密级：限定发布

南墙 WEB 应用防火墙
使用手册 V3.0

“不撞南墙不回头”

目 录

1 产品概述

1.1 产品介绍

南墙 WEB 应用防火墙（简称：uuWAF）是有安科技推出的一款全方位网站防护产品。通过有安科技专有的 WEB 入侵异常检测等技术，结合有安科技团队多年应用安全的攻防理论和应急响应实践经验积累的基础上自主研发而成。协助各级政府、企/事业单位全面保护 WEB 应用安全，实现 WEB 服务器的全方位防护解决方案。

手册适合的对象:

《南墙 WEB 应用防火墙使用手册》适用于希望了解本产品功能，并熟练掌握产品的配置及日常操作维护的运维人员。

公司联系方式 :

用户可以通过如下的联系方式详细了解该产品:

- 市场销售:

  邮箱：support@uusec.com

- 支持服务:

  邮箱：support@uusec.com

- 官方站点:

  网址：http://www.uusec.com

1.2 技术优势

1.2.1 先进语义引擎

南墙采用业界领先的 SQL、XSS、RCE、LFI 4 种基于语义分析的检测引擎，结合多种深度解码引擎可对 base64、json、form-data 等 HTTP 内容真实还原，从而有效抵御各种绕过 WAF 的攻击方式，并且相比传统正则匹配具备准确率高、误报率低、效率高等特点，管理员无需维护庞杂的规则库，即可拦截多种攻击类型。

1.2.2 智能 0day 防御

南墙创新性的运用机器学习技术，使用异常检测算法对 http 正常与攻击流量进行区分识别，并对正常流量进行白名单威胁建模。通过机器学习算法自动学习正常流量中的参数特征，并转化成对应的参数白名单规则库，可以在面对各种突发 0day 漏洞时，无需添加规则即可拦截攻击，免除网站管理者一出现漏洞就需挑灯夜战升级的痛苦。

1.2.3 高级规则引擎

南墙积极运用 nginx 的高性能和 luajit 的高性能、高灵活性特点，除了提供对普通用户友好性较好的传统规则创建模式，还提供了高扩展性、高灵活性的 lua 脚本规则编写功能，使得有一定编程功底的高级安全管理员可以创造出一系列传统 WAF 所不能实现的高级漏洞防护规则，用户可以编写一系列插件来扩展 WAF 现有功能。从而使得在拦截一些复杂漏洞时，可以更加得心应手。

2 使用介绍

2.1 登录管理

2.1.1 登录界面

访问 https://ip :4443/首次登录用户名为 admin 密码为 Passw0rd!，输入后点击登录进入，界面如下：

登录界面

2.1.2 安全态势

登录后首页态势感知界面展示了网站攻击类型以及最近的攻击趋势信息，如下：

首页界面

2.2 功能介绍

2.2.1 站点管理

对保护的网站进行管理和配置，支持规则选择、负载均衡、防护模式、websocket、url 白名单、ip 白名单、客户端真实 ip 获取等多个配置选项（注意：https 站点需要在证书管理中上传 pem 格式的网站证书才能访问），如下图所示：

