RACETEC® 锐西科技

零信盾产品白皮书

Web业务的虚拟堡垒

锐西版权所有

锐西科技 | 2024

前言

锐西科技（北京）有限公司是一家数字安全创新技术服务提供商，于 2016 年创立，总部位于北京，在长沙和沈阳设有产品研发和运营中心，在广州、厦门、郑州、太原、昆明、贵阳、南宁、拉萨等中心城市设有机构办事处。

公司以“聚焦业务安全的持续运营，致力于成为客户背后的数字安全专家”为经营理念，专注于为政府、企业等提供基于零信任理念的数字安全解决方案，赋能更加高效、智慧、安全的数字化应用场景和安全托管运营服务。

公司依托核心技术优势、丰富实践经验和前瞻性发展战略，通过安全原生创新和场景化创新，构建了以零信任、托管运营服务两大战略为核心的产品及服务体系，覆盖云安全、身份安全、业务安全、数据保护多个领域，已经在网站群隔离防护、政务服务基层延伸、应急办公安全接入等多个应用场景帮助客户建立起自主可控的安全防御体系，实现无边界业务数据安全保障。

公司经过长期的技术积累获得了多项发明专利，通过 ISO9001、27001、20000、14001 和 45001 等质量体系认证，荣获国家高新技术企业证书、中关村高新技术企业证书，是云安全联盟大中华区(CSA GCR)会员单位，拥有信息安全风险评估、安全集成和安全运维服务资质。

公司秉承诚信、精技、高效、创新的企业精神，以质量为基石，以客户至上为核心，专注产品创新与卓越服务，得到了政府、财政、卫生医疗、运营商等国内行业客户的认可和信任。

未来，锐西科技将继续坚持以创新技术驱动业务数字安全为理念，用工匠精神撑起安全创新情怀，探索技术创新，助推政府和企业数字化转型发展进程，提升业务安全主动防御水平，用零信任理念赋能每一个客户。

锐西版权所有

目 录

锐西版权所有

锐西版权所有

1. 背景

1.1. Web 安全防护不可忽视

在当今数字化时代，互联网的快速发展使得 Web 应用成为了政务、企业和个人进行业务交流、信息共享的核心平台。然而，随着 Web 应用的广泛普及，网络安全威胁也日益严重，给这些重要业务带来了前所未有的挑战。一份来自某国际知名咨询公司的分析报告指出，在调查的企业数据中心中，92%的 Web 应用存在安全缺陷，80%存在跨站攻击的风险，而高达 62%存在 SQL 注入漏洞。攻击者利用 Web 应用的安全漏洞，肆意窃取用户数据、篡改网页内容或植入恶意代码，给企业和个人带来了巨大的经济损失和声誉损失。

对于政企用户而言，Web 应用不仅是其业务运营的重要支撑，更是其对外形象和公信力的展现。一旦遭受攻击或数据泄露，不仅会导致业务中断或服务降级，更可能引发公众信任危机和社会舆论压力。如何在不断变化的威胁情景下保持防御，是每家拥有网络业务的企业都面临的挑战。因此，政企用户对 Web 应用保护的关注程度非常高，更为迫切地需要一款能够提供全面防护、易于使用、快速部署和高性价比的 Web 应用保护产品来确保其 Web 应用的安全性。

1.2. Web 安全防护面对的挑战

1.2.1. 传统安全模式陷入“马后炮”的防护困境

随着网站攻击事件的频发，许多企业发现传统的安全防护模式已无法满足当今复杂多变的安全威胁。这种传统的安全防护模式存在着诸多隐患，导致企业陷入了一种“马后炮”的防护困境。

在传统的安全防护模式中，大多数是基于“规则检测”实施的防御措施，这种防护措施依赖于经验的积累和已知的威胁情报，仅能够防御部分的已知攻击行为，无法做到 100%的风险识别，更无法提前发现问题并开启主动防御能力。这就如同“事后

诸葛亮”一般，在发生攻击威胁之后才采取的防护手段，无法有效应对持续演变的威胁。

与此同时，Web 应用的源代码没有做到真正的隐藏，使得源代码一览无余的提供给“黑客”，这些资源对任何人都可见且能够被轻易的分析，为“黑客”实施漏洞挖掘提供了可进出的大门，使得 Web 应用变得脆弱和透明，缺乏有效的隐身保护。

另外，Web 应用中包含了众多可攻击的资源与第三方框架，资源与框架相对通用，缺乏安全因素的考虑，如同给“黑客”提供了一个攻击模板，在同类资源框架上进行复制攻击，这无疑增加了防护难度，使得传统的安全防护模式更加的捉襟见肘。

传统的安全防护模式在面对不断演变和复杂的 Web 威胁时显得力不从心。

1.2.2. 新型攻击手段不断涌现

在数字化时代，Web 应用的安全防护面临着不断演变的新型攻击手段，这些攻击手段对传统的安全防护手段构成了严峻的挑战。尽管已经有了如网页防篡改、Web 应用防火墙（WAF）、IDS/IPS 和 VPN 等手段来提高安全性，但这些手段在面对高级黑客的新型攻击手段时仍然显得力不从心。

高级黑客能够绕过传统的安全设备的检测机制，传统的防护手段在面对这种攻击时显得无能为力。这种绕过行为让攻击者能够轻易地获取未授权的数据访问权限，对企业的数据安全构成严重威胁。

