

# Supernova 测试仪 Web 应用检测配置手册

网测科技

2021-01-22



# 目录

1.	文档说明	3
2.	网络拓扑	3
3	创建测试用例	Δ
٥. ۸	5. 法行并收测用例	+
4.	连1]开血测用例	
5.		5



### 1. 文档说明

本文档主要介绍 Web 应用检测用例的配置使用过程。随着需求的不断改变,可能会对用例配置进行修改和升级,从而改变配置过程,所以有任何问题,请联系我们的售前或售后支持人员。

## 2. 网络拓扑

以测试仪测试端口和被测网络在同一网段为例,测试仪 port2 和被扫描应用服务器直连。网络拓扑如下所示:





#### 3. 创建测试用例

1)登录系统,依次点击,用例->系统安全测试->安全检测评估->Web 应用 检测->增加,单击增加,在弹出的选择用例选项中,编辑用例网络选项,根据需 要修改配置参数,然后点击确定,进入用例配置页面。

<b>◎ </b> 网测科技	H H					る服告	1 5100	admin					V20.12.06	Supe	ernova-88D
E Richard O o Alexandro O E shireshi o O	;	Veb <u>Ny⊞</u> ł¢ namc±nas	M web発型、主	凯名、特定目录	d, escalat.	sq注入漏洞	9, cookie, #	的Ecomming,按同主机的许能http機式調整。	当新共包含14种扫描调整。支持10种	编码技术。					
Interpreted o     associated o     associated o     associated o		160列表	2 ##*			905							Vanto	R	
<ul> <li>■ Web如用绘制</li> <li>▶ 网络银号性制</li> <li>● Dool532曲</li> </ul>		日 编号 显示行数: 10	0-0	of 0	598.8	HP.		选择用例选项	27		526	2.98	inecia	朝田	Britsche
で 10:00:00:00:00     またいな話を知られ      たいな話を知られ      たいな話を知られ								IP版本 受到设备纠然	● <sup>14</sup> 应用服用 ~						
e Fredright o								新式(K和立用服务器) 网络配置	● 在地-子向 ○ 由词-MHR 服氏人類教 >>						

2)点击确定,进入用例配置界面,配置子网信息。被扫描主机 IP 即与测试 仪相连的应用服务器网卡的 IP,服务器端口可以指定一个或多个。

基本信息(Web应用检测)		
用例寫称 WebScann 合法字符图型	r_TP_admin_20210122-09:41:58 A-Z / a-z / 0-9 / : / - / _ (不支持中文符号)	
网络参数记录		
保守网络设置	客户端 port1	选择与受测设备连通的测试口 🜌 🗷 🗷 🗷 🗷 🗷
	子网 0	Wer Gerall On 63:41:24
	篇1个子网	期記20第ロP時年 18.1.2.2   第記20第日時年 18.1.2.2   第記20第日時年 17.1.1   ● 第記20第日時年   ● 第記20第日時年   ● 第記20第日時年   ● 第記20第日時年   ● 第記20第日時年   ● 第記20第日時年   ● ●   ● 受別设备日期年
		E337 - 第238

3)进行参数配置。扫描类型控制用不同的方式来扫描目标主机,编码技术 选项是指定 IDS 的躲避技术,这里采用的是 LibWhisker 的 IDS 躲避技术。配置 完成后,保存用例。

网络 参数 记录	
<b>用例参数</b> 通用参数	
演行部件间隔	
扫描关型	
编码技术	
ssi模式	
	强制使用50%成尤,紫心不使用



### 4. 运行并监测用例

1)保存后自动返回主页面,点击运行配置保存的 Web 应用检测用例。

<b>◎ 网测科</b> netitest.c	支		「「「「」」	派告	新统 admin					V20.12.0	Sup	ernova-88D
■ 阿关設前測试 ◎	ß	Web应用检测										
◎ 代理设备测试 ●	Θ	扫描描定主机的web能型 主机名	特定日录 rasi	副家 satiti 入海県	cookie 特定coi服用 读回主机	分许的tto様式等等。当前并包含 14 和	印描图题,支持10.种编码技术。					
■ 应用服务测试 ⊙	0											
日 终端客户激词 <del>0</del>		用例列表										
9 <u>Skotn</u> i 0												
由安全经测行法		+ 1220 8 889										8 時入 27 RBF
▶ 系统屬何扫描		- #9 - 55	任务列表	甩户	名字			9945	党政	详细信息	导出	历史记录
▶ Web应用检测 ▶ 网络服务检测	0	□ 1 <b>★</b>	8	admin	WebScanner_TP_admin_	20210122-09:41:58		1	41	æ	R	0
DOoSREE		显示行数: 70 - 1-1 of 1	点击此按领	田 运行编辑	冒保存的测试用例							e 1 3
C INTERMEN												
1. 四大用箭略拉用												
+ 防火場自动化检测												
ピ网络治胆分析の												