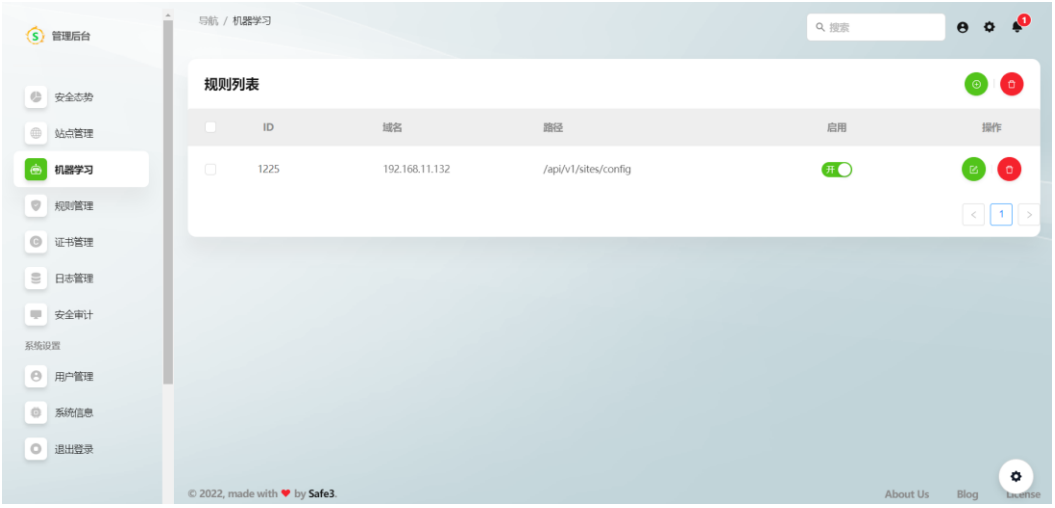
站点管理界面

2.2.2 机器学习

对机器学习产生的规则进行管理和配置，可按照以下步骤使用机器学习功能：

1. 在菜单站点管理->基本设置中点击开启开始学习按钮，南墙自动进入学习模式，学习后产生的规则会显示在机器学习主菜单。
2. 待机器学习的规则自动生成的差不多了后，进入站点管理->基本设置中将防护模式设置为观察模式，再关闭开始学习按钮。此时南墙进入规则生效模式，可进一步观察安全日志中是否有误报规则，可在机器学习主菜单修改调整。待没有误报则可

