

硕 士 研 究 生 课 程 报 告



题目 宜家中国网站安全测试报告

测试成员 徐超、冯夏巍

学科专业 软件工程

所在学院 软件学院

提交日期 二○一九年二月

**目录**

[1 概述 1](#_Toc967779)

[1.1 测试信息 1](#_Toc967780)

[1.2 测试网站介绍 1](#_Toc967781)

[1.3 测试工具 1](#_Toc967782)

[2 测试过程 3](#_Toc967783)

[2.1 端口扫描 3](#_Toc967784)

[2.2 漏洞检测 4](#_Toc967785)

[3 网站漏洞及解决方案 6](#_Toc967786)

[3.1 HTML表单缺少CSRF保护 6](#_Toc967787)

[3.2 缺少X-Frame-Optios头部 7](#_Toc967788)

[3.3 Cookies没有设置HttpOnly标记 8](#_Toc967789)

[3.4 Cookies没有设置Secure标记。 8](#_Toc967790)

# 概述

## 测试信息

|  |  |
| --- | --- |
| 目标网站 | www.ikea.cn |
| 测试工具 | Acunetix Web Vulnerability Scanner 12.0  Nmap 7.70 |
| 客户机环境 | Windows10/Intel Core i5-6200U/8G RAM |
| 测试时间 | 2019.2.13 |
| 测试员 | 徐超、冯夏巍 |

## 测试网站介绍

宜家（IKEA）是一家来自瑞典的家具品牌，目前已成为全球最大的家具家居用品销售企业。继承北欧的鲜艳温设计风格的宜家在中国受到许多年轻人的喜爱。2018年8月以前，宜家并不提供电商服务，网上商城的作用仅仅是让消费者可以浏览所有家具，提前列好购物清单，最终还是要前往实体店购买。在2018年底，宜家已经面向全国149个城市提供电商服务，今后会有更多的消费者选择在宜家网上商城购物。本次测试的目标网站为宜家中国的官方网站（www.ikea.cn），该网站可供消费者在线选购家具及购买。

## 测试工具

本次测试采用Nmap 7.70作为端口扫描工具。Nmap（Network Mapper）是一款开源的网络探测和安全审核工具，可以用于检测主机是否在线、端口开放情况、侦测运行的服务类型及版本信息等。

Acunetix Web Vulnerability Scanner（简称AWVS），是一款知名的Web网络漏洞扫描工具，它通过网络爬虫来测试网站安全，检测流行安全漏洞，如SQL诸如和跨站点脚本测试等。AWVS可以自动扫描可能被利用的漏洞，为分析现有的Web应用程序提供了强大而独特的解决方案。目前AWVS有免费和付费两个版本，本测试采用的是付费的AWVS 12.0版本。

