

BOMGAR™

# Vulnerability Scans

Security

### Contents

About Vulnerability Scanning .....	3
QualysGuard PCI Report .....	4
McAfee Report .....	18
IBM Rational AppScan .....	33

## About Vulnerability Scanning

To ensure the security and value of our product, Bomgar incorporates vulnerability scanning in our software testing process. We eagerly commit to addressing, with the utmost urgency, security vulnerabilities as they are detected by industry security professionals.

We track the results of vulnerability scans performed prior to a software release and prioritize resolution based on severity and criticality of any issues uncovered. Should a critical or high-risk vulnerability surface after a software release, a subsequent maintenance version release addresses the vulnerability. Updated maintenance versions are distributed to our customers via the update manager interface within the Bomgar administrative interface. Where necessary, Bomgar support will contact customers directly, describing special procedures to follow to obtain an updated maintenance version.

Our customers can rely on our commitment to address security issues at our earliest opportunity.

Note: The contents of this document are comprised of the latest scan results from Qualys, McAfee, and IBM RationalApp Scan. All scans were performed against an installation of Bomgar 11.1.

# Scan Results

10/04/2011

The scan was started on 09/22/2011 at 20:31:03 and took 04:06:51 to complete. The scan was run against the following IP addresses:

# Not a certified PCI report

## IP Addresses

12.182.217.176

The scan option profile used includes:

### Scan Settings

Scanned TCP Ports	Full
Scanned UDP Ports	Standard Scan
Scan Dead Hosts	Off
Load Balancer Detection	Off
Password Brute Forcing	Standard
Vulnerability Detection	Complete
Windows Authentication	Disabled
SSH Authentication	Disabled
Oracle Authentication	Disabled
SNMP Authentication	Disabled
Perform 3-way Handshake	Off
Overall Performance	Custom
Hosts to Scan in Parallel-External Scanner	10
Hosts to Scan in Parallel-Scanner Appliances	10
Processes to Run in Parallel-Total	10
Processes to Run in Parallel-HTTP	1
Packet (Burst) Delay	Maximum

### Advanced Settings

Host Discovery	TCP Standard Scan
	UDP Standard Scan
	ICMP On
Ignore RST packets	Off
Ignore firewall-generated SYN-ACK packets	Off
ACK/SYN-ACK packets during discovery	Send

## Report Summary

Company:	Bomgar Corporation
User:	Tal Guest
Template Title:	Scan Results
Active Hosts:	1
Total Hosts:	1
Scan Type:	On Demand
Scan Status:	Finished
Scan Title:	11.1.2
Scan Date:	09/22/2011 at 20:31:03
Reference:	scan/1316723469.12520
Scanner Appliance:	64.39.111.24 (Scanner 5.17.57-1, Web 6.21.72-1, Vulnerability Signatures 1.28.226-3)
Duration:	04:06:51
Options:	Payment Card Industry (PCI) Options
Target:	12.182.217.176

## Summary of Vulnerabilities

Vulnerabilities Total	15	Average Security Risk		2.0
-----------------------	----	-----------------------	---	-----

### by Severity

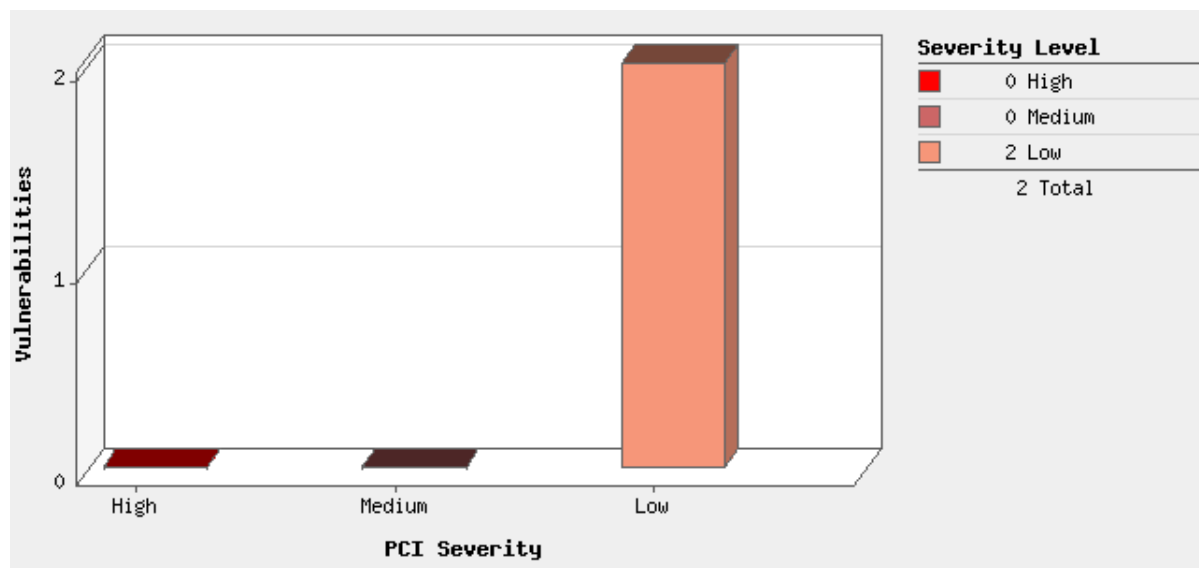
Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	0	0	0
2	2	0	2	4
1	0	0	11	11
Total	2	0	13	15

### by PCI Severity

PCI Severity	Confirmed	Potential	Total
High	0	0	0
Medium	0	0	0
Low	2	0	2
Total	2	0	2

