



Executive Security Report

1. Special Notes

This report has been generated using N-Stalker Free Edition 2012. Get your copy at <http://www.nstalker.com/>.

2. Legal Disclaimer

This report and any supplements are CONFIDENTIAL and may be protected by one or more legal privileges. It is intended solely for the use of the addressee identified in the report. If you are not the intended recipient, any use, disclosure, copying or distribution of the report is UNAUTHORIZED. If you have received this report in error, please destroy it immediately.

N-Stalker Web Application Security Scanner assessments ("Services") are provided on an "As Is, As Available" basis without any warranty of any kind. By accepting this report, you understand that assessing computer security is highly complex and changeable. N-Stalker Web Application Security Scanner makes no warranty that the "Services" will find every vulnerability in your Web Application or Web Server(s), or that the solutions suggested and advice provided in this report will be complete or error-free. N-Stalker Web Application Security Scanner shall be held harmless and free from all liabilities for any use or application of the information provided by aexcea in connection with using the "Services". You use the "Services" at your own risk. You are solely responsible for any damage to your devices as a result of using the "Services".





N-Stalker Web Application Security Scanner MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE IN CONNECTION WITH THIS AGREEMENT OR YOUR USE OF THE SERVICES.

3. Technical Summary

3.1. Scan Session Information

URL :	http://localhost/zblogphp/
Date:	Jul 10, 2018 13:28:24
Scan Policy:	Unnamed Free Edition Policy
SSL Cipher (Algorithm):	N/A
Server Reported Banner:	Apache/2.4.33 (Win64) PHP/5.6.35
Server Technology (Banner):	Unknown Server
Server Technology Detected:	Unknown Server
Server-side Technologies:	[PHP]

3.2. Issues Found

Status	# Found
 High	1
 Medium	13
 Low	4
 Informational	3

3.3. Scan Session Statistics

Total Duration:	00 hours 07 minutes
Number of Pages (URLs):	54 pages
Total Requests:	5,011 requests
Total Bytes In:	2,716,443 bytes
Total Bytes Out:	1,545,366 bytes
Average Response Time:	0 ms
Average Transfer Rate:	338,797.00 KB/s
Average Page Size:	47,217 bytes

3.4. Scan Policy Details

? **N-Stalker Web Application Security Scanner HTTP Attack Signatures Database**

? **Ataque Common File & Directory**

- ? Search for Hidden Directories

? **Web Server Security**

- ? Search for Files susceptible to download
- ? Ensure SSL channel is using strong encryption
- ? Search for Insecure HTTP Methods
- ? Identify server technology through HTTP fingerprints
- ? Search for Web Server software vulnerabilities
- ? Search for issues in SSL server's certificate