针对软件供应链的攻击和 0/N Day 利用也是高级黑客常用的手段。这些攻击利用软件中未知的安全漏洞，在软件厂商发现并修补这些漏洞之前就发起攻击。这种攻击方式具有极高的隐蔽性和破坏性，使得传统的安全防护手段难以应对。

此外，跨站脚本攻击（XSS）、机器人攻击和 DDoS 攻击也是常见的攻击手段。XSS 攻击利用用户的浏览器执行恶意脚本，窃取用户信息或改变用户界面；机器人攻击利用大量恶意流量导致服务无法正常提供给合法用户；DDoS 攻击则是通过大量恶意流量的涌入来耗尽服务器的资源。这些攻击方式都对 Web 应用的安全性和稳定性构成了严重威胁。

锐西版权所有

1.2.3. 复杂安全威胁，持续网络攻击日益严重

随着黑客技术的不断进步，Web 应用遭受的安全威胁也变得越来越复杂和严重。这些威胁包括持续演变的攻击手法、多样化的攻击向量、专业化和商业化的黑客以及新型的零日漏洞利用等。

(1) 威胁持续演变：攻击手法不断演变，使得预测和防范变得困难。攻击者不断寻找新的漏洞和弱点，利用各种技术和手段进行攻击，使得防御变得更加困难。

(2) 攻击的向量也在不断多样化：传统的攻击主要集中在服务器端，但随着 Web 应用的不断发展，攻击者开始利用客户端、API 等渠道进行攻击。这使得防御的范围变得更加广泛，需要全方位地进行防护。

(3) 黑客服务专业化和商业化：即使是非专业人士也可以通过购买黑客服务来发起攻击，这使得安全威胁变得更加复杂和难以防范。

(4) 零日漏洞利用的兴起：零日漏洞利用的显著增加带来了巨大的补丁管理挑战，尤其是在具有遗留系统的企业中，出于不同的目的，企业总有一些正当的商业理由来维护这些遗留系统。打补丁说起来容易做起来难。大大小小的供应商发现很难跟上发现漏洞的速度，导致了从发现、报告的实际漏洞到供应商修补再到消费者修补这段时间的长期摩擦，给攻击者更大的利用机会。

这些威胁使得传统的安全防护手段无法有效应对，从而导致了持续的网络攻击日益严重。

1.3. 用户需求

1.3.1. 高效可靠的安全防护方案

随着大规模网络安全事件的爆发，例如网站遭受境外组织攻击、高危漏洞注入构造恶意请求等。用户已深刻意识到在日益增长的网络威胁面前，一个高效可靠的安全防护解决方案是保卫他们的 Web 网站不可或缺的防线。不仅要自动识别各种形式的

锐西版权所有

网络攻击行为，如爬虫攻击、SQL 注入、跨站攻击、敏感信息窃取等，而且能够及时进行有效防御，防止安全事件发生。当面对新出现的威胁时还能够迅速响应，保持对新安全风险的抵御能力。

1.3.2. 实时防护的紧迫性需求

随着网络攻击的日益频繁和复杂，实时防护的紧迫性愈发凸显。用户期望能够获得一个能够全天候 7*24 持续监测的防护系统，以应对各种有害的网络行动。需要具备高度的敏感性和准确性，能够及时地识别并响应有害的网络行动，尤其是那些新出现的和未知的威胁。

由于网络攻击往往具有突发性，一旦发生，可能会在短时间内对网站造成严重的危害。一个能够快速反应的防护系统，在攻击发生时能够迅速采取措施，防止或减轻损失。这种快速反应能力对于保证网站的持续安全运行至关重要。

1.3.3. 降本增效的运营模式

随着 Web 应用的快速发展，Web 应用防护的硬件和软件成本已经成为企业运营的一大负担。用户更希望的是能够在不牺牲防护质量的前提下，显著减少硬件和软件的直接成本，能够利用先进的技术来降低长期的运营维护开销，配置简单，管理维护方便。

与此同时，要能够提供智能报告和分析能力，帮助快速洞察安全态势，优化安全策略和响应措施。

1.3.4. 满足安全合规性要求

网络攻击行为愈演愈烈，随着国家将网络安全上升为国策，Web 网站防护在满足法律法规的合规性要求方面将面临更高要求。用户期望产品能够帮助他们轻松达到甚至超过这些合规性要求，减少因合规失败带来的法律风险和罚款。同时，能够更好地应对重保、HW 等攻防演练的考验。

锐西版权所有

1.4. 当前行业发展趋势

Web 安全防护是网络安全领域中的一个重要细分市场。随着网络攻击的日趋频繁和复杂，Web 安全领域不断发展，以满足日益增长的安全需求。

当前主流的 Web 安全防护的技术手段主要包括：防火墙技术、内容过滤技术、访问控制技术、远程浏览器隔离技术等。而远程浏览器隔离（RBI）技术是近几年出现的一种新的网络安全防护技术，通过将网页内容加载到远端浏览器上，在远端的浏览器上执行渲染后，将渲染的结果以图像的方式传到用户端浏览器上显示。即使网页中存在恶意代码，也攻击不到用户，彻底消除了用户受攻击的可能性。此外，远程浏览器隔离（RBI）还有数据防泄密的好处，企业的敏感数据也只能存在于远程浏览器上，无法下载到本地。

