观镜 WEB 应用安全防护系统

用户使用手册

2020年2月



Bubble Web Application Security System

电话:021-62090100 产品服务电话:400-728-0510

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

目录

第1章	章	系统概述	5
1 1	I	같므	-
1.1		月京	
1.2	2.	目的	5
第21	章	前置知识	5
2.1	L.	操作系统	5
	2.1.1	. LINUX 操作系统	5
	2.1.2	. Windows 操作系统	5
2.2	2.	HTTP 协议基础	6
	2.2.1	. HTTP 请求方法	6
	2.2.2	. HTTP 状态码	6
2.3	3.	MYSQL 基础知识	7
2.4	ł.	WEB 安全基础知识	8
	2.4.1	. SQL 注入攻击测试	8
	2.4.2	2. XSS 跨站攻击测试	8
	2.4.3	。 自动化扫描工具	9
第3章	章	系统操作	9
3.1	L.	登录系统	9
上海观	吃信	息技术股份有限公司	电话:021-62090100
技术支	を 持 邮	牛:websec@idss-cn.com	产品服务电话:400-728-0510
地址:	上海市	节普陀区大渡河路 388 弄 5 号华宏商务中心 6 层	

3	3.2.	忘记密码	
第4	4章	系统功能	
Z	1.1.	首页	
	4.1.1	攻击画像	
	4.1.2	?. 被攻击业务统计列表	
	4.1.3	3. 被攻击地址统计列表	
	4.1.4	9. 自动化工具统计列表	
	4.1.5	5. 来源 IP 访问统计列表	
	4.1.6	5. 来源浏览器统计列表	
2	1.2.	站点管理	
	4.2.1		
	4.2.2	?. 节点管理	
	4.2.3	3. 证书管理	
	4.2.4	<i>1. 业务匹配</i>	
2	1.3.	防御配置	25
	4.3.1	!. 主动防御配置	
	4.3.2	?. 基础防御配置	
	4.3.3	3. <i>数据脱敏配置</i>	
	4.3.4	4. 规则引擎配置	
上海	现安信	息技术股份有限公司	电话:021-62090100
技才	、支持邮	件:websec@ldss-cn.com	产品服务电话:400-728-0510
地址	L:上海i	市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层	

4.3.5.	虚拟验证码	
4.3.6.	规则字典管理	
4.3.7.	威胁情报管理	
4.3.8.	页面监控配置	
4.4. 用	〕户画像	
4.5. E]志管理	
4.5.1.	安全防御日志	
4.5.2.	系统操作日志	
4.5.3.	告警通知日志	
4.6. 系	系统管理	53
4.6.1.	用户管理	
4.6.2.	存储配置	54
4.6.3.	告警配置	55
4.6.4.	系统信息	

上海观安信息技术股份有限公司 技术支持邮件:websec@idss-cn.com 地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

第1章系统概述

1.1.背景

观镜 Web 应用安全防护系统系统的设计理念源于团队成员十余年安全服务经验,并且结合当前大数据技术、流量分析 技术等领先技术,将 Web 安全防御系统置于客户系统之前,在不影响客户机原有业务的情况下,将客户系统的 web 数据 进行混淆和加密,将攻击阻挡在网站之前。同时,该系统可以拦截网络上常见自动化工具的恶意请求,有效的保护企业网站 安全。它具有功能强大、部署简单、多引擎、易扩展等特点。

1.2. 目的

观镜 Web 应用安全防护系统支持通过 WEB 管理界面进行配置站点以及管理。本手册主要介绍如何使用观镜 Web 应 用安全防护系统进行对站点的防护和管理、策略配置以及常见场景防御配置等操作。

第2章前置知识

2.1. 操作系统

2.1.1. LINUX 操作系统

需要具备基本的 Linux 系统操作能力,针对常见的操作命令等等需要熟练掌握:

2.1.2. Windows 操作系统

需要掌握日常的办公操作、软件安装卸载,掌握在 Windows 上搭建与部署网站,熟练使用 Vmare Workstation 和 VirtualBox 等虚拟化平台操作,熟练使用 MySQL 等数据库管理系统。

上海观安信息技术股份有限公司 技术支持邮件:websec@idss-cn.com 地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

2.2. HTTP 协议基础

HTTP 协议是 Hyper Text Transfer Protocol(超文本传输协议)的缩写,是用于从万维网服务器传输超文本到本地浏览器的传送协议。HTTP 协议工作于客户端-服务端架构上,浏览器作为 HTTP 客户端通过 URL 向 HTTP 服务端即 WEB 服务器发送所有请求,WEB 服务器根据接收到的请求后,向客户端发送响应信息,其默认端口号为 80。

2.2.1. HTTP 请求方法

序号	方法	中文描述
1	GET	请求指定的页面信息,并返回实体主体。
2	HEAD	类似于 GET 请求,但返回的响应中没有具体的内容,用于获取报头。
		向指定资源提交数据进行处理请求(例如提交表单或者上传文件)。数据被
3	POST	包含在请求体中。POST 请求可能会导致新的资源的建立和/或已有资源的
		修改。
4	PUT	从客户端向服务器传送的数据取代指定的文档的内容。
5	DELETE	请求服务器删除指定的页面。
6	CONNECT	HTTP/1.1 协议中预留给能够将连接改为管道方式的代理服务器。
7	OPTIONS	允许客户端查看服务器的性能。
8	TRACE	回显服务器收到的请求,主要用于测试或诊断。
9	PATCH	是对 PUT 方法的补充,用来对已知资源进行局部更新。

2.2.2. HTTP 状态码

当浏览者访问一个网页时,浏览者的浏览器会向网页所在服务器发出请求。当浏览器接收并显示网页前,此网页所在

的服力备去这回一个也占可口了 扒芯锅的后总大用以响应闪见备用水。 下面走吊见的口口了 扒芯锅
--

状态码	英文名称	中文描述
100	Continue	继续。客户端应继续其请求。

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388弄5号华宏商务中心6层

200	ОК	请求成功。一般用于 GET 与 POST 请求。
201	Created	已创建。成功请求并创建了新的资源。
201	Moved Permanently	永久移动。请求的资源已被永久的移动到新URL 返回信息会包括新的URL,
301	Moved Permanently	浏览器会自动定向到新 URL。今后任何新的请求都应使用新的 URL 代替。
202	Found	临时移动。 与 301 类似。 但资源只是临时被移动。 客户端应继续使用原有
302	Found	URL。
400	Bad Request	客户端请求的语法错误,服务器无法理解。
403	Forbidden	服务器理解请求客户端的请求,但是拒绝执行此请求。
40.4	Net Found	服务器无法根据客户端的请求找到资源(网页)。通过此代码,网站设计人
404	Not Found	员可设置"您所请求的资源无法找到"的个性页面。
405	Method Not Allowed	客户端请求中的方法被禁止。
500	Internal Server Error	服务器内部错误,无法完成请求。
501	Not Implemented	服务器不支持请求的功能,无法完成请求。
502	Red Cateway	作为网关或者代理工作的服务器尝试执行请求时,从远程服务器接收到了一
502	Bad Galeway	个无效的响应。
EQE	HTTP Version not	
505	supported	版方岙个又好明水的 FIIF 财议的版本,无法元成处理。

2.3. MYSQL 基础知识

需要会使用基础的 MYSQL 语句进行相应的数据库操作,包括创建数据库、创建表、创建用户、给用户赋予权限、修改数据库密码、导入文件等等不同基本情况。

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

2.4. WEB 安全基础知识

2.4.1. SQL 注入攻击测试

SQL 注入就是通过把 SQL 命令插入到 Web 表单递交或输入域名或页面请求的查询字符串,最终达到欺骗服务器执行 恶意的 SQL 命令。具体来说,它是利用现有应用程序,将(恶意) SQL 命令注入到后台数据库引擎执行的能力,它可以通 过在 Web 表单中输入(恶意) SQL 语句得到一个存在安全漏洞的网站上的数据库,而不是按照设计者意图去执行 SQL 语句。总结产生 SQL 注入的位置,一是站点使用输入内容构造动态的 SQL 语句访问数据库,二是站点代码使用存储过程,存 储过程作为包含未筛选的用户输入的字符串来传递,这两种情况都会发生 SQL 注入。但总的来说,只要存在数据库交互的 点就有可能存在 SQL 注入漏洞。

Ġ₽	SQL 注入攻击测试语句说明		
17-2	语句内容	验证判断	
1	?id=1 and 1=1		
2	and 1=(select @@version)	查询数据库版本	
3	and exists (select * from user_tables)	查询是否存在 user_tables 表	
4	' and '1'='2	判断是否为字符型注入	
5	and '%'='%/%'	判断是否为字符型注入	
6	and user>0	获取当前数据库用户名	
7	order by 10	判断当前查询语句的字段数	

需要掌握常见的 SQL 注入攻击的测试语句,这里作简单基本介绍:

2.4.2. XSS 跨站攻击测试

XSS 跨站脚本攻击是一种常见的 Web 安全漏洞,它主要是指攻击者可以在页面中插入恶意脚本代码,当受害者访问这些页面时,浏览器会解析并执行这些恶意代码,从而达到窃取用户身份/钓鱼/传播恶意代码等行为。

需要掌握常见的测试 XSS 跨站攻击的测试语句,这里作简单基本介绍:

序号	XSS 跨站攻击测试语句说明	
上海观安信息技	支术股份有限公司	电话:021-62090100
技术支持邮件	: websec@idss-cn.com	产品服务电话:400-728-0510
地址:上海市智	皆陀区大渡河路 388 弄 5 号华宏商务中心 6 层	

	语句内容	验证判断
1	<script>alert(1)</script>	触发弹框
2	<iframe \="" onload="prompt(1)</th" src=""><th>触发弹框</th></iframe>	触发弹框
3	<svg onload="alert(1)</th"><th>触发弹框</th></svg>	触发弹框
4	`-alert(1)">'onload="` <svg 1="</th><th>触发弹框</th></tr><tr><th>5</th><th>"><script></script></svg>	

2.4.3. 自动化扫描工具

需要掌握相关常见不同类型的自动化扫描工具,以方便对防护站点进行功能测试:

序号	工具名称	实现功能
1	AWVS	Web 安全扫描
2	Nmap	端口扫描
3	APPSCAN	Web 安全扫描
4	ZAP	Web 安全扫描
5	Burp Suite	Web 安全扫描

第3章系统操作

3.1. 登录系统

观镜 Web 应用安全防护系统 2.1 采用 B/S 架构,可直接在浏览器输入部署服务前地址,打开登录界面,首次登录需

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388 弄5号华宏商务中心6层

要先进行注册,然后才可以正常登录,首次注册的用户权限默认为管理员"admin",登录成功之后可在管理界面对用户进行增加或删除等管理。登录界面不提供"密码找回"功能,如您不慎遗忘密码,可由管理员登录进入用户管理界面进行重置密码,如只有当前一个用户,请联系厂商进行密码找回或重置。

根据配置好的 IP 地址访问管理端后会有以下提示:



图 3-1

点击高级显示出详情:

上海观安信息技术股份有限公司 技术支持邮件:websec@idss-cn.com 地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

A	
您的连接不是私	密连接
攻击者可能会试图从 息)。 <u>了解详情</u> NET::ERR_CERT_AUTHORITY_I	窃取您的信息(例如:密码、通讯内容或信用卡信 INVALID
□ 自动向 Google 发送一些	<u>系统信息和网页内容</u> , 以帮助检测危险应用和网站。 <u>隐私权政策</u>
隐藏详情	返回安全连接
此服务器无法证明它是 的原因可能是配置有误或;	。 您的连接被拦截了。
继续前往 (不安全	<u>全)</u>

图 3-2

点击"继续前往 X.Y.Z.W (不安全)"即可正常访问,随后进入以下界面:

WEB应用安全防护系统初始设置 WKG&・安KG在	
帐号	admin
密码	清输入登录密码
确认密码	请再次输入密码
	保存

图 3-3

输入密码完成注册,然后即可正常登陆。

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

★ WEB应用安全防护系统-登录 × + ← → C ▲ 不安全 192.168.254.154.61234	-	0	×
上海观安信息技术股份有限公司			

图 3-4

3.2. 忘记密码

如果用户忘记密码,请及时联系厂家进行密码找回。

第4章系统功能

4.1.首页

4.1.1. 攻击画像

观镜 Web 应用安全防护系统系统可根据对网站防护的数据生成攻击画像,通过攻击画像可直观查看网站的访问状况,被攻击业务 TOP10、访问 IP TOP10、攻击类型 TOP 10 以及被攻击 URL 等信息。

模块说明:

模块名称	模块说明	备注		
上海观安信息技术	股份有限公司	电话:021- 62090100		
技术支持邮件:w	ebsec@idss-cn.com	产品服务电话:400-728-0510		
地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层				
	12 / 56			

处理请求	统计对防护站点的所有请求数量,不包括透传模式下请求数据	
保护请求	统计对防护站点在拦截模式下的所有请求	
异常请求	统计对防护站点在拦截模式下检测到的异常请求总数	
正常请求	统计对防护站点在拦截模式下的所有正常请求	

9	現安 IDS			— WEB应用	安全防护系统 —				🜲 🌗 🛓 admin -
● 首页	~								
 ✓ 站点管理 ● 防御研究 	*	② 空町 最近2小时 最近12小时 今天 前天 本周	」上周本月上月 自寇义 (11)						· · · · · · · · · · · · · · · · · · ·
(2) 用户画像	÷						站点选择 全部		
 2月戸毎後 日本哲学 日本哲学 (2)系統哲学 		中國攻击中面Top 10				7			<u>424</u> 448
		22: HEIMIOODHI			arteenancoosed				~
		0.000(1)		-O-KBRUDDE -O-RPHODE	75.8 10 0.40 0.40				-O-15988 -O-17988
		0 1007 1017 1027 1027 1027 1027 1027 1027	1647 1657 1467 1617 1627 1637 1647 1657 1657 1657 1657	1 15:17 15:47 15:47 16:07 16:17 16:27 16:17 16:47 16:57 1	08 767 1207 1202	1217 1252 1107 11	12 1017 1052 1407 1422 1	417 1452 1507 1522 1517 1552 1	6.07 36.22 36.37 36.52 37.07
			संग	1887 1887 1887 1887 1887 1887 1887 1887	81 81 1207 1222	1217 1252 1107 11	12 3837 3852 3607 3622 3	417 1460 1507 1522 1537 1582 1	607 1452 1453 1453 1767 前法 平 34
		ing do do to de do tie do tie do tie Activitation	ster ster ster ster ster ster ster ster	- 150 160 160 160 160 160 160 160 1 「京町吉田列表 <u>市号 絶址</u> 英型	7er 1222	2017 202 202 20 SA	2 1817 1852 1869 1852 1 1455 1869 1852 1	สีกา หยัง (กังกา กรังกา กรังกา กรังกา) 1950	संग संग संग संग गोग काल प स प्राह

图 4-1

4.1.2. 被攻击业务统计列表

被攻击业务查询	请求URL地址	请求时间		音· 询	^
被攻击业务统计列表				_	
序号 业务名称	URL地址	次数	请求时间	操作	
		暂无数据			

图 4-2

上海观安信息技术股份有限公司 电话:021-62090100 技术支持邮件:websec@idss-cn.com 产品服务电话:400-728-0510 地址:上海市普陀区大渡河路388弄5号华宏商务中心6层

4.1.3. 被攻击地址统计列表

	被攻击地 请求URL地	业查询 址 最新请求时间	查询				^
I	被攻击地均	业统计列表					
1	茅号	URL地址	业务名称	次数	最新请求时间	操作	
		1. 47/		425	2019-07-23 15:48:02	操作▼	
2	2	usiness/BCommonPage/HideFrame.aspx		333	2019-06-20 16:07:53	操作▼	
	3	www 125 dss		318	2019-06-13 15:13:19	操作▼	
4	1	xsc'i nanager/html		265	2019-07-09 17:19:12	操作▼	

图 4-3

4.1.4. 自动化工具统计列表

┃ 自动化	七工具查询						~
自动化	工具名称	最新IP	最新请求时间			查询	
自动化	比工具统计列表						
序号	自动化工具名称	UID	最新IP	次数	最新请求时间		操作
			暂无数据				

图 4-4

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

4.1.5. 来源 IP 访问统计列表

来源IP) 来源IP	方问查询 最新请求时间	童询			^
来源IPi	方问统计列表				
序号	UID	来源IP	次数	最新请求时间	操作
1		192.1 1.33	1042	2019-07-23 15:54:00	操作▼
2	5be5t 34aaf47079a87)654fee	10. 0.	773	2019-07-14 11:38:11	操作▼
3	804cceet	1(20.8	438	2019-07-17 20:00:08	操作▼
4	Ja5a8a78ci. 5b0ca5abade	1: 58.10	368	2019-06-17 15:34:06	操作▼
5	L .42505.	1922 🖹	344	2019-06-17 17:47:50	操作▼

图 4-5

4.1.6. 来源浏览器统计列表

来源浏览器查询						
移动端浏	览器类型	PC端浏览器类型	来源IP			
最新请求时间						
■来源浏览	览器统计列表					
序号	浏览器类型	UID	来源IP	次数	最新请求时间	操作
1	Firefox		192.168.10.33	931	2019-06-13 15:13:19	操作 ▼
2	Chrome	5be5e46c84aaf47079a87bfff0654fee	10.10.20.8	773	2019-07-14 11:38:11	操作▼
3	Chrome	804cceef11f9b5d69de335d56ddb425e	10.10.20.8	426	2019-07-17 20:00:08	操作▼
4	Chrome	8d490ba5a8a78cf225c785b0ca5abade	192.168.10.33	368	2019-06-17 15:34:06	操作▼
5	Chrome	31da930273e6e56127e425c87e632867	192.168.10.22	344	2019-06-17 17:47:50	操作▼
6	Chrome	f5fa8d5394847e567c00b1012486c8ff	10.10.20.8	317	2019-06-17 20:59:06	操作▼

图 4-6

4.2. 站点管理

系统配置可通过管理界面先配置站点以及策略,然后关联节点即可完成保护,站点保护支持普通模式保护,即一个节点

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388 弄5号华宏商务中心6层

防护一个服务器,一个节点防护多个不同类型的服务器,还支持负载均衡模式,即一个节点防护一个站点的多个服务器。

4.2.1. 站点配置

新增站点即增加需要保护的网站,站点名称可自定义名称,访问地址即保护后用户访问的地址,保护站点地址输入真 实服务器的 IP 地址或域名信息,当前支持 HTTP、HTTPS 和 WebSocket 协议,当选择 HTTPS 协议时需要上传证书以保 障正常访问。

添加站点时可选三种保护模式(拦截模式、监控模式和透传模式),系统默认为拦截模式,具体拦截内容根据所选策略进行,监控模式只对请求进行记录不做拦截操作,透传模式将所有请求放行不进行任何操作,在新增站点后可根据实际业务需求选择保护模式,以免影响网站的业务正常运行。

站点配置支持普通模式和负载均衡模式,负载均衡模式可以通过配置一个节点服务器来保护一个站点多个不同的服务器。

普通模式添加如下:

新增站点一普通模式	
* 站点名称:	
*访问地址:	ألم المعام المعام المعام المعام المعام المعام (مال المعام المعام المعام المعام المعام المعام المعام المعام الم
*受保护站点地址:	如www.baidu.com、156.56.23.10
* 目标端口:	十 添加
	HTTP v 80 删除
保护模式:	拦截模式 监控模式 透传模式
	拦截模式:根据选择的策略对用户发出的请求进行加密发送,拦截并记录攻击请求!
*基础防御策略:	请选择
主动防御策略:	
告警通知:	
	保存

新增普通站点-图 4-7

负载均衡模式添加如下:

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388弄5号华宏商务中心6层

负载模式站点-新增	保护站点		
	*集群组别名称:	请选择 v 新建组别	
	*访问地址:	如www.baidu.com、156.56.23.10 添加站点	
	*受保护站点名称:		Ŵ
	*受保护站点地址:	如www.baidu.com、156.56.23.10	
	*目标满口:	「「「」	
		HTTP V 80 Hilk	
	保护模式:	拦截模式 监控模式 送传模式	
		拦截模式:根据选择的策略对用户发出的请求进行加密发送,拦截并记录攻击请求!	
	*基础防御策略:	请选择	
	主动防御策略:		
	告廖通知:		
		利用金	

新增负载均衡站点-图 4-18

站点管理提供拓扑结构图,可直观查看当前节点防护站点情况:





4.2.1.1. HTTP 类型站点配置

* 站点名称:	Testfire
* 访问地址:	www.testfire.net
*受保护站点地址:	www.testfire.net
* 目标端口:	◆添加
	HTTP V 80 删除
保护模式:	拦截模式 监控模式 透传模式
	拦截模式:根据选择的策略对用户发出的请求进行加密发送,拦截并记录攻击请求!
*基础防御策略:	防爬虫
主动防御策略:	防御恶意攻击
告警通知:	
	站内通知
	邮件通知
	保存

图 4-20 新增 HTTP 类型防护站点

▋普通模	普通模式站点列表									
序号	站点名称	访问地址	受保护站点地址	协议	端日	动态防御节点IP	策略	保护模式	保护状态	更新时间
1	Testfire	www.testfire.net	www.testfire.net	HTTP	80	未配置	防爬虫	拦截模式	未配置	2019-10-10 23:33:41
2				НТТР	80			拦截模式	运行中	2019-10-08 10:00:15
3				HTTP	80			拦截模式	运行中	2019-09-26 10:54:16
4				НТТР	80			拦截模式	运行中	2019-09-19 15:10:08
5				HTTP	80			拦截模式	运行中	2019-09-12 14:13:25
6				HTTP	80			拦截模式	运行中	2019-09-10 15:29:11
7				НТТР	81			拦截模式	运行中	2019-09-09 17:21:28
								titan the s		

图 4-21 站点列表初始更新

步骤 2 点击"操作"栏 📝 按钮进行关联节点服务器,根据提示选择需要关联的"动态防御节点 IP 地址"以及"动态

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388弄5号华宏商务中心6层

防御节点端口",随后选择对应的"保护模式"以及"基础防御策略"和"主动防御策略",点击【保存】,如图 4-22 所示;

站点列表二次更新状态,当前保护状态显示为"已停止",如图 4-23 所示。

* 站点名称:	Testfire
*访问地址:	www.testfire.net
*受保护站点地址:	www.testfire.net
*受保护站点端口:	HTTP • 80
* 工作模式:	普通模式
动态防御节点IP地址:	10.10.10.254
动态防御节点端口:	899
保护模式:	拦截模式 监控模式 透传模式
	拦截模式:根据选择的策略对用户发出的请求进行加密发送,拦截并记录攻击请求!
*基础防御策略:	防爬虫
主动防御策略:	防御恶意攻击
告警通知:	
	站内通知
	邮件通知
	保存

图 4-22 节点服务器关联

普通模式	普通模式站点列表									
序号	站点名称	访问地址	受保护站点地址	协议	端口	动态防御节点IP	策略	保护模式	保护状态	更新时间
1	Testfire	www.testfire.net	www.testfire.net	НТТР	80	10.10.10.254:899	防爬虫	拦截模式	已停止	2019-10-10 23:42:18
2				нттр	80			拦截模式	运行中	2019-10-08 10:00:15
3				НТТР	80			拦截模式	运行中	2019-09-26 10:54:16
4				нттр	80			拦截模式	运行中	2019-09-19 15:10:08
5				НТТР	80			拦截模式	运行中	2019-09-12 14:13:25
6				HTTP	80			拦截模式	运行中	2019-09-10 15:29:11
7				HTTP	81			拦截模式	运行中	2019-09-09 17:21:28
8				HTTP	80			拦截模式	运行中	2019-09-05 14:55:18
9				HTTP	80			拦截模式	运行中	2019-08-29 15:06:17
10				НТТР	80			拦截模式	运行中	2019-08-28 15:51:55