? **DOM Security Check**

- ? Search for Information Exposure on Meta Tags

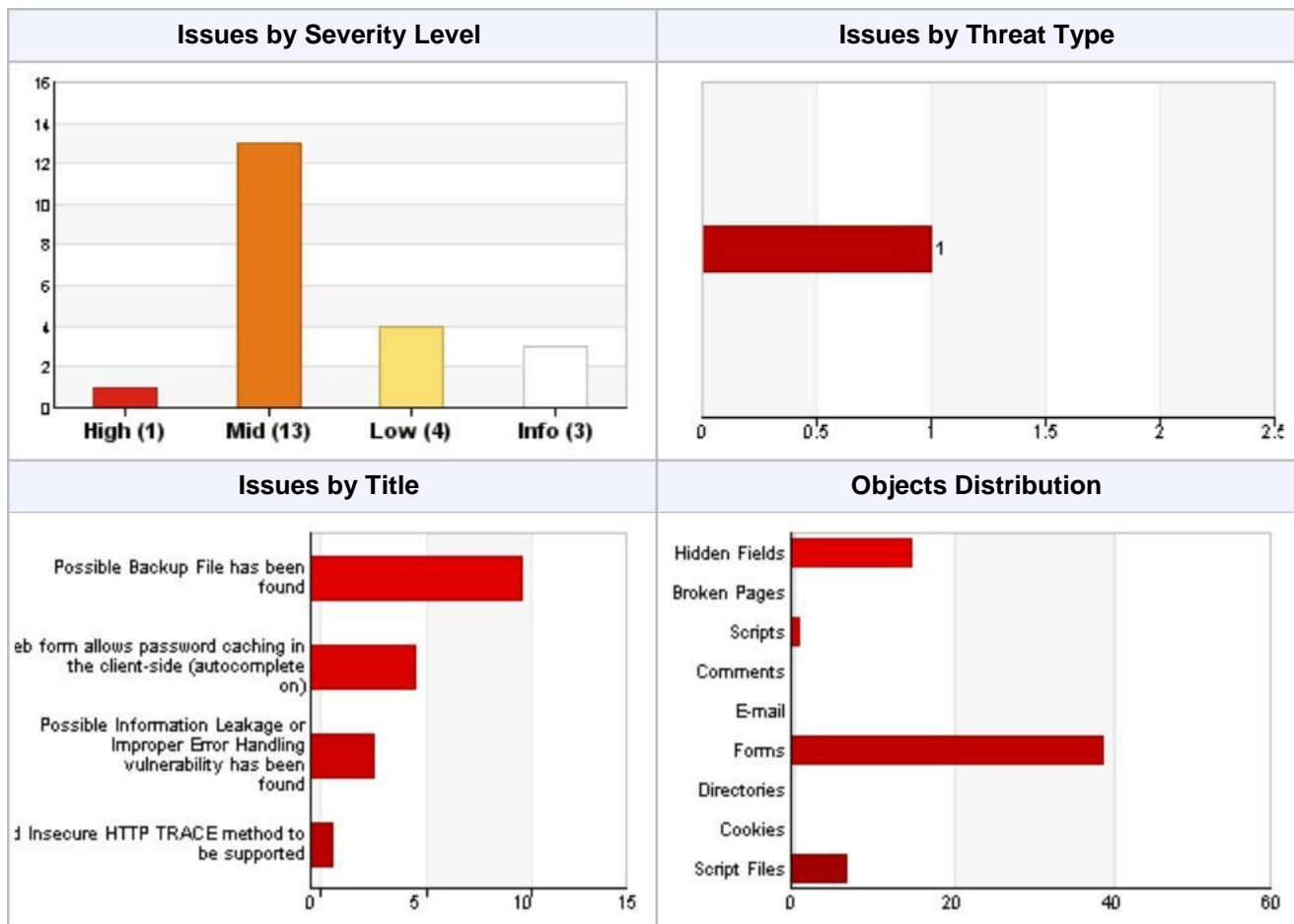
? **Web Form Security**

- ? Search for Web Forms that allow for password-cache
- ? Search for information leakage in Web Forms (external action)
- ? Search for Unprotected Authentication Web Forms (outside SSL)
- ? Search for Unprotected General Web Forms (outside SSL)
- ? Search for suspicious hidden values in Web Forms
- ? Search for Insecure Web Form Methods (non-POST)

? **Attack Modules**

- ? Cross-Site Scripting Assessment
- ? Information Leakage Assessment
- ? WebDAV Detection Module
- ? Flash/Silverlight Cross-domain Inspection Module
- ? Cookie Inspection Module
- ? Clickjacking Inspection Module
- ? HTTP Parameter Pollution Assessment
- ? Cross-site request forgery Assessment

4. Graphical Details



5. Items that require your attention

5.1. Infrastructure Issues

4 Informational	Webserver will disclose platform details or version information (Server Version)	
Target Server	http://localhost/	
# of Occurences	1	

Why is it an issue ?	
Your webserver is exposing information about its version and platform details that might assist an attacker while assessing an effective attack against your infrastructure.	

4 Informational	Webserver will disclose platform details or version information (Platform Details and Version)	
Target Server	http://localhost/	
# of Occurences	1	

Why is it an issue ?	
Your webserver is exposing information about its version and platform details that might assist an attacker while assessing an effective attack against your infrastructure.	

4 Informational	Webserver will disclose platform details or version information (HTTP Information)	
Target Server	http://localhost/	
# of Occurences	1	

Why is it an issue ?	
Your webserver is exposing information about its version and platform details that might assist an attacker while assessing an effective attack against your infrastructure.	

1 High	Old PHP 5.x Versions might be susceptible to security flaws	
Target Server	http://localhost/	
# of Occurences	1	

Why is it an issue ?

N-Stalker provides a full set of common attack signatures to detect vulnerable web server infrastructure and 3rd-party components. By running a set of HTTP requests crafted by well-known signatures, N-Stalker may detect if a vulnerability is present in a particular server.