2) Web 应用检测用例启动后进入运行状态,扫描到主机和端口的信息后会显示到页面上,显示最新的10条结果。

						ADDIELSE		
t i	占用	SR	最近的10个结果:			用例名称	用户名称	运行
内存 Gliss	94.54%	64322 MB	URI	HTTP请求方式	WE CONTRACT OF CONTRACT.			
			/icons/README	GET	Apache detault hie tound.			
			/icons/	GET	Directory indexing found.			
				IRACE	HTTP TRACE method is active, suggesting the nost is vulnerable to XST			
				OPTIONS	Allowed HTTP Methods: GET, HEAD, KOST, OPTIONS, TRACE			
			1	GET	PHY//L - PHY //L is the or Life and only receives security updates, it will be unsupported after 2019-12-01.			
			,	HEAD	OpenSCI (1.0 3)-free sensers to be outdated (current is at least 1.1 to). OpenSCI (1.0 3)-free sensers to be outdated (current is at least 1.1 to).			
			,	HEAD	OHD/71 31 annears to be outdated (current is at least 7 2 31) or DH2 7 1 27 for the 7 1 v branch			
				GET	The XiCnsteet June.Ontions header is not set. This could allow the user anent to render the content of the site in a different fashion to the h			
				CET	The V VPP Personnel is not defined. This bands are highly been even to be extend and the control of VPP			

#### 5. 查看报告

1) 点击报告->查看报告,找到刚刚运行的用例,点击打开测试结果按钮。

🚫 网测科技 🚆 🤗	<b>1</b> 8 <b>2</b> 12	≪▲ 1825 - 新務	admin			V20.12.06	Supernova-88D
报告类型							
<ul> <li>説試目标 金郎 マ</li> <li>用砂絵果 金郎 マ</li> </ul>			用999年21 金55 M 8月15月16日 デビニョンドロ - メニニャンドル	用例案物	1088121. 279		
报告列表							
8 888 8 889/FN ■ 201888 点击查	看测试报告						C Rust
· 编号 再次运行 运行计学 · · · · · · · · · · · · · · · · · · ·	用例类型	测试用户	用制名称	开始时间	结束时间	THE	克隆
1 🖈 • 🕬	Web任用检测	ədmin	WebScanner_TP_admin_20210122-09:41:58	2021-01-22 09:47:54	2021-01-22 09:50:09	*	Ø