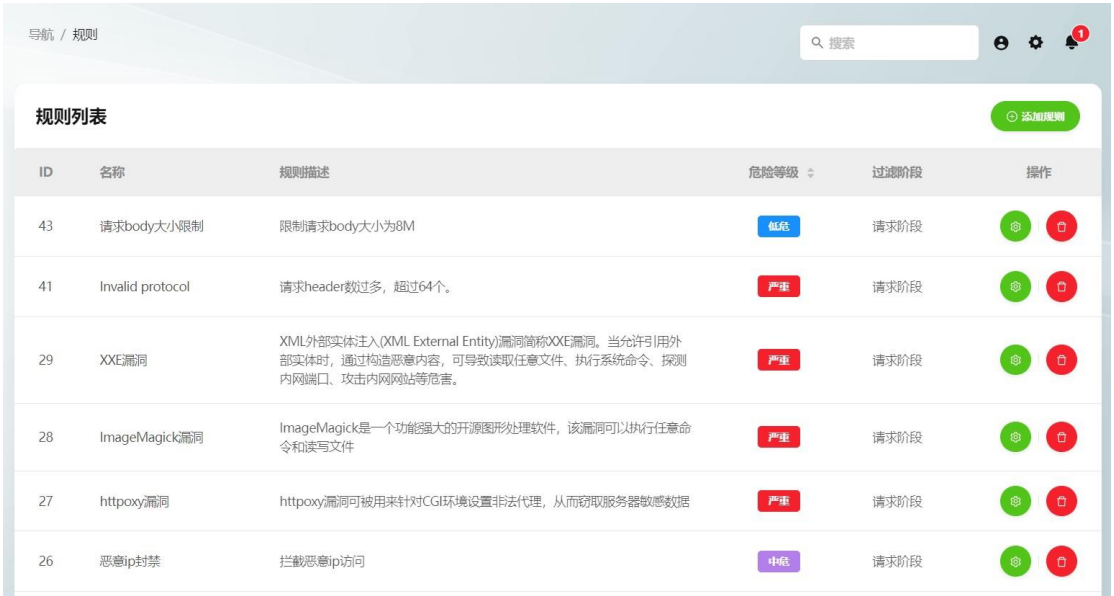
以在站点管理->基本设置中将防护模式设置为拦截模式。



机器学习界面

2.2.3 规则管理

规则管理界面可以添加、编辑、查询和启用 waf 规则如下图所示：



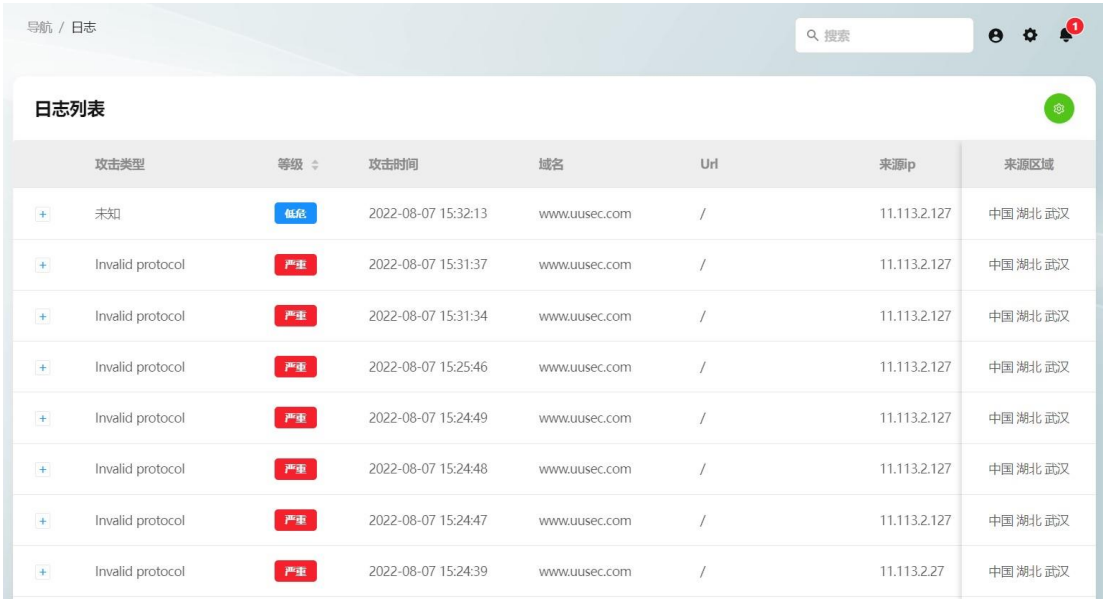
规则管理界面

规则编辑界面，过滤阶段可以分为"请求阶段"（过滤客户端发来的数据）、"返回 http 头"（返回的 http 头部内容）、"返回页面"（返回的网页内容）三个阶段。规则内容为 dsl 语言或 lua 脚本语言（详情可以参考第 3 章->规则介绍->外置规则），如下图所示：

规则编辑界面

2.2.4 日志管理

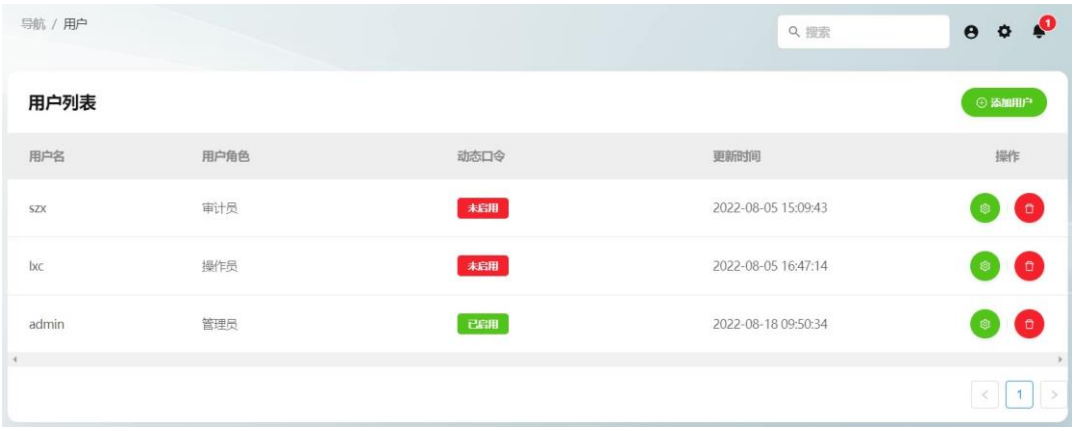
攻击查询页面可以根据攻击时间、攻击类型和域名等信息查询攻击事件并导出报表，如下图所示：