图 4-23 站点列表二次更新

状态如图 4-25 所示。

节点列	康					
序号	动态防御节点IP	运行状态	受管状态	启动时间		操作
1	10.10.10.254	运行中	已受管	2019-10-09 14:29:1	3 先停止随后后动	• •
			图 4 24 共占昭	夕 殿に行五子		

含 4-24	卫从服务都运行开大	

序号	动态防御节点IP	运行状态	受管状态	启动时间	操作
1	10.10.10.254	未运行	已受管	2019-10-09 14:29:13	> (%)



步骤 4 重新启节点服务器开关,节点服务器状态为" 💻"(开启)时查看普通模式站点列表,"保护状态"更新为"运行

中"	,如图	4-26	所示。
----	-----	------	-----

■普通模式	普通横式站点列表									
序号	站点名称	访问地址	受保护站点地址	协议	端口	动态防御节点IP	策略	保护模式	保护状态	更新时间
1	Testfire	www.testfire.net	www.testfire.net	HTTP	80	10.10.10.254:899	防爬虫	拦截模式	运行中	2019-10-10 23:42:18
2				HTTP	80			拦截模式	运行中	2019-10-08 10:00:15
3				HTTP	80			拦截模式	运行中	2019-09-26 10:54:16
4				HTTP	80			拦截模式	运行中	2019-09-19 15:10:08
5				HTTP	80			拦截模式	运行中	2019-09-12 14:13:25
6				HTTP	80			拦截模式	运行中	2019-09-10 15:29:11
7				НТТР	81			拦截模式	运行中	2019-09-09 17:21:28

图 4-26 站点防御配置完成

步骤 5 站点防护测试配置,若为本地测试,因未绑定域名,所以通过域名访问时需先在 Windows 下配置 hosts,如图 4-27 所示;需要注意的是,这里仅作为本地测试的方式,但对于客户业务来说,需要用户通过 DNS 域名解析服务将访问流量 重定向至观镜防御节点的 IP 地址。

上海观安信息技术股份有限公司 技术支持邮件:websec@idss-cn.com 地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

🥘 *hosts - 记事本
文件(E) 编辑(E) 格式(Q) 查看(Ⅴ) 帮助(H)
Copyright (c) 1993-2009 Microsoft Corp.
#
This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
This file contains the mappings of IP addresses to host names. Each
entry should be kept on an individual line. The IP address should
be placed in the first column followed by the corresponding host name.
The IP address and the host name should be separated by at least one
space.
#
Additionally, comments (such as these) may be inserted on individual
lines or following the machine name denoted by a "#" symbol.
For example.
$^{\#}$ 102.54.94.97 rhino acme com $\#$ source server
38.25.63.10 v.acme.com # v.client.host
localhost name resolution is handled within DNS itself.
127.0.0.1 localhost
::1 localhost
10.10.10.254 www.testfire.net

图 4-27 本地 host 修改配置

步骤 8 浏览器端访问测试站点,地址不再是原先的访问地址,而是"http(s)://动态防御节点 IP 地址:动态防御节点端口",

查看是否和原先访问地址展示的 Web 界面一致, 如图 4-28 所示。

AltoroMutual		sign. In I Cor	tact la Feedback Search 60 DEMO SITE ONLY
ONLINE AMERICA LOGIN BISONAL - Beposit Perduct - Receive and the second second - Carde Products - Carde - Conducts - Car	PERSONAL Office Landing with FET Column Ell Evel Stanges, envelopes, checks to write give you more time to spind on the things you enjoy. Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description	EXALL BUSINESS	INSIDE ALTORO MUTUAL PHOLE ALTORO MUTUAL The 2000 employees of Altoro Mutual are dedicated to protectin type project and security. We pledge to provide you with the information and resources that you need to the jaccure your information and keep it confidential. This is our promise.
cy Policy Security Statement Server Status	Check REST API © 2019 Altoro Mutual, Inc.	This web application is open source!	<u>Get your copy from GitHub</u> and take advantage of advanced feat

图 4-28 动态防御效果展示界面

上海观安信息技术股份有限公司 技术支持邮件:websec@idss-cn.com 地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

4.2.1.2. HTTPS 类型站点配置

HTTPS 类型的站点进行防护配置时,在"站点管理>站点管理>新增站点"时,遵循的协议由"HTTP"变更为"HTTPS", 此时注意需要证书的上传,如图 4-29 所示,其余的配置顺序和 HTTP 类型的站点基本一致,可参照前文。

* 站点名称:	
* 访问地址:	如www.baidu.com、156.56.23.10
受保护站点地址:	如www.baidu.com、156.56.23.10
* 目标端口:	+ 添加
	HTTPS ▼ 443 上传证书 上传密钥 删除
保护模式:	拦截模式 监控模式 透传模式
	拦截模式:根据选择的策略对用户发出的请求进行加密发送,拦截并记录攻击请求!
*基础防御策略:	请选择
主动防御策略:	
告警通知:	
	保存

图 4-29 配置 HTTPS 类型防护站点

4.2.1.3. 注意事项

- 在当前已有站点处于保护状态中且节点运行的情况下,如果需要新增站点进行防护,需要在站点配置完毕、节点关联 完成显示当前站点运行保护状态为"已停止"时,重新启动相关节点服务器,以便新增的防护站点配置正常生效。
- 在配置一个节点一个端口保护多个不同站点时,如果使用"节点 IP+端口"形式访问站点,则只会访问最先添加的站点,如要正常访问则根据站点配置中的访问地址进行访问即可。

上海观安信息技术股份有限公司 技术支持邮件:websec@idss-cn.com 地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

4.2.2. 节点管理

节点配置中不需要在管理端进行添加,在部署系统的时候,通过配置数据库文件上报节点信息即可。

节点管理界面可对已上报的节点进行快捷关联站点、启动、停止和删除的操作。节点管理界面有节点信息统计,包含

内存状态、CPU 状态、磁盘状态等。

节点管理					
节点服务器					~
运行节点	2天19小时21分钟47秒				り历史消息
29.5 10	≠ 1%/ ∞	20	CPU 0 ¹ / ₆ 0 10 100	磁盘 9/78% 180 100	
节点列表列表查询					^
ip lp查询 查询					
■ 节点列表					
序号 动态防御节点IP	运行状态	受管状态	启动时间	操作	
1 192	运行中	已受管	2020-02-07 17:19:07	N 1	
版本号:2.2.0.5869				由观安	信息技术股份有限公司提供

图 4-30

4.2.3. 证书管理

Ξ	站点管	锂/证书管理							
证书	管理	1							
11	E书列表	Ę							
序	号	受保护站点名称	受保护站点地址		端口	证书	密钥	操作	
				暂无数据					

证书管理主要针对 HTTPS 站点的证书更新和删除操作。



上海观安信息技术股份有限公司 技术支持邮件:websec@idss-cn.com 产 地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

* 站点名称:	
* 访问地址:	如www.baidu.com、156.56.23.10
*受保护站点地址:	如www.baidu.com、156.56.23.10
* 目标端口:	+添加
	HTTPS V 443 上传证书 上传密钥 删除
	证书文件: ssl.crt
	密钥文件: ssl.key
保护模式:	拦截模式 监控模式 透传模式
	拦截模式:根据选择的策略对用户发出的请求进行加密发送,拦截并记录攻击请求!
*基础防御策略:	请选择
主动防御策略:	
告警通知:	
	保存

图 4-32 更新证书

4.2.4. 业务匹配

业务匹配功能主要将防护站点中的特定 URL 地址与业务相匹配用于识别被攻击业务的信息,支持通过普通模式、正常模式和字典模式进行匹配,支持设置全局业务字典以及单个站点业务匹配。

9	观安 3886310+92	DSS (ROE	新增业务匹配	D 贞田ウ스时拍系统 X		🌲 🖀 admin 👻
◎ 首页		站在管理 金秀匹配 10.10.10.47详情	• URLibbi:			
✓ 站点管理		业务匹配 业务字典	* 业务名称:			
站点管理 节点管理		▌ 10.10.10.47谨慎	描述:			• 22
证书管理		匹配的问: 7天 *		1 1000		
● 防御配置		更新时间: 2020-02-10 12:45:30 四般时间: 从更改时间计算, 原来日常访问形式获取保护站点的1	和思想,并将印度他却与父亲学师进行外的天祥			
[2] 用户画像						+ 85 20 20 20 20 20 20 20 20 20 20 20 20 20
🗒 日志管理		座号 URL 业务名称		i Hit	史職的回	lieff:
系统管理				16 7.00.05		
		版本号-2.2.0.5869				由现安信息技术股份有限公司提供

图 4-33 业务关联

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388弄5号华宏商务中心6层

4.3. 防御配置

防御配置包括主动防御配置、基础防御配置、数据脱敏配置、规则引擎配置、虚拟验证码、规则字典管理、威胁情报管理和页面监控配置。

4.3.1. 主动防御配置

主动防御配置提供系统默认三种策略模板以及自定义编辑策略,支持节点加密对象控制、敏感请求信息防护、反爬

虫配置。

I	主动防	御策略列表						
						新增	H	除
		序号	策略名称	保护站点地址	备注	操作		
		1	防爬虫	10.10.10.47(10.10.10.47-10.10.10.254:84)	适用于反爬虫防御	0		Ø
		2	防御恶意攻击	ys.fgj.taiyuan.gov.cn(ys.fgj.taiyuan.gov.cn-10.10.10.254:80), weixin(weixin.fgj.taiyuan.gov.cn-10.1	防御恶意攻击	0		Ø
		3	敏感信息保护		保护敏感信息,请在下面填写敏感信息防护URL	0		6
				共3条	上一页 1 下一页 10条/页 🗘 到第		页	确定

图 4-34 策略列表

4.3.2. 基础防御配置

基础防御配置提供系统默认三种策略模板以及自定义编辑策略,支持 HTTP 协议控制,异常页面重定向、文件上传限制及静态页面加速,支持设置站点白名单控制,添加在白名单内的路径不受策略限制,可有效提高兼容性,确保业务正常运行。

基础防	御策略列表	Ę			
					向导式新增新增量除
	序号	策略名称	保护站点地址	备注	操作
	1	防御恶意攻击	C(, , , , , , , , , , , , , , , , , , ,	防御恶意攻击	0 🗏 🕜
	2	敏感信息保护	10.	保护敏感信息,请在下面填写敏感信息防护URL	0 🗏 🕼
	3	防爬虫		适用于防爬虫防御	0 🗏 🕼
	4	xhs	X		
	5	test	p.4+1+1/40.40 17 11 ()		
				共5条 上一页 1 下一页 (10 条页 ▼ 到第 页 稀淀

图 4-35 策略列表

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388 弄5号华宏商务中心6层

策略中配置请求头部消息保护、敏感信息请求保护、敏感信息响应保护时支持使用普通匹配、正则匹配和字典匹配,

其中字典匹配可根据提示进行配置。

HTTP协议控制 站点白名单	单控制 其他									
HTTP请求方法控制		启用此功能,会对HTTP请求方法进行预定义控制								恢复默
HTTP状态码控制		允许的HTTP方法				禁止的	HTTP方	法		
HTTP请求编码控制			GET	POST	HEAD	PUT	CON	IECT	OPTION	IS
HTTP请求资源控制			TRACE			RCH	MOVE	COPY		LETE
HTTP响应内容控制			UNLOC	к мкс	OL S	UBSCRIE	BE U	NSUBSC	RIBE	BCOPY
HTTP请求头部控制			BDELE	TE BM	OVE E	BPROPF		3PROPP/	АТСН	
HTTP响应头部控制			X_MS_I	ENUMATTS	6					
HTTP响应头部控制										

图 4-36 策略配置

4.3.2.1. HTTP 协议控制——请求方法

策略配置

步骤1 当观镜完全部署后,以测试站点"www.testfire.net"为例。选择"防御配置>基础防御配置>基础防御策略列表",

点击【新增】添加策略,或者点击序号1~3系统默认自带的三种策略下的" 1" 按钮直接编辑即可,新增策略如图 4-37 所示。

offens		
香輸入策略名称	策略描述	
制其他		
启用此功能,会对HTTP请求方法进行预定义控制		10.500 (0.50) (0.500 (0.50) (0.500 (0.50) (0.500 (0.500 (0.50) (0.500 (0.500 (0.50) (0.500 (0.50) (0.500 (0.50) (0.500 (0.50) (0.50) (0.500 (0.50) (0
允许的HTTP方法		荣止的HTTP方法
		GET POST HEAD PUT CONNECT OPTIONS TRACE PATCH
		SEARCH MOVE COPY DELETE PROPFIND PROPPATCH NOTIFY
		BDELETE BMOVE BPROPFIND BPROPPATCH X_MS_ENUMATTS
	817	
	NUNEW 当日、二年の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の	NUNN