Gartner Research 的一份名为“远程浏览器隔离的创新洞察”的研究报告对当时的 RBI 技术进行了深入调研。报告中指出，公共互联网是一个充满攻击的环境，许多攻击都是通过日常的浏览网页或点击电子邮件中的 URL 等行为传递给企业用户。攻击者经常能够绕过传统的预防性控制措施，如基于签名的恶意软件扫描、防火墙和安全 Web 网关（SWG）等。基于浏览器的攻击是攻击者利用合法用户作为主要威胁载体的一种方式，易受攻击的 Web 浏览器和插件是攻击者的主要目标。无论我们认为自己在修补和阻止攻击方面做得有多好，这种威胁仍然存在。

报告强调了 RBI 技术的价值，并指出该技术可以作为一种有效的解决方案来解决这些问题。通过将用户的浏览器会话运行在远程隔离环境中，RBI 技术能够减少潜在的攻击面并增强安全性。这种方法可以防止恶意软件和攻击者直接访问用户的本地系统，从而减少恶意代码的执行和数据泄露的风险。

为解决 Web 安全防护的核心问题，锐西科技基于“远程浏览器隔离”技术，结合 HTML5 渲染技术和容器技术，打造自主可控远程浏览器隔离技术的安全防护产品——RACE Web 应用保护系统（零信盾）。

锐西版权所有

2. 产品概述

2.1. 产品介绍

RACE Web 应用保护系统（以下简称：零信盾）突破传统静态规则防御的思维，国内首创“Web 应用隔离保护”概念，其技术核心是远程浏览器隔离技术、容器技术以及 Html5 渲染技术的结合，将 Web 应用的“安全防护关口前移”，对网站或 Web 业务系统进行安全防护，彻底隔离攻击源，实现针对 Web 应用的“绝对”安全防护。

2.2. 产品架构

产品总体分成四层架构：包括数据存储、核心引擎、功能应用、用户交互以及管理平台。

(1) 数据存储：结构化数据存储在 MySQL 数据库中，主要包括：系统配置数据、操作审计日志、统计分析数据。为了提升存储和查询效率，日志数据存储在 NoSQL 数据库 Elasticsearch 中，主要包括访问日志、下载日志、攻击日志等数据。

(2) 核心引擎：容器调度模块为每个用户分配一个专属容器，在专属容器中运行远程浏览器引擎，为用户提供网站隔离访问服务，通过 Websocket 协议与用户交互层实时通信；网关服务实时接收用户本地浏览器发过来的操作指令请

求，进行合法性验证和解密，操作指令解析引擎再将其解析成正常的 http/https 访问请求，通过私有 DNS 域名解析后将请求转发给网站服务器，私有 DNS 接收到网站服务器的响应后由远程浏览器引擎将所有活动脚本执行完，自定义页面渲染引擎将执行完的网页转换成视觉编码，再发给用户本地浏览器，实现网页的访问。

(3) 功能应用：主要用于隔离未知攻击方式、自动化攻击源、服务器通信、Cookie、注入式攻击、Webshell 功能。

(4) 用户交互：运行在用户本地浏览器上，通过 Websocket 协议与核心引擎层实时通信，用户无需安装任何插件。操作指令采集器采集鼠标键盘输入事件，操作指令编码器将操作指令编码成核心引擎层可识别的私有机器语言，操作指令发送器将私有编码的指令请求发给核心引擎层；接收核心引擎层反馈的响应，对视觉编码流量进行解码，利用 html5 技术将解密后的流量渲染成网页镜像，并通过 diff 算法计算出网页的实时变化，实现网页的访问以及实时操作回显。

(5) 管理平台：管理平台是管理员的操作平台。通过管理平台进行安全防护与分析、监控、配置管理、健康检查、操作审计日志、操作审计日志、用户管理等操作。

2.3. 技术实现

2.3.1. 远程浏览器隔离技术

远程浏览器隔离技术主要基于 Chromium 开源项目、WebSocket 协议、HTML5 技术、容器技术等技术进行开发。

(1) 基于 Chromium 开源项目：

远程浏览器隔离技术基于 Chromium 开源项目，实现远程浏览器视觉编码抓取和事件分发。Chromium 是一个广泛使用的开源浏览器项目，提供了丰富的渲染和交互功能。通过使用 Chromium，远程浏览器隔离技术能够确保网页渲染和交互的准确性

和性能，为用户提供流畅的浏览体验。

(2) 基于 Websocket 协议：

远程浏览器隔离技术利用 Websocket 协议实现自适应远程浏览视觉流传输子协议。Websocket 协议允许双向实时通信，使得远程浏览器的用户体验与原生浏览器的体验保持一致。通过 Websocket 协议，远程浏览器隔离技术能够高效地传输网页内容和用户操作事件，确保实时性和准确性。

(3) 基于 HTML5 技术：

远程浏览器隔离技术使用 HTML5 技术实现网页的高速渲染。HTML5 作为现代 Web 开发的标准化技术，提供了丰富的功能和接口，如 Canvas 和 SVG 等图形渲染工具。通过使用 HTML5 技术，远程浏览器隔离技术能够加速网页的渲染速度，并在客户端使用 HTML5 进行高速重绘，提供流畅的用户体验。

(4) 基于 HTML5 技术的用户操作模拟：

远程浏览器隔离技术使用 HTML5 技术抓取客户端的键盘、鼠标事件，并进行编码。这些事件通过 Websocket 私有子协议传输到远程浏览器中，模拟用户的操作。这种方式确保了用户在远程浏览器上的操作与本地浏览器一致，提供无缝的交互体验。

