Web 风险评估报告

重庆邮电大学

网站风险评估报告

——《信息安全工程》报告

课程名称 信息安全工程

班　　级

专　　业 信息安全

任课教师

学　　号

姓　　名 _____

名目

一、评估预备

1、安全评估目标

在工程评估阶段，为了充分了解 SecurityTweets 这个网站的安全系数，因此需要对 SecurityTweets 这个网站当前的重点效劳器和 web 应用程序进展一次抽样扫描和安全弱点分析，对象为 SecurityTweets 全站，然后依据安全弱点扫描分析报告，作为提高SecurityTweets 系统整体安全的重要参考依据之一。

2、安全评估范围

本小组将对如下系统进展安全评估：

承受 linux 系统的 web 效劳器〔IP 地址：176.28.50.165〕

承受 nginx 效劳器程序的 web 站点

承受 MySQL 的数据库

3、安全评估团队

成员组成：

组员	姓名	班级	学号

使用工具：

1、Acunetix Web Vulnerability Scanner

2、BurpSuite

4、安全评估量划

1、此次针对网站的安全评估分为 2　个步骤进展。第一步利用现有的优秀安全评估软件来模拟攻击行为进展自动的探测安全隐患；其次步依据第一步得出的扫描结果进展分析由小组成员亲自进展手动检测，排解误报状况，查找扫描软件无法找到的安全漏洞。

2、第一步我们承受两种不同的渗透测试软件对网站做总体扫描。承受两种工具是由于这两个工具的　侧重点不同，可以互为补充，使得分析更为准确。然后生成测试报告。

3、依据上一步生成的测试报告，由组员亲自手动验证报告的可信性。

4、依据安全扫描程序和人工分析结果写出这次安全评估的报告书。

二、风险因素评估

1. 威逼分析

1.1.　威逼分析概述

本次威逼分析是对一个德国的 SecurityTweets　网站进展的。威逼分析包括的具体内容有：威逼主体、威逼途径、威逼种类。

1.2.　威逼来源

SecurityTweets　网站是基于 Internet　体系构造建立，网络业务系统大都承受 TCP/IP 作为主要的网络通讯协议，其自身供给了各种各样的接口以供使用和维护，然而，这些接口同样可能向威逼主体提供了攻击的途径：

来源		描述
环境因素		断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震、意外事故等环境危害或自然灾难，以及软件、硬件、数据、通讯线路等方面的故障
人为因素	恶意人员	不满的或有预谋的内部人员对信息系统进展恶意破坏；采用自主或内外勾结的方式盗窃机密信息或进展篡改，猎取利益

		外部人员利用信息系统的脆弱性，对网络或系统的保密性、完整性和可用性进展破坏，以猎取利益或炫耀力量
	非恶意人员	内部人员由于缺乏责任心，或者由于不关心或不专注，或者没有遵循规章制度和操作流程而导致故障或信息损坏； 内部人员由于缺乏培训、专业技能缺乏、不具备岗位技能要求而导致信息系统故障或被攻击

1.1. 威逼种类：

1.描述

这个脚本是可能简洁受到跨站点脚本〔XSS〕攻击。

跨站点脚本〔也被称为 XSS〕是一种漏洞，允许攻击者发送恶意代码〔通常在 Javascript 中的形式〕给其他用户。由于扫瞄器无法知道是否该脚本应当是可信与否，它会在用户上下文中，允许攻击者访问被扫瞄器保存的任何 Cookie 或会话令牌执行脚本。

虽然传统的跨站点脚本漏洞发生在效劳器端的代码，文档对象模型的跨站点脚本是一种类型的漏洞会影响脚本代码在客户端的扫瞄器。

2. 描述

基于堆的缓冲区溢出在 nginx1.3.15 的SPDY 执行 1.4.7 和 1.5.x 版本 1.5.12 之前之前允许远程攻击者通过特制的恳求执行任意代码。该问题影响的 ngx_ _spdy_module 模块〔默认状况下不编译〕，并编译 nginx 的 - 与调试配置选项，假设“听”指令的“SPDY”选项用于在配置文件中。

3. 描述

您使用的是脆弱的 Javascript 库。一个或多个漏洞报告这个版本的JavaScript 库。询问攻击细节和 Web 引用有关受影响的库，并进展了报道，该漏洞的具体信息。

4.描述

XML 支持被称为“外部实体”，它指示 XML 处理器来检索和执行内嵌的设施包括 XML 位于特定 URI 的。一个外部 XML 实体可以用来追加或修改与 XML 文档相关联的文档类型定义〔DTD〕。外部 XML 实体也可以用于对 XML 文档的内容中包含的 XML。

现在假设 XML 处理器解析数据从下攻击者掌握的一个光源发出。大多数时候，处理器将不会被确认，但它可能包括替换文本从而引发意想不到的文件翻开操作，或 传输，或任何系统 IDS 的 XML 处理 器知道如何访问。

以下是将使用此功能包含本地文件〔/ etc / passwd 文件〕的内容的例如 XML 文档

<? XML 版本=“1.0”编码=“UTF-8”？>

<! DOCTYPE 的 Acunetix[

<! 实体 acunetixent 系统“文件:/// etc / passwd 文件”>

]>

<XXX>&acunetixent;</ XXX>

4.描述

此警报可能是假阳性，手动确认是必要的。

跨站恳求伪造，也称为一次单击攻击或会话骑马和缩写为 CSRF 或者 XSRF，是一种类型的恶意攻击网站即未经授权的命令是从一个用户，该网站信任传递的。

WVS 的 Acunetix 找到一个 HTML 表单与实施没有明显的 CSRF 保护。具体信息请询问有关受影响的 HTML 表单的信息。

5.描述

用户凭据的传送是在一个未加密的通道。这些信息应当始终通过加密通道〔 S〕，以避开被拦截恶意用户转移。

6.描述

点击劫持〔用户界面补救的攻击，用户界面补救攻击，用户界面救济的权利〕是诱骗网络用户点击的东西从什么用户会感觉到他们是点击，从而有可能泄露机密资料，或利用其电脑同时掌握不同的恶意技术点击看似无害的网页。

该效劳器没有返回的 X 帧选项头这意味着该网站可能是在点击劫持攻击的风险。 X 框，选择响应头可以被用于指示扫瞄器是否应当被允许以呈现页面中的<frame>或<IFRAME>。网站可以利用这一 点避开点击劫持攻击，以确保其内容不会嵌入到其他网站。

7.描述

一个常见的威逼 Web 开发人员面对的是一个密码猜测攻击被称为蛮力攻击。蛮力攻击是试图通过系统地尝试字母，数字和符号的每个可能的组合，直到你觉察工作一个正确的组合来觉察密码。

这个登录页面没有对密码猜测攻击〔蛮力攻击〕的任何保护。它的建议，以实现一个定义不正确的密码尝试次数后，某些类型的帐户锁定的。对于询问有关解决此问题的具体信息的 Web 引用。

8.描述

OPTIONS 方法在此 Web 伺服器已启用。 OPTIONS 方法供给了由 web 效劳器所支持的方法列表，它代表约可在觉察 Request-URI 的恳求/响应链中的通讯选项信息的恳求。

9.描述

一个可能的敏感名目已经找到。这个名目不是直接从 website.This 检查一下常见的敏感资源，如备份名目链接，数据库转储，治理页面，临时名目。这些名目中的每一个可以帮助攻击者更多地了解他 的目标。