# 测试过程

## 端口扫描

从nmap官网（<https://nmap.org/）下载7.70版的nmap>并安装。

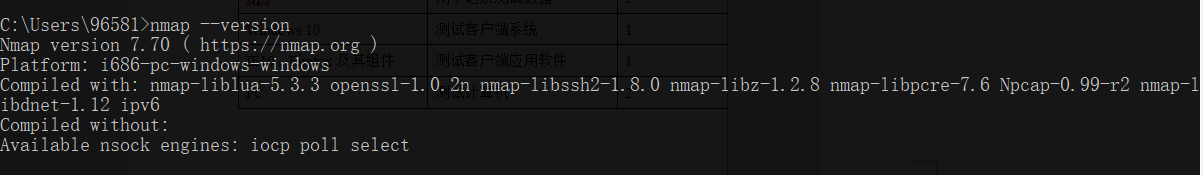


图2.1. 端口扫描工具nmap

安装完成后，运行如下命令：

1. nmap -T4 -A -v www.ikea.cn

-A选项启用系统和版本检测、脚本扫描、路由跟踪，-T4选项是为了更快的执行速度。

运行完成后的结果如图2.2所示。

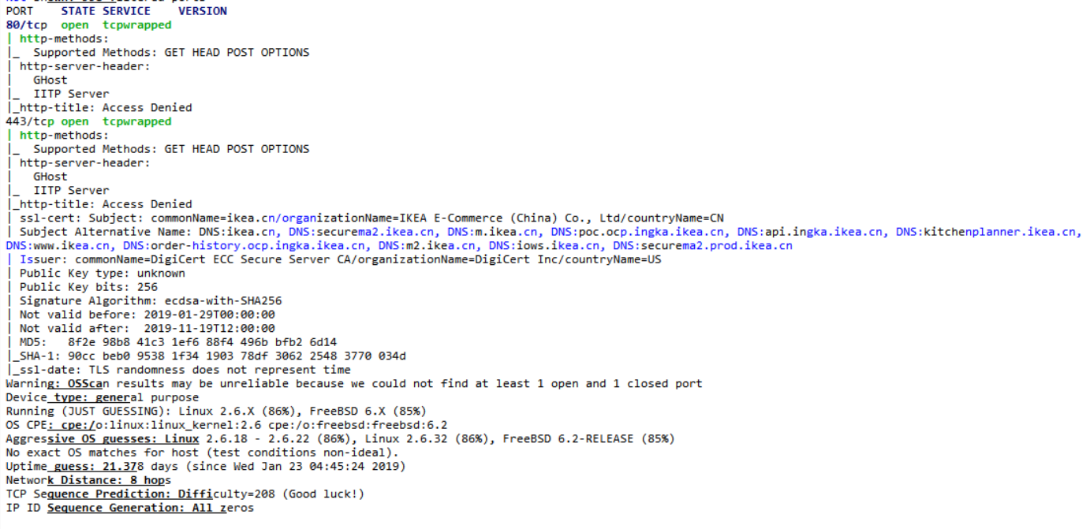
从图2.2中可以看到：该网站服务器只开放了80 端口和443端口；使用的系统可能是Linux 2.6.X或FreeBSD 6.X.