图 4-37 基础防御配置编辑策略

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388弄5号华宏商务中心6层

步骤 2 按提示对应输入"策略名称"、"策略描述"以及"关联站点",例如:新建策略名称为"test",关联站点为 "<u>www.testfire.net"(观镜对此站点的防护地址为"10.10.10.254</u>:88"),选择"HTTP协议控制>HTTP请求方法控制", 开启功能开关" " 选中允许的 HTTP请求方式为"GET""POST""HEAD",其余项默认保持禁止,点击【保存】,

如图 4-38 所示。

编辑策略		avee+****	
"面暗否称	tëst	加加西加西	
关联站点	× www.testfire.net(10.10.254-10.10.10.254:88)		
HTTP协议控制站点白名单	控制 其他		
HTTP请求方法控制	日用此功能,会对HTTP请求方法进行规定义控制		防御
HTTP状态码控制	允许的HTTP方法		禁止的HTTP方法
HTTP请求编码控制	GET POST HEAD		CONNECT OPTIONS TRACE PATCH SEARCH MOVE COPY DELET
HTTP请求资源控制			PROPFIND PROPPATCH NOTIFY POLL LOCK UNLOCK MKCOL
			SUBSCRIBE UNSUBSCRIBE BCOPY BDELETE BMOVE BPROPFIND
TTTP NO A CHARGE AND			BPROPPATCH X_MS_ENUMATTS PUT
HTTP响应内容控制			
HTTP请求头部控制			
HTTP响应头部控制			
		RT	

图 4-38 HTTP 请求方法控制策略配置

策略验证

以上配置完成后,针对服务器被禁止的 HTTP 请求方式时,就会被观镜阻拦,并且生成告警日志。使用 Burp Suite 抓 包改包构造如上的请求方式,修改情况如图 4-39、图 4-40 所示,选择"日志管理>安全防御日志"查看告警日志,结果如

图 4-41 所示。

🚯 Burp Suite	Professional	v2.0.11	beta - Ter	nporary Pr	oiect - lio	ensed to I	3v rr					
Burp Project Int	ruder Repeate	r Window	Help		- j		· · ·					
Dashboard Ta	rget Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options			
Intercept HTT	P history We	ebSockets	history 0	ptions								
Request to h	✓ Request to http://10.10.254:88											
Forward	Drop		ntercept is o	on A	ction							
Raw Params Headers Hex												
GET / HTTP/1.1												
Host: 10.10.10.25	1:88	NT 40.0			001001	04 51 4 100						
Oser-Agent: Mozil	a/5.0 (Window	s NT 10.0;	VVIN64; x64	; N:69.0) Ge I:a=0.9 */*:a=	0.9	U1 Firefox/69	.0					
Accept. textritini, Accept.l anguage:	zb-CN zb:a=0	8 zb-TW-c	=0.7 zh-HK	n=0.5,7,4-	0.0 :a=0.3 en:0	n=0.2						
Accept-Encodina:	azip, deflate	.0,211 111,0	0.1,211111	, q 0.0,01 00	, 4 0.0,000,0	1 0.2						
Connection: close	3-111											
Cookie: zngsessio	nid=9a04863a6	5ffd0b8797	ff5d5f6a8527	⁷ 8c; zA7uZW	GUB1=7kL	l3mta1l7B7∨	cOnBpq2Efd	ZiFVWrsWYqkJN	4w==; JSESSIC	NID=CE6531DEED071BED66B90331E70D7463		
ZNGIDSSTK747=p	66R2TyP3630	8387H9B4	AWPeB+vR	YCJDL2kk/q	qjH0AMbA	Ay1+xt57bO	BMxEOhdn	CEGrB0byy2KHX	tdB7fcXuK6vy3d	qUc/3iCALk8Quja3c/XpWsaGshH01Hw=; acopen		
ZNGIDSSTK754=4	Yt8s3ne4a0b1	55fGe7LC	JuNk8qtAU	CA4GFHdgR	کojdwXvwU	7Bm8ssUTJI.	JGzEf1SIJ71	20VpNvQvA1bn3+	-1o5hBcrkM5lq8	3SL7/n0aT2YIxxK5nk861rHiCkEs=		
Upgrade-Insecure-	Requests: 1											

图 4-39 Burp Suite GET 请求抓包结果

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388弄5号华宏商务中心6层

Burn Project Int	ruder Depente	r Window	Holp		-					
	ruuer Repeate	n vindow		~		~	~	~	·	
Dashboard Ta	arget Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	
Intercept HTT	P history W	ebSockets	history C	ptions						
🖉 Request to h	ttp://10.10.10.	254:88								
Forward	Drop		Intercept is	on A	ction					
Raw Params	Headers	lex								
UT / HTTP/1.1										
lost: 10.10.10.25	4:88									
lser-Agent: Mozil	la/5.0 (Window	s NT 10.0;	Win64; x64	4; rv:69.0) Ge	:ko/201001	01 Firefox/69	.0			
ccept: text/html,	application/xht	ml+xml,ap	plication/xm	nl; q=0.9,*/*; q=	0.8					
ccept-Language:	zh-CN,zh;q=0	.8,zh-TW;	zh-Hk, 7, zh-Hk	(;q=0.5,en-US	;q=0.3,en;o	q=0.2				
ccept-Encoding:	gzip, deflate									
onnection: close										
ookie: zngsessio	nid=9a04863a	6ffd0b8797	'ff5d5f6a852'	78c; zA7uZW	GUB1=7kU	/3mta1l7B7V	cOnBpq2Efc	lZiFVWrsWYqkJN	4w==; JSESSIC	NID=CE6531DEED071BED66B90331E70D74
NGIDSSTK747=p	66R2TyP3630	8387H9B4	AWPeB+vR	YCJDL2kk/qf	ʻqjH0AMbA	Ay1+xt57bO	BMxEOhdn	oCEGrB0byy2KHX	tdB7fcXuK6vy3	qUc/3iCALk8Quja3c/XpWsaGshH01Hw=; acop
NGIDSSTK754=4	Yt8s3ne4a0b1	55fGe7LC	UuNk8qtAU	CA4GFHdgR	کojdwXvwU	7Bm8ssUTJL	JGzEf1SIJ71	20VpNvQvA1bn3-	+1o5hBcrkM5lq6	SSL7/n0aT2Y1xxK5nk861rHiCkEs=
pgrade-Insecure-	Requests: 1									



≡	同志	管理/ 安	全防御日志											
安全	的街	旧志	查询											^
查道	时间			关键字 所有字	設機糊查询	=	a 是否只查看	威胁日志						
安全	的街	旧志	列表											
													展示	위 국 開除 목 出
C		序号	时间	UID	威胁标签	规则ID	規則名称	攻击详情	URL地址	请求方法	来源IP	归属地默认	状态码	操作
		1	2019-10-18 12:05:22	771c36ab55764d578973d6cebfc158b5	HTTP协议检查	70031	HTTP请求方法控制		10.10.10.254/	PUT	192.168.100.84	局域网	403	操作▼

图 4-41 HTTP 请求方法控制告警日志

4.3.2.2. HTTP 协议控制——状态码

策略配置

步骤1 当观镜完全部署后,以测试站点"www.testfire.net"为例。选择"防御配置>基础防御配置>基础防御策略列表",

点击【新增】添加策略,或者点击序号1~3系统默认自带的三种策略下的"¹"按钮直接编辑即可,新增策略如图 4-42 所示。

上海观安信息技术股份有限公司 技术支持邮件:websec@idss-cn.com 地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

■ 防御配置/基础防御配置/	斜眼镜 睛		
编辑策略			
*策略名称	test	策略描述	
关联站点	× www.testfire.net(10.10.10.254-10.10.10.254:88)		
HTTP协议控制站点白名的	控制 其他		
HTTP请求方法控制	自用此功能,会对HTTP状态局进行预定义控制		清加 疾制致认
HTTP状态码控制		允许的状态码	
HTTP请求编码控制	200 301 302 302		
HTTP请求资源控制			
HTTP请求内容控制			
HTTP响应内容控制			
HTTP请求头都控制			
HTTP响应头部控制			
	1		
		_	
		保持	

图 4-42 基础防御配置编辑策略

步骤 2 按提示对应输入"策略名称"、"策略描述"以及"关联站点",例如:新建策略名称为"test",关联站点为 "<u>www.testfire.net"(观镜对此站点的防护地址为"10.10.10.254</u>:88"),选择"HTTP协议控制>HTTP状态码控制",开 启功能开关" " 选中允许的 HTTP 响应状态码为"200"" 301"" 302"(也可点击【添加】按钮编辑新的状态

码), 点击【保存】, 如图 4-43 所示。

编辑策略			
*策略名称	test	策略描述	
关联站点	× www.testfire.net(10.10.10.254-10.10.10.254.88)		
HTTP协议控制站点白名	拉制 其他		
HTTP请求方法控制	自用此功能,会对HTTP状态码进行预定义控制		添加 快速默认
HTTP状态码控制		允许的状态码	
HTTP请求编码控制	200 X 301 X 302 X		
HTTP请求资源控制			
HTTP请求内容控制			
HTTP响应内容控制			
HTTP请求头部控制			
HTTP响应头部控制			
	I		
		_	
		6.7	

图 4-43 HTTP 状态码控制策略配置

策略验证

选择"日志管理>安全防御日志"查看告警日志,结果如图 4-44 所示。

Ξ	B	志管理/	安全防御日志							
ī	安全即	5御日7	志查询							
	查询时	0		关键字	所有字段模糊查询		2 10	是否只查看威胁日志		
i.	安全即	方御日元	志列表							
										展示列▼ 翻除 5
		序号	时间	UID	威胁标签	规则ID	规则名称	攻击详情	URL地址	i
		1	2019-10-18 14:21:58	al5a6267c819699650619e08dl3bc8c5	HTTP协议检查	10215	HTTP状态码控制	RESP_STATUS:304	10.10.10.254/images/pf_lock.glf	



4.3.2.3. HTTP 协议控制——请求编码

策略配置

步骤1 当观镜完全部署后,以测试站点"10.10.10.47"为例。选择"防御配置>基础防御配置>基础防御策略列表",点击

【新增】添加策略,或者点击序号1~3系统默认自带的三种策略下的" 📝" 按钮直接编辑即可,新增策略如图4-45 所

	2013/0192	
	an artistaut	
编辑策略		
*策略名称	test	策略描述
关联站点	x www.testfire.net(10.10.10.254-10.10.10.254:88)	
HTTP协议控制站点白名的	自控制 其他	
HTTP请求方法控制	启用此功能,会对HTTP请求编码进行预定义控制	6-BERNA
HTTP状态码控制	允许的HTTP请求编码	禁止的HTTP请求编码
HTTP请求编码控制		UNICODE BASE64 URL HEX
- HTTP请求资源控制		
HTTP请求内容控制		
HTTP响应内容控制		
HTTP请求头部控制		
HTTP响应头部控制		
		保存

图 4-45 基础防御配置编辑策略

步骤2 按提示对应输入"策略名称"、"策略描述"以及"关联站点",例如新建策略名称为"test",关联站点为"10.10.10.47"

<u>(观镜对此站点的防护地址为"10.10.10.254</u>:90")选择"HTTP协议控制>HTTP请求编码控制"开启功能开关"

上海观安信息技术股份有限公司 技术支持邮件:websec@idss-cn.com 地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