## Vulnerabilities by PCI Severity

---



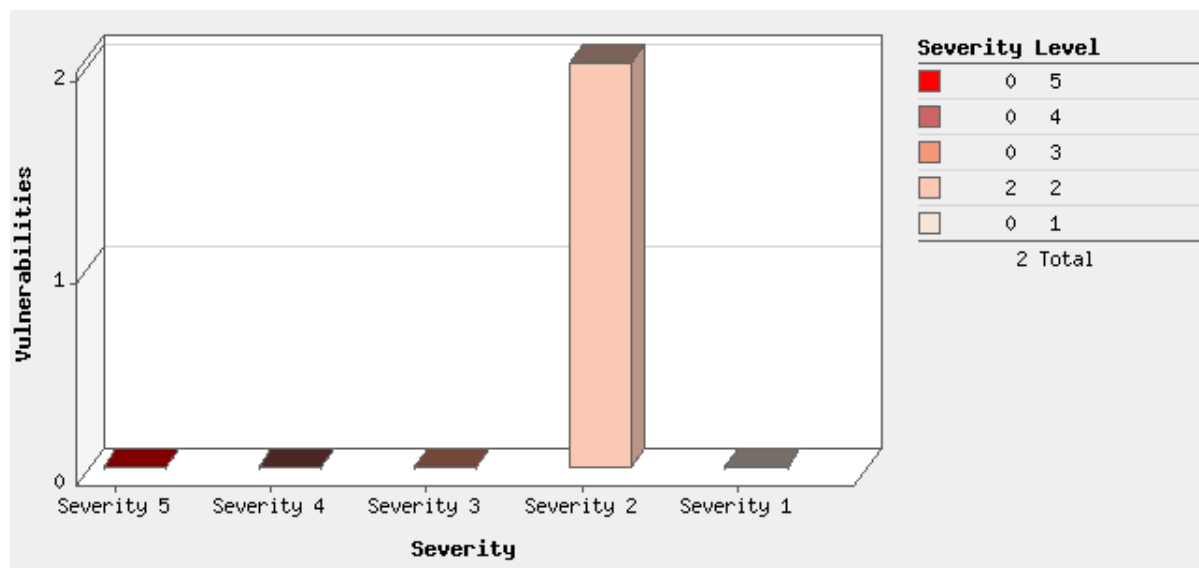
## Potential Vulnerabilities by PCI Severity

---

There is no data available

## Vulnerabilities by Severity

---



## Potential Vulnerabilities by Severity

---

There is no data available


# Detailed Results


12.182.217.176

Bomgar Appliance

Vulnerabilities Total **15** Security Risk  2.0 Compliance Status **PASS**

## Vulnerabilities (2)

 2 Path-Based Vulnerability port 80/tcp

QID:	150004	CVSS Base:	2.1	PCI Severity:	
Category:	Web Application	CVSS Temporal:	1.9		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	10/19/2007				

**THREAT:**

A potentially sensitive file, directory, or directory listing was discovered on the Web server.

**IMPACT:**


The contents of this file or directory may disclose sensitive information.


**SOLUTION:**

Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

**RESULT:**

url: http://12.182.217.176/files/  
matched: HTTP/1.1 200 OK

 2 SSL Certificate - Subject Common Name Does Not Match Server FQDN port 443/tcp over SSL

QID:	38170	CVSS Base:	2.6	PCI Severity:	
Category:	General remote services	CVSS Temporal:	2.1		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	09/29/2008				

**THREAT:**

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:  
If the common name of the certificate uses a wildcard such as \*.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for QualysGuard to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

**IMPACT:**

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

**SOLUTION:**

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

**RESULT:**

Certificate #0 CN=\*.bomgar.com,OU=Remote\_Support,O=Bomgar\_Corporation,L=Ridgeland,ST=Mississippi,C=US (\*.bomgar.com) doesn't resolve (bomgar.com) and IP (12.182.217.176) don't match (\*.bomgar.com) doesn't resolve

Information Gathered (13)

2 Operating System Detected

QID: 45017
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 02/09/2005

**THREAT:**

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that for the firewall instead of for the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB\_II.system.sysDescr" for the operating system.

**IMPACT:**

Not applicable

**SOLUTION:**

Not applicable

**RESULT:**

Table with 3 columns: Operating System, Technique, ID. Row 1: Bomgar Appliance, TCP/IP Fingerprint, U1723:80

2 Host Uptime Based on TCP TimeStamp Option

QID: 82063

Category: TCP/IP  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 05/29/2007

**THREAT:**

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.

Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

**RESULT:**

Based on TCP timestamps obtained via port 80, the host's uptime is 35 days, 0 hours, and 6 minutes. The TCP timestamps from the host are in units of 10 milliseconds.

 1 DNS Host Name

QID: 6  
Category: Information gathering  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 01/01/1999

**THREAT:**

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

**RESULT:**

IP address	Host name
12.182.217.176	No registered hostname

 1 Host Scan Time

QID: 45038  
Category: Information gathering  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 11/19/2004

**THREAT:**

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

**RESULT:**

Scan duration: 14750 seconds

Start time: Thu, Sep 22 2011, 20:31:09 GMT

End time: Fri, Sep 23 2011, 00:36:59 GMT



#### 1 External Links Discovered

port 80/tcp

QID: 150010  
Category: Web Application  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 10/19/2007

#### THREAT:

The external links discovered by the Web application scanning engine are provided in the Results section. These links were present on the target Web application, but were not crawled.

#### RESULT:

Number of links: 2  
<http://www.bomgar.com/>  
<http://www.bomgar.com/virtualsupportolutions/>



#### 1 Scan Diagnostics

port 80/tcp

QID: 150021  
Category: Web Application  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 01/16/2009

#### THREAT:

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

#### IMPACT:

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

#### SOLUTION:

No action is required.

