发及上报检测结果，鹰眼 WSIMS 可查看并导出多种格式的不同维度报表。支持漏洞列表的全量导出，依据用户业务的需要可自定义时间段导出单域名或全部域名的漏洞信息，其中包含漏洞的全量详细数据，可导出漏洞等级分布、漏洞类型分布 TOP10、域名漏洞数量统计的结果信息。支持的格式有：Excel、PDF、Word 等。帮助运维人员掌握综合漏洞信息的同时，又方便将结果进行分发审阅。

5. 部署拓扑

5.1. 单机部署

根据需要，可部署在企业的办公区、对外的网站机房或 IDC 机房处，以旁路接入的方式部署在待检测 Web 服务器流量经过的交换机处即可。如图所示：

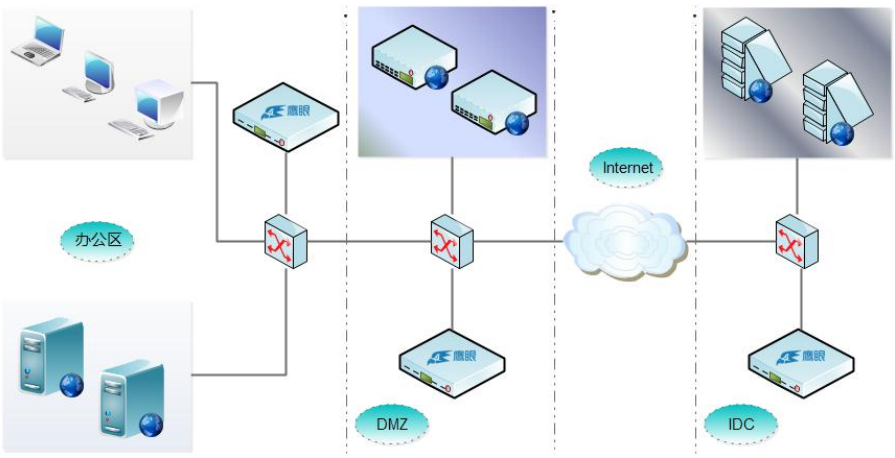

图-1　单机部署拓扑图

5.2. 多级分布式部署

鹰眼 WSIMS 支持多级分布式部署，统一管理。此种部署方式适用于上级监管部门对下级网站进行监督、评测、考核。通过鹰眼 WSIMS 的分级部署，能够在上级对全网漏洞进行综合展示及查看漏洞的修复情况。如图所示：

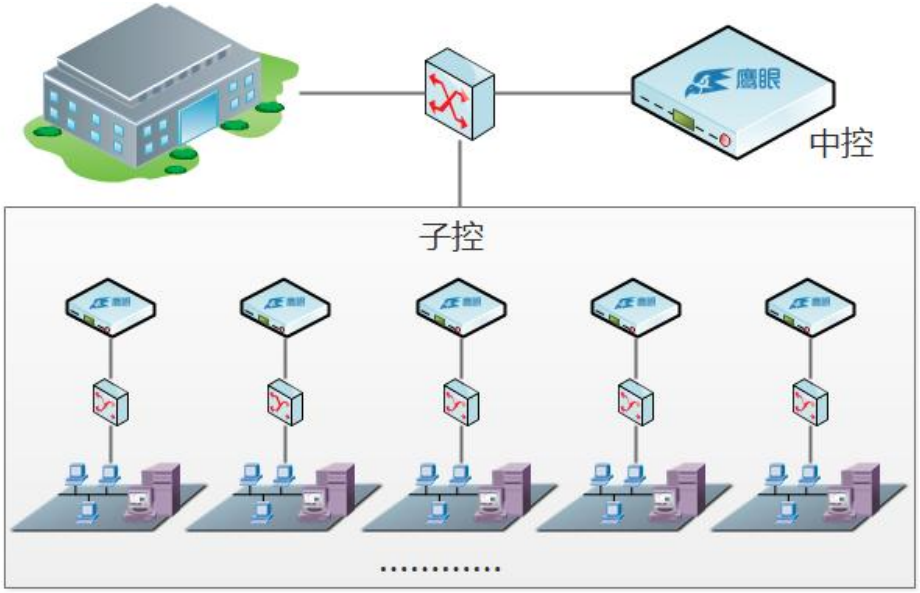

图-2　级联分布式部署拓扑图

6. 产品优势

6.1. 域名管理更便捷

鹰眼 WSIMS 通过旁路镜像，解析 url。可自动提取出一级域名作为根节点，如“*.360.cn”。一次添加后即可覆盖到全部相关子域及匹配的 url。当后续有新业务上线时，只要与该域名匹配，也会自动加入扫描。

传统的 web 漏洞扫描器基于主动的爬虫技术，只能通过一个顶级域名向下爬取 url。这就需要人工搜集域名并且手工录入，有一点遗漏就会影响网站的整体安全。并且当有新业务上线时需要业务人员及时通知，再次手工录入。如果传达不及时或忘记通知，就会形成遗漏，埋下安全隐患。