(5) 基于容器技术的分布式调度系统：

远程浏览器隔离技术基于容器技术（如 Docker）开发了远程浏览器分布式调度系统。该系统能够为每个用户提供一个独立的运行环境，实现存储、网络、进程、用户、内存等资源的隔离。通过资源隔离，可以确保用户之间的互不干扰，提高安全性并降低潜在的风险。

(6) 容器的实时分配与销毁：

分布式调度系统能够实现容器的实时分配和销毁。根据用户需求和系统资源状况，调度系统能够快速地创建、部署和释放容器。这种动态管理方式确保了系统的灵活性和高效性，能够快速响应用户的需求并提供稳定的远程浏览器服务。

锐西版权所有

2.3.2. 远程浏览器隔离防护原理

远程浏览器隔离技术的核心在于在用户与网站之间建立严格的网络隔离，确保用户的安全。每个访问的用户都会获得一个独立的一次性“远程浏览器”云容器执行环境，从而避免任何潜在的恶意行为或数据泄露。

该技术通过一系列核心技术实现，包括自主研发的隔离引擎、高效的网页重绘渲染算法以及 DOM 树重构等，确保了原始网页在经过加载和执行后，其呈现的内容能够被重新转码并形成网页镜像。镜像会通过专有的私有协议进行传输，为用户提供清晰且安全的浏览体验。

更重要的是，远程浏览器在与网站进行交互后，会立即销毁所有原始网页数据，如源代码、API 接口和第三方框架信息等，彻底实现了网页数据的隔离处理，确保了用户数据的完整性和安全性。

3. 产品功能

3.1. 隐藏活动脚本和 API

零信盾将活动脚本和 API 进行隐藏，当用户通过远程浏览器访问网站时，原网站的活动脚本、API、网站结构、目录、敏感字段以及传输内容都被隐藏起来。所有活动脚本和 API 都只在远程浏览器中执行，用户浏览器无法直接访问这些内容。原本公开于互联网上的网站信息转变为“私有信息”，使得第三方无法轻易获取或利用这些信息，大大降低了网站遭受攻击的风险。

锐西版权所有

举例子说，攻击者通常会对网站的活动脚本和 API 进行扫描和分析，试图挖掘出原网站程序、第三方 Web 框架或中间件软件的漏洞，并利用这些漏洞发起攻击。然而，当这些活动脚本和 API 被隐藏后，攻击者无法进行扫描和探测，更无法进一步分析和挖掘漏洞。这大大降低了网站被攻击的可能性，提高了整体的安全性。