10. 描述

虚拟主机是一台效劳器〔或效劳器池〕上托管多个域名〔每名独立处理〕的方法。这允许一个效劳器共享它的资源，诸如存储器和处理器周期，而无需供给使用一样的主机名的全部效劳。

这个 Web 效劳器响应不同，当主机头操纵以及各种常见的虚拟主机进展测试。这可能说明有一个虚拟主机存在。

11.描述

此 cookie 不具备 Only 标志设置。当一个 cookie 设置与 Only 标志，它指示该 cookie 只能由效劳器而不是由客户端脚本访问的扫瞄器。这是一个会话 cookie 的一个重要的安全保护。

12. 描述

当一个的名称，并输入密码的形式和提交表单时，扫瞄器会询问密码应当是 saved.Thereafter 显示表单时，该名和密码自动填充或完成输入名称。与本地访问攻击者可以从扫瞄器缓存中猎取明文密 码。

2. 安全评估

2.1. 高危漏洞：

1.影响

恶意用户可能注入的 JavaScript，VBScript 中，的 ActiveX，HTML 或 Flash 成为一个易受攻击的应用程序来哄骗用户，以便从他们那里收集数据。攻击者可以窃取会话 cookie 并接收帐户，冒充用户。另外，也可以修改呈现给用户的网页的内容。

2.影响

攻击者可以导致堆内存缓冲区溢出的工作进程通过使用特制的恳求，可能导致任意代码执行。

3.影响

攻击可以包括公开本地文件，其中可能包含敏感数据，如密码或用户的私人数据，使用文件：系统识别打算或相对路径。由于攻击发生相对于应用程序处理 XML 文档，攻击者可能会利用此受信任的应用程序转动到其他内部系统，有可能泄露通过 〔S〕恳求其他内部内容。

2.2. 中级漏洞

1.影响

攻击者可能会迫使一个 Web 应用程序的用户执行攻击者"的选择的行动。一个成功的 CSRF 攻击会危及最终用户的数据和操作的状况下，一般用户的。假设最终的目标用户是治理员帐户，这可能会危及 整个 Web 应用程序。

2. 影响

第三方可以通过拦截一个未加密的 连接来读取用户凭据°

2.3. 低级漏洞

1.影响

影响取决于受影响的 Web 应用程序。

2.影响

攻击者可能试图通过系统地尝试字母，数字和符号的每个可能的组合，直到觉察工作的一个正确组合，以觉察一个弱口令。

3.影响

OPTIONS 方法可能暴露敏感信息可以帮助一个恶意用户编写更先进的攻击。

4.影响

此名目可能暴露敏感信息，可以帮助恶意用户预备更高级的攻击。

5.影响

可能的敏感信息泄露。

三、 综述

Scan of http://testhtml5.vulnweb.com:80/

Scan details

Scan information	
Start time	2014/6/29 14:30:59
Finish time	2014/6/29 14:39:09
Scan time	8 minutes, 10 seconds

Server information	
Responsive	True
Server banner	nginx/1.4.1
Server OS	Unknown
Server technologies	

Threat level

acunetix threat level

Level 3: High

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

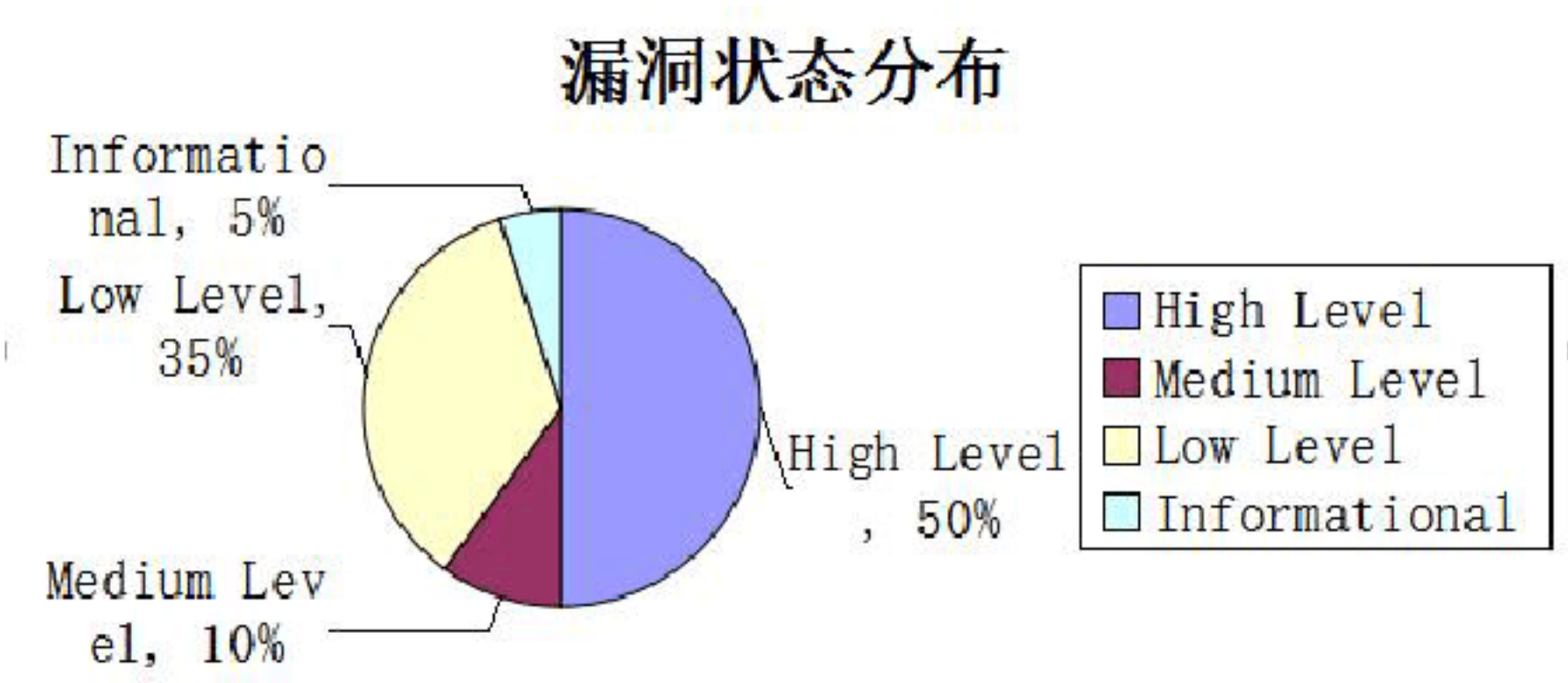
Total alerts found	20
High	10
Medium	2
Low	7
Informational	1