You must consider assessing the issue to define if it represents a real problem to your application.

5.2. Application Issues

2 Medium	Web form allows password caching in the client-side (autocomplete on)	
Target Server	http://localhost/	
# of Occurences	1	

Why is it an issue ?	
<p>Auto-complete feature is common feature in all available web browsers. It keeps users from re-typing basic information such as authentication credentials, personal information, etc. While it represents a good user-driven feature, storing credentials (user/password) is not a good security practice as unassisted computers (browsers) may easily become target of an access violation attack.</p> <p>N-Stalker recommends you to adopt "autocomplete=off" directive to at least your password forms.</p>	

3 Low	Found Insecure HTTP TRACE method to be supported	
Target Server	http://localhost/	
# of Occurences	1	

Why is it an issue ?	
<p>N-Stalker has found an uncommon HTTP method supported by your webserver infrastructure that can be used for malicious activity.</p> <p>The HTTP TRACE method returns the contents of client HTTP requests in the entity-body of the TRACE response. Attackers could leverage this behavior to access sensitive information, such as cookies or authentication data, contained in the HTTP headers of the request.</p>	

3 Low	Possible Information Leakage or Improper Error Handling vulnerability has been found	
Target Server	http://localhost/	
# of Occurences	3	

Why is it an issue ?	
-----------------------------	--

Tampering with parameters to force an application to generate uncommon error messages or even unauthorized access is well-known attack against Web applications. An error message is usually something that is not correctly filtered and additional information about system platform, directory location and even confidential information may be exposed. Attacks may include:

- ? Parameter deletion (removing all parameters from a valid URL)
- ? Boolean parameter modification (modifying boolean parameters to force different conditions)
- ? Special Parameter Addition (such as debug and verbose).

Consequences of that attack would include:

- ? Confidential Information disclosure
- ? System Information disclosure
- ? Unauthorized remote access

According to OWASP:

Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Applications can also leak internal state via how long they take to process certain operations or via different responses to differing inputs, such as displaying the same error text with different error numbers. Web applications will often leak information about their internal state through detailed or debug error messages. Often, this information can be leveraged to launch or even automate more powerful attacks.

2 Medium

Application might be vulnerable to clickjacking attacks

Target Server

http://localhost/

of Occurences

1

Why is it an issue ?

N-Stalker has found your system is vulnerable to clickjacking attack which allows malicious users to manipulate legitimate user interactions within your application.

2 Medium

Possible Backup File has been found

Target Server

http://localhost/

of Occurences

10

Why is it an issue ?

File/Directory Attacks are common in Web Applications and may represent a critical threat. N-Stalker will test for the following exposures:

- ? Presence of backup files (that will expose source code or system information)
- ? Presence of password/system files (that will expose confidential information)
- ? Presence of configuration files (that will expose system configuration information)

This certainly represents a problem because attackers may take advantage of that information to escalate the attack to a more complex level and with additional critical consequences.