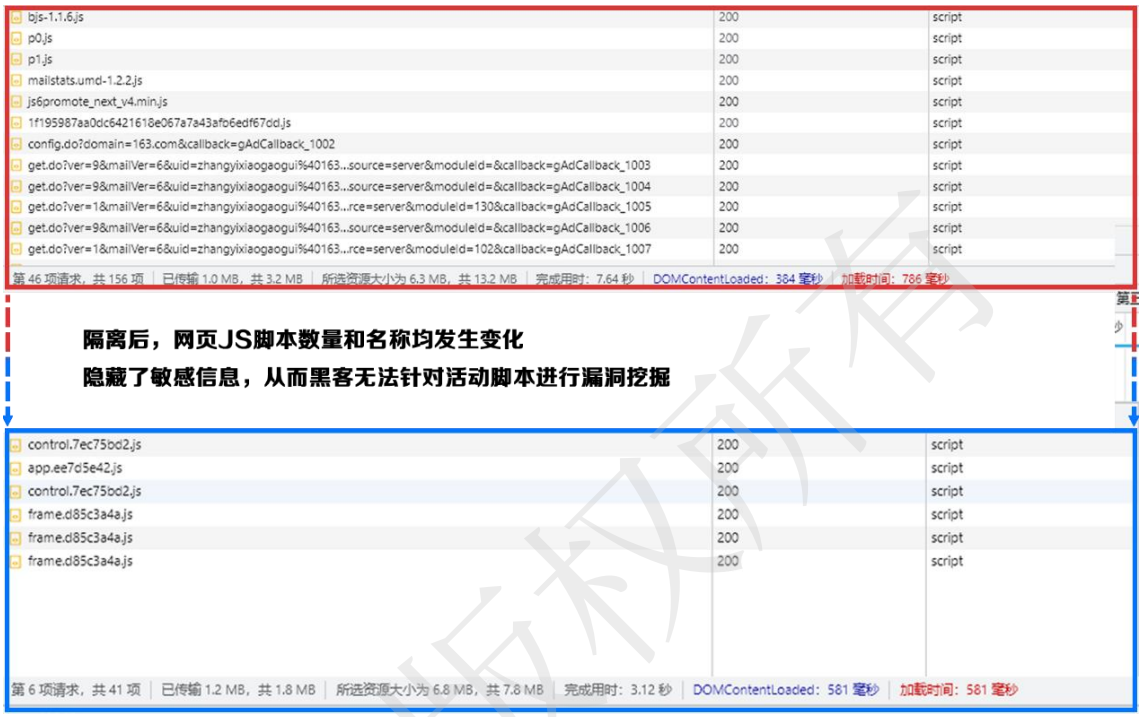


图 隐藏活动脚本

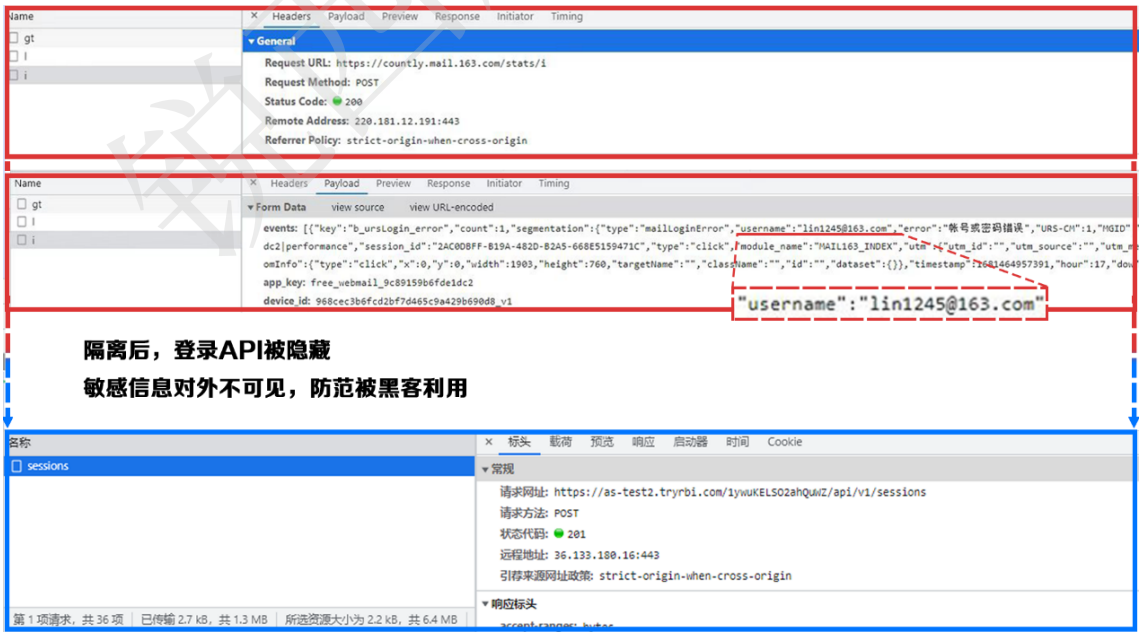


图 隐藏 API

3.2. 隐藏用户凭证

在传统的 Web 应用中，用户登录后的凭证信息，如 Cookie，通常会将其存储在用户的浏览器中。这些信息容易受到攻击者的窃取和滥用，增加了安全风险。

通过零信盾，用户登录后的凭证信息不再存储在用户的浏览器中，而是仅存放在远程浏览器中。敏感信息不会被传递给用户浏览器，完全阻止了攻击者盗取用户凭证并冒用合法身份进行攻击的可能性。

以 Cookie 为例，攻击者原先可以轻易地读取和解码存储在用户浏览器中的原网站 Cookie，利用这些信息发起攻击。但在隔离防护后，原网站的 Cookie 信息不再存放在用户浏览器中，而是由隔离平台自身生成并加密成难以破解的内容。即使用户的浏览器被注入恶意脚本，也无法利用这些 Cookie 信息对原网站进行攻击。

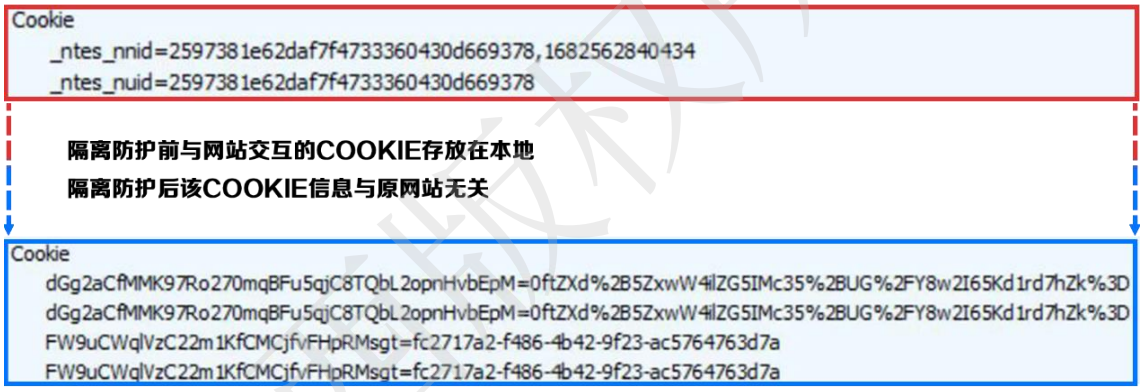


图 隐藏 Cookie 信息

3.3. URL 加密

零信盾对网页访问地址中的 URI 和参数部分进行加密，确保只有合法的用户才能访问到正确的网址，而攻击者无法获取或利用这些信息。

支持静态加密和动态加密两种模式，可以根据实际需求选择合适的加密方式。当隔离平台收到加密的 URL 后，会进行解密并转发给原网站。如果解密失败，用户将被重定向到指定的页面，确保不会出现因解密问题导致的访问错误。除非加密算法被破解，否则攻击者无法访问到这些加密的 URL，从而有效防止了 0/N Day 漏洞和后

门被利用。

比如，攻击者原先可能通过获知网站存在的 SQL 漏洞和 XSS 漏洞的网址，轻松发起攻击。但当使用 URL 加密后，这些漏洞的网址被加密保护，攻击者无法直接访问，从而彻底切断了他们挖掘和利用漏洞的途径。