#### RESULT:

Collected 10 links overall.  
Path manipulation: estimated time < 10 minutes (72 tests, 10 inputs)  
Path manipulation: 72 vulnsigs tests, completed 367 requests, 13 seconds. All tests completed.  
WSEnumeration estimated time: no tests enabled  
Batch #1 URI parameter manipulation: estimated time < 1 minute (33 tests, 2 inputs)  
Batch #1 URI parameter manipulation: 33 vulnsigs tests, completed 32 requests, 8 seconds. XSS optimization removed 34 links. Completed 32 requests of 66 estimated requests (48%). All tests completed.  
Batch #1 URI blind SQL manipulation: estimated time < 1 minute (19 tests, 2 inputs)  
Batch #1 URI blind SQL manipulation: 19 vulnsigs tests, completed 38 requests, 20 seconds. All tests completed.  
Batch #1 URI parameter time-based tests: estimated time < 1 minute (5 tests, 2 inputs)  
Batch #1 URI parameter time-based tests: 5 vulnsigs tests, completed 10 requests, 3 seconds. All tests completed.  
Batch #2 URI parameter manipulation: estimated time < 1 minute (33 tests, 1 inputs)  
Batch #2 URI parameter manipulation: 33 vulnsigs tests, completed 16 requests, 5 seconds. XSS optimization removed 17 links. Completed 16 requests of 33 estimated requests (48%). All tests completed.  
Batch #2 URI blind SQL manipulation: estimated time < 1 minute (19 tests, 1 inputs)  
Batch #2 URI blind SQL manipulation: 19 vulnsigs tests, completed 19 requests, 10 seconds. All tests completed.

Batch #2 URI parameter time-based tests: estimated time < 1 minute (5 tests, 1 inputs)  
 Batch #2 URI parameter time-based tests: 5 vulnsigs tests, completed 5 requests, 2 seconds. All tests completed.  
 Batch #3 URI parameter manipulation: estimated time < 1 minute (33 tests, 0 inputs)  
 Batch #3 URI parameter manipulation: 33 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.  
 Batch #3 URI blind SQL manipulation: estimated time < 1 minute (19 tests, 0 inputs)  
 Batch #3 URI blind SQL manipulation: 19 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.  
 HTTP call manipulation estimated time: no tests enabled  
 Cookie manipulation: estimated time < 1 minute (26 tests, 1 inputs)  
 Cookie manipulation: 26 vulnsigs tests, completed 81 requests, 12 seconds. XSS optimization removed 153 links. Completed 81 requests of 234 estimated requests (35%). All tests completed.  
 Header manipulation: estimated time < 1 minute (26 tests, 9 inputs)  
 Header manipulation: 26 vulnsigs tests, completed 153 requests, 23 seconds. XSS optimization removed 153 links. Completed 153 requests of 468 estimated requests (33%). All tests completed.  
 Total requests made: 800  
 Average server response time: 0.24 seconds  
 Most recent links:  
 200 http://12.182.217.176/help.ns?show\_help=help\_issues\_menu  
 200 http://12.182.217.176/content/appliance.css  
 200 http://12.182.217.176/content/style.css  
 200 http://12.182.217.176/content/screen.css  
 200 http://12.182.217.176/content/mobile.css  
 200 http://12.182.217.176/content/nsjs.js  
 200 http://12.182.217.176/  
 200 http://12.182.217.176/help.ns?show\_help=help\_rep\_list  
 200 http://12.182.217.176/help.ns?show\_help=help\_session\_keys  
 200 http://12.182.217.176/help.ns?show\_help=help\_issues\_menu  
 Scan launched using PCI WAS combined mode.  
 HTML form authentication unavailable, no WEBAPP entry found

 1 SSL Web Server Version port 443/tcp

QID: 86001  
 Category: Web server  
 CVE ID: -  
 Vendor Reference: -  
 Bugtraq ID: -  
 Last Update: 01/01/1999

**RESULT:**

Server Version	Server Banner
-	Bomgar

 1 SSL Web Server Version security2.bomgar.com:443/tcp

QID: 86001  
 Category: Web server  
 CVE ID: -  
 Vendor Reference: -  
 Bugtraq ID: -  
 Last Update: 01/01/1999

**RESULT:**

Server Version	Server Banner
-	Bomgar

 1 Web Server Version port 80/tcp

QID: 86000

Category: Web server  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 01/01/1999

**RESULT:**

Server Version	Server Banner
-	Bomgar

 1 Links Crawled

port 80/tcp

QID: 150009  
Category: Web Application  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 10/21/2008

**THREAT:**

The list of unique links crawled by the Web application scanner appear in the Result section. This list may contain fewer links than the maximum threshold defined at scan launch. The maximum links to crawl includes links in this list, requests made via HTML forms, and requests for the same link made as an anonymous and authenticated user.

**RESULT:**

Duration of crawl phase (seconds): 7.00  
Number of links: 9  
(This number excludes form requests and links re-requested during authentication.)

http://12.182.217.176/  
http://12.182.217.176/content/appliance.css  
http://12.182.217.176/content/mobile.css  
http://12.182.217.176/content/nsjs.js  
http://12.182.217.176/content/screen.css  
http://12.182.217.176/content/style.css  
http://12.182.217.176/help.ns?show\_help=help\_issues\_menu  
http://12.182.217.176/help.ns?show\_help=help\_rep\_list  
http://12.182.217.176/help.ns?show\_help=help\_session\_keys

 1 Open TCP Services List

QID: 82023  
Category: TCP/IP  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 06/15/2009

**THREAT:**

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

**IMPACT:**

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

**SOLUTION:**

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

**RESULT:**

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
80	www	World Wide Web HTTP	http	
443	https	http protocol over TLS/SSL	http over ssl	

 1 Firewall Detected

QID: 34011  
Category: Firewall  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 10/16/2001

**THREAT:**

A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

**RESULT:**

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 111, 135, 445, 1.