选中允许的 HTTP 请求编码为"HEX""BASE64",禁止的 HTTP 请求编码为"URL"、"UNICODE",点击【保存】, 如

图 4-46 所示。

防御配置/基础防御配置/	编辑策	調					
编辑策略							
*策略名称	test	t.	策略描述	E			
关联站点	× 10.	.10.10.47(10.10.10.47-10.10.10.254:90)					
HTTP协议控制站点白名的	单控制	其他					
HTTP请求方法控制		后用此功能,会对HTTP请求编码进行预定义控制					恢复默认
HTTP状态码控制		允许的HTTP请求编码				萘止的HTTP请求编码	
HTTP请求编码控制		BASE64 HEX			URL UNICODE		
HTTP请求资源控制							
HTTP请求内容控制							
HTTP响应内容控制							
HTTP请求头部控制				J			
HTTP响应头部控制							
	1						
			_				
			保持				

图 4-46 HTTP 请求编码控制策略配置

策略验证

以上配置完成后,针对服务器触发被禁止 HTTP 请求编码例如 "URL"时,就会被观镜阻拦,并且生成告警日志,选择 "日志管理>安全防御日志"查看告警日志,结果如图 4-47 所示。

目志管理	型/安全防御日志						
安全防御E	日志查询						^
查询时间		关键字	所有字段模糊查询			是否只查看威胁日志	
■ 安全防御E	日志列表						
							展示列 🕶 📑 🗮 🛱 🖽
□ 序号	8 BIO	UID	威胁标签	规则ID	規则名称	攻击详情	URLIEtz
1	2019-10-19 14:39:14	3a15f6e5cec2988e787a5780dbce6f0d	非法的请求编码	10302	HTTP请求编码控制	REQ_ARGS:owaspbwa	10.10.10.254/awstats/awstats.pl?config=owaspbwa

图 4-47 HTTP 请求编码控制告警日志

4.3.2.4. HTTP 协议控制——请求资源

策略配置

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388 弄5号华宏商务中心6层

步骤1 当观镜完全部署后,以测试站点"www.testfire.net"为例。选择"防御配置>基础防御配置>基础防御策略列表",

点击【新增】添加策略,或者点击序号1~3系统默认自带的三种策略下的" 🗾" 按钮直接编辑即可,新增策略如图4-48

所示。

防御配置/基础防御配置/	编辑策略				
编辑策略					
*策略名称	test		策哨描述		
关联站点	×www.testfire.net(10.10.10.254	10.10.10.254:88)			
HTTP协议控制站点白名的	単控制 其他				
HTTP请求方法控制	自用此功意。	会对HTTP请求的资源进行预定义控制			16aa
HTTP状态码控制	名称	内容	匹配模式	状态	操作
HTTP请求编码控制			智无数据		
HTTP请求资源控制					
HTTP请求内容控制					
HTTP响应内容控制					
HTTP请求头部控制					
HTTP响应头部控制					
	1				
			保存		

图 4-48 基础防御配置编辑策略

步骤 2 按提示对应输入"策略名称"、"策略描述"以及"关联站点",例如:新建策略名称为"test",关联站点为 "<u>www.testfire.net"(观镜对此站点的防护地址为"10.10.10.254</u>:88"),选择"HTTP协议控制">"HTTP请求资源控制",开启功能开关""",点击【添加】,新增HTTP请求资源控制,对应填入"名称"、"匹配模式"、"内容"、"动 作",这里以禁止请求访问 htm 资源为例,点击【保存】,如图 4-49 所示。

		WED应用立今防	拍友弦			
	新增HTTP请求资源	原控制	×			
编辑策略	*名称:	test				
	匹配模式:	通配符	¥			
test	• 内容:	htm				
× www.testfire.net(10.10.10.25	10. 动作:	禁止访问	•			
		确定				
单控制 其他		佛定				
单控制 其他	, 会对HTTP请求的资源进行预定义	2002	-			添加
#控制 其他	。 会对HTTP语求的资源进行预定义 内容	905 2288 2588-5		N.S.	服作	添加
	。 会到HITTP请求的思想进行现在义 内容	9296 92969	前无数服	378	副作	添加
単記制 其他	, 会對HTTP请求的實證近行操定文 內容	E266	猶无愈還	¥6	Rft	80
単記刻 其他	。 会到HTTP请求的资源进行预定义 内容	9286 92.62.45.25	前无动语	¥.ő	Bit:	(A)
	。 会到HTTP请求的原意进行预定义 内容	ERM USANEST	新无款派	378	Bit	800

图 4-49 HTTP 请求资源控制策略配置

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388弄5号华宏商务中心6层

策略验证

以上配置完成后,针对服务器请求访问被禁止的 htm 资源时,就会被观镜阻拦,并且生成告警日志,选择"日志管理> 安全防御日志"查看告警日志,结果如图 4-50 所示。

日志管理	對 安全防御日志									
安全防御日	志查询									^
查询时间		关键字	所有字段機關查询		書词	是否只查看威胁日志				
安全防御日	志列表									
								展示列▼	881¢	母出
□ 序号	助问	UID	威胁标签	规则ID	規則名称	攻击详情	URL地址	请	求方法	来源IP
1	2019-10-19 13:17:08	771c36ab55764d578973d6cebfc158b5	HTTP协议检查			REQ_URI:/index.jsp?content=personal_savings.htm	10.10.10.254/index.jsp?content=personal_savings.htm	GE	T	10.10.20.8

图 4-50HTTP 请求资源控制告警日志

4.3.2.5. HTTP 协议控制——请求内容

策略配置

步骤1 当观镜完全部署后,以测试站点"www.testfire.net"为例。选择"防御配置>基础防御配置>基础防御策略列表",

点击【新增】添加策略,或者点击序号1~3系统默认自带的三种策略下的" 📝"按钮直接编辑即可,新增策略如图4-51

所示。

编辑策略								
*策略名称	test			館職指	谜			
关联站点	×www.testfire.net(10.10.10.254-10.10.10.2	54:88)					
HTTP协议控制 站点白名	单控制 其他							
HTTP请求方法控制		启用此功能,会对HTTP	青求的内容进行预定义控制					添加
HTTP状态码控制	名称	URL	业务标识	检测参数	匹配模式	内容	动作	操作
HTTP请求编码控制					暂无数据			
HTTP请求资源控制								
HTTP请求内容控制								
HTTP响应内容控制								
HTTP请求头部控制								
HTTP响应头部控制								
				6.17				

图 4-51 基础防御配置编辑策略

上海观安信息技术股份有限公司 技术支持邮件:websec@idss-cn.com 地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

步骤 2 按提示对应输入"策略名称"、"策略描述"以及"关联站点",例如 新建策略名称为"test",关联站点为"<u>10.10.10.47"</u> (观镜对此站点的防护地址为"10.10.10.254:90")选择"HTTP协议控制>HTTP请求内容控制",开启功能开关"¹", 点击【添加】,新增HTTP请求内容控制,对应填入"名称"、"URL"、"检测参数"、"匹配模式"、"内容"、"动作",这里以 禁止请求 URL 路径为"/awstats/awstats.pl"下当参数"config"内容为"owaspba"为例,点击【保存】,如图 4-52 所示。

		WED应用它会防护系统		
	新增HTTP请求内容		×	
御記習/基础的御記習/ 编辑性略	* 名称:	test		
略	* URL:	/awstats/awstats.pl		
*策略名称 test	业务标识:	请输入业务标识		
关联站点 ×10.10.10.47(10.10.10.47-10.10.1	检测参数:	config		
	匹配模式:	普通模式 ▼		
的议控制 站点白名单控制 其他	* 内容:	owaspbwa		
南求方法控制 ①	动作:	禁止访问		
代态码控制 名称 URL		确定		内容 动作
南求编码控制		智无数	过度	
青求资源控制				
構成の実施制				

图 4-52 HTTP 请求内容控制策略配置

策略验证

以上配置完成后,针对服务器触发被禁止返回的 HTTP 请求内容时,就会被观镜阻拦,并且生成告警日志,选择"日志管理>安全防御日志"查看告警日志,如图 4-53 所示。

安全	防御日	志列表							展示列▼	100
	序号	时间	VID 拦截日至	威胁标签	规则ID	规则名称	攻击详情	URL地址		请求方法
	1	2020-02-21 10:07:22	e6e861cc3f423fd2e98ef6b57411	4537 请求内容检测	10700	HTTP请求内容控制	REQ_BODY:123456	10.10.10.254/dvwa/	login.php	POST
版本号:2.3	2.0.586	9							由观安信期	制技术股份有限公司提
	HT	TP协议控制站点白名	S单控制 其他 日本的 新 日本 「 日本 」 「 日本	,会对HTTP请求的内容进	行操定义控	朝 策略	配置			24.55
~	н	TTP状态码控制	名称	URL 业务标	识	检测参数	匹配模式	内容	动作	操作
~	H	TTP请求编码控制	请求内容检测	/		password	普通模式	123456	禁止访问	Ð

图 4-53 请求内容控制验证

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388弄5号华宏商务中心6层

4.3.2.6. HTTP 协议控制——响应内容

策略配置

步骤 1 当观镜完全部署后,以测试站点"10.10.10.47"为例。选择"防御配置>基础防御配置>基础防御策略列表",点击【新增】添加策略,或者点击序号 1~3 系统默认自带的三种策略下的" 逻" 按钮直接编辑即可,新增策略如图 4-54

所示。

防御配置/基础防御配置/	编辑策略							
编辑策略								
*策略名称	test				策略描述			
关联站点	× 10.10.10.47(10.10	.10.47-10.10.10.254:90)						
HTTP协议控制站点白名	单控制 其他							
HTTP请求方法控制		启用此功能, 会对HTTP响8	室的内容进行预定义控制					添加
HTTP状态码控制	名称	URL	位置	内容	匹配模式	长度限制	动作	操作
HTTP请求编码控制					暂无数据			
HTTP请求资源控制								
HTTP请求内容控制								
HTTP响应内容控制								
HTTP请求头部控制								
HTTP响应头部控制								
					-			
					BK77			

图 4-54 基础防御配置编辑策略

步骤 2 按提示对应输入"策略名称"、"策略描述"以及"关联站点",例如 新建策略名称为"test",关联站点为"<u>10.10.10.47"</u> (观镜对此站点的防护地址为"10.10.10.254;90"),选择"HTTP协议控制>HTTP响应内容控制",开启功能开关" " 点击【添加】,新增 HTTP响应内容控制,对应填入"名称"、"URL"、"内容"、"动作",这里以禁止请求 URL 路径为 "/wordpress/"下的"New Plug-ins"内容为例,如图 4-55 所示。

上海观安信息技术股份有限公司 技术支持邮件:websec@idss-cn.com 地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

		新增HTTP响应内容	WEB市田ウム防守支法 控制	×		
基础防御配置/ 编辑策略						
		* 名称:	test			
		* URL:	/wordpress/			
*策略名称 test		位置:	body •			
关联站点 × 10.10.10.4	7(10.10.10.47-10.10.1	匹配模式:	通配符 🔻			
		* 内容:	New Plug-ins			
站点白名单控制 其	他	*长度限制:	0			
拉制	启用此功能,会	动作:	禁止访问			
潮 名称	URL		确定		长度限制	动作
控制			暫	无数据		
1空布]						
控制						

图 4-55 HTTP 响应内容控制策略配置

策略验证

以上配置完成后,针对服务器触发被禁止的 HTTP 响应内容时,就会被观镜阻拦,并且生成告警日志,选择"日志管

理>安全防御日志"查看告警日志,结果如图 4-56 所示。

=	E	志管理	/安全防御日志					
13	安全國	6御日	志查询					^
1	查询时	间		关键字	所有字段模糊查询		重调	最高兴查查编编的日本
13	安全家	師日	志列表					
								展示引 マ 189 年出
		序号	时间	UID	威胁标签	规则ID	规则名称	改击详續
		1	2019-10-19 14:12:10	3a15f6e5cec2988e787a5780dbce6f0	d HTTP协议检查			RESP_BODY: <doctype *="" *http:="" 1.0="" <html="" dtd="" en*="" html="" iw3c="" public="" td="" tr="" transitional="" www.w3.org="" xhtml="" xhtml1="" xhtml1-transitional.dtd*="" xmln<=""></doctype>