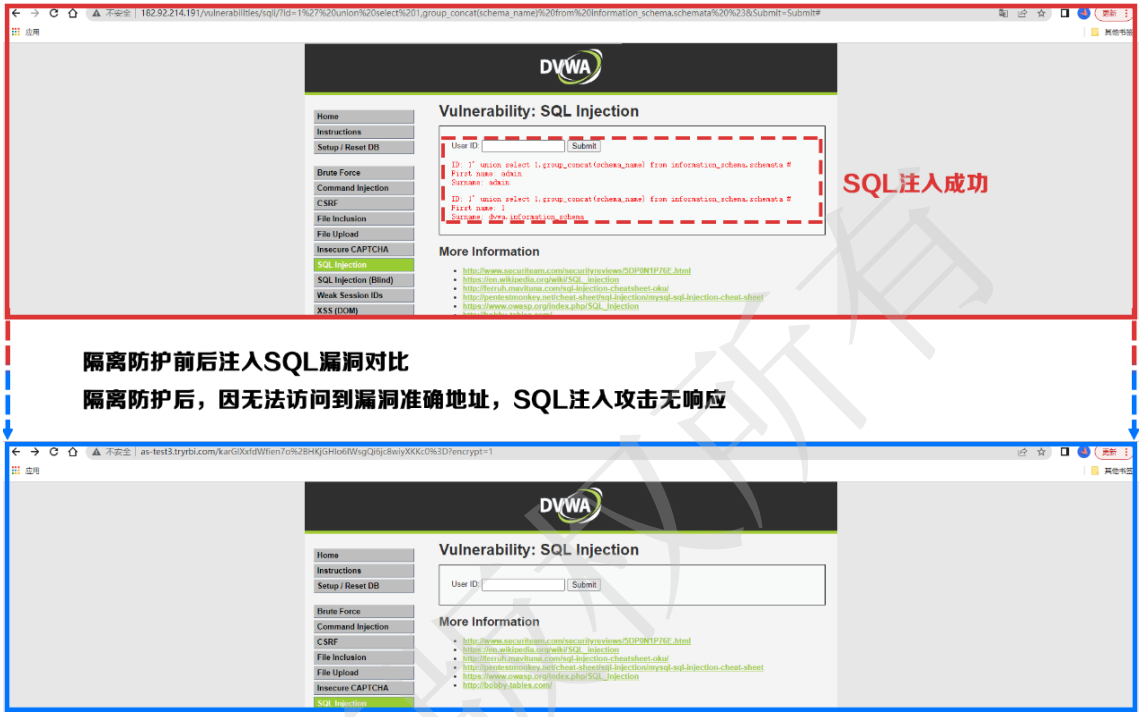


图 SQL 漏洞防护

锐西版权所有

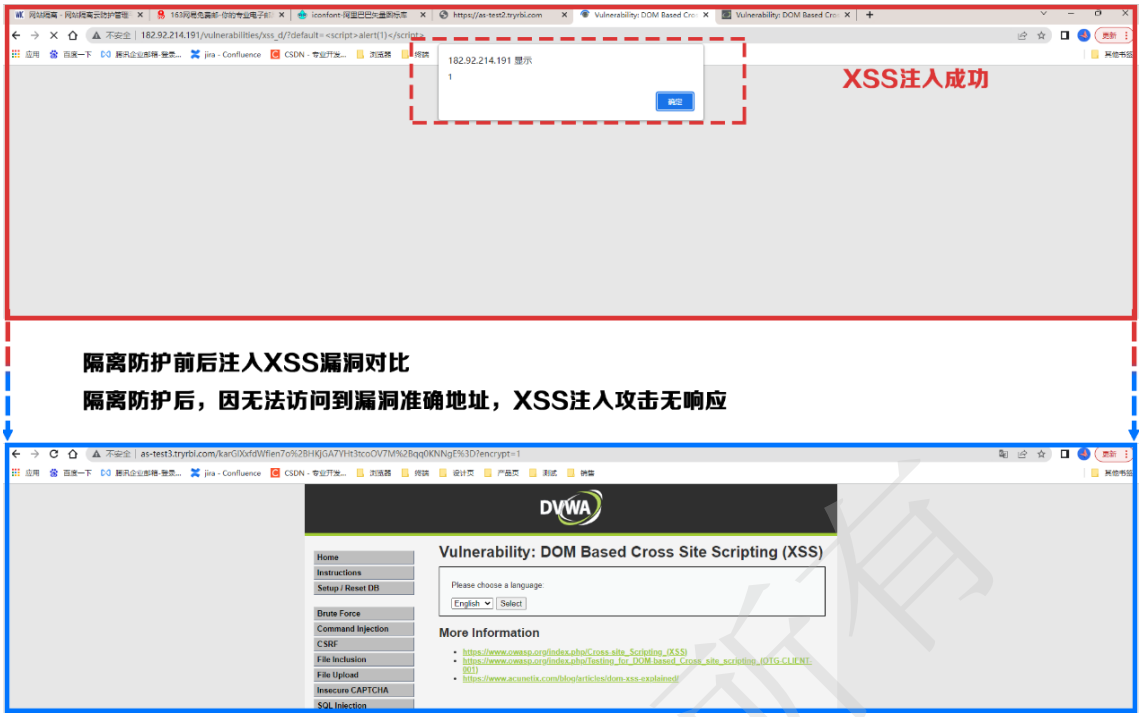


图 XSS 漏洞防护

3.4. URL 隐藏

URL 隐藏目的是防止网络爬虫攻击和保护敏感数据。通过隐藏 URL 链接，有效地隐藏了爬虫的入口，使攻击者难以发起爬虫攻击。

网络爬虫是一种自动化程序，不断地读取页面内容中的链接，并进一步读取这些链接背后的内容。这个过程会不断循环，直到爬虫发现隐藏在网站底层的敏感数据。恶意网络爬虫可能会利用这些敏感数据实施非法行为，如数据泄露或滥用。