Listed below are the ports filtered by the firewall.  
No response has been received when any of these ports is probed.  
1-79,81-442,444-2100,2102-5491,5493-5504,5506-5549,5551-5559,5561-5569,  
5571-5579,5581-6013,6015-6128,6130-7009,7011-9989,9991-10109,10111-65535

 1 Traceroute

QID: 45006  
Category: Information gathering  
CVE ID: -  
Vendor Reference: -  
Bugtraq ID: -  
Last Update: 05/09/2003

**THREAT:**

Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

**RESULT:**

Hops	IP	Round Trip Time	Probe
1	64.39.111.2	0.34ms	ICMP
2	64.14.1.121	0.70ms	ICMP
3	216.33.4.53	0.57ms	ICMP
4	204.70.200.217	0.62ms	ICMP
5	204.70.200.221	0.88ms	ICMP
6	204.70.203.22	1.28ms	ICMP
7	192.205.36.5	2.59ms	ICMP

8	12.122.137.122	56.59ms	ICMP
9	12.122.3.122	81.99ms	ICMP
10	12.122.31.190	57.71ms	ICMP
11	12.122.1.18	57.32ms	ICMP
12	12.122.30.138	58.25ms	ICMP
13	12.122.1.142	57.26ms	ICMP
14	12.123.153.9	55.94ms	ICMP
15	12.91.167.118	61.34ms	ICMP
16	12.182.217.176	61.61ms	TCP

## Appendices

### Hosts Scanned

12.182.217.176

### Option Profile

#### Scan

Scanned TCP Ports:	Full
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Load Balancer Detection:	Off
Password Brute Forcing:	Standard
Vulnerability Detection:	Complete
Windows Authentication:	Disabled
SSH Authentication:	Disabled
Oracle Authentication:	Disabled
SNMP Authentication:	Disabled
Perform 3-way Handshake:	Off
Overall Performance:	Custom
Hosts to Scan in Parallel-External Scanner:	10
Hosts to Scan in Parallel-Scanner Appliances:	10
Processes to Run in Parallel-Total:	10
Processes to Run in Parallel-HTTP:	1
Packet (Burst) Delay:	Maximum

#### Advanced

Hosts Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore RST packets:	Off
Ignore firewall-generated SYN-ACK packets:	Off
Do not send ACK or SYN-ACK packets during host discovery:	Off

### Report Legend

#### Payment Card Industry (PCI) Status






The Detailed Results section of the report shows all detected vulnerabilities and potential vulnerabilities sorted by host. The vulnerabilities and potential vulnerabilities marked PCI FAILED caused the host to receive the PCI compliance status FAILED. All vulnerabilities and potential vulnerabilities marked PCI FAILED must be remediated to pass the PCI compliance requirements. Vulnerabilities not marked as PCI FAILED display vulnerabilities that the PCI Compliance service found on the hosts when scanned. Although these vulnerabilities are not in scope for PCI, we do recommend that you remediate the vulnerabilities in severity order.




A PCI compliance status of PASSED for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS compliance standards set by the PCI Council, were detected on the host. An overall PCI compliance status of PASSED indicates that all hosts in the report passed the PCI compliance standards.

A PCI compliance status of FAILED for a single host/IP indicates that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards set by the PCI Council, was detected on the host. An overall PCI compliance status of FAILED indicates that at least one host in the report failed to meet the PCI compliance standards.

#### Vulnerability Levels





A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.


Severity	Level	Description
 1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
 2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
 3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
 4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
 5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.




Severity	Level	Description
 LOW	Low	A vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
 MED	Medium	A vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
 HIGH	High	A vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

#### Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.




Severity	Level	Description
 1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
 2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
 3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
 4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.

 5 Urgent If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
	Low	A potential vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
	Medium	A potential vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
	High	A potential vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

#### Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
	1 Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
	2 Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
	3 Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.

## Security Report - By Device

**Bomgar Corporation**

**04-OCT-2011 08:55**

### **Confidential Information**

The following report contains confidential information. Do not distribute, email, fax or transfer via any electric mechanism unless it has been approved by your organization's security policy. All copies and backups of this document should be maintained on protected storage at all times. Do not share any of the information contained within this report with anyone unless you confirm they are authorized to view the information.

### **Disclaimer**

This, or any other, vulnerability audit cannot and does not guarantee security. McAfee makes no warranty or claim of any kind, whatsoever, about the accuracy or usefulness of any information provided herein. By using this information you agree that McAfee shall be held harmless in any event. McAfee makes this information available solely under its Terms of Service Agreement published at [www.mcafeesecure.com](http://www.mcafeesecure.com).

## Executive Summary

This report was generated by PCI Approved scanning vendor, McAfee, under certificate number 3709-01-05 in the framework of the PCI data security initiative.

As a Qualified Independent Scan Vendor McAfee is accredited by Visa, MasterCard, American Express, Discover Card and JCB to perform network security audits conforming to the Payment Card Industry (PCI) Data Security Standards.

To earn validation of PCI compliance, network devices being audited must pass tests that probe all of the known methods hackers use to access private information, in addition to vulnerabilities that would allow malicious software (i.e. viruses and worms) to gain access to or disrupt the network devices being tested.

NOTE: In order to demonstrate compliance with the PCI Data Security Standard a vulnerability scan must have been completed within the past 90 days with no vulnerabilities listed as MEDIUM (numerical severity ranking 3) or HIGH (numerical severity ranking of 4 or 5) present on any device within this report. Additionally, Visa and MasterCard regulations require that you configure your scanning to include all IP addresses, domain names, DNS servers, load balancers, firewalls or external routers used by, or assigned to, your company, and that you configure any IDS/IPS to not block access from the originating IP addresses of our scan servers.