图2.2 nmap扫描结果

## 漏洞检测

AWVS 12.0以后提供了基于Web页面的测试界面，操作更加方便。

安装好AWVS之后进入，主界面如图2.3所示。

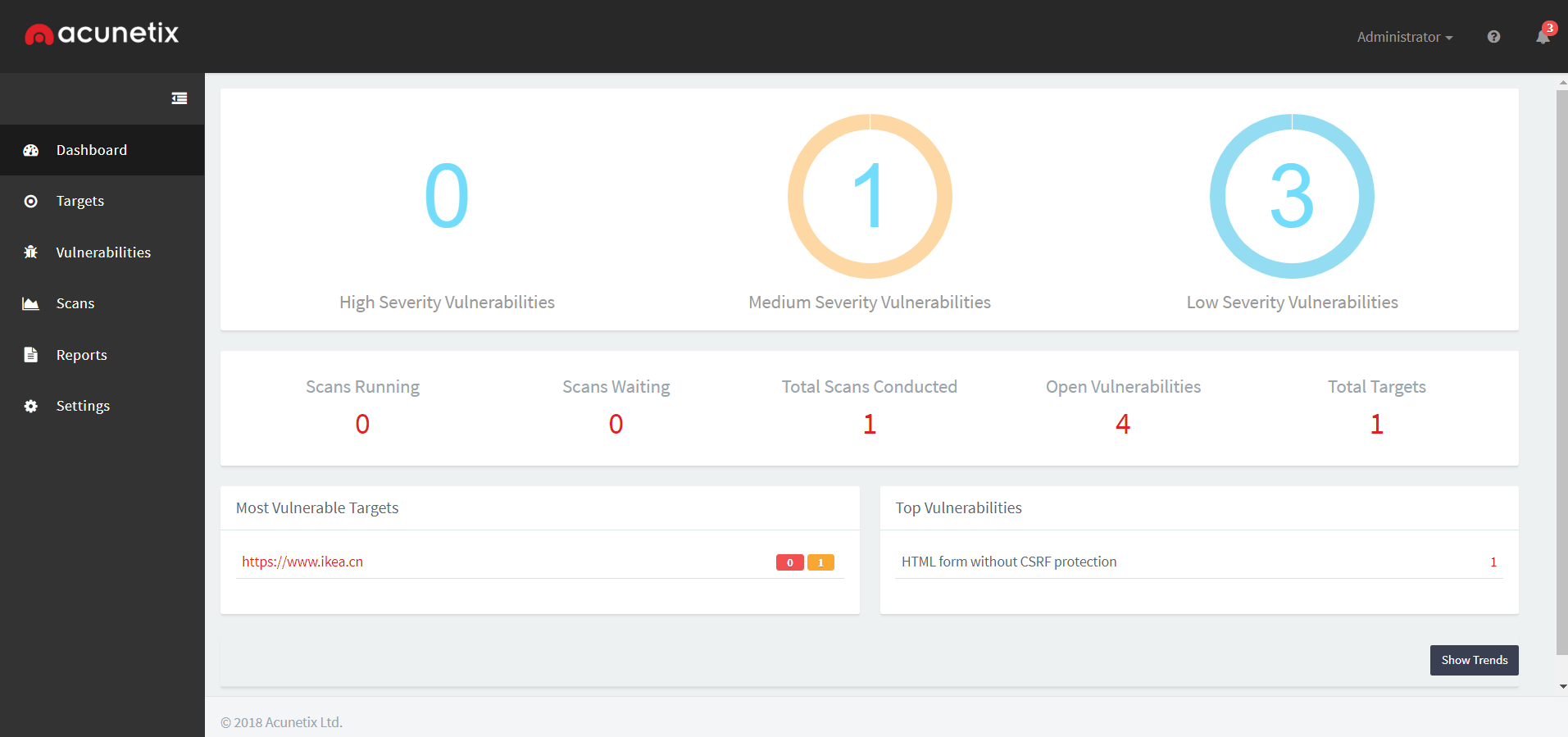


图2.3 AWVS主界面

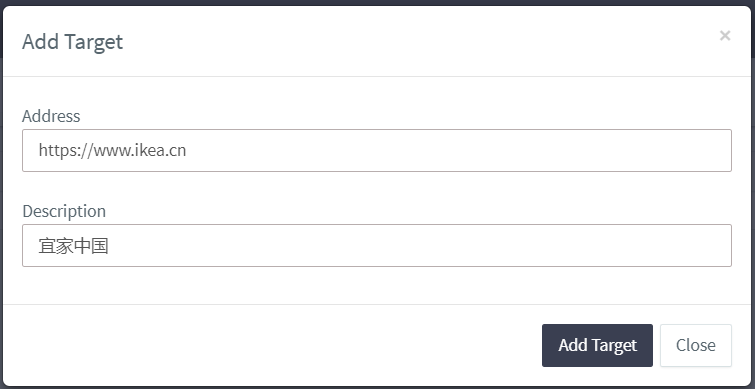
在Target一栏中选择Add Target，输入目标URL，再点击Scan即可开始扫描。