攻击查询界面

2.2.5 用户设置

用户设置页面可以修改 waf 管理账户的用户名以及密码等信息，包括动态口令、管理角色（管理员、操作员、审计员）等，如下图所：



用户设置界面

2.2.6 系统信息

系统信息页面可以查看当前系统资源占用以及系统版本等信息，如下图所示：

系统信息界面

3 规则介绍

南墙 WEB 应用防火墙采用 dsl 语言或 lua 脚本作为规则引擎，可以很方便编写各种复杂的安全防护规则。例如：类似 padding oracle 漏洞需要对请求 url、querystring、返回 http 状态以及返回网页内容等 http 多个处理阶段做关联过滤，传统 waf 只能对其中的某一阶段过滤从而造成拦截不精准、误报等问题，有安科技 WAF 可以轻松解决。再如：一般请求中携带单引号，如果直接拦截则会造成误拦截，有安科技 WAF 可以在判断请求中携带单引号的同时判断返回状态是否为 500、302 以及返回内容中是否包含 sql 报错来精准拦截 sql 注入攻击。

3.1 高级规则

外置规则为用户自定义规则，可通过 waf 网站界面管理，并通过 lua 语法编辑的外部规则，最新规则文档可参考在线版 https://waf.uusec.com/#/api/README 。

- lua 过滤函数

1.waf.startWith(sstr,dstr)

参数:sstr 为原字符串，dstr 为查找字符串

功能:判断字符串 sstr 是否以 dstr 开头

返回值:true 或 false

2. waf.endWith(sstr,dstr)

参数:sstr 为原字符串，dstr 为查找字符串

功能:判断字符串 sstr 是否以 dstr 结尾

返回值:true 或 false

3. waf.toLower(sstr)

参数:sstr 为原字符

功能:将字符串 sstr 转化为小写

返回值:sstr 小写

4. waf.contains(sstr,dstr)

参数:sstr 为原字符串，dstr 为查找字符串

功能:判断字符串 sstr 是否在 dstr

返回值:true 或 false

5. waf.rgxMatch(sstr,pat,ext)

参数:sstr 为原字符串，pat 为正则表达式，ext 为正则属性

功能:在字符串 sstr 中匹配正则表达式 pat

返回值:true 或 false

6. waf.kvFilter(v,match,valOnly)

参数:v 为要匹配对象，match 为匹配函数,valOnly 为 true 则只匹配 value

功能:用于匹配 cookie、queryString 等 key，value 键值对数据，在对象 v 中用 match 函数匹配内容

返回值:true,匹配内容或 false,nil

7. waf.knFilter(v,match,p)

参数:v 为要匹配对象，match 为匹配函数，p 为 1 时匹配上传文件名，为 0 时文件内容

功能:用于过滤上传文件信息，在对象 v 中用 match 函数匹配内容

返回值:true,匹配内容或 false,nil

8. waf.jsonFilter(v, match,parsed,valOnly)

参数:v 为要匹配对象，match 为匹配函数，parsed 为 false 时解析类型为字符串 v 值，为 true 时解析类型为 table 的 v 值，valOnly 为 true 则只匹配 value

功能:用于遍历过滤请求中的 json 数据，在对象 v 中用 match 函数匹配内容

返回值:true,匹配内容或 false,nil

9. waf.base64Decode(str)

参数:str 为要解码的 base64 字符串

功能:用于解码 base64 数据为明文数据

返回值: 明文字符串或 nil

10. waf.checkSQLI(str)

参数:str 为要检测的字符串

功能:基于语义引擎检测 sql 注入攻击

返回值: true 或 false

11. waf.checkRCE(str)

参数:str 为要检测的字符串

功能:基于语义引擎检测命令注入攻击

返回值: true 或 false

12. waf.checkPT(str)

参数:str 为要检测的字符串

功能:基于语义引擎检测路径遍历攻击

返回值: true 或 false

13. waf.strCounter(sstr,dstr)

参数:sstr 为原字符串，dstr 为查找字符串

功能:计算字符串 dstr 在 sstr 中出现的次数

返回值:整数

13. waf.pmMatch(sstr,dict)

参数:sstr 为原字符串，dict 为查找字典，以 lua 表的形式，如：{"aaa", "bbb", "ccc"}

功能:高效多模匹配多个字符串，发现其中一个字符串立即返回

返回值:true，字典中的字符串或 false，nil

13. waf.urlDecode(sstr)

参数:sstr 为原字符串

功能:将 sstr 进行 url 解码还原成原字符串

返回值:url 解码后的字符串

14. waf.htmlEntityDecode(sstr)

参数:sstr 为原字符

功能:将字符串 sstr 进行 html 实体解码

返回值:解码后的字符串

15. waf.hexDecode(sstr)