## Certification of Regulatory Compliance

Sites are tested and certified daily to meet all U.S. Government requirements for remote vulnerability testing as set forth by the National Infrastructure Protection Center (NIPC). They are also certified to meet the security scanning requirements of Visa USA's

Cardholder Information Security Program (CISP), Visa International's Account Information Security (AIS) program, MasterCard International's Site Data Protection (SDP) program, American Express' CID security program, the Discover Card Information Security and Compliance (DISC) program within the framework of the Payment Card Industry (PCI) Data Security Standard.

## Report Overview

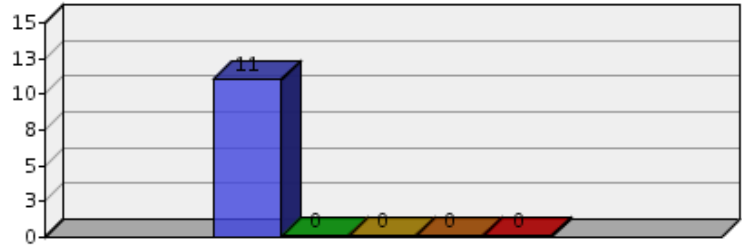
Customer Name	Bomgar Corporation
Date Generated	04-OCT-2011 08:55
Report Type	Security - By Device
Devices	1
Device Groups	0
Vulnerabilities	9

## Report Contents

- Vulnerabilities By Severity
- Vulnerabilities By Category
- Device Overview
- Services Detected
- All Vulnerabilities Found
- Device Detail
- Appendix

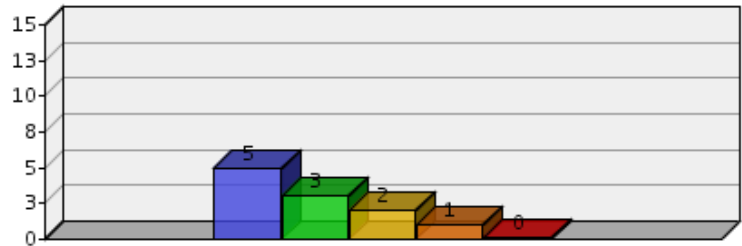
## Vulnerabilities By Severity

Severity	
<b>5</b> 0	Urgent
<b>4</b> 0	Critical
<b>3</b> 0	High
<b>2</b> 0	Medium
<b>1</b> 11	Low



## Vulnerabilities By Category (Top 5)

Category	
5	Web Application
3	Information Gathering
2	Other
1	Web Server
0	



## Services Detected - All 1 Devices

Port	Protocol	Service	Devices
80	tcp	http	1
443	tcp	https	1

## All Vulnerabilities Found

Name	Category	Devices
<b>1</b> AutoComplete attribute is true	Information Gathering	1
<b>1</b> OS Identification	Other	1
<b>1</b> Parent or Sub-Domains Identified	Other	1
<b>1</b> Hidden Fields Found - Potential Information Leakage	Web Application	1
<b>1</b> SSL Certificate Information	Web Server	1
<b>1</b> Discoverable Email Addresses	Web Application	1
<b>1</b> Text (ASCII) File(s) found	Information Gathering	1
<b>1</b> Web Server Directory Enumeration	Web Application	1
<b>1</b> SSL Cipher Suites Supported	Web Application	1

## Device Overview

Name	<b>5</b> Urgent	<b>4</b> Critical	<b>3</b> High	<b>2</b> Medium	<b>1</b> Low	Open Ports
security2.bomgar.com	0	0	0	0	11	2

## Overview - security2.bomgar.com

Last Audit Date	5 Urgent	4 Critical	3 High	2 Medium	1 Low	Total
20-SEP-2011 07:55	0	0	0	0	11	11

## Open Ports - security2.bomgar.com

Port	Protocol	Service	Banner
80	tcp	http	http
443	tcp	https	https

## Vulnerabilities - security2.bomgar.com

### Information Disclosures - security2.bomgar.com

#### 1 SSL Cipher Suites Supported

Port	First Detected	Category
443	20-SEP-2011 07:20	Web Application

Protocol	Impact
HTTPS	Information Disclosure

Description
This script detects which SSL ciphers are supported by the remote service for encrypting communications.

CVSS
2.6

Solution
n/a

Detail
--------

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)

SSLv3

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

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

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

TLSv1

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

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

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

The fields above are :

{OpenSSL ciphername}

Kx={key exchange}

Au={authentication}

Enc={symmetric encryption method}

Mac={message authentication code}

{export flag}

#### Links

[www.openssl.org/docs/apps/ciphers.html](http://www.openssl.org/docs/apps/ciphers.html)

[Apache Module mod\\_ssl](#)

## Related

None

## 1 SSL Certificate Information

Port	First Detected	Category
443	20-SEP-2011 07:20	Web Server

Protocol	Impact
HTTPS	Information Disclosure

### Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

### CVSS

0.0

### Solution

Please disable if you have any low strength ciphers

### Detail

Subject Name:

Country: US  
State/Province: Mississippi  
Locality: Ridgeland  
Organization: Bomgar Corporation  
Organization Unit: Remote Support  
Common Name: \*.bomgar.com

Issuer Name:

Country: US  
Organization: DigiCert Inc  
Organization Unit: www.digicert.com  
Common Name: DigiCert High Assurance CA-3

Serial Number: 02 EC F3 7A 75 55 42 AE 8C 85 83 00 D7 02 42 8A

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Jan 29 00:00:00 2010 GMT

Not Valid After: Feb 19 23:59:59 2013 GMT

Public Key Info:

Algorithm: RSA Encryption

Public Key: 00 DE 52 96 DF 4C 75 B3 46 C7 32 5E FB 4A 91 88 FE EA 6D 32  
FE D6 E2 D8 69 66 58 CA 62 DE C7 DD 6F B5 DB 49 31 CA 54 AE  
24 56 CF F8 CD 5B D4 21 28 76 0E FA DD 19 AF 50 EF 80 E3 F3  
D7 02 8E 25 85 40 42 87 5C 3C 2F 77 27 AF 0D 20 C9 3B 80 4F  
FE 84 C3 52 A5 49 C9 9E 9F B8 3F EE 22 FA 40 52 94 1F 7B 5D  
7B F4 82 61 CB 28 FF 18 75 55 6C FB 23 A9 6F 0D 8E F9 7D 4D  
CC 51 6A F9 DE 37 88 B2 EB D6 80 34 C8 E0 76 B3 1F 01 E6 17  
F2 9B 18 51 36 A2 8B 59 77 17 23 A1 FC 1B F3 00 08 AD 87 EC  
82 DE C6 C7 A1 FC 58 93 9E DA 4F F9 BB 04 0E 7A 13 13 07 8E  
3A 29 FA 72 43 5E A9 AD 65 E3 AA A3 68 60 40 45 D0 71 01 61  
4D F3 87 CE B8 3B 05 74 D7 AB 02 19 9C D8 FA 8B 2D 86 97 3A  
AF CD DC F7 54 0C D1 6A DB 8E EB 4E 50 0D 93 CC A9 07 90 7D  
D9 AE 73 65 81 9B 38 2D DB CA F7 E2 B5 C7 82 A9 21  
Exponent: 01 00 01

Signature: 00 20 2D F9 42 E3 D6 7F F6 C8 05 99 37 A8 45 1F B3 61 45 AC  
07 F0 0C 33 52 73 53 06 3D 24 4F 9F F6 04 EB C5 90 FE E5 65  
7A 97 24 2E C8 E2 E3 87 EA 8C 3F E9 AB BF 8C 95 A6 7F 27 81  
E0 00 5E B1 B2 56 95 7C 6F 65 F3 6B AE B8 0A FC CD B1 CB AF  
A7 68 0B 23 48 F1 2B 9D 4B 48 76 83 15 13 67 01 D5 08 DE 60  
40 E2 92 AB 90 AC AB 5B B0 23 E5 80 E2 89 AD F6 02 BD 9F 8E

0A 15 0D FE CB 19 CF D2 D9 45 6E 36 57 AD A0 D9 67 9B 5F 31  
F0 20 F4 68 CA E9 D5 04 42 66 BE C7 7A 03 AF 95 74 10 4D DE  
D3 9B C6 B0 7D 79 F1 7C 53 06 69 8D 88 79 4C 36 5C 14 E5 E2  
F0 D2 FB F9 E3 10 4F 78 74 AA 7A 6A A7 62 98 87 4D 9E 36 6C  
F4 DF 3C BE A6 8B CA 01 5F AD 60 DF 71 17 B8 5A 4C F6 30 57  
8D A8 3D 4C 92 6D 63 27 3A 4A 24 79 5D 36 93 C0 9C 7A C8 C8  
B9 99 6D 59 AC 0E 33 8D 56 F3 AD 2E FE 5D 33 FF E3

Extension: Authority Key Identifier (2.5.29.35)  
Critical: 0

Extension: Subject Key Identifier (2.5.29.14)  
Critical: 0  
Subject Key Identifier: 5F 78 14 58 48 39 3A FB 32 2E 92 E1 84 DB 22 FD BA A9 25 D8

Extension: Subject Alternative Name (2.5.29.17)  
Critical: 0  
DNS: \*.bomgar.com  
DNS: bomgar.com

Extension: Authority Information Access (1.3.6.1.5.5.7.1.1)  
Critical: 0  
Method#1: Online Certificate Status Protocol  
URI: http://ocsp.digicert.com  
Method#2: Certificate Authority Issuers  
URI: http://www.digicert.com/CACerts/DigiCertHighAssuranceCA-3.crt

Extension: Key Usage (2.5.29.15)  
Critical: 1  
Key Usage: Digital Signature, Key Encipherment

Extension: Basic Constraints (2.5.29.19)  
Critical: 1  
Data: 30 00

Extension: CRL Distribution Points (2.5.29.31)  
Critical: 0  
URI: http://crl3.digicert.com/ca3-2010a.crl  
URI: http://crl4.digicert.com/ca3-2010a.crl

Extension: Policies (2.5.29.32)  
Critical: 0  
Policy ID #1: 2.16.840.1.114412.1.3.0.1  
Qualifier ID #1: Certification Practice Statement (1.3.6.1.5.5.7.2.1)  
CPS URI: http://www.digicert.com/ssl-cps-repository.htm  
Qualifier ID #1: ()

Extension: Extended Key Usage (2.5.29.37)  
Critical: 0  
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)  
Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2)

#### Links

[Transport Layer Security](#)  
[SSL 2.0](#)  
[IBM HTTP Server](#)  
[Disabling SSLv2 in IIS \(English\)](#)  
[Mozillazine](#)

#### Related

None

### 1 OS Identification

Port	First Detected	Category
0	20-SEP-2011 07:20	Other

Protocol	Impact
----------	--------

**Description**

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc...) it is possible to guess the name of the remote operating system in use, and sometimes its version

**CVSS**

2.6

**Solution**

Please ensure that your OS is patched and updated

**Detail**

Synopsis :

It is possible to guess the remote operating system

Description :

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc...) it is possible to guess the name of the remote operating system in use, and sometimes its version

Solution :

N/A

Risk factor :

None

Plugin output :

Remote operating system : Linux Kernel 2.6  
 Confidence Level : 65  
 Method : SinFP

The remote host is running Linux Kernel 2.6

**Links**

[ICMP Usage In Scanning](#)  
[IIS URLScan](#)  
[IIS 6](#)

**Related**

None

**1 Hidden Fields Found - Potential Information Leakage**

Port	First Detected	Category
443	20-SEP-2011 07:55	Web Application

Protocol	Impact
HTTP	Information Disclosure

**Description**

This check identifies unique hidden fields used within forms on the page. Potentially sensitive information may be contained within hidden fields which could be misused by an attacker.