图2.4 AWVS添加扫描目标

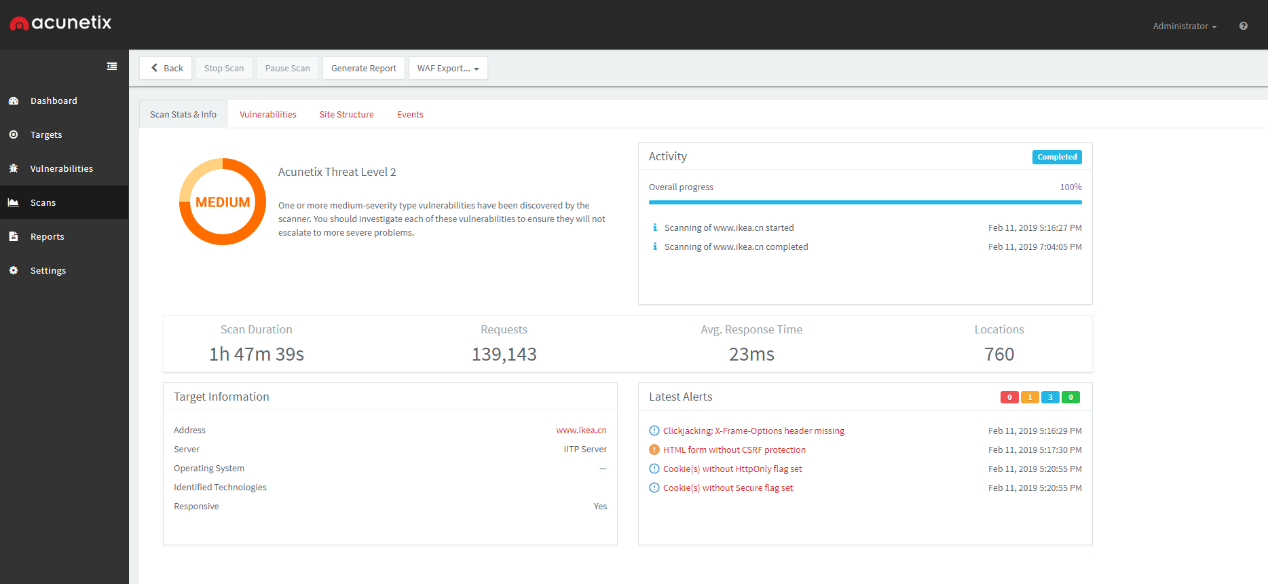
测试完成后点击Scans菜单可以查看检测结果统计：

图2.5 AWVS检测结果统计

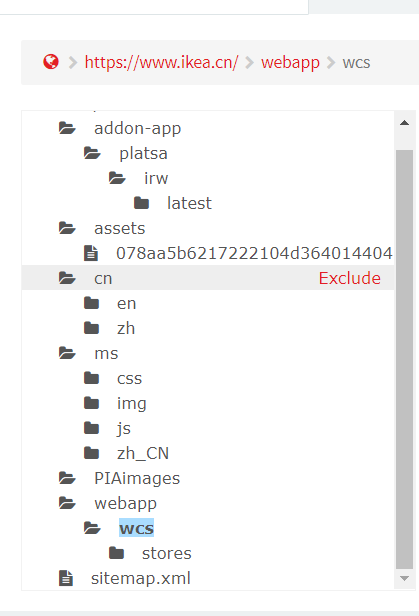
检测结果显示，宜家中国有一个中等严重程度的漏洞和三个低等级严重程度的漏洞。关于这4个漏洞的详细信息及解决方案在下一章中详细说明。该站点的结构如下：

图2.6 站点结构图

# 网站漏洞及解决方案

## HTML表单缺少CSRF保护

这种一个中等严重程度的漏洞。跨站请求伪造（Cross-site require forgery），缩写为CSRF或XSRF，是一种挟持用户在当前已登陆的Web应用程序上执行非本意的操作的攻击方法。与站点脚本（XSS）相比，XSS利用的是用户对指定网站的信任，CSRF利用的是网站对用户网页浏览器的信任。下面是使用<img>标签来进行CSRF的示例：

**<img** src="http://example.com/changePassword/?newPassword=attackerPassword"**>**

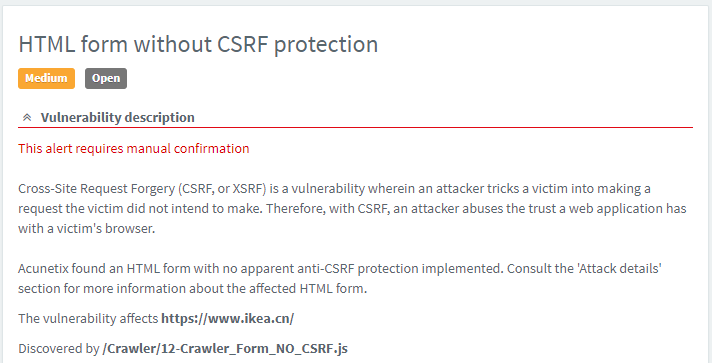


图3.1 HTML表单缺少CSRF保护漏洞

发现该漏洞的HTTP请求如下：

1. GET /cn/zh HTTP/1.1
2. Cookie: eaesssn=6ddcdd3c510f00006c3d615ce80000005c2f0000;device=desktop;\_abck=465E01365C55F231DBA33686FFF6DABD3CDDDC6D510F00006C3D615C9DE8BA69~-1~bdp1CAXNWvCmEBoUUQy686gQwFVo2E9fWoNLalFu69o=~-1~-1;bm\_sz=C6BFEA60F3A3BCEE4C1279597C8C8419~YAAQbdzdPN6cTrFoAQAAyO7X2wLMcPTucYzBKgrt5Rj8Ucc9DNApykWiJKe5wdOA/LnesE1NjMxaCDQUnzz65/dqY+KyjFV+BkwMQcl+C7Kqn4bMD37jbjopr4SIbQbGdIjQbzNWRbbL0pZkPPfZ72ABs79oxCQBmxvp0D1+Ojtbgzj7eHaKRhT8Z5JF
3. Accept: \*/\*
4. Accept-Encoding: gzip,deflate
5. Host: www.ikea.cn
6. User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
7. Connection: Keep-Alive

解决方案如下：

1. 对每个用户Session都应有独立的反CSRF令牌；
2. 在适当时长过后会话应当失效；
3. 反CSRF令牌长度应该足够长且是加密的随机值；
4. 反CSRF令牌应当是加密安全的，由强伪随机数生成器算法（PRNG）生成；
5. 反CSRF令牌作为比偶表单或者URL那的隐藏字段添加；
6. 当反CSRF令牌未通过验证时，服务器应拒绝操作请求。

## 缺少X-Frame-Optios头部

服务器没有返回X-Frame-Options头部，意味着该往网站可能面临点击劫持攻击的风险。X-Frame-Options HTTP响应头可用于指示是否应允许浏览器在iframe内呈现页面。