4.3.2.7. HTTP 协议控制——请求头部

策略配置

步骤 1 当观镜完全部署后,以测试站点"10.10.10.47"为例。选择"防御配置>基础防御配置>基础防御策略列表",点击【新增】添加策略,或者点击序号 1~3 系统默认自带的三种策略下的"¹"按钮直接编辑即可,新增策略如图 4-57 所示。

防御配置/基础防御配置/参	耀策略							
编辑策略								
*策略名称	test			策略描述				
关联站点	× 10.10.10.47(10.1	0.10.47-10.10.10.254:90)						
HTTP协议控制站点白名单	控制 其他							
HTTP请求方法控制		启用此功能,会对HTTP请求头部进行预定	义的控制				必要条件	添加
HTTP状态码控制	字段	控制目标	控制策略	内容	匹配模式	t	操作	
HTTP请求编码控制				智无数据				
HTTP请求资源控制							規則条件	添加
HTTP请求内容控制	宁段	控制目标	控制策略	内容	匹配模式	动作	操作	
HTTP请求头部控制				智无数据				
HTTP响应头部控制								
				保存				

图 4-57 基础防御配置编辑策略

			WEB应用点人				
		新增HTTP请求头部	形规则	×			
基础防御配置/编辑	副箔略	* 字段:	User-Agent				
		控制目标:	内容	*			
*策略名称 [1	lest	控制策略:	包含	*			
关联站点	10.10.10.47(10.10.10.47-10.10.1	匹配模式:	通配符	•			
		• 字典类型:	Mozilla				
站点白名单约	空制 其他	动作:	禁止访问	•			
迎朝	(1) 約用此功能, 4		确定				必要条件
鄉	学段	空制目标	控制策略	内容	匹配模式		操作
控制				智无数据			规则条件
	字段	控制目标	控制策略	内容	匹配模式	动作	操作
(1218) 對空制	User-Agent	内容	包含	Mozilla	通配符	禁止访问	۲
短期							

图 4-58 HTTP 请求头部控制策略配置

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

策略验证

以上配置完成后,针对服务器触发被禁止返回的 HTTP 请求头部信息时,就会被观镜阻拦,并且生成告警日志,选择

"日志管理>安全防御日志"查看告警日志,结果如图 4-59 所示。

日本管理	/ 安全防御日志						
安全防御日;	志查询						^
查询时间		关键字	所有字段機關查询		西河	是西只會看編勝日志	
安全防御日	志列表						
						■元3]▼ ■■■	98
□ 序号	时间	UID	威胁标签	规则ID	规则名称	攻击详销	
1	2019-10-19 14:29:57	3a15f6e5cec2988e787a5780dbce6f0d	HTTP协议检查			REQ_User-Agent:Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safarl/537.36	

图 4-59 HTTP 状态码控制告警日志

4.3.2.8. HTTP 协议控制——响应头部

策略配置

步骤 1 当观镜完全部署后,以测试站点"10.10.10.47"为例。选择"防御配置>基础防御配置>基础防御策略列表",点击【新增】添加策略,或者点击序号 1~3 系统默认自带的三种策略下的"¹"按钮直接编辑即可,新增策略如图 4-60 所示。

■ 防御配置/基础防御配置/編	建物理		
编辑策略 *證略名称 关职站点	est www.testfice.net(10.10.10.254-10.10.10.254.80)	1049163.6	
HTTP协议控制 站点白名单	 一 直用此功能、会对HTTP状态同进行预定又控制 		(1800) · 研約(1853)
HTTP場求場時控制 HTTP場求場時控制 HTTP場求の時控制 HTTP場求の時控制 HTTP場定内容控制 HTTP場求失差控制	200 3 301 3 302 3	901489100FB	
HTTP病应失器控制		an .	

图 4-60 基础防御配置编辑策略

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388弄5号华宏商务中心6层

步骤 2 按提示对应输入"策略名称"、"策略描述"以及"关联站点",例如 新建策略名称为"test",关联站点为"<u>10.10.10.47"</u> (观镜对此站点的防护地址为"10.10.10.254:90"),选择"HTTP协议控制>HTTP响应头部控制",开启功能开关以及规则条件开关" " ,点击【添加】,对应填入"字段"、"控制目标"、"控制策略"、"匹配模式"、"字典类型"、"动作",

这里以禁止访问当字段"Set-Cookie"下的内容为"zngsessionid"为例,点击【保存】,如图 4-61 所示。

			~	WED前田空へ	陆市东休				
			新增HTTP响应头部	3规则		×			
防御配置/基础》	方御配置/ 編集	和物格	* 字段:	Set-Cookie					
編策略			控制目标:	内容	•				
*甜椒	888 1	est	控制策略:	包含	*				
×	美彩态后	10 10 10 47(10 10 10 47-10 10 1	四配模式:	通配符	•				
			*字典类型:	zngsessionid					
TTP协议控制	站点白客单担	記刻 其他	动作:	禁止访问	¥				
TTP请求方法控制		自用此功能, 4	e.	确定					必要条件
TTP状态码控制		7Q	控制目标	控制策略		内容	匹配模式		操作
TTP请求编码控制					877-8410				
TTP请求资源控制					H./Laxua				规则条件
TTP请求内容控制			v El la	175 Actions	du 🛱	_	0.528.t	7047	154
TTP响应内容控制		318	21-4 MP	17.0336ed	134		COMPANY.	-11/2	Tak I

图 4-61 HTTP 响应头部控制策略配置

策略验证

以上配置完成后,针对服务器触发被禁止返回的 HTTP 响应头部信息时,就会被观镜阻拦,并且生成告警日志,选择 "日志管理>安全防御日志"查看告警日志,结果如图 4-62 所示。

E F	志管理	安全防御日志						
安全	方御日元	志查询						~
查询时	间		关键字	所有字段模糊查询		查询	2015日本 2015日本	
安全	方御日言	志列夷						
								展示列 🔻 🏙 🗍 🖽
	序号	时间	UID	威胁标签	规则D	规则名称	攻击详简	URL地址
	1	2019-10-19 14:35:33	3a15f6e5cec2988e787a5780dbce6f0d	HTTP协议检查			RESP_Set-Cookie:zngsessionid=366ea26fd3397a50b4b6249e06a0d730;path=/;httponly;	10.10.10.254/v

图 4-62 HTTP 响应头部控制告警日志

上海观安信息技术股份有限公司 技术支持邮件:websec@idss-cn.com 地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

4.3.2.9. 异常页面重定向

策略配置

步骤1 当观镜完全部署后,以测试站点"10.10.10.47"为例。选择"防御配置>基础防御配置>基础防御策略列表",点击

【新增】添加策略,或者点击序号 1~3 系统默认自带的三种策略下 " 💴 "按钮直接编辑即可,新增策略如图 4-63	3所示。
--	------

防御配置/基础防御配置/	编辑策略				
编辑策略 "放略名称 关联站点	test * 10 10 10 47(10 10 10 47-10 10 10 254 90)	10000			ب ا
HTTP协议控制 站点自名单 异常页面重定向	单控制 其他 主用此功差,异定页面会被服定的封闭定页面				1630
名称	响应码	重定向URL地址		操作	
文件上传租制	启用此功能,文件上传夹型将受到用树	暫无数退	Ξ.		添加
名称	文件后缀		备注	操作	
静态页面加速配置 维存有效期 24	RARDE, HIHRPLANDORRESH	裕 无政策	÷		
		Rtf			

图 4-63 基础防御配置编辑策略

步骤 2 按提示对应输入"策略名称"、"策略描述"以及"关联站点",例如 新建策略名称为"test",关联站点为"<u>10.10.10.47"</u> (观镜对此站点的防护地址为"10.10.10.254:90"),选择"其他>异常页面重定向",开启功能开关" "",点击【添 加】,新增异常页面重定向配置,输入"名称"、"响应码"、"重定向 url 地址",这里以当响应码为"403"时,重定向页面 至 "http://www.baidu.com"为例,点击【保存】,如图 4-64 所示。

新增异常	重定向配置	×	
防衛配置/基础防衛配置/编辑策略	舌称: test		
策略	如码: 403		
*策略各称 test * 重定向	也止: http://www.baidu.com		
关联独立 (×10.10.10.47(10.10.10.47-10.10.10	确定		
协议控制 站点白名单控制 其他			

图 4-64 异常页面重定向策略配置

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388弄5号华宏商务中心6层

策略验证

以上配置完成后,针对服务器触发被状态码 "403"时,就会被观镜阻拦,并重定向至百度首页,结果如图 4-65 所示。

匪 百度 https://www.baidu.com								4
			新闻	<u>hao123</u>	<u>地图</u>	视频	贴吧	<u>学术</u>
	Baidu百度							
		0 ====	-					
		回自度	- K					
○ 我的关注	推荐 导航							
	當以下信息根据您的兴趣推荐	实时热点	<					
第七届世界	军人运动会开幕式举行 文艺表演美轮美奂	墨西哥大毒枭之子	陈坤为周迅庆生					

图 4-65 异常页面重定向结果

4.3.2.10. 文件上传限制

策略配置

步骤1 当观镜完全部署后,以测试站点"10.10.10.47"为例。选择"防御配置>基础防御配置>基础防御策略列表",点击 【新增】添加策略,或者点击序号1~3系统默认自带的三种策略下的"¹ 了"按钮直接编辑即可,新增策略如图4-66所



图 4-66 基础防御配置编辑策略

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388 弄5号华宏商务中心6层

步骤 2 按提示对应输入"策略名称"、"策略描述"以及"关联站点",例如 新建策略名称为"test",关联站点为"<u>10.10.10.47"</u> (观镜对此站点的防护地址为"10.10.10.254;90"),选择"其他>文件上传限制",开启功能开关" "",点击【添加】, 新增文件上传限制配置,输入"名称"、"备注"、"文件后缀",这里文件后缀为"php"限制上传为例,点击【保存】,如图 4-67 所示。

	新增文件上传限制酶	記置	×	
防御配置/基础防御配置/编辑策略			<u></u>	
	* 名称:	test		
議策略	*文件后缀:	php]	
*策略名称 test	备注:			
9489845		織定		
P协议控制站点白名单控制其他				
t页面重定的 🕥 前用此功能,异常页面会被重定的	倒搬定页面			
称 响应码		重定向URL地址		操作
		智无数据		

图 4-67 文件上传限制策略配置

策略验证

以上配置完成后,针对服务器上传 php 文件时时,就会被观镜阻拦,并且生成告警日志,选择"日志管理>安全防御

日志"查看告警日志,结果如图 4-68 所示。

≡	Bi	は管理/	安全防御日志												
■安	全防	御日志	·查询												~
查	的时间	1		关键字	所有字段模糊查询		査論	是否只查看威胁	日志						
5	のAR用ロナ利車														
	(土羽)	JEH CI VG	A79-04										展示列 ▼	BIR I	导出
		序号	时间	UID	威胁标签	规则ID	规则名称	攻击详情	URL地址	请求方法	来源IP	归属地默认	状态码	操作	_
		1	2019-10-19 15:32:34	3a15f6e5cec2988e787a5780dbce6f0d	PHP温洞攻击	70039	PHP脚本攻击检测	FILES: 1.php	10.10.10.254/WackoPicko/piccheck.php	POST	10.10.20.8	局域网	403	操作▼	

图 4-68 文件上传限制告警日志

4.3.3. 数据脱敏配置

通过配置指定的位置,选择响应的加密算法对数据进行脱敏配置。

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388弄5号华宏商务中心6层

当前已	当前已脱敏的URL 今返回												
										新增			
	序号	更新时间	UBL	加密方式	位置	内容	脱敏	算法	运行状态	操作			
	1	2019-07-23 15:57:15	/Fire d/h-* robl	解密	argument	nid=([-()&proje :([-0-9]+)	nid: .projectid=	低	拦截	Ø			
	2	2019-06-14 18:14:10	/F: rfc/put Prc	加密	body	show! ew\('(-? +)', '(-?[0-9]+)'	sh BView('\$1','	低	拦截	8			
	3	2019-06-14 16:53:03	sthan /pu /r	加密	body	pid= -9]+)	рі	低	拦截				
	4	2019-06-14 16:53:00	-irsthand/	加密	body	nid= 9]+)&proj =(-?[0-9]+)	ni &projectid	低	拦截	(
	5	2019-06-14 16:52:57	Firsthand/ty	加密	body	getł eBaseInfr ?[0-9]+)"\)	ge JseBasr (/\$1')	低	拦截	Ø			
	6	2019-06-14 16:52:54	Firsthapr' sh/ L	加密	body	sho jInfo\('(-']+)^\)	sh rglr ،')	低	拦截	Ø			
	7	2019-06-14 16:52:50	and/tyfc/sho	加密	body	pid= 0-9]+`	pid=	低	拦截	Ø			
	8	2019-06-14 16:52:41	/TYFC/wx/publish/ProjListForP	加密	body	"prc "-9]+)"	"propid":"\$1"	低	拦截	@			