**CVSS**

2.6

**Solution**

Prevent using session handling and/or storing sensitive personal information in hidden fields such as authentication credentials, email addresses, credit card numbers and social security numbers.

**Detail**

/login/login.ns: --> <input type="hidden" name="redirect" value="/login/" />, <input type="hidden" name="form\_id" value="i1e1dAoHmrDst3aHVnFpC21owLI=" />,

#### Links

None

#### Related

None

### 1 AutoComplete attribute is true

Port	First Detected	Category
443	20-SEP-2011 07:55	Information Gathering

Protocol	Impact
Other	Information Disclosure

#### Description

The remote web server contains form fields that allow for auto completion. Depending on the values entered into these fields, future users could obtain sensitive information previously entered by past users.

Fields that contain sensitive information, such as credit card and social security numbers and passwords, must be disallowed from caching information.

#### CVSS

2.6

#### Solution

To disable all entries in a form from being cached, the autocomplete value of the form tag must be set to "off", such as:

```
<form method="POST" action="handlepayment.asp" autocomplete="off">
```

The autocomplete attribute can also be used on an individual form element such as:

```
<input type="password" autocomplete="off" name="password">
```

#### Detail

**Protocol** https **Port** 443 **Read Timeout** 10000 **Method** GET  
**Path** /login/login.ns  
**Query** redirect=%2Flogin%2F  
**Headers** Host=security2.bomgar.com  
Referer=https%3A%2F%2Fsecurity2.bomgar.com%2Flogin%2F

**Protocol** https **Port** 443 **Read Timeout** 10000 **Method** POST  
**Path** /login/login.ns  
**Query** redirect=%2Flogin%2F  
Referer=https%3A%2F%2Fsecurity2.bomgar.com%2Flogin%2Flogin.ns%3Fredirect%3D%252Flogin%252F  
**Headers** Content-Type=application%2Fxml-www-form-urlencoded  
redirect=/login/  
form\_id=i1e1dAoHmrDst3aHVnFpC21owLI=  
**Body** login[username]=  
login[password]=  
login[submit]=Login  
submit\_button=Login

Form on page: /login/login.ns?redirect=%2Flogin%2F

#### Links

None

#### Related

None

### 1 Text (ASCII) File(s) found

Port	First Detected	Category
443	20-SEP-2011 07:55	Information Gathering

Protocol	Impact
HTTP	Information Disclosure
Description	
The scanner has detected text files on the server. These files could potentially contain data of a sensitive nature. Sensitive information, such as usernames and passwords, can disclose important information to hackers that can lead to system compromise.	
CVSS	
0.0	
Solution	
Review the files manually to verify they contain no sensitive information.	
Detail	

**Protocol** https **Port** 443 **Read Timeout** 10000 **Method** GET  
**Path** /content/templates/31bf091e1372c338e485155de9473d4a2458a0b1/help\_icon.txt  
**Headers** Host=security2.bomgar.com  
Referer=https%3A%2F%2Fsecurity2.bomgar.com%2F

help\_icon.txt  
**Protocol** https **Port** 443 **Read Timeout** 10000 **Method** GET  
**Path** /files/file.txt  
**Query** view=0  
**Headers** Host=security2.bomgar.com  
Referer=https%3A%2F%2Fsecurity2.bomgar.com%2Ffiles%2F

file.txt

#### Links

None

#### Related

None

### 1 Web Server Directory Enumeration

Port	First Detected	Category
443	20-SEP-2011 07:55	Web Application
Protocol	Impact	
HTTP	Information Disclosure	
Description		
This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.		
CVSS		
2.6		
Solution		
n/a		
Detail		
<b>Protocol</b> https	<b>Port</b> 443	<b>Read Timeout</b> 10000 <b>Method</b> GET
<b>Path</b> /files/	<b>Headers</b> Host=security2.bomgar.com	
/files/		
Links		
<a href="http://projects.webappsec.org">projects.webappsec.org</a>		

## Related

OWASP [OWASP-CM-006](#)

### 1 Discoverable Email Addresses

Port	First Detected	Category
80	20-SEP-2011 07:55	Web Application

Protocol	Impact
HTTP	Information Disclosure

#### Description

Scanner found email address(es) on your website.

#### CVSS

0.0

#### Solution

Please review

#### Detail

/content/templates/31bf091e1372c338e485155de9473d4a2458a0b1/help\_icon.txt: --> 555-555-0199@example.com,

#### Links

None

#### Related

None

### 1 Text (ASCII) File(s) found

Port	First Detected	Category
80	20-SEP-2011 07:55	Information Gathering

Protocol	Impact
HTTP	Information Disclosure

#### Description

The scanner has detected text files on the server. These files could potentially contain data of a sensitive nature. Sensitive information, such as usernames and passwords, can disclose important information to hackers that can lead to system compromise.

#### CVSS

0.0

#### Solution

Review the files manually to verify they contain no sensitive information.

#### Detail

**Protocol** http **Port** 80 **Read Timeout** 10000 **Method** GET  
**Path** /content/templates/31bf091e1372c338e485155de9473d4a2458a0b1/help\_icon.txt  
**Headers** Host=security2.bomgar.com  
Referer=http%3A%2F%2Fsecurity2.bomgar.com%2F

help\_icon.txt

**Protocol** http **Port** 80 **Read Timeout** 10000 **Method** GET  
**Path** /files/file.txt  
**Query** view=0  
**Headers** Host=security2.bomgar.com  
Referer=http%3A%2F%2Fsecurity2.bomgar.com%2Ffiles%2F

file.txt

**Links**

None

**Related**

None

**1 Web Server Directory Enumeration**

Port	First Detected	Category
80	20-SEP-2011 07:55	Web Application

Protocol	Impact
HTTP	Information Disclosure

**Description**

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

**CVSS**

2.6

**Solution**

n/a

**Detail**

**Protocol** http **Port** 80 **Read Timeout** 10000 **Method** GET

**Path** /files/

**Headers** Host=security2.bomgar.com

/files/

**Links**

[projects.webappsec.org](http://projects.webappsec.org)

**Related**

OWASP [OWASP-CM-006](#)

**1 Parent or Sub-Domains Identified**

Port	First Detected	Category
0	20-SEP-2011 07:55	Other

Protocol	Impact
HTTP	Other

**Description**

The web application scanner has found one or more links to parent or sub-domains of the domain being scanned. These parent or sub-domains should also be scanned for security vulnerabilities.