2) 打开之后可以看到详细的扫描结果,包括 URI、请求方式、详细描述、目的端口、网站域名、网站 IP 地址等信息。

<b> 信息</b>							
名 用户 结果	WebScanr admin ● 測試运行	er_TP_admin_20210 T正常结束	2122.09-41.58 用時使実型 Web回用短期 开始期间 2021-01-22.09-47.54 戦策時间 2021-01-22.09-50-09				
数据							
再次這	行 [2	) 1.500 E	下题HTML [] 下题FOF ] 下版Word				<b>會 删除此记</b>
iort1							
编号	URI	HTTP请求方式	(##	日約達口	网站城安	网站中地市	
			JEACT.	P-IN2MAP-1	1-3-14-52-1-4	A-2NHU NENT	OSVDBID
1	1	GET	Heart - Elicijacking X-Frame-Options header is not present.	80	18.1.1.100	18.1.1.100	OSVDB-0
1 2	// /	GET GET	The anti-clicijacking X-Frame-Options header is not present. The XXSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS	80	18.1.1.100 18.1.1.100	18.1.1.100 18.1.1.100	OSVDB-0 OSVDB-0
1 2 3	/ / /	GET GET GET	The anti-clospacking X-Frame-Options header is not present. The NXSP-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS The X-Content-Type-Option header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.	80 80 80	18.1.1.100 18.1.1.100 18.1.1.100	18.1.1.100 18.1.1.100 18.1.1.100	OSVDB-0 OSVDB-0 OSVDB-0
1 2 3 4	1 1 1 1	GET GET HEAD	The anti-clicitacting X-Frame-Options header is not present. The ANXSE-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS The X-XOTEMT-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type PHP/71.31 appears to be outdated (current is at least 7.2.21) or PHP 71.27 for the 7.1 x branch.	80 80 80 80 80	18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100	18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100	OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0
1 2 3 4 5	/ / / / /	GET GET HEAD HEAD	The anti-clicitacting X-Frame-Options header is not present. The Anti-clicitacting X-Frame-Options header is not present. The X-XDS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XDS The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the ste in a different fashion to the MIME type PHP/7.131 appears to be outstated (ourner is at least 7.2.21) or PHP 7.1.27 for the 7.1 x branch. OpenSSU-10.28-fips appears to be outstated (current is at least 1.1.1c). OpenSSL 1.0.00 and 0.9.8z are also current.	80 80 80 80 80 80 80 80 80 80	18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100	18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100	OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0
1 2 3 4 5 6	/ / / / /	GET GET HEAD HEAD HEAD	The anti-clicityacking X-Frame-Options header is not present. The Anti-clicityacking X-Frame-Options header is not present. The XXSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS The X-Content Type-Options header is not set. This could allow the user agent to protect against some forms of XSS The X-Content Type-Options header is not set. This could allow the user agent to protect against some forms of XSS The X-Content Type-Options header is not set. This could allow the user agent to protect against some forms of XSS The X-Content Type-Options header is not set. This could allow the user agent to protect against some forms of XSS OptionSLI 10.2 Advance to be outstated (current is at least 1.11(1) OptionSLI 1.0.00 and 0.9.8cc are also current. Apache/2.4.6 appears to be outstated (current is at least 1.428), Apache 2.2.34 is the EOL for the 2.x branch.	80 80 80 80 80 80 80 80 80 80	18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100	18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100	OSVD8-0 OSVD8-0 OSVD8-0 OSVD8-0 OSVD8-0 OSVD8-0 OSVD8-0
1 2 3 4 5 6 7	1 1 1 1 1 1 1 1 1 1	GET GET HEAD HEAD HEAD GET	The anti-clicityacking X-Frame-Options header is not present. The Anti-clicityacking X-Frame-Options header is not present. The XXSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS The X-Content Type-Options header is not set. This could allow the user agent to protect against some forms of XSS PHP7/1.31 apparent to be outdated (current is at least 7.221) or PHP 7.122 for the 7.124 branch. OpenSSU10.224 fpg appears to be outdated (current is at least 7.114). OpenSSU 10.00 and 0.9 & are also current. Apache/2.46 appears to be outdated (current is at least 7.124). PHP7/1.1 - PHP 7.1 is End of Life and only receives security updates. It will be unsupported after 2019-12.01.	80 80 80 80 80 80 80 80 80 80	18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100	18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100	OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0
1 2 3 4 5 6 7 8	1 1 1 1 1 1 1 1 1 1 1	GET GET HEAD HEAD GET OPTIONS	The anti-clicitading X-Frame Options header is not present. The Anti-clicitading X-Frame Options header is not present. The X-SDS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS The X-Content Type-Options header is not set. This could allow the user agent to protect against some forms of XSS The X-Content Type-Options header is not set. This could allow the user agent to protect against some forms of XSS The X-Content Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type PHP/7.1.971 agpears to be outdated (current is at least 7.221) or PHP 7.1.27 for the 7.1.x branch. OpenSUL10.2x-fips appears to be outdated (current is at least 7.221) or PHP 7.1.27 for the 7.1.x branch. PHP/7.1.PHP 7.1.EVP 7.1.20 for the 2.0 of Life and only receives security updates. It will be unsupported after 2019.12.0. Allowed HTTP Methods: GET, HEAD, PGST, OPTIONS, TRACE	80 80 80 80 80 80 80 80 80 80	18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100	18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100	OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0
1 2 3 4 5 6 7 8 9	1 7 7 7 7 7 7 7 7	GET GET HEAD HEAD GET OPTIONS TRACE	The anti-clicityacking X-Frame-Options header is not present. The anti-clicityacking X-Frame-Options header is not present. The X-SDF-Protection header is not defined. This header can hirt to the user agent to protect against some forms of XSS The X-Content-Type-Options header is not set. This could allow the user agent to protect against some forms of XSS The X-Content-Type-Options header is not set. This could allow the user agent to protect against some forms of XSS The X-Content-Type-Options header is not set. This could allow the user agent to protect against some forms of XSS The X-Content-Type-Options header is not set. This could allow the user agent to protect against some forms of XSS PHP/7.1.31 appears to be outdated (current is at least 7.22.1) or PHP 7.1.27 for the 7.1.x branch. Oper/SCJ/1.02.rbps appears to be outdated (current is at least 7.22.1) or PHP 7.1.27 for the 7.1.x branch. PHP/7.1 - PHP 7.1 Is End of Life and only receives security updates. It will be unsupported after 2019-12.01. Allowed HTP Methods: GET, HEAD. POST, OPTIONS, TRACE HTTP TRACE method is active, suggetting the host is vulnerable to XST	80 80 80 80 80 80 80 80 80 80 80	18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100	18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100 18.1.1.100	OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0 OSVDB-0

4) 点击生成文档,可以将报告以 HTML/PDF/Word 格式下载下来。