图 4-69 数据脱敏配置列表

策略配置

步骤1 当观镜完全部署后,以测试站点"<u>www.testfire.net"为例。</u>选择"防御配置>数据脱敏配置>基础防御策略列表", 找到目标站点后,开启功能开关" ",点击【新增】,添加目标站点下需要脱敏的 URL,填入"加密方式"、"URL"、 "内容"、"脱敏"、"算法"、"加密方式"、"运行状态"、"是否启动"相关信息后,点击【确定】,这里以 URL 路 径为"/index.jsp"下的"Phone"内容中的"1.800.555.0002"脱敏为"xxxx"为例,配置结果如图4-70 图4-71 所示。

	_	WEP应用空合比拍系统			
	添加		×		
防御配置/ 数据脱敏配置/ 当前已脱敏的URL	加密方式	力D225 、			
当前已脱敏的URL	位置	body •			
	* URL	/index.jsp		算法	运行状态
	*内容	1.800.555.0002			
	*脱敏	XXXXX			
	算法	低 *			
	运行状态	监控 ▼			
		是 ▼ 確定	_		

图 4-70 数据脱敏配置编辑策略

上海观安信息技术股份有限公司 技术支持邮件:websec@idss-cn.com 地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

≡	防御	配置/ 数据脱	軟配置/ 当前已脱脓的URL							(2月成功)		×
当前	ne.	皺的URL								🗸 क् राव्यक्रफ		×
												新増
		序号	更新时间	URL	加密方式	位置	内容	BRAK	算法	运行状态	操作	
C		1	2019-10-19 16:34:56	/index.jsp	地遊	body	1.800.555.0002	жнок	低	监控	2	
								共1条 上一页	1	回 10条/页 ¥	912E	风闲定



策略验证

以上配置完成后,针对服务器目标站点刷新页面后,会发现 "Phone" 内容中 "1.800.55.002" 成功脱敏为 "xxxx",

对比结果如图 4-72、图 4-73 所示。

PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL				
Contact Us						
Have a question? It's easy to reach us.						
E-mail						
Filling out the <u>online form</u> is the most efficient method of contact. If you listed below.	are requesting a change to your account, please call the phone number					
Phone		Altoro Mutual is				
To open a new account, please call: 1.800.555.0001 8:00 a.m 6:00 p.m., Eastern Time, Monday - Friday	→	headquartered at the Altoro Mutual Tower in Anywhere, MA.				
For assistance with your account, please call: 1.800.555.0002 24-hour touch-tone banking information is available 7 days a week.	数据脱敏前					
Mail						
To contact us by mail, you may send inquiries to: Altoro Mutual Altoro Mutual Tower Anywhere, MA	To contact us by mail, you may send inquiries to: Altoro Mutual Altoro Mutual Tower					
E-mail Security						
Any inquiry you send to Altoro Mutual via our Contact Us page uses Secu information remains confidential.	ire Socket Layer (SSL) encryption. SSL helps to ensure that your personal					
To take advantage of SSL, however, you must have an SSL-compatible be	rowser. Altoro Mutual recommends you use the following browsers:					
Windows and Unix operating systems: Netscape Navigator 4.08 of 4.01 or later. Macintosh: Netscape Navigator 4.08 or later, Netscape Communicative Statement of the systems of the	Windows and Unix operating systems: Netscape Navigator 4.08 or later, Netscape Communicator 4.7 or later, and Microsoft Internet Explorer 4.01 or later. Machinetic Materian Navionator 4.08 or later, Netscape Communicator 4.7 or later, and Microsoft Internet Explorer					
Go to Netscape or Microsoft for downloads.	Go to Netscape or Microsoft for downloads.					
Mail Subscription						
Altoro Mutual often introduces new and exciting promotions. We encoura offers.	ge all visitors to subscribe to our mailing list to receive these incredible					

图 4-72 数据脱敏前后目标站点内容

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388 弄5号华宏商务中心6层

PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
Contact Us Have a question? It's easy to reach us.		
E-mail		
Filling out the <u>online form</u> is the most efficient method of contact. listed below.	If you are requesting a change to your account, please call the phone number	
Phone		
To open a new account, please call: 1.800.555.0001		Altoro Mutual is headquartered at the Altoro Mutual Tower in Anwhere Mi
8:00 a.m 6:00 p.m., Eastern Time, Monday - Friday		Allywhere, ma,
For assistance with your account, please call: xxxxx 24-hour touch-tone banking improvedien is available 7 days a week	κ.	
Mail	······································	
To contact us by mail, you may send inquiries to: Altoro Mutual Altoro Mutual Tower Anywhere, MA	数据脱敏后	
E-mail Security		
Any inquiry you send to Altoro Mutual via our Contact Us page use information remains confidential.	s Secure Socket Layer (SSL) encryption. SSL helps to ensure that your personal	
To take advantage of SSL, however, you must have an SSL-compar-	tible browser. Altoro Mutual recommends you use the following browsers:	
 Windows and Unix operating systems: Netscape Navigator 4.01 or later. 	4.08 or later, Netscape Communicator 4.7 or later, and Microsoft Internet Explor	rer
Macintosh: Netscape Navigator 4.08 or later, Netscape Commi	unicator 4.7 or later, and Microsoft Internet Explorer 4.5 or later.	
Go to Netscape or Microsoft for downloads.		
Mail Subscription		
Altoro Mutual often introduces new and exciting promotions. We en	ncourage all visitors to subscribe to our mailing list to receive these incredible	

图 4-73 数据脱敏后后目标站点内容

4.3.4. 规则引擎配置

规则引擎为用户提供了自定义规则的功能,为了更完善的适应站点的业务,根据站点日常访问量来精准的配置更适合站点的策略,通过 UID 来精准识别访问源,可以更精准的防范恶意访问而不误杀,支持配置访问触发规则时的处理方式,如界面通知或邮件通知,以及拉入恶意 IP 库等。

*规则名称	请输入规则名称							
• 地址	请输入地址							
* 规则	请求方法 GET POST HEAD OPTION TRACK DELETE PUT 其他							
	· 响应状态码 □ 10X □ 20X □ 30X □ 40X □ 50X □ 其他							
	访问频次 1 次 1 秒							
	持续时间 请输入 分							
• 动作	 ✓ 告警 ※遵iP加入恶意iP席 将UID加入恶意UID列表 「拒绝访问 」 虚拟验证码 							
	告警等级 🔿 低 📀 中 🔿 高							
	濾知 💟 页面递知 🦳 創箱							
描述								
	保存							

图 4-74 规则引擎配置列表

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388 弄5号华宏商务中心6层

策略配置

步骤1 当观镜完全部署后,以测试站点"10.10.10.47"为例。选择"防御配置>规则引擎配置>规则引擎列表",点击【新

建规则】添加规则,对应输入"规则名称"、"地址"、"规则"、"动作",点击【确定】,新建规则如图 4-75、图 4-76 所示。

防御配置/规则引擎配置/规则列表-添加规则	
▌规则列表-添加规则	
* 规则名称	test
* itetat	/wordpress
* 规则	请求方法 SET SEP OST SEP HEAD SEPTION SET TRACK SEP DELETE SEPTIFIES HEAD
	响应状态码
	访问规次 1 次 20 秒
	特號制刷 1 分
* zb/fe	✓ 告答 □ 持衛や加入影響中先 □ 持UID加入影響UID列表 □ 目時切詞
	告醫等级 〇 砥 🧿 中 〇 高
	避知 🏹 页面通知 🗌 邮箱
描述	
	<u>(k</u> H)

图 4-75 规则引擎配置编辑策略

■ 約個化型/規則当年公理										
1 规则引擎列表								新建規則		
		序号	规则名称	地址	规则详情	动作	告警等级	更新时间	操作	
		1	testfire5	/wordpress	访问频次:20秒1次 持续时间:1分钟 响应状态码:10X 20X 30X 40X 50X 请求方法 GET POST	告誓 虚拟给证码	中	2019-10-19 15:36:05	■ 🕜 ■	

图 4-76 规则引擎配置编辑策略完成

步骤 2 择"防御配置>虚拟验证码",开启功能开关" 💶 ",选择"验证复杂程度"、"验证码长度"、"默认验证配

置"、"失败验证配置",点击【确定】, 配置结果如图 4-77 所示。

防御配置/ 虚拟验证码	
虚拟验证码	
虚拟验证码开关	
验证复杂程度	纯数字 纯字母 数字+字母
验证码长度	4
默认验证配置	2 次 10 秒
失败验证配置	2 次
	 ○ 禁止访问 5分钟 ▼ ○ 将IP加入恶意IP库 ○ 将UID加入恶意UID列表

图 4-77 虚拟验证码配置

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

电话:021-62090100 产品服务电话:400-728-0510

地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

策略验证

以上配置完成后,针对服务器目标站点按规则频次访问后,就会被观镜阻拦,提示验证码信息,结果如图 4-78 所示。



图 4-78 规则引擎触发告警

4.3.5. 虚拟验证码

虚拟验证码用于在出发规则引擎后的处置动作,支持配置复杂度及验证次数等。

虚拟验证码开关		
验证复杂程度	纯数字 纯字母 数字+字母	
验证码长度	7	*
默认验证配置	5 次 10	秒
失败验证配置	2	次
	 ○ 禁止访问 永久 ◆ ○ 将・P加入恶意!P库 ✓ 将UID加入恶意UID列表 	
	确定	

图 4-79 虚拟验证码

4.3.6. 规则字典管理

字典管理用来对策略配置中选择的字典进行管理,对站点的业务关联提供全局字典等。字典类型包括业务关联、头部 保护、敏感信息和敏感响应四类,支持普通模式和正则模式两种。

上海观安信息技术股份有限公司 技术支持邮件:websec@idss-cn.com 地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

添加字典		×
* 字典名称	请输入字典名称	
字典类型	业务关联	
字典描述	业务关联 头部保护	
匹配模式	敏感信息 敏感响应	
	请灭内容	
	网 4 90 今世 町 署	

图 4-80 字典配置

4.3.7. 威胁情报管理

威胁情报管理当前版本主要用于对恶意 IP、恶意用户以及 IP 安全组的管理,系统内置数十万条全球范围内的恶意 IP

三 防	御配置	/威胁情报配置					
恶意用户列	扆	IP安全组管理 IP威胁情报	库				
IP情报	查询						~
IP地址			添加方式	关键字 IP位置情报标签描述		登陆时间	查询
IP情报	列表						
							删除添加IP
	序号	; IP地址	登陆时间	IP位置	情报标签	添加方式	苗述 操作
	1	1	2020-02-05 13:12:50	test		人工添加	R 🕑
	2	21 - 27	2018-08-02 16:53:24			情报库	R 🖉
	3	81011000	2018-08-05 15:18:14			情报库	R 🖉
	4	121.221.122.104	2018-08-02 17:36:40			情报库	R 🖉
	5	٤ · ـ ـ ٢	2018-08-05 19:33:27			情报库	R 🖉
	6		2018-08-03 12:11:19	德克萨斯州		情报库	R 🖉
版本号:2.2.	0.5869						由观安信息技术股份有限公