6.2. 全面的发现策略

网站安全可以理解为木桶效应，有一块短板就会对网站的整体安全构成影响。鹰眼 WSIMS 依靠流量解析 url，无需考虑是已知站点还是未知站点，或是孤岛页面，只要有访问，都可精准定位，即刻检测。利用独有的域名匹配和 IP 关联双重的发现机制，能够帮助网站运维者发现未知站点的存在，当有私搭网站被访问时可做到及时发现、区分展示，直观呈现。对提升网站的整体安全提供有力保证。

6.3. 高效的检测机制

网站被攻击的根本原因就是黑客先于我们发现并利用漏洞，最终达到信息获取、网页篡改等目的。这时时间对抗就显得尤为重要。鹰眼 WSIMS 利用自动解析 URL 技术，可做到访问即检测。不仅定位更精准，而且检测周期更短，根据用户配置可做到实时扫描。告别传统 Web 漏洞扫描器的扫描周期过长无法及时发现漏洞的问题，为网站的整体安全在时间对抗中提供有力保证。

6.4. 网站服务更稳定

鹰眼 WSIMS 凭借着技术创新，解析流量后本地还原 URL，与 Web 服务器没有任何交互，不会对网站的稳定性及性能构成任何影响。保证了网站的稳定运行。除此之

外，鹰眼 WSIMS 检测引擎源于 360webscan，其已连续为 200 万网站进行过漏洞检测，页面累计 17 亿。如今与鹰眼 WSIMS 整合后，采用嵌入式系统，通过内核级优化，具有更好的性能、稳定性和安全性。通过精心优化的检测规则及自适应的检测机制，使得鹰眼 WSIMS 能够在保证准确性的前提下，尽可能地降低扫描全过程对目标站点的干扰，保障网站业务持续稳定运行。

6.5. 大而全的漏洞库

鹰眼 WSIMS 凭借 360 独有的漏洞响应平台，通过上万名网络安全人员的不断挖掘、精挑细选建立的通用漏洞库。不仅支持 OWASP 公布的 TOP10 网络应用漏洞，而且能够全面检测 Web 服务的安全配置合敏感内容。借助专业的检测技术和上千种国内外应用系统漏洞，检测准确率高达 95%，有效保证了鹰眼 WSIMS 的漏洞发现能力。

6.6. 移动终端 APP 后台服务检测能力

智能手机的兴起催生了移动 APP 产业的快速发展。然而在快速发展的背景下，病毒、后门、盗取用户信息等行业乱象也成为人们所关心的问题。大量移动 APP 通过 Web api 服务的方式与服务端进行交互，此种模式也将移动安全与 Web 安全捆绑在一起。但由于部分应用不是直接将网页嵌入在 APP 中，导致爬虫无法获取链接，进而无法完成检测。鹰眼 WSIMS 凭借着技术创新，利用流量解析能够解析到移动 app 中嵌入的 URL，进而检测到移动 app 服务提供商自身的安全漏洞。填补了传统 Web 漏洞扫描器对移动 app 后台无法检测的空白。

7. 用户价值

7.1. 节省人力成本，提升运维效率

无需人工搜集域名，手工录入等工作。鹰眼 WSIMS 利用流量解析，自动还原 url 可以帮助网站运维者做到自动搜集、自动整理、一键式添加顶级域名，即可做到网站的全部覆盖。后续有新业务上线也无需二次搜集，利用域名匹配和 IP 关联即可做到自动发现、自动检测。结合多种多样的报表、详细易懂的漏洞结果，方便运维的同时大大提升了运维人员的工作效率。

7.2. 网站覆盖更广，告别遗漏烦恼

鹰眼 WSIMS 可根据访问精准定位到任意页面，无需考虑网站的深度广度，及未知、孤岛页面。保证了对网站的全面发现、全面检测。同时依靠鹰眼 WSIMS 独有的监控技术，能够做到精确定位、区分展示、直观呈现，帮助运维人员发现私搭网站的存在，保障网站整体安全的同时，无需担心遗漏的烦恼。

7.3. 高效与稳定并存，使用更安心

从以往的经验来看，扫描器在发现漏洞的同时也会对网站的性能及稳定性造成一定的影响。这就使得用户产生了用与不用的矛盾心理。鹰眼 WSIMS 利用技术创新，自身还原 url 的特点，无需对网站进行爬取。另外，凭借其精准定向的技术特点，做到访问即扫描，配合自适应调节的均衡并发数，即可做到高效检测的同时，保证网站的持续稳定的运行。

7.4. 详细的检测结果，辅助修复

详细的漏洞检查结果，帮助运维、开发人员更好的分析漏洞原因。通过 360 安全专家深入浅出的解决方案，无需过深的专业知识，即可完全理解。辅助运维及其他相关人员分析、修复已发现的漏洞，提升网站安全。