当使用 URL 隐藏功能后，爬虫无法通过常规方式获取到页面中的链接，从而有效地阻止了爬虫的访问。这样，即使有恶意网络爬虫尝试发起攻击，也无法找到敏感数据的入口，从而保护了底层的重要数据。

锐西版权所有

图 URL 隐藏

3.5. 隐藏攻击面

在传统的 Web 应用中，服务器信息是公开可见的，这给攻击者提供了机会来探测和利用这些资源。零信盾将所有服务器信息，包括活动脚本、API 接口、第三方框架以及中间件软件等，都被设计为对外完全不可见。屏蔽攻击入口，使攻击者无法探测和分析可被利用的资源，大大提高了网站的安全性。攻击者无法探测和分析服务器信息，就无法找到可以利用的漏洞并发起攻击。全方位的隐藏和保护措施确保了用户和网站的数据安全，降低了网站遭受攻击的风险。

3.6. 隔离各类 web 攻击

在传统的 Web 应用中，攻击者常常利用各种工具对网站进行漏洞扫描、暴力破解等攻击。这些攻击手段利用了与服务器之间的直接通信，试图获取敏感信息或执行恶意操作。零信盾采取了私有交互协议，确保只响应键盘和鼠标的网页操作命令。所有的攻击工具都无法与源站服务器进行直接通信或发送攻击数据，彻底杜绝了各类漏洞扫描、弱口令暴力破解、撞库等 Web 攻击手段。

通过只响应键盘和鼠标的网页操作命令，确保了所有通信都是合法和预期内的。任何尝试使用攻击工具进行通信的行为都会被拒绝，从而确保了源站服务器和用户数据的安全。

3.7. 网页防篡改

当服务器信息被彻底隐藏后，攻击者无法接触网页脚本和数据，从而无法进行攻击或篡改网页。在传统的 Web 应用中，服务器信息是公开可见的，攻击者可以利用这些信息找到漏洞并进行篡改。然而，在零信盾的保护下，服务器信息被彻底隐藏，使得攻击者无法获取这些关键信息。用户可以放心地浏览和使用网站，不用担心数据被篡改或恶意操作。为用户提供一个更加安全和可靠的浏览环境，降低网站遭受攻击的风险。

3.8. 防爬虫反克隆

爬虫是一种自动化的程序，能够读取和复制网站的内容。一些不法分子会利用爬虫技术来克隆网站，复制其内容和结构，以此来进行欺诈、钓鱼等非法活动。这种行为不仅侵犯了原创网站的权益，还给用户带来了严重的安全风险。

通过零信盾，网站可以隐藏其内容和结构，使得爬虫无法获取到关键信息。这样，即使有恶意分子尝试克隆网站，也无法得到完整和准确的内容，从而大大降低了其非法活动的成功率。

同时，零信盾能够对用户的访问行为进行监控和限制，防止任何可疑的爬虫行为。一旦发现有非法的爬虫访问，系统可以立即采取相应的安全措施，记录日志、报警等。

3.9. 隔离 Webshell 后门

攻击者常常利用网站漏洞上传后门程序，进而控制网站并进行恶意操作。这些后门程序可能是攻击者事先植入或通过漏洞利用获得的。一旦后门被利用，攻击者可以利用这些后门进行进一步的攻击或窃取敏感信息。

零信盾能够有效隔离和隐藏服务器所有 Web 漏洞，使得攻击者难以利用网站漏

锐西版权所有

洞上传后门程序。即使攻击者事先潜伏了后门，零信盾使用 URL 加密技术阻断攻击者对后门的访问，从而有效防止后门被利用，有效地降低了网站遭受进一步攻击的风险。用户可以放心地使用网站服务，不用担心数据被窃取或滥用。

3.10. 非授权访问控制

攻击者利用跨站脚本、中间人攻击和网页木马等手段来窃取用户的敏感信息。这些攻击手段可能利用了网站系统自身设计缺陷引起的水平越权和垂直越权逻辑漏洞，在用户不知情的情况下，窃取其个人信息，如账号、密码等。攻击者利用其他用户的权限进行非法操作，窃取或篡改数据。零信盾可以确保每个用户的操作都在其权限范围内进行，有效防止了越权操作的发生。

3.11. 敏感数据防护

SQL 注入和命令注入是常见的攻击手段，攻击者通过在输入字段中注入恶意 SQL 或命令，试图获取或篡改数据库中的敏感数据。零信盾能够对用户输入进行严格的验证和过滤，防止任何恶意 SQL 或命令的执行。

对于爬虫的爬取行为也能够进行有效的阻拦。爬虫通常用于大量抓取网站内容，有些恶意爬虫可能会尝试获取敏感数据或进行其他非法操作，零信盾可以识别并限制可疑的爬取行为，保障敏感信息不被窃取。