数据, 支持人工添加 IP, 支持从日志中快捷添加至恶意 IP 库中以阻止访问, 并且可以对恶意 IP 进行导出操作。

图 4-81 恶意 IP

安全组管理支持用户自定义访问规则,设置指定 IP 或 IP 段允许访问、透传访问或禁止访问,并更具规则优先级进行

执行,方便用户在特殊环境下对网站进行安全操作。

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388弄5号华宏商务中心6层



4.3.8. 页面监控配置

		静态页面配置	×				
防御	配置/页面监控配置/页面监持	空 监控周其	3天 7天 15天				
┃ 页面监控	Ż	告警配置	t 🗌				◆ 返回
访问地址			确定		數量	孤立页面访问数量	更新时间
	:.cn:80	l - U	U	U		0	
▌静态页面	面监控列表						
							除添加页面静态页面配置
序号	URL	录入MD5	当前MD5	监控状态		更新时间	操作
				暂无数据			
▌ 孤立页面	面监控列表						
							除添加页面 孤立页面配置
序号	URL	监控状态		更新时间			操作
				暂无数据			

图 4-83 页面监控配置

4.4. 用户画像

通过各种指纹将来访用户标记为唯一用户,并统计该用户的访问信息。

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

观镜 WEB 应用安全防护系统

用户使用手册



图 4-84 用户画像

4.5. 日志管理

4.5.1. 安全防御日志

防御日志中可查看所有保护站点记录的请求记录,支持通过多种条件进行组合查询,方便用户对攻击进行溯源。支持通过快捷操作将访问日志中的 IP 地址添加至安全组规则或恶意 IP 库,支持将访问日志中的被访问 URL 地址添加至策略中的站点白名单,以免一项正常业务的运行。

上海观安信息技术股份有限公司 技术支持邮件:websec@idss-cn.com 地址:上海市普陀区大渡河路388 弄5号华宏商务中心6层

安全防	御日	志查询														~	_
查询时) (1)			关键字	所有字段模糊	査询	2	询	是否只查	看威胁日志	I						
安全防	御日	志列表															
														展示列 ▼	删除	导出	1
	序号	时间	UID		威胁标签	规则ID	规则名称	攻击详情	URL地	ιŁ				 ✓ 序号 ✓ 时间 		请求方法	
	1	2019-07-23 16:32:00	40b36aa3415ea3b3152c7	7b57d2b02095					уь				1mon/j	que VID	ding.gif	GET	
	2	2019-07-23 16:31:59	40b36aa3415ea3b3152c7	7b57d2b02095					ys.fgj.t.				olish/g	■ 規則的型		POST	
	3	2019-07-23 16:31:59	40b36aa3415ea3b3152c7	7b57d2b02095					ys	go	Fi	nd/t	plist	 ✓ 規則名称 ✓ 攻击详情 		POST	
	4	2019-07-23 16:31:59	40b36aa3415ea3b3152c7	7b57d2b02095					ys e	¢	/Fi	nd	vlist.	◎ 业务名称		GET	
	5	2019-07-23 16:31:53	40b36aa3415ea3b3152c7	7b57d2b02095					ys :		/			● 事件类型 ✓ URL地址		GET	
	6	2019-07-23 16:22:39	299a8c9c864244b54bdbe	9d40ff9c867							/F		rfc: sh/P	□ 访问端口 □ 请求方法		POST	
	7	2019-07-23 16:22:34	299a8c9c864244b54bdbe	9d40ff9c867					3	V BL	.Cı.	t)	rfc/psh/g	POST内容		POST	
	8	2019-07-23 16:22:34	299a8c9c864244b54bdbe	9d40ff9c867						v	.cn/l	1 13	sh/r	 ✓ 来源IP ✓ 归属地默认 		POST	
	9	2019-07-23 16:22:34	299a8c9c864244b54bdbe	9d40ff9c867					11	yua .	çn/(h b	fc /	✓ 状态码		GET	
	10	2019-07-23 16:22:31	299a8c9c864244b54bdbe	9d40ff9c867						_		b	nu. Jubi	User-Agent		POST	
														 客户端浏览器 ■ 客户端操作系统 			
					共 6585 务	t L-	页 1	2	3	4 6	5		659	► Referer		页 确定	£
	-										-			● 普戶端请求大小 ● 服务器响应大小			
														☑ 操作	J		

图 4-85 防御日志

发至恶意IP库		×
* IP地址	10.00	
描述		
	确定 取消	

图 4-86 快捷发送至恶意 IP 库

发至规则		×
*安全组名称:	Test1 •	
* 规则类型:	允许透传访问 ▼	
* 授权对象	10.0.0	
规则描述:		
	(长度为2-256个字符,不能以http://或https://开头)	
	确 定 取消	Ĭ

图 4-87 快捷发送至安全组规则

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388弄5号华宏商务中心6层

发至策略白名单		×
* 选择策略: * 授权对象:	防御自动化工具扫描	T
		确定 取消

图 4-88 快捷发送至策略白名单

4.5.2. 系统操作日志

系统操作日志提供当前系统登录登出以及功能操作等信息记录,方便用户查看系统操作信息。

▲ 系统操作	乍日志查询				^
用户名	请输入用户名	操作时间 请输入查询时间		查询	
系统操作	乍日志列表				鲁田
序号	时间	用户名	来源IP	操作内容	结果
1	2019-07-23 16:33:55	admin	1 - 00	IP安全组IP安全组启动关闭	操作成功
2	2019-07-23 16:00:57	admin	2 0	登录模块通过用户名密码登入	操作成功
3	2019-07-23 15:57:15	admin	na2. 1	数据脱敏编辑脱敏规则	操作成功
4	2019-07-23 15:31:23	admin	1	登录模块通过用户名密码登入	操作成功
5	2019-07-23 15:19:59	admin	19/ .1	节点管理模块节点启停	操作成功
6	2019-07-23 15:19:53	admin	15 3.1	节点管理模块节点启停	操作成功
7	2019-07-23 15:19:46	admin	3.	站点管理模块更新站点	操作成功
8	2019-07-23 15:19:00	admin		站点管理模块新增站点	操作成功
9	2019-07-23 15:05:20	admin	э:	规则字典规则编辑	操作成功
10	2019-07-23 14:42:34	admin	19:	登录模块通过用户名密码登入	操作成功
			共 700 条 上一页	1 2 3 4 5 70 下一页 10	条/页 ≑ 到第 页 确定

图 4-89 系统操作日志

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388弄5号华宏商务中心6层

4.5.3. 告警通知日志

1 1	告警证	通知日志	适询													^	
	最新IP			告	警时间	查询											
	告警通知日志列表																
														【标记为已	读	删除	
		序号	事件类型	自动化工具名称	级别	详情	目标	地址						UID	最亲	ĥIP	
		1			低	規则引擎名称: /Firsthand/tyfc/publish/p/Projinfo.do	ş	thand		list	0	J.		f8228c8c3ccab84be95ddb72b28bf261			
		2			中	规则引擎名称: 爬虫	,	hand	24	Пř	4	11	o.do	c32741d06e8a7031f5390241f4f4aa5f	1"		10
		3			中	規则引擎名称: 爬虫	/F	iand	24	μ	h	It	o.do	c32741d06e8a7031f5390241f4f4aa5f	۲		7.10
		4			中	规则引擎名称: /Firsthand/tyfc/publish/probld/NBView.do	/Fi	and	a	li	r	Vie	,	d3966475d5207dc642608dd3f56126a0	ŧ	э.,	1
		5			中	規则引擎名称: /Firsthand/tyfc/publish/probld/NBVIew.do	/Fi	an(CJ	II	r	Vie	E.	9a09f39fe993c6c386ff8feb44564496	1	5.:	١¢
		6			中	規则引擎名称: /Firsthand/tyfc/publish/probld/NBView.do	/Fi	3Di	۲.	1	r	Vle	1	9a09f39fe993c6c386ff8feb44564496	15	54)	1
		7			中	规则引擎名称: 爬虫	/Fi	and	c/	ł		ise	do	ab4eef045de02a68e9c9eb312c277ad7	22:	2	
		8			中	规则引擎名称: 爬虫	/Fi	зn	c/		OL	i ise	do	dcbf18693626f0681c39161bfa28d2ee	124		E.
		9			中	规则引擎名称: 爬虫	/FI	an	c/l	e	101	1 3SC	do	cb22ac827efc8fd7c229042f33d3a224	59.	Э	3
		1 0			中	规则引擎名称: 爬虫	/Firs		'c/j		3/1		.do	a0be1b4c95ae1200765e6894fdffb7a8	59.		38

图 4-90

4.6. 系统管理

4.6.1. 用户管理

用户管理界面支持增加和更新用户信息,支持创建普通用户和管理员两种角色用户,其中管理员角色拥有系统所有操 作权限,普通角色用户只有查看权限,还可以通过用户管理对用户进行锁定和解锁操作,支持配置登入策略,当连续失败 N 次时锁定设定时间。

新增用户		×
*用户名	请输入用户名	
*密码	请输入密码	
* 密码确认	再次确认密码	
*角色	管理员	
姓名	请输入姓名	
联系电话	请输入联系电话	
邮箱	请输入邮箱	
	确定	

图 4-91

登录策略管理					
登录失败次数	请输入登录失败次数	次			
锁定时间	请输入锁定时间	分			
密码更换提醒周期	请输入密码更换提醒周期	天			
	确定				

图 4-92

Ľ	用户列	表								
									#	除 新建用户 登录策略管理
		序号	用户名	角色	邮箱	电话	用户状态	创建时间	最近登录时间	操作
		1	1	管理员			正常	2020-02-10 12:54:43		- € € 🛍
		2	admin	超级管理员			正常	2020-02-03 15:10:59	2020-02-10 11:56:25	- C *
								共2条	上一页 1 下一页 10	象/页 ▼ 到第 页 确定

图 4-93

4.6.2.存储配置

日志配置提供通过 Syslog 和 FTP 来管理日志服务器,可通过配置输出指定类型的日志,为避免持续访问造成的日志

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层

量过大,提供日志磁盘归档管理,当日志容量达到设定阈值时则对旧日志进行归档操作。

日志导出配置							
* 日志类型	防御日志 原始日志						
*服务器类型	syslog ftp						
• 主机	请输入主机						
*协议	\$						
*端口	514						
	保存						
存储容量配置							
当前可用最大磁盘空间	1.28GB						
日志服务器最大磁盘容量	G						
当日志量达到设定的阈值时,将会删除最早的部分数据,新数据做追加							
	保存						
日志存储配置							
当前储存路径	/opt						
日志储存路径	请输入日志储存路径						
	保存						

图 4-94 日志配置

4.6.3. 告警配置

通过告警配置对系统告警进行统一管理。

告警事件配置告警服务器配置	告警接收配置
节点状态告誓配置	告警等级高中低
系统监控告警配置	页面通知
安全防御告警配置	邮件通知
规则引擎告警配置	确定
页面监控告警配置	

图 4-95 告警配置

上海观安信息技术股份有限公司

技术支持邮件:websec@idss-cn.com

地址:上海市普陀区大渡河路388弄5号华宏商务中心6层

配置邮箱服务器作为发送端,如未正确配置则无法发送邮箱告警功能。

邮箱服务器配置				
邮箱发送地址:	请输入发送地址	发送端口:	请输入端口	
邮箱账户:	请输入邮箱账户	发送密码:	请输入密码	
是否SSL加密:				
				測试连接 确定 取消

图 4-96 日志配置

4.6.4. 系统信息

通过版本信息可以直接查看观镜 Web 应用安全防护系统 2.1 的当前版本以及授权信息,可以通过上传更新包离线升

版本信息 当前系统版本 2.1.0.9727 升级引擎 请上传引擎升级文件(.tar.gz)和引擎签名文件(.sig) 当前规则库 升级规则库 授权信息 唯一机器码 a6c1cb49c2b65e38e5ef7d337e608774 授权状态 软件已授权 授权有效期 20370728 更新授权 状态监控 序号 服务器地址 服务器类型 磁盘告警阈值 内存告警阈值 CPU告警阈值 软件异常监控 监控状态 操作 1 管理端服务器 无 未监控 • 1 80% 80% 80% 2 管理端服务器 80% 80% 80% 无 未监控 • 3 节点服务器 80% 80% 80% 无 未监控 •

级系统以及更新授权文件,如下图所示:

图 4-97 系统信息

上海观安信息技术股份有限公司 技术支持邮件:websec@idss-cn.com 地址:上海市普陀区大渡河路 388 弄 5 号华宏商务中心 6 层