参数:sstr 为原字符，格式\xaa\xbb

功能:将字符串 sstr 进行 hex 解码

返回值:解码后的字符串

- 请求阶段变量

waf.ip 客户端访问 ip

waf.host 客户端访问 host 头

waf.requestLine 原始的 request line 数据

waf.uri 解码处理过的 URI，不带参数

waf.method 请求方法

waf.reqUri 原始 URI，带参数

waf.userAgent 客户端请求的 User-Agent 头数据

waf.referer 客户端请求的 Referer 头数据

waf.reqContentType 客户端请求的 Content-Type 头数据

waf.XFF 客户端请求的 X-Forwarded-For 头数据

waf.origin 客户端请求的 Origin 头数据

waf.reqHeaders 请求的所有 header 对象

waf.hErr 请求 header 出错信息

waf.isQueryString 是否存在请求参数，值 true 或 false

waf.reqContentLength 请求 body 内容长度，整数值

waf.queryString 请求参数 key、value

waf.qErr 请求参数出错信息

waf.form 请求 body 对象

waf.form["RAW"] 原始数据: 请求 body 的原始数据

waf.form["FORM"] 表单: {uid="12",vid={[1]="select",[2]="a from b"}}

waf.form["FILES"] 文件: {name={[1]="filename",[2]="file content"}}

waf.fErr 请求 body 出错信息

waf.cookies 请求 cookie key、value

waf.cErr 请求 cookie 出错信息

- 返回 http 头阶段新增变量

waf.status 返回 http 状态，整数值

waf.respHeaders 返回的所有 header 对象

waf.respContentLength 返回 body 内容长度，整数值

waf.respContentType 服务端返回的 Content-Type 头数据

- 返回页面阶段新增变量

waf.respBody 返回 body 页面内容

- 外置规则过滤 user agent 示例：

```
local ua = waf.reqHeaders.user_agent
local contains = waf.contains
if ua then
    if type(ua) ~= "string" then
        return true,"Malform User-Agent",1
    elseif contains(ua,"sqlmap") or contains(ua,"nessus") or contains(ua,"arachni") or contains(ua,".nasl") or contains(ua,"dirbuster") or contains(ua,"nmap nse") or contains(ua,"nikto") or contains(ua,"w3af") or contains(ua,"hydra") then
        return true,ua, true
    end
end
```

返回参数 1：true 表示规则匹配成功，false 表示规则不匹配

返回参数 2：ua 为要记录拦截日志的拦截数据

返回参数 3：true 表示拦截攻击，false 表示只记录不拦截

4 关于我们

有安科技成立于 2005 年 2 月，提供专业的信息安全服务与信息安全产品，是你值得信赖的网络安全顾问！

有安科技凭借多年的安全漏洞研究与安全服务基础，研发的成熟产品包括“南墙 WEB 应用防火墙”、“太极主动防御系统”和“万象漏洞扫描系统”等多款安全产品，并且在人工智能、大数据、云安全、威胁情报、漏洞挖掘、红蓝对抗等领域取得多项技术成果。

4.1 技术能力

有安科技研究人员对网络基础设施、系统与网络应用安全具有深入研究，研究范围包括网络设备及安全设备（交换机、路由器、防火墙、入侵检测系统等）、操作系统平台（Windows、AIX、HP-UX、Solaris、IRIX、Linux 等）、Web Server 与框架（Nginx、Tomcat、Apache、Java、PHP、ASP.NET 等）。

有能力完成：

* 安全托管服务 MSS（Managed Security Service）
* 网络架构评估与设计（Architecture review and design）
* 安全定制开发（Software customization development）
* 源代码审计（Source code review）
* 渗透测试（Penetration testing）
* 调查取证与数据恢复（Forensics&Recovery）

4.2 团队力量

有安科技核心人员来自 360、华为等知名企业，其中不乏曾参加过中美黑客大战的老一代安全前辈，具有极其丰富的网络安全实践经验。

公司愿景：安全创造价值。

公司使命：成为用户身边最值得信赖的信息安全产品和服务提供商。

公司战略：通过持续不断的技术创新为用户提供最佳安全实践。

公司价值观：以专业的精神，向客户提供最具竞争力的产品和服务，尽心尽责。