Alerts summary

1.1 具有最多安全性问题的文件

URL	漏洞数
	4
[redacted]	2
	3

1.1web 风险分布统计

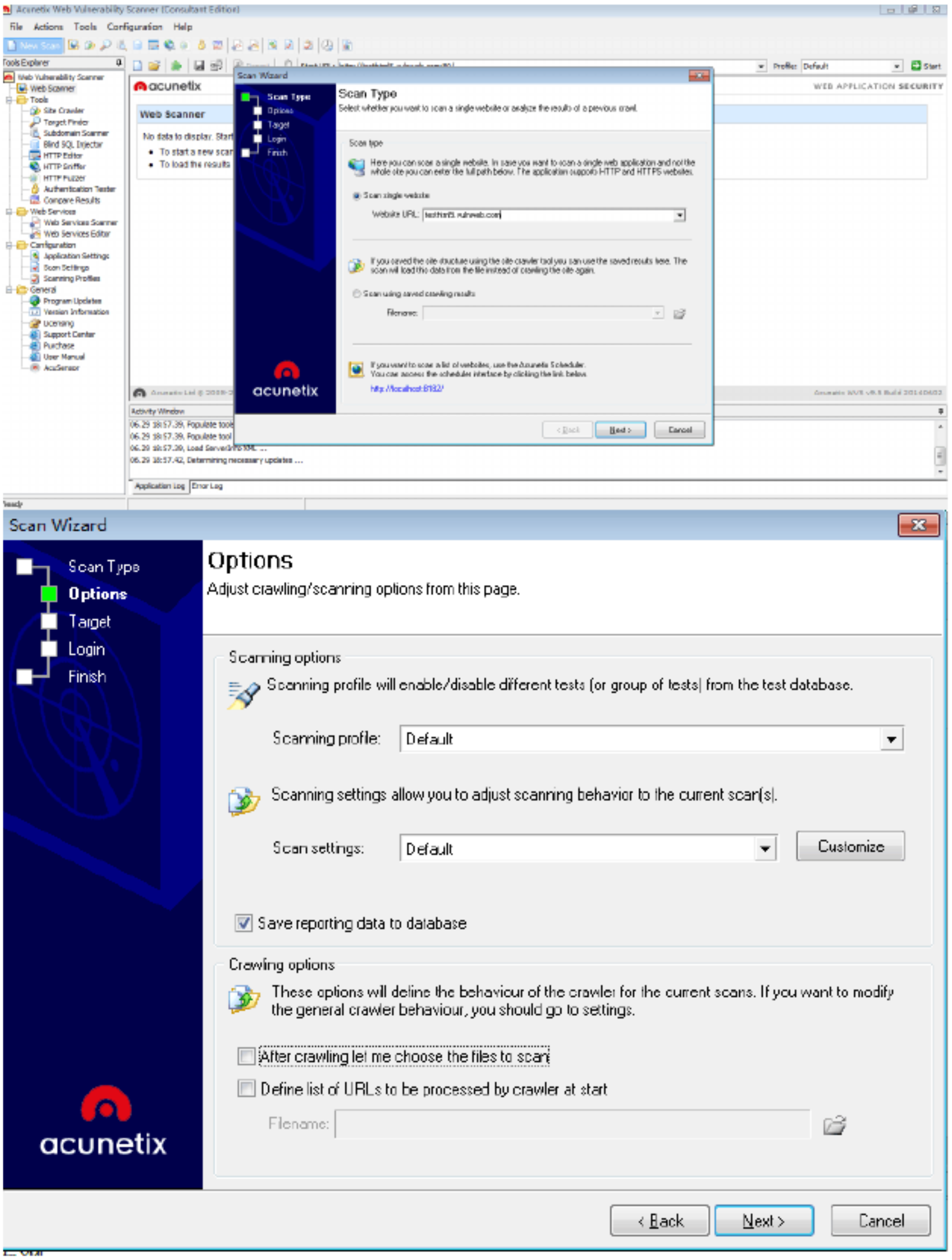


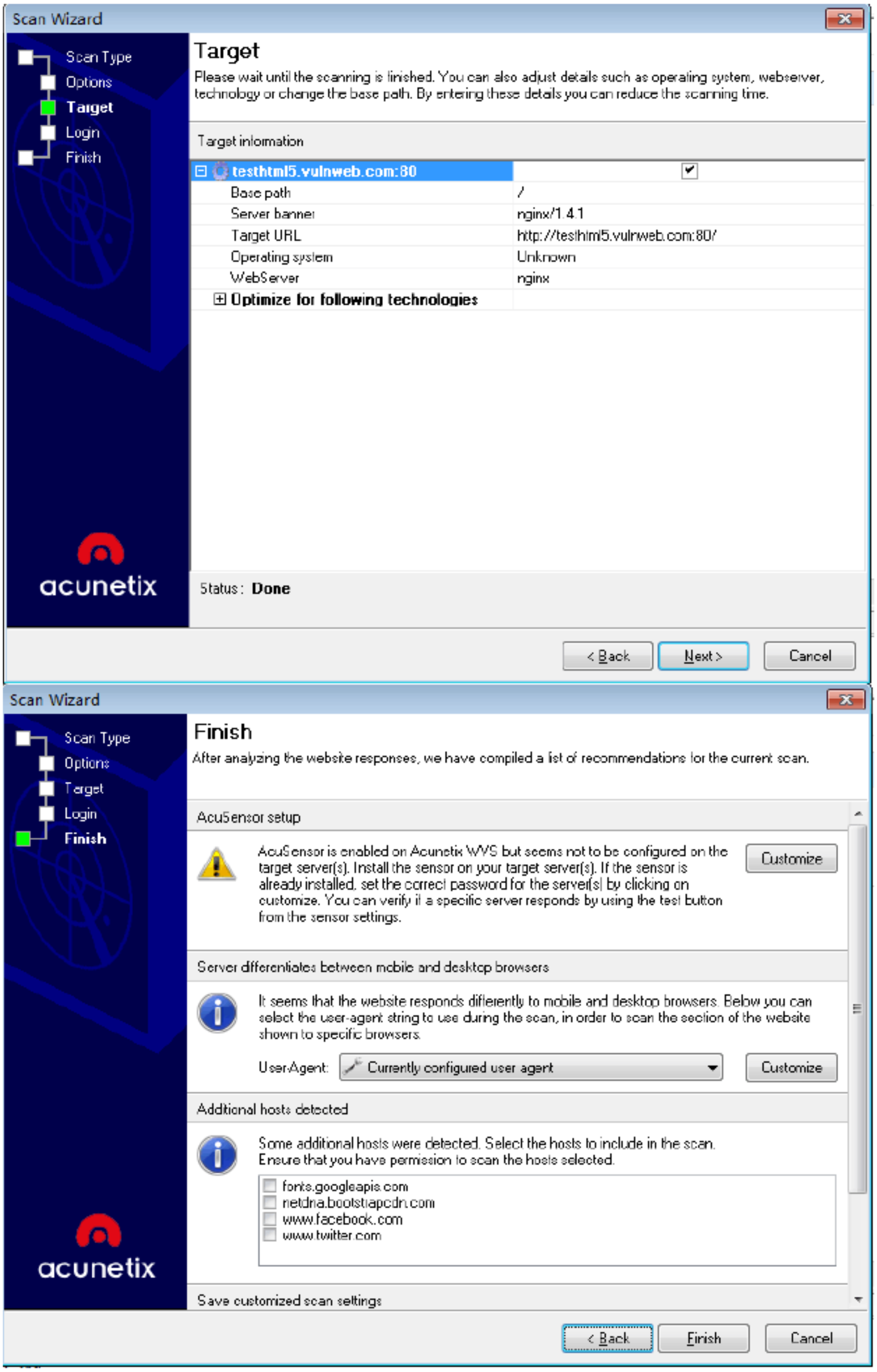
2. Web 风险类别分布

分类别	高风险	中风险	低风险	总计
跨站脚本攻击	3	2	0	5
信息泄露	2	0	5	7
内容哄骗	1	0	0	1
系统命令执行	3	0	0	3
功能滥用	1	0	1	2
资源位置可推测	0	2	0	2
其他	0	0	1	1

