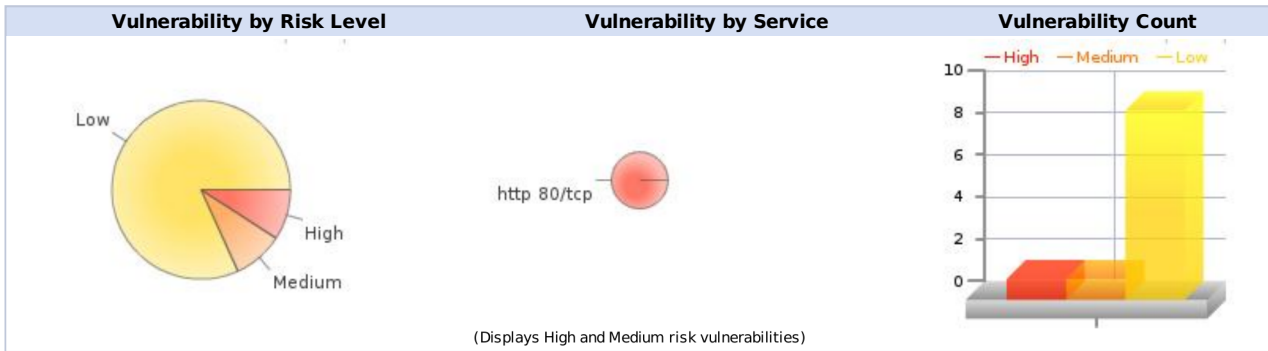




Scan Results	
Hostname	example.com
Scan date	2008-08-06
Vulnerability Score	63.00 (D) ? Score ranges between 0 and 100. A low score means you are vulnerable to attack.
Vulnerability Summary	
High	1 Expand details »
Medium	1 Expand details »
Low	9 Expand details »
Total	11



High risk vulnerabilities results for: example.com	
1. Vulnerabilities in Custom Web Code (High) back	
Port:	http (80/tcp)
Summary:	SQL Injection via GET - http://example.com/login.htm?url=a®Token=b&referringUrl=c&channel=d&email='
	The remote web server suffers from an SQL Injection vulnerability. This could enable a remote attack to gain direct access to the database and in some cases execute commands remotely on the web server. The URL above shows how the vulnerability can be observed.
Recommended Solution:	Filter out any user provided data from inappropriate characters (especially ' (), and ").
Impact:	Attackers can take control over your database, and in some cases over the operating system (using master..xp_cmdshell, CREATE LIBRARY, etc).
More information:	See http://www.securiteam.com/securityreviews/5DP0N1P76E.html , http://www.securiteam.com/securityreviews/5UP010A6AA.html , http://www.securiteam.com/securityreviews/5IP030K8AA.html , and http://www.securiteam.com/securityreviews/5GP0E2K7FO.html
Test ID:	2062

Medium risk vulnerabilities results for: example.com	
1. F5 BIP-IP Cookie Persistence (Medium) back	
Port:	http (80/tcp)

Summary:

The remote host appears to be a F5 BigIP load balancer which encodes within a cookie the IP address of the actual web server it is acting on behalf of. Additionally, information after 'BIGipServer' is configured by the user and may be the logical name of the device. These values may disclose sensitive information, such as internal IP addresses and names.

More

information: <http://www.f5.com/solutions/archives/techbriefs/cookie.html>

Test ID: 9321

Low risk vulnerabilities results for: example.com

1. Supported SSL Ciphers Suites (Low) [back](#)

Port: https (443/tcp)

Summary:

This test detects which SSL ciphers are supported by remote service for encrypting communications.

Export Ciphers

SSLv2

EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export

EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export

SSLv3

EXP-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES(40) Mac=SHA1 export

EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export

EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export

EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export

TLSv1

EXP-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES(40) Mac=SHA1 export

EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export

EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export

EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export

Low Strength Ciphers (excluding export, < 128-bit key)

SSLv2

DES-CBC-MD5 Kx=RSA Au=RSA Enc=DES(56) Mac=MD5

RC4-64-MD5 Kx=RSA Au=RSA Enc=RC4(64) Mac=MD5

SSLv3

EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES(56) Mac=SHA1

DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1

TLSv1

EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES(56) Mac=SHA1

DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1

Medium Strength Ciphers (128-bit key)

SSLv2

RC2-CBC-MD5 Kx=RSA Au=RSA Enc=RC2(128) Mac=MD5

RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5

SSLv3

RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5

RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

TLSv1

RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5

RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

High Strength Ciphers (> 128-bit key)

SSLv2

DES-CBC3-MD5 Kx=RSA Au=RSA Enc=3DES(168) Mac=MD5

SSLv3

EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1

DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1

TLSv1

EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1

DHE-RSA-AES128-SHA Kx=DH Au=RSA Enc=AES(128) Mac=SHA1

DHE-RSA-AES256-SHA Kx=DH Au=RSA Enc=AES(256) Mac=SHA1

DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1

AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1

AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1

The fields above are:

{OpenSSL ciphername}

Kx={key exchange}

Au={authentication}

Enc={symmetric encryption method}

Mac={message authentication code}

{export flag}

More information:	http://www.openssl.org/docs/apps/ciphers.html
Test ID:	9819
2. Deprecated SSL Protocol Usage (Low) back	
Port:	https (443/tcp)
Summary:	
The remote service accepts connections encrypted using SSL 2.0, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.	
Recommended Solution:	
Consult the application's documentation to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead.	
For Microsoft's IIS server, see: * http://support.microsoft.com/kb/187498	
More information:	http://www.schneier.com/paper-ssl.pdf
Test ID:	9329
3. robot(s).txt Detection (Low) back	
Port:	http (80/tcp)
Summary:	
Some webmasters use a file called robot(s).txt to supply information to search engines and other indexing tools. This file exists on your server: make sure it doesn't contain sensitive information. 'robots.txt' contains the following: # http://example.com/robots.txt	
User-agent: *	
# Requires login Disallow: /clipper.htm Disallow: /login.htm Disallow: /logout.htm Disallow: /message.htm Disallow: /myaccount.htm	
# Not web page Disallow: /contentAsset.htm Disallow: /e/	
Recommended Solution:	
Make sure the file doesn't contain any sensitive information.	
Impact:	
This file can be viewed by anyone, and it might contain sensitive information about the server. For example, specifying which directories shouldn't be indexed tells the attacker where the sensitive files are.	
Test ID:	968
4. TCP Timestamps Retrieval (Low) back	
Port:	general/tcp
Summary:	
The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can be sometimes be computed.	
The uptime was estimated to 5236207s, i.e. about 60 days. (Note that the clock is running at about 100 Hz and will overflow in about 42949672s, that is 497 days)	
More information:	http://www.ietf.org/rfc/rfc1323.txt
Test ID:	10399
5. HTTP Packet Inspection (Low) back	
Port:	https (443/tcp)
Summary:	
This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc.	
Protocol version: HTTP/1.1 SSL: yes	

More information: http://www.adobe.com/devnet/flashplayer/articles/cross_domain_policy.html, http://www.adobe.com/go/tn_14213, http://blogs.adobe.com/stateofsecurity/2007/07/crossdomain_policy_files_1.html and <http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html>

Test ID: 11058

8. Flash Cross-Domain Policy File (Low) [back](#)

Port: http (80/tcp)

Summary:

The remote web server contains a cross-domain policy file. This is a simple XML file used by Adobe's Flash Player to allow access to data that resides outside the exact web domain from which a Flash movie file originated.

We were able to obtain a cross-domain policy file from the remote host using the following URL:

```
http://example.com/crossdomain.xml
<?xml version="1.0"?>
<cross-domain-policy>
<allow-access-from domain="*.example.com" />
</cross-domain-policy>
```

Recommended Solution:

Review the contents of the policy file carefully. Improper policies, especially an unrestricted one with just '*', could allow for cross-site request forgery and cross-site scripting attacks against the web server.

More information: http://www.adobe.com/devnet/flashplayer/articles/cross_domain_policy.html, http://www.adobe.com/go/tn_14213, http://blogs.adobe.com/stateofsecurity/2007/07/crossdomain_policy_files_1.html and <http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html>

Test ID: 11058

9. robot(s).txt Detection (Low) [back](#)

Port: https (443/tcp)

Summary:

Some webmasters use a file called robot(s).txt to supply information to search engines and other indexing tools. This file exists on your server: make sure it doesn't contain sensitive information.

'robots.txt' contains the following:

```
# http://example.com/robots.txt
```

```
User-agent: *
```

```
# Requires login
```

```
Disallow: /clipper.htm
```

```
Disallow: /login.htm
```

```
Disallow: /logout.htm
```

```
Disallow: /message.htm
```

```
Disallow: /myaccount.htm
```

```
# Not web page
```

```
Disallow: /contentAsset.htm
```

```
Disallow: /e/
```

Recommended Solution:

Make sure the file doesn't contain any sensitive information.

Impact:

This file can be viewed by anyone, and it might contain sensitive information about the server. For example, specifying which directories shouldn't be indexed tells the attacker where the sensitive files are.

Test ID: 968

DISCLAIMER: This report is not meant as an exhaustive analysis of the level of security now present on the tested host, and the data shown here should not be used exclusively to judge the security level of any computer system. This scan was performed automatically, and unlike a manual penetration test it does not reveal all the possible security holes present in the system. Some vulnerabilities that were found might be 'false alarms'.

The information in this report is provided "as is" and no liability for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages will be accepted.