3.12. 0day 漏洞屏蔽

通过有效隔离和隐藏服务器所有 Web 资源，将用户浏览器弱化成一个显示工具，使得攻击者无法手动或自动扫描探测漏洞。即使攻击者通过其他途径挖到了漏洞，零信盾使用 URL 加密技术让攻击者无法访问到漏洞，从而杜绝了漏洞被利用的可能性。

3.13. IPv6 转换

提供 IPv6 网络改造能力，通过在 IPv4 到 IPv6 双向通信过程中通过 CNAME 域名解析指向零信盾，完成 IPv4&IPv6 双向转译工作，实现 IPv4 和 IPv6 的双向接入服

务。接入方式简单，无需改变软硬件结构即可平滑升级支持 IPv6。

4. 产品优势

4.1. 创新自主“远程浏览器隔离”技术防护死角

锐西科技创新自主“远程浏览器”技术从根源上解决网站 Web 安全问题，从根源上提升网络安全的防护手段。通过远程浏览器代替用户浏览器去访问互联网，阻止自动化攻击、漏洞利用、后门攻击、暴力破解、注入等各类攻击手段，构筑信息安全的铜墙铁壁，为网站 Web 安全保驾护航，为客户提供防得住的保障，真正实现全方位无死角的防护效果。

4.2. “绝对”安全防护

通过隐藏网页源码、阻断自动化攻击和 URL 加密等手段，有效提升黑客攻击的难度。在源头直接拦阻攻击者，确保了网站的安全稳定运行。面对监管和重保时期无压力，确保网站符合相关要求和标准。

4.3. 阻断自动化攻击

通过私有协议与访问者交互，使互联网上几乎所有（近百款）web 自动化攻击程序（爬虫、僵尸网络等）和几十种扫描器无效，几乎无法通过自动化攻击软件探测网站信息。

4.4. 防护利用 0day 攻击

URL 具备动态加密功能，在 URL 动态加密与隐藏网页源码的情况下，攻击者无法访问到 web 网站指定资源，几乎完全防护利用 0day 发起的攻击。

锐西版权所有

4.5. 屏蔽已知风险，防御未知风险

通过“远程浏览器技术”做到隐藏 web 网站的源码信息、活动脚本、API、cookie、URL 等，隐藏已知的漏洞及攻击风险，全力预防未知风险攻击行为。

4.6. 零部署、零配置、零运维

零信盾产品为客户提供 SaaS 化的服务模式，客户可以根据实际需求选择不同的服务计划并快速上线启用，同时，锐西科技提供专业化的技术支持和维护服务，无需客户自行维护复杂的软件，极大降低维护成本和难度，真正实现零部署、零配置、零运维。

5. 客户价值

5.1. OWASP 威胁攻击全防护

OWASP 威胁攻击长期对用户 Web 业务影响最严重的安全风险，零信盾的“远程浏览器技术”能够从根源上解决网站 Web 安全问题，将用户的浏览器会话运行在远程隔离环境中，减少潜在的攻击面并增强安全性，实现全方位防护。

5.2. 实时防护，持续监测

全天候 7*24 的持续监测，高度敏感性和准确性，及时识别和应对有害攻击行为，快速反应能力确保了网站的持续安全运行，减轻潜在损失，为客户提供了强大的安全保障。

5.3. 降本增效，构筑安全城墙

零信盾的 SaaS 化模式，免去了客户的硬件和软件的直接成本，显著降低成本和运营维护开销，同时为客户提供报告和分析能力，帮助优化安全策略和响应措施，构筑 Web 网站安全城墙。

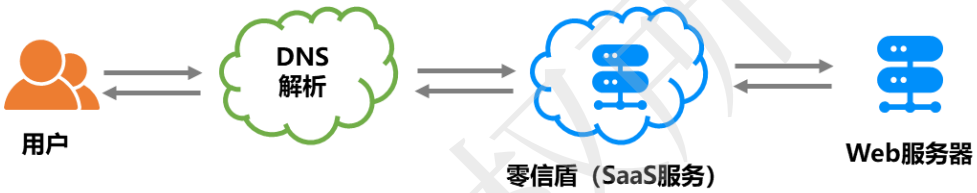
锐西版权所有

5.4. 构建安全合规堡垒

满足网络安全法、数据安全法、个人信息保护法、关保条例、等级保护等法律法规对应用安全的防护要求，帮助客户轻松达到甚至超过这些合规性要求，构建安全合规堡垒，减少因合规失败带来的法律风险和罚款，同时更好地应对重保、HW 等攻防演练的考验。

6. 典型部署

6.1. SaaS 服务模式（推荐）



客户调整公网的 DNS 域名解析，修改业务系统的域名指向，以 CNAME 的方式将域名指到零信盾上，当用户访问业务系统的域名时，流量先到零信盾，由零信盾去请求后端 Web 业务，将请求结构渲染重绘后，返还给访问用户。

零信盾产品为客户提供 SaaS 化的服务模式，可以根据实际需求选择不同的服务计划，节省大量购买软件和硬件设备，同时，锐西科技为客户配备管家式的技术支持人员提供运维服务，免去了客户对运维的资金投入，极大降低维护成本和难度。

6.2. 本地/私有模式

零信盾部署在网站服务器和防火墙之间，用户访问流量先到零信盾，零信盾去请求后端网站服务器，将请求结果渲染重绘后，返还给访问用户。