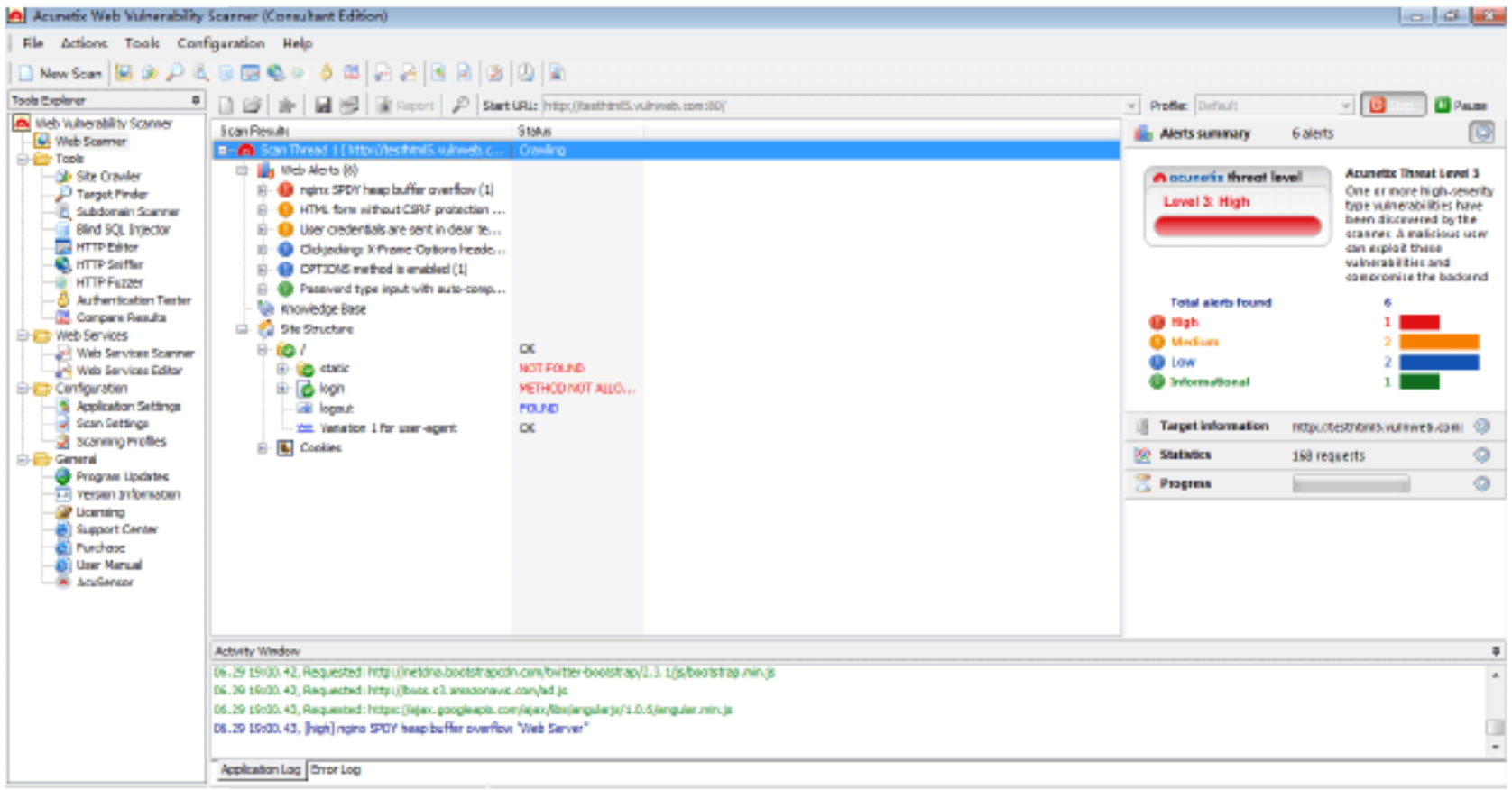
3. 渗透测试

输入网址 **testhtml5.vulnweb** ，然后开头扫描

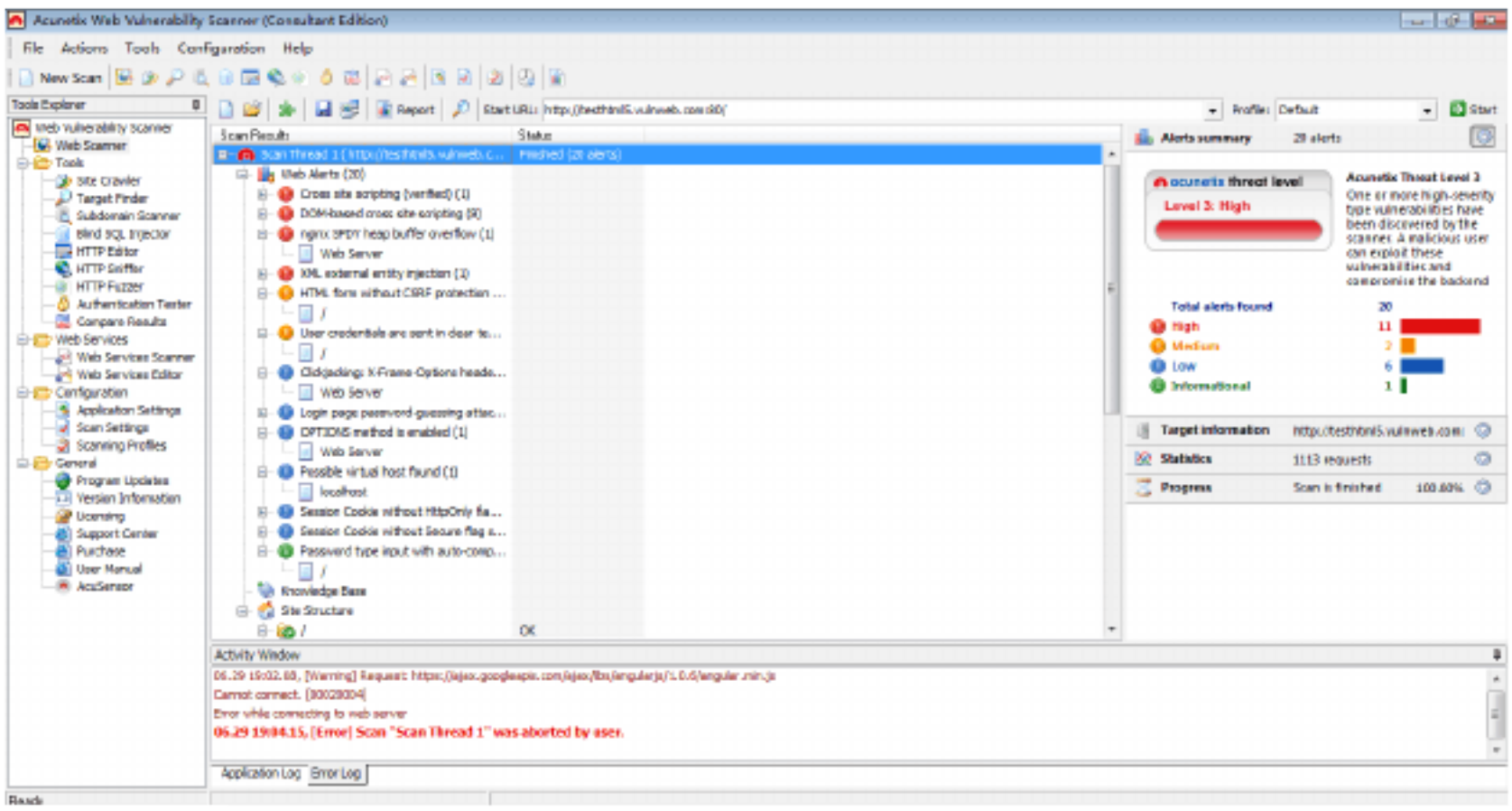


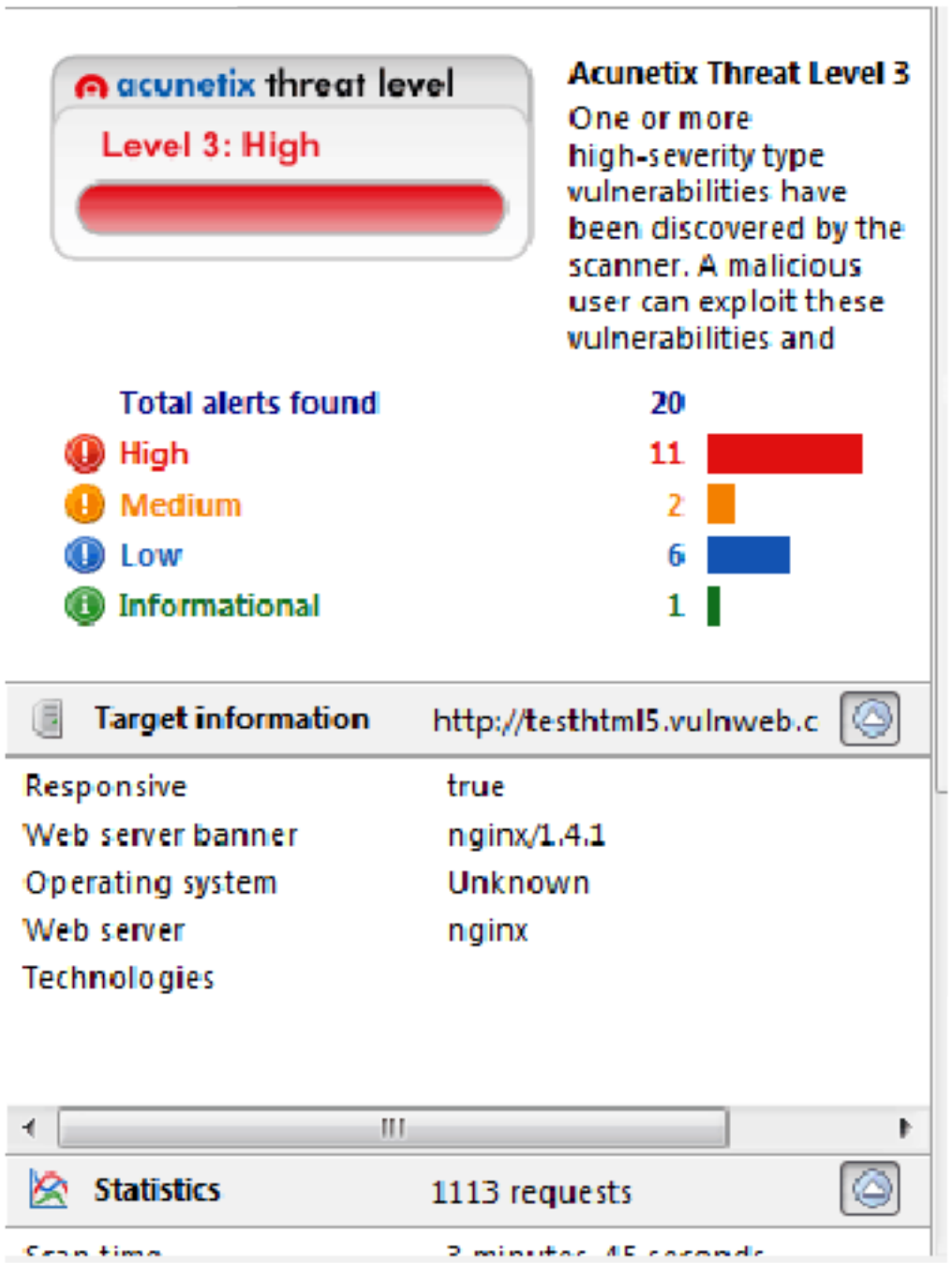

Scan Wizard
Scan Type
Options
Target
Login
Finish
Target
Please wait until the scanning is finished. You can also adjust details such as operating system, webserver, technology or change the base path. By entering these details you can reduce the scanning time.
Target information
testhtml5.vulnweb.com:80
Base path /
Server banner nginx/1.4.1
Target URL http://testhtml5.vulnweb.com:80/
Operating system Unknown
WebServer nginx
Optimize for following technologies
acunetix
Status: Done
< Back
Next >
Cancel
Scan Wizard
Scan Type
Options
Target
Login
Finish
Finish
After analyzing the website responses, we have compiled a list of recommendations for the current scan.
AcuSensor setup
AcuSensor is enabled on Acunetix WVS but seems not to be configured on the target server(s). Install the sensor on your target server(s). If the sensor is already installed, set the correct password for the server(s) by clicking on customize. You can verify if a specific server responds by using the test button from the sensor settings.
Customize
Server differentiates between mobile and desktop browsers
It seems that the website responds differently to mobile and desktop browsers. Below you can select the user-agent string to use during the scan, in order to scan the section of the website shown to specific browsers.
UserAgent: Currently configured user agent
Customize
Additional hosts detected
Some additional hosts were detected. Select the hosts to include in the scan.
Ensure that you have permission to scan the hosts selected.
fonts.googleapis.com
netdna.bootstrapcdn.com
www.facebook.com
www.twitter.com
Save customized scan settings
acunetix
< Back
Finish
Cancel

