# 百草味网站安全测试报告

## 一、报告总结：

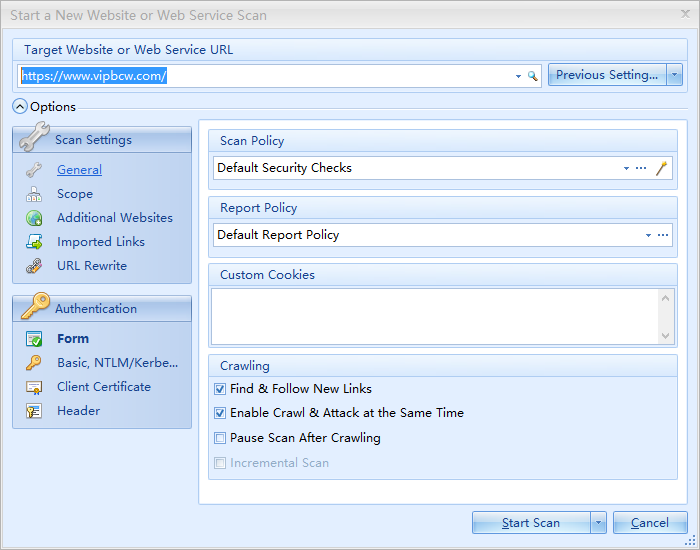
|  |  |
| --- | --- |
| 目标URL | <https://www.vipbcw.com/> |
| 扫描日期 | 05/01/2018 14:58:48 (UTC+08:00) |
| 报告日期 | 05/01/2018 15:18:51 (UTC+08:00) |
| 持续时间 | 00:17:49 |
| Netsparker版本 | 4.9.5.19049-4.9.5-hf6-7503ef9 |

## 二、工具选择

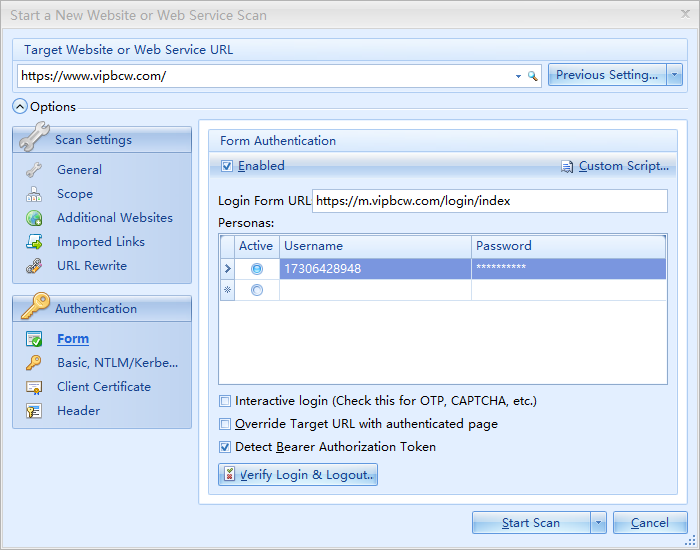
Netsparker：Netsparker是一款安全简单的web应用安全漏电扫描工具。该软件功能非常强大，使用方便.Netsparker与其他综合 性的web应用安全扫描工具相比的一个特点是它能够更好的检测SQL Injection和 Cross-site Scripting类型的安全漏洞。