**Medium****Multiple Cross-site request forgery vulnerability has been found****Target Server**

http://localhost/

of Occurrences

1

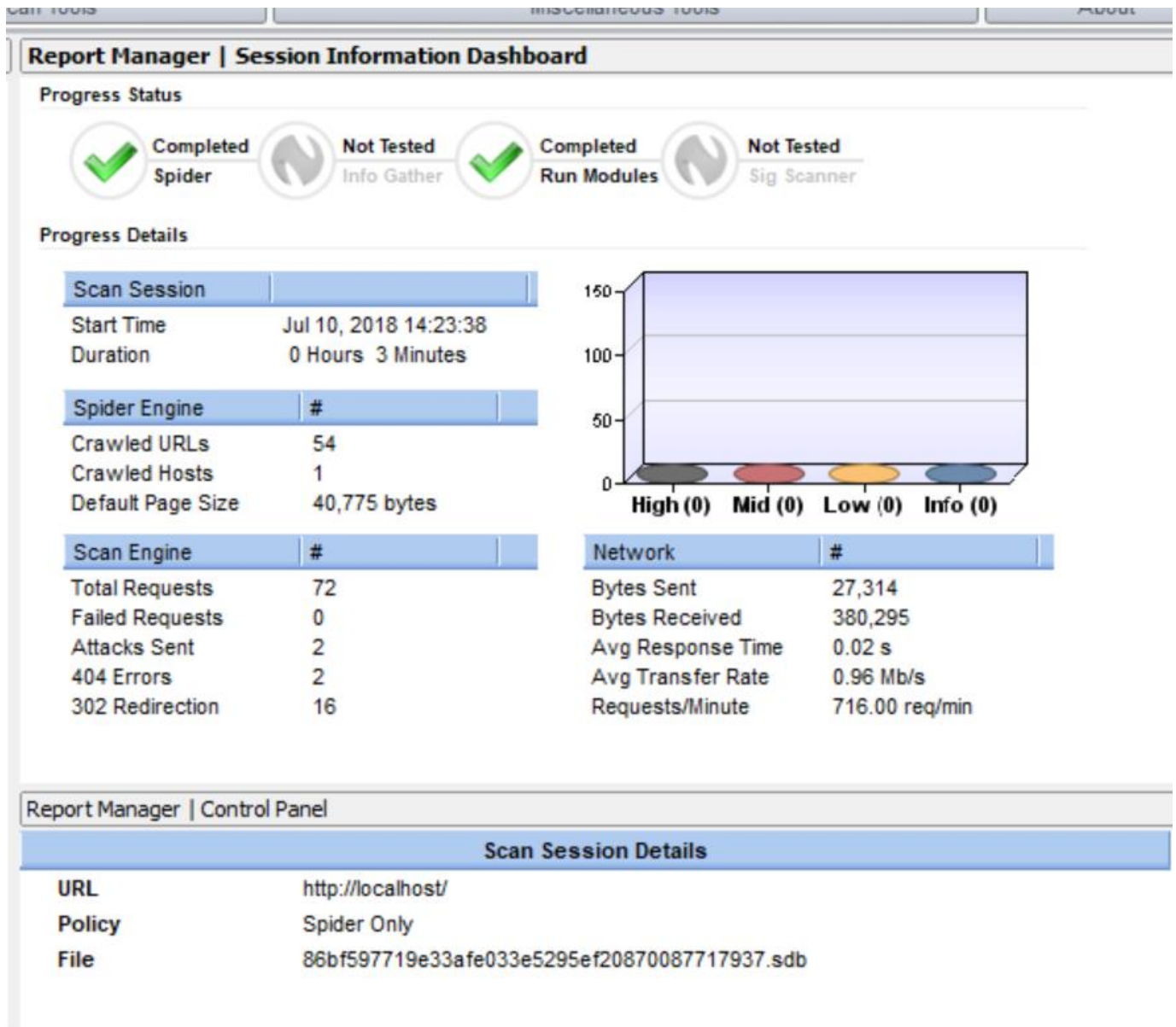
Why is it an issue ?

Cross-Site Request Forgery (CSRF) is an attack that tricks the victim into loading a page that contains a malicious request. It is malicious in the sense that it inherits the identity and privileges of the victim to perform an undesired function on the victim's behalf, like change the victim's e-mail address, home address, or password, or purchase something. CSRF attacks generally target functions that cause a state change on the server but can also be used to access sensitive data.

5.3. Confidentiality Issues

No Issues found.

总体概览



以上是由 N-Stalker 扫描个人博客系统生成的检测报告。同时考虑到这个 web 应用是部署在本地，除了由个人笔记本电脑的性能不足造成的问题外，个人博客系统的整体安全情况是不错的。为了防止 SQL 注入，在查询函数的时候不采用拼接。为了防止注入，过滤客户端提交的危险字符。同时为了进一步加强安全性，可以隐藏后台地址。

方法：

1、将下列代码加入源代码主题目录下 include.php 的 <?php 后：

```
function zblog_login_encrypt(){
    global $zbp;
    $wen="question"; //问题，请在引号内输入问题，注意不要使用中文
    $da="answer "; //答案，请在引号内输入答案，不要使用中文
    if($_GET["$wen."] != ".$da.") {
        Redirect($zbp->host);
        die();
        //如输入错误，返回首页，终止一切代码
    }
}
```

2、将下列代码加入到源代码主题目录下 include.php 的 function ActivePlugin_主题 ID() 内：

```
Add_Filter_Plugin('Filter_Plugin_Login_Header','zblog_login_encrypt');//挂载登录页接口
```

3、这样一来直接点击后台登陆按钮是不行的，必须输入

网站域名/zb_system/login.php? question=answer （PS：地址中的 question=请自行替换为自己的问题，answer 也请自行替换为自己的答案。）