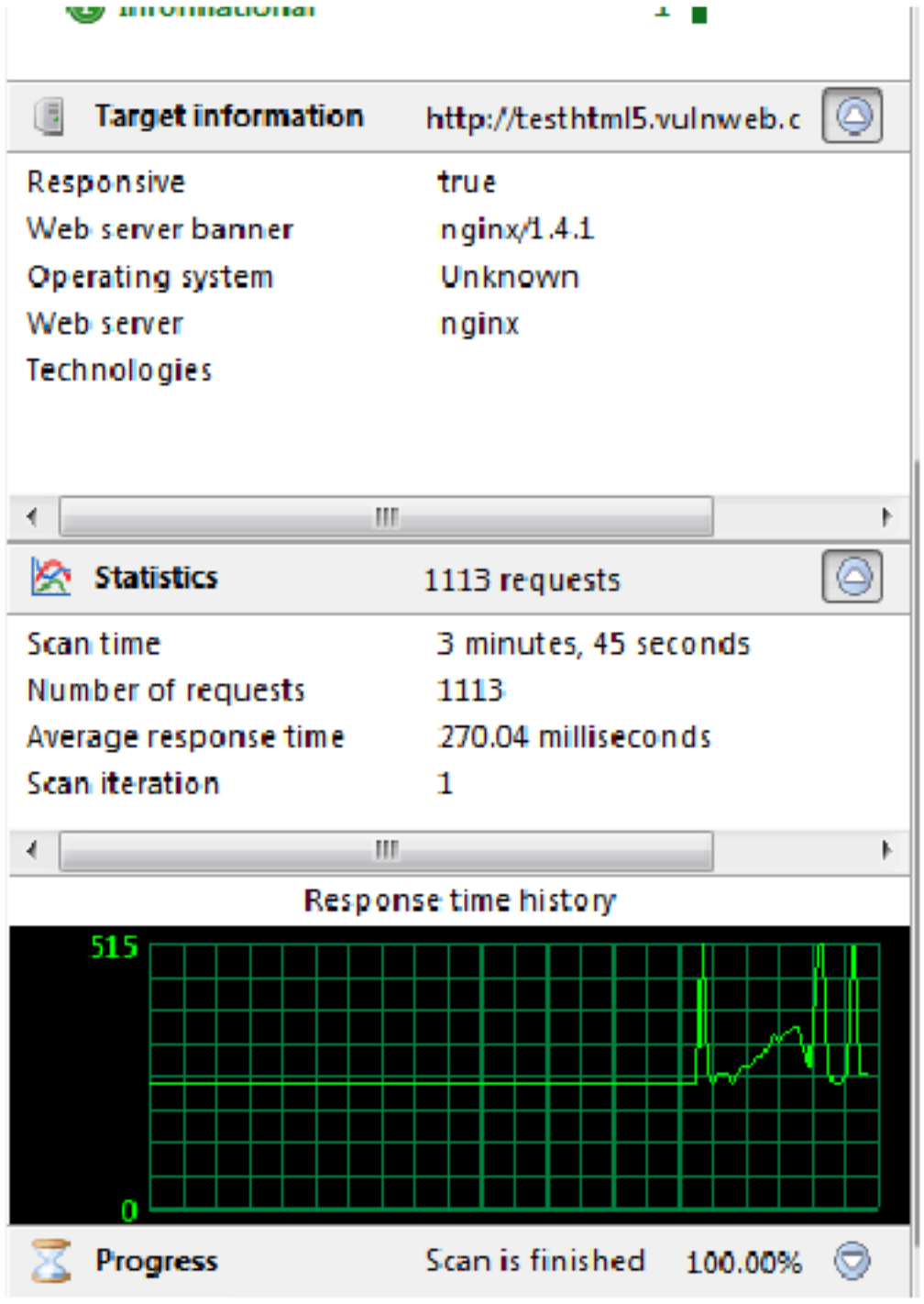
正在扫描该网站



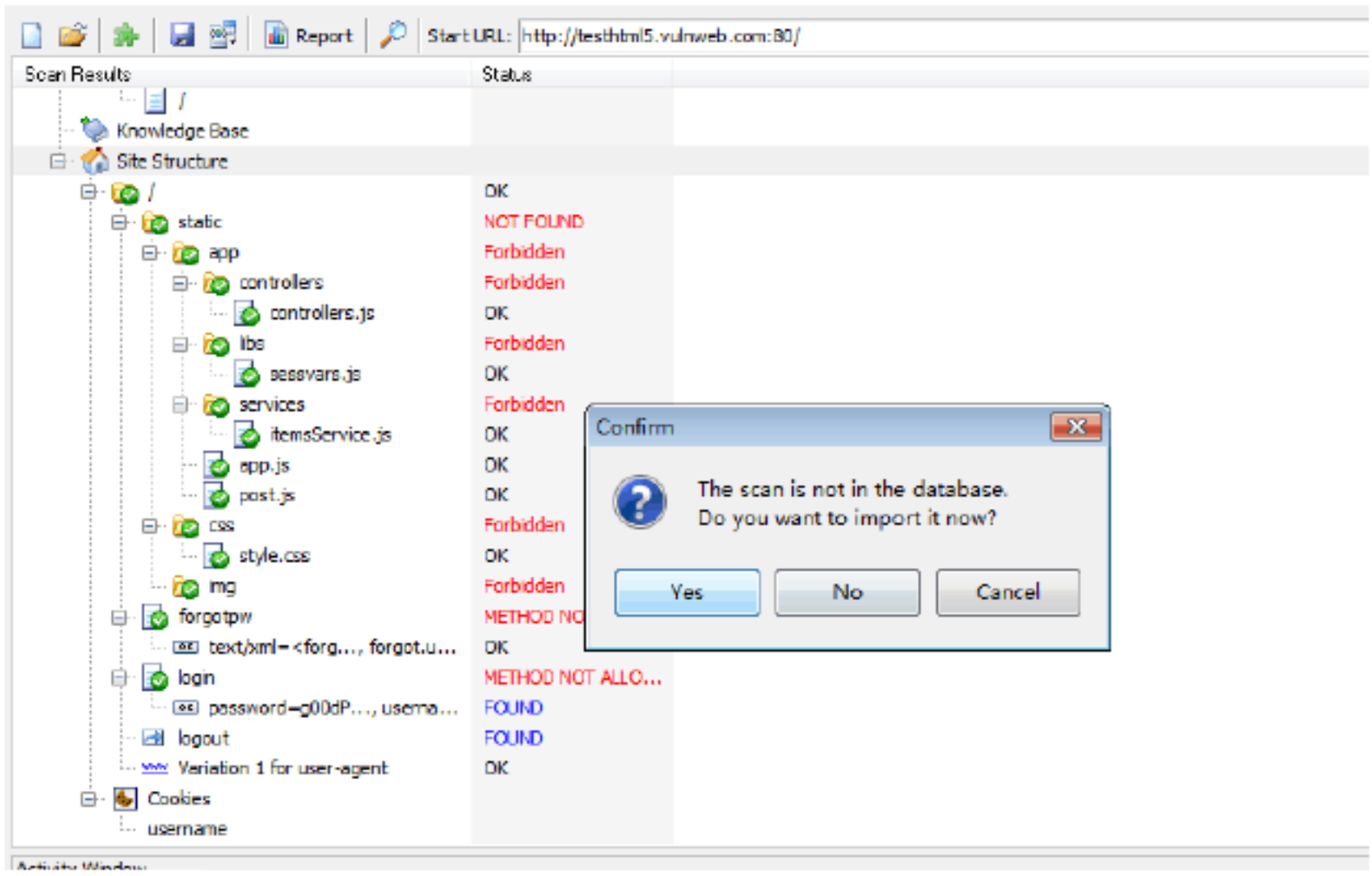
扫描完毕，共 *20* 个漏洞。


Acunetix Web Vulnerability Scanner (Consultant Edition)
File Actions Tools Configuration Help
New Scan
Tools Explorer
Web Vulnerability Scanner
Web Scanner
Tools
Site Crawler
Target Finder
Subdomain Scanner
Blind SQL Injector
HTTP Editor
HTTP Sniffer
HTTP Fuzzer
Authentication Tester
Compare Results
Web Services
Web Services Scanner
Web Services Editor
Configuration
Application Settings
Scan Settings
Scanning Profiles
General
Program Updates
Version Information
Licensing
Support Center
Purchase
User Manual
AcuSensor
Report
Start URL:
Profile: Default
Start
Scan Results
Status
Scan thread 1 (http://testhtml5.vulnweb.c... Finished (20 alerts)
Web Alerts (20)
Cross site scripting (verified) (1)
DOM-based cross site scripting (9)
nginx SPDY heap buffer overflow (1)
Web Server
XML external entity injection (1)
HTML form without CSRF protection ...
/
User credentials are sent in clear te...
/
Clickjacking: X-Frame-Options heade...
Web Server
Login page password-guessing attac...
OPTIONS method is enabled (1)
Web Server
Possible virtual host found (1)
localhost
Session Cookie without HttpOnly fla...
Session Cookie without Secure flag s...
Password type input with auto-comp...
/
Knowledge Base
Site Structure
/
OK
Alerts summary
20 alerts
acunetix threat level
Level 3: High
Acunetix Threat Level 3
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend
Total alerts found 20
High 11
Medium 2
Low 6
Informational 1
Target information http://testhtml5.vulnweb.com
Statistics 1113 requests
Progress Scan is finished 100.00%
Activity Window
06.29 19:02.03, [Warning] Request: https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js
Cannot connect. [80028004]
Error while connecting to web server
06.29 19:04.15, [Error] Scan "Scan Thread 1" was aborted by user.
Application Log
Error Log
Ready