## 三、测试过程

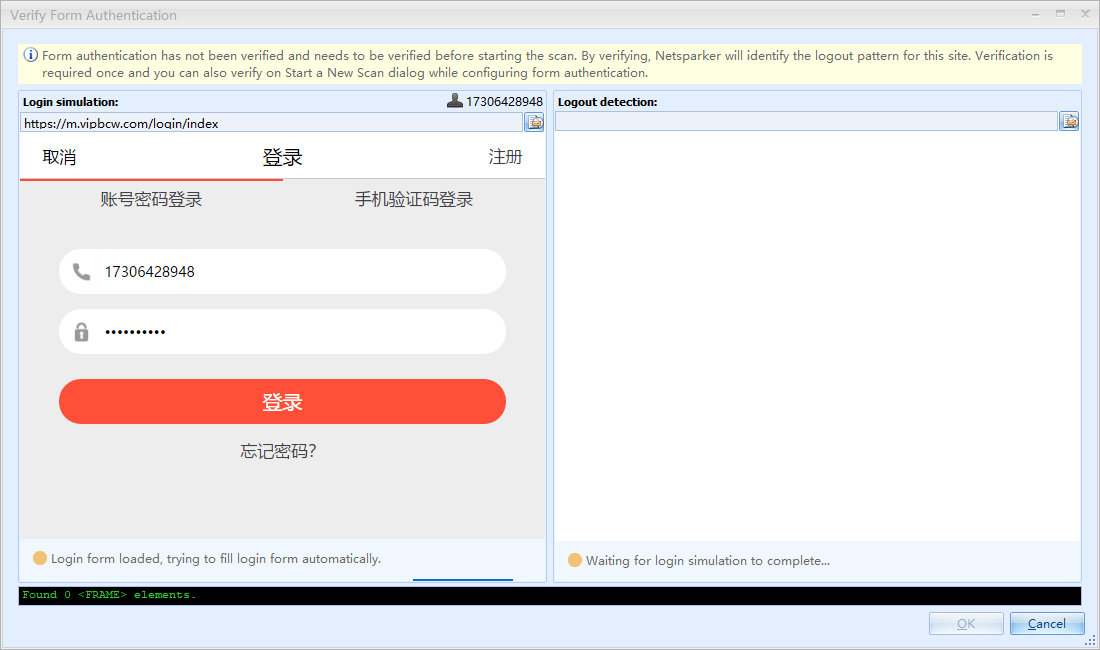
1. 打开软件如图，填入需要扫描的网站url：



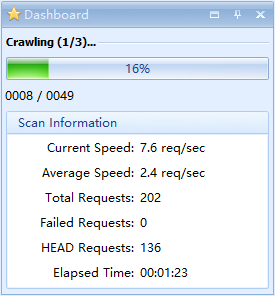
1. 点击Form，输入网站url和cookie：



1. 登录登出认证

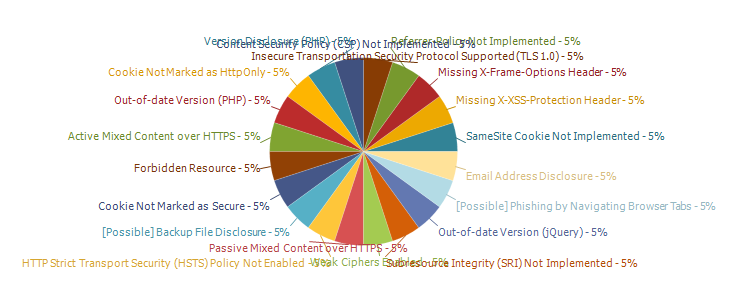


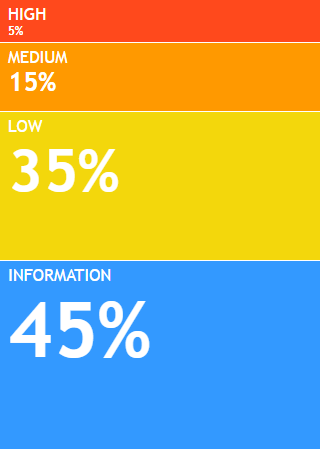
1. 等待扫描结果：



## 四、扫描结果

缺陷饼图：





## 五、缺陷分析：

1. Cookie未被加密

Netsparker识别出未加密的cookie，并通过HTTPS传输。这意味着该cookie可能被攻击者窃取，攻击者可以成功地拦截和解密通信，或者进行中间人攻击。

影响：这个cookie将通过HTTP连接传输，因此如果这个cookie很重要(比如会话cookie)，攻击者可能会截获它并劫持受害者的会话。如果攻击者能够执行中间人攻击，则他可以迫使受害者发出HTTP请求来窃取cookie。

解决方案：

1. 使用MD5进行加密。
2. 隐私信息不应该存在cookie中，比如登陆信息，只应存储登陆状态。
3. 允许弱密码

Netsparker检测到在安全通信(SSL)期间启用了弱密码。应该只允许web服务器上的强密码，以保护与访问者的安全通信。

影响：攻击者可能解密服务器和访问者之间的SSL通信。

解决方案：

1. 对于Apache，修改httpd.conf中的SSLCipherSuite指令。

SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

1. 对于Microsoft IIS，对系统注册表进行一些更改。

单击“开始”，单击“运行”，键入“regedt32”或“键入regedit”，然后单击“确定”。

在注册表编辑器中，找到以下注册表项:HKLM\SYSTEM\CurrentControlSet\Control\ securityprovider。

将“Enabled”DWORD设置为以下注册表项:

SCHANNEL\Ciphers\DES 56/56

SCHANNEL\Ciphers\RC4 64/128

SCHANNEL\Ciphers\RC4 40/128

SCHANNEL\Ciphers\RC2 56/128

SCHANNEL\Ciphers\RC2 40/128

SCHANNEL\Ciphers\NULL

SCHANNEL\Hashes\MD

1. HTTPS使用活动混合内容(Active Mixed Content)

Netsparker检测到在HTTPS页面中加载了HTTP的活动内容。

影响：

活动内容是一种可以在页面上下文中运行的资源，而且可以改变整个页面。如果HTTPS页面包含了通过常规的cleartext HTTP检索的脚本或样式表等活动内容，那么连接只是部分加密的。未加密的内容可以通过嗅探器访问。

中间人攻击者可以截获HTTP内容的请求，并重写响应，包括恶意代码。恶意的活动内容可以窃取用户的凭证，获取用户的敏感数据，或者试图在用户身上安装恶意软件。

解决方案：

有两种技术可以防御混合内容问题:

1. HTTP的严格传输安全性(HSTS)是一种强制安全资源检索的机制，即使在面对用户错误(试图再80端口访问您的web站点)和实现错误(您的开发人员将一个不安全的链接放入安全页面)时，也是如此。
2. 内容安全策略(CSP)可以用来阻止来自第三方网站的不安全资源检索。
3. 此外，您可以使用“protocol relative URLs”让用户的浏览器根据用户所连接的协议自动选择HTTP或HTTPS。
4. jQuery版本过期

Netsparker检测到目标软件使用的jQuery版本已经被弃用并且过期。

影响：

由于使用了很旧的版本，所以可以存在漏洞而被攻击。

解决方案：

更新jQuery版本到最新版。

1. Cookie 没有被设置为HttpOnly标识

HttpOnly标识的cookie不可以被客户端的脚本读取，所以将cookie标记为HttpOnly可以有效的防止跨域脚本攻击。

影响：

在黑客使用跨域脚本攻击的时候，攻击者可能更加容易的获取到cookie和劫持用户的session。

解决方案：

1. 将cookie设置成HTTPOnly，这将为跨站脚本攻击(XSS)提供额外的防护，但是这并不是绝对安全的，也就是说不能完全阻止跨站脚本攻击，因为攻击者可以使用工具(XSS Tunnel)来绕过这层防御。
2. PHP版本泄露

在HTTP的response中发现了PHP的版本信息

影响：

此类信息可以帮助攻击者获取到系统运行环境，也就可能发起对特定PHP版本的攻击。

解决方案：

配置网站服务器，使其阻止此类信息的泄露，将其从HTTP的response中去除。