该漏洞严重程度较低，可以通过配置web服务器使其返回X-Frame-Options头部。

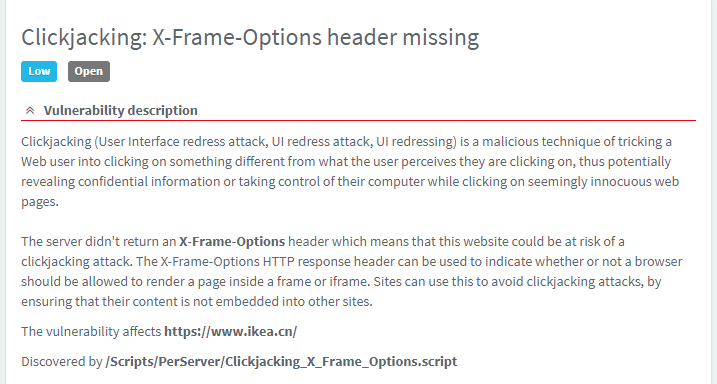


图3.2 X-Frame-Options缺少头部

## Cookies没有设置HttpOnly标记

www.ikea.cn 的cookies没有设置HttpOnly标记。HttpOnly的标记指示浏览器cookies只能有服务器访问而不能由客户端的脚本访问，这是会话cookies的重要安全保障。

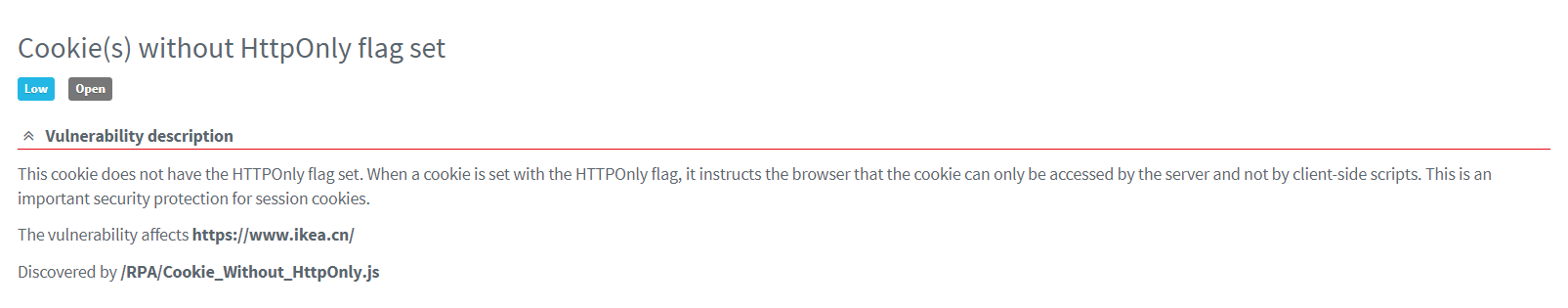


图3.3 Cookies没有设置HttpOnly标记

解决方案：将Cookie的HttpOnly标记置位即可，严重程度较低。

## Cookies没有设置Secure标记。

Cookies没有设置Secure标志。当设置cookie的Secure标志时，它表明浏览器只能通过安全的SSL通道访问cookie，这也是会话Cookies的重要安全保障。

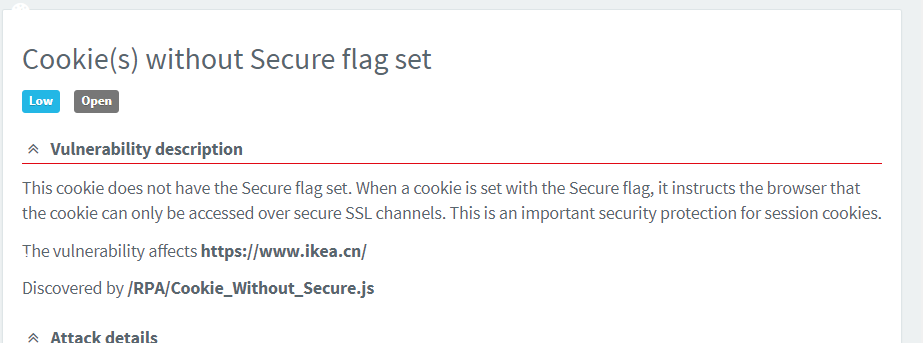


图3.4 Cookie没有设置Secure标志

解决方案：与上一个漏洞类似，设置Secure标志即可。