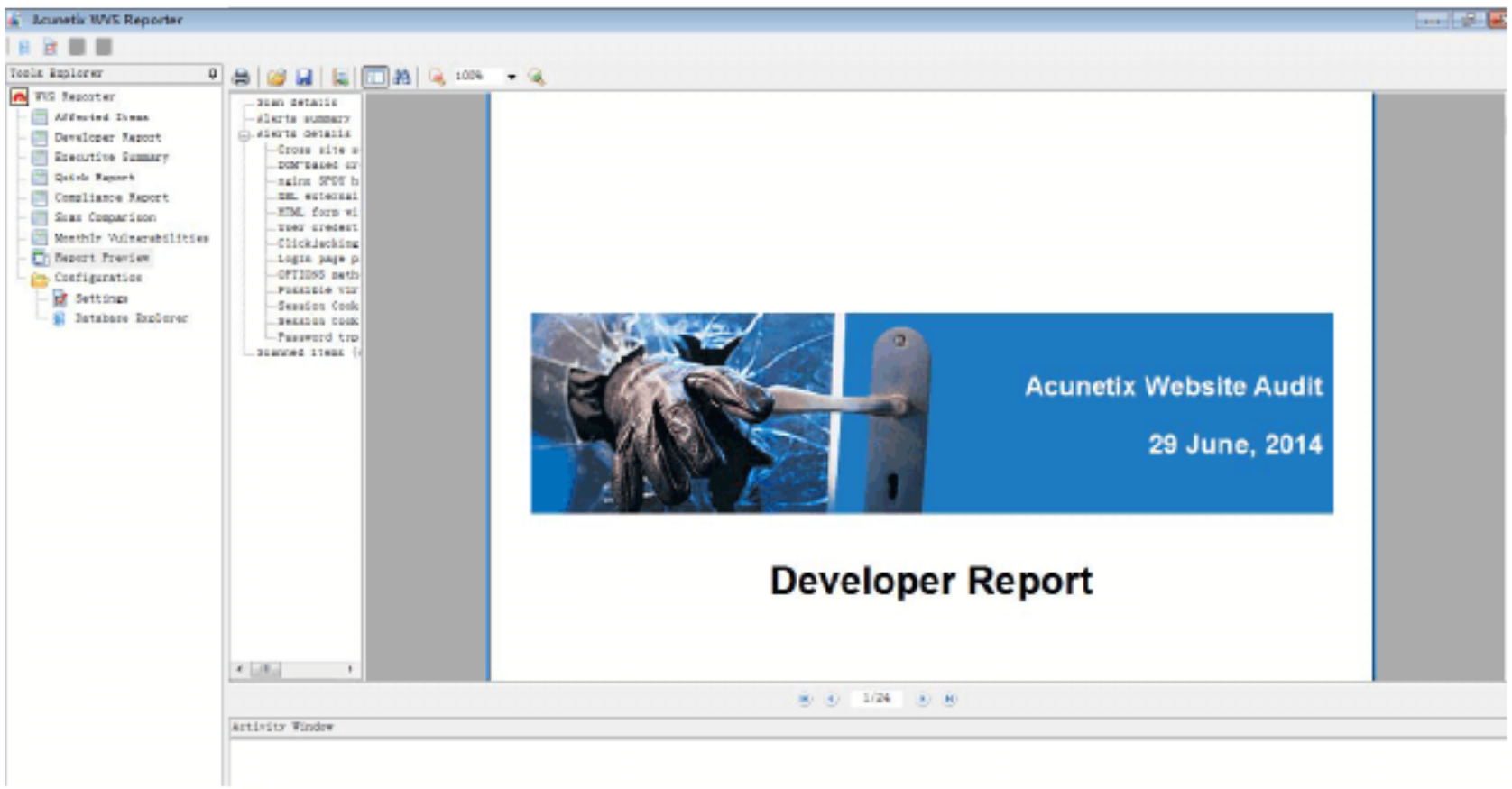

acunetix threat level
Level 3: High
Acunetix Threat Level 3
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and
Total alerts found 20
High 11
Medium 2
Low 6
Informational 1
Target information http://testhtml5.vulnweb.c
Responsive true
Web server banner nginx/1.4.1
Operating system Unknown
Web server nginx
Technologies
Statistics 1113 requests



点击 **Report** 生成报告



软件自动生成的扫描报告



4. 漏洞信息

Cross site scripting (verified)

Classification	
CVSS	Base Score: 4.4 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-79

Affected items	Variatio
/	1

DOM-based cross site scripting

Classification	
CVSS	Base Score: 4.4 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-79

Affected items	Variatio
/	6

nginx SPDY heap buffer overflow

Classification	
CVSS	Base Score: 5.1 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CWE	CWE-122
CVE	CVE-2014-0133

Affected items	Variatio
Web Server	1

Vulnerable Javascript library

Classification	
CVSS	Base Score: 6.4 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-16

Affected items	Variatio
/static/app/libs/sessvars.js	1

XML external entity injection

Classification	
CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CWE	CWE-611

Affected items	Variatio
/forgotpw	1

HTML form without CSRF protection

Classification	
CVSS	Base Score: 2.6 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-352

Affected items	Variatio
/	1

User credentials are sent in clear text

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-310

Affected items	Variatio
/	1

Clickjacking: X-Frame-Options header missing

Classification	
CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CWE	CWE-693

Affected items	Variatio
Web Server	1

Login page password-guessing attack

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-307

Affected items	Variatio
/login	1

OPTIONS method is enabled

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variatio
Web Server	1

Possible sensitive directories

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variatio
/admin	1

Possible virtual host found

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variatio
localhost	1

Session Cookie without HttpOnly flag set

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variatio
/	1

Session Cookie without Secure flag set

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variatio
/	1

Password type input with auto-complete enabled

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variatio
	1

四、风险评价

安全威逼是一种对系统、组织及其资产构成潜在破坏力量的可能性因素或者大事。产生安全威逼的主要因素可以分为人为因素和环境因素。人为因素包括有意的和无意的因素。环境因素包括自然界的不行抗力因素和其他物理因素。威逼可能源于对 web站点的直接或间接攻击，例如非授权的泄露、篡改、删除等，在机密性、完整性或可用性等方面造成损害。威逼也可能源于偶发的或蓄意的大事。一般来说，威逼总是要利用 web站点的系统、应用或效劳的弱点才可能成功造成损害。因此威逼分析是围绕信息系统的可用性、保密性、完整性、可控性、可审查性、

可抵赖性进展的。

安全风险则是一种可能性，是指某个威逼利用弱点引起某项信息资产或一组信息资产的损害，从而直接地或间接地引起企业或机构的损害的可能性。

本次风险分析主要承受自顶向下和自底向上分析、定性分析与定量分析相结合的分析方法。首先自顶向下识别关键，然后自底向上承受定性、定量相结合的方法进展风险分析。形成一个分层次的树形分析体系。

在这次评估中，整体系统存在的威逼和其产生的安全风险主要有以下几个方面：

1、针对主机的攻击威逼

包括针对linux系统以及其使用的nginx等组件的安全漏洞的攻击威逼，攻击者可能由此猎取系　统的信息资源或对系统信息进展破坏。

2、针对数据库的攻击威逼

包括在对数据库系统的攻击行为，包括非法猎取、篡改、删除数据库信息资源和进展其他形式的效劳攻击。

3、治理不当所引起的威逼

包括由于用户治理策略不当使得攻击者可能猎取某一级别的用户的访问权限，并由此提升用户权限，造成用户权限的滥用和信息资源的泄露、损毁等；由于承受远程治理而引发的威逼；缺乏足够的安全审计致使对安全大事不敏感，无法觉察攻击行为等。

4、配置不当所引起的威逼

包括在主机上开放了未做安全防范的效劳所造成的威逼。

5、程序规律漏洞造成的威逼

包括编码时由于对用户输入处理考虑不完全以及代码本身的bug被利用所造成的威逼。

在现场核查测试完毕后，我们将对得到的脆弱性、威逼数据进展风险分析。我们认为在简单的系统风险评估过程中，不能将定性分析和定量分析两种方法简洁的割裂开来。而是应当将这两种方法融合起来，承受综合的评估方法。在信息系统风险分析过程中，定性分析是灵魂，是形成概念、观点，作出判断，得出结论所必需依靠的。定量分析则是手段，是定性分析的根底和前提，定性分析应建立在定量分析的根底上才能提醒客观事物的内在规律。是为作出推断和得出结论。

对于所识别出的各类安全风险，处理方式有四种，即预防、避开、降低、转移和承受，但对于整个系统而言，风险不行能完全被消灭。在风险识别后，应依据风险程度的轻重缓急和自身的经济实力及安全需求，综合考虑法律法规的要求、机构自身的进展需要、风险评估的结果等众多因素，实施处理风险的各类措施。对不行承受的风险选择适当的处理方式及掌握措施，并形成风险处理打算。掌握措施的选择应兼顾治理与技术，并特别关注本钱与风险的平衡。

五、风险掌握建议

安全这个话题是多层次的，一个网站要安全必需满足物理安全、链路安全、网络级安全、应用安全和用户安全这 5 个层次。大多数网站没有完整的实行防护措施，因此，建立一套有效的网络安全机制就显得尤为重要，以下是必需考虑的安全防护要点：

1、部署防火墙

在互联网与效劳器之间部署硬件防火墙，这样，通过互联网进来的用户只能访问到对外公开的一些效劳〔如 W W W、E - m a i l、F T P、D N S 等 〕，既保护内网资源不被非法访问或破坏，也阻挡了内部用户对外部不良资源的使用，并能够对发生的安全大事进展跟踪和审计。在网站的效劳器上安装软件防火墙后还要进一步设置访问策略。

2、漏洞及补丁治理

Web 效劳器是一个由多协议、多应用、多用户组成的网络环境，网络设备、操作系统统、数据库、应用软件都存在难以避开的安全漏洞。为了要保障网站的安全，必需做好漏洞治理。

3、入侵检测工作

作为效劳器的日常治理，入侵检测是一项格外重要的工作，在寻常的检测程序中，主要包含日常的效劳器安全例行检查和遭到入侵时的入侵检查，也就是分为在入侵进展时的安全检查和在入侵前后的安全检查。系统的安全性遵循木桶原理，木桶原理指的是：一个木桶由很多块木板组成，假设组成木桶的这些木板长短不一，那么这个木桶的最大容量不取决于长的木板，而取决于最短的那块木板。应用到安全方面也就是说系统的安全性取决于系统中最脆弱的地方，这些地方是日常的安全检测的重点所在。

4、数据备份和恢复

数据是整个网络的核心。数据一旦被破坏或丧失，对于 W e b 效劳器，严峻影响网站的形象，影响到 web 效劳的正常进展。所以做一套完整的数据备份和恢复机制可以在效劳器发生故障时将损失降低到最小。

5、安装反病毒软件

病毒、木马、蠕虫等恶意代码是网站的主要安全隐患，必需做到有效掌握。现在的反病毒件查杀面也格外广，在网站效劳器上安装反病毒软件能从邮件、FTP 文件、网页、软盘、光盘等全部可能的信息源进展监控和安全拦截。安装完后要准时升级，这样杀毒软件查杀力量能够掩盖最的恶意代码。

6、网站的密码安全。

关于密码设置，我们可以从 CSDN 大事中看到，很大一局部人承受的甚至数字密码，这类 密码很简洁被破解。尤其是治理员密码，我们需要学习下国外网站的设置，承受大小写字母加数字，甚至特别字符夹杂在里面作为密码。

7、网站维护治理的频率。

我们网站也需要和人一样做定期检查体检，检查文件的日志，一般我们网站文件都有时 间日志的，被修改后时间日志会更。我们需要查看文件被修改的时间。即便我们网站能够正常访问，也需要查看文件是不是被挂黑链接，由于黑链接产品也格外猖 狂。鉴于自己的网站安全和权重考虑，也是需要进展安全体检的。

8、检查站点程序是否存在漏洞

站点程序的完整性能够确保网站在进展的过程中有一个完善的进展过程，选择技术和组建的时候一定要留意淘汰与选择，不要拿自己的网站去测试程序的利与弊。

附录：

Scan of ://testhtml5.vulnweb :80/

Scan details

Scan information	
Start time	2023/6/29 14:30:59
Finish time	The scan was aborted
Scan time	8 minutes, 10 seconds
Profile	Default

Server information	
Responsive	True
Server banner	nginx/1.4.1
Server OS	Unknown
Server technologies	

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	20	
High	10	
Medium	2	
Low	7	
Informational	1	

Alerts summary

Cross site scripting (verified)

Classification

CVSS	**Base Score: 4.4** **- Access Vector: Network** **- Access Complexity: Medium** **- Authentication: None** **- Confidentiality Impact: None** **- Integrity Impact: Partial** **- Availability Impact: None**
CWE	**CWE-79**

Affected items	Variations
/	1

DOM-based cross site scripting

Classification	
CVSS	Base Score: 4.4 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-79

Affected items	Variations
/	6

nginx SPDY heap buffer overflow

Classification	
CVSS	Base Score: 5.1 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CWE	CWE-122
CVE	CVE-2023-0133

Affected items	Variations
Web Server	1

Vulnerable Javascript library

Classification	
CVSS	Base Score: 6.4 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-16

Affected items	Variations
/static/app/libs/sessvars.js	1

XML external entity injection

Classification	
CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CWE	CWE-611

Affected items	Variations
/forgotpw	1

HTML form without CSRF protection

Classification	
CVSS	Base Score: 2.6 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-352

Affected items	Variations
/	1

User credentials are sent in clear text

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-310

Affected items	Variations
/	1

Clickjacking: X-Frame-Options header missing

Classification	
CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CWE	CWE-693

Affected items	Variations
Web Server	1

Login password-guessing attack

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-307

Affected items	Variations
/login	1

OPTIONS method is enabled

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variations
Web Server	1

Possible sensitive directories

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variations
/admin	1

Possible virtual host found

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variations
localhost	1

Session Cookie without Only flag set

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variations
/	1

Session Cookie without Secure flag set

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variations
/	1

Password type input with auto-complete enabled

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variations
/	1