**CVSS**

0.0

**Solution**

Verify that these domains have been added to your account.

**Detail**

www.bomgar.com

**Links**

None

**Related**

---

None

---

None

---

**Resolved Items - security2.bomgar.com**

None

---

## Vulnerability Levels

Severity	Level	Description
5	Urgent	<p>Intruders can easily gain control of the device being tested, which can lead to the compromise of your entire network security. Or hackers can use this device to access sensitive information from other devices in your network. Hackers are often actively scanning for this type of vulnerability.</p> <p>For example, vulnerabilities at this level may include full read and write access to files or databases, remote execution of commands, gaining Administrator or Root level access, and the presence of Trojans or backdoors.</p>
4	Critical	<p>Intruders can possibly gain direct control of the device being tested, or there may be potential leakage of highly sensitive information.</p> <p>For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users hosted on the device.</p>
3	High	<p>Intruders may be able to gain access to specific information stored on the device being tested, including security settings. This could result in potential misuse of, or unauthorized access to the device or information stored on it.</p> <p>For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services such as mail-relaying.</p>
2	Medium	<p>Intruders may be able to collect sensitive information from the host, such as the precise version of OS or software installed or directory structure. While this level of vulnerability is not directly exploitable itself, with this information intruders can more easily exploit possible vulnerabilities specific to software versions in use.</p>
1	Low	<p>Intruders can collect general information about the device being tested (open ports, OS or software type, etc.). Hackers may be able to use this information to find exploitable vulnerabilities.</p>

# Web Application Report

**This report includes important security information about your Web Application.**

## **The Payment Card Industry Data Security Standard (PCI) Version 2.0 Compliance Report**

This report was created by IBM Rational AppScan 8.0.0.3  
10/4/2011 10:52:07 AM

# The Payment Card Industry Data Security Standard (PCI) Version 2.0

## Web Application Report

Scanned Web Application: <https://security2.bomgar.com>

Scan Name: security2-bomgar

## Content

This report contains the following sections:

- Description
- Compliance Scan Results
- Unique Compliance-related Issues Detected
- Compliance-Related Issues and Section References

## IMPORTANT INFORMATION ABOUT THIS REPORT

This Compliance Scan Results Report is based on the results of an automated Web Application Security scan, performed by AppScan.

An AppScan scan attempts to uncover security-related issues in web applications, testing both the http frameworks (e.g. web servers) and the code of the application itself (e.g. dynamic pages). The testing is performed over HTTP, and is limited only to those issues that are specified for testing and identified in an automated fashion via the HTTP channel. The scan is also limited to those specific issues included in an automatic and/or manual explore performed during the scan. The security-related issues detected are compared to selected regulatory or industry standard requirements to produce this report. There may be areas of compliance risk associated with such regulation or standard that are not specified for testing by AppScan. This report will not detect any compliance-related issues in areas of compliance risk that are not tested by AppScan. The report identifies areas where there may be a compliance risk, but the exact impact of each uncovered issue type depends on the individual application, environment, and the subject regulation or standard. Regulations and standards are subject to change, and the scans performed by AppScan may not reflect all such changes. It is the user's responsibility to interpret the results in this report for determination of impact, actual compliance violations, and appropriate remedial measures, if any.

Section references to regulations are provided for reference purposes only. The issues reported are general compliance-related risks and are not to be interpreted as excerpts from any regulation.

**The information provided does not constitute legal advice. IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.**

# Description

## Summary

The PCI data security standard offers a single approach to safeguarding sensitive data for all card brands. The PCI DSS version 2.0, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is intended to protect cardholder data-wherever it resides and to ensure that members, merchants, and service providers maintain a high information security standard.

The PCI Data Security Standard consists of twelve basic requirements supported by more detailed sub-requirements. These requirements apply to all system components, which is defined as any network component, server, or application that is included in or connected to the cardholder data environment. "System components" also include any virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.

The cardholder data environment is comprised of people, processes and technology that store, process or transmit cardholder data or sensitive authentication data.

Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.

Server types include, but are not limited to the following: web, application, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS).

Applications include all purchased and custom applications, including internal and external (for example, Internet) applications.

## Covered Entities

PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data.

## Compliance Penalties

If a merchant or service provider does not comply with the security requirements or fails to rectify a security issue, the card companies may fine the acquiring member, or impose restrictions on the merchant or its agent.

## Compliance Required By

PCI DSS version 2.0 has replaced PCI DSS v.1.2 and is effective as of January 1st 2011. The PCI DSS v.1.2 may be used for PCI DSS compliance until December 31, 2011.

## Regulators

The PCI Security Standards Council, and its founding members including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International.

For more information on the PCI Data Security Standard, please visit:

<https://www.pcisecuritystandards.org./index.htm>

For more information on securing web applications, please visit <http://www-01.ibm.com/software/rational/offerings/websecurity/>

Copyright: The PCI information contained in this report is proprietary to PCI Security Standards Council, LLC. Any use of this material is subject to the PCI SECURITY STANDARDS COUNCIL, LLC LICENSE AGREEMENT that can be found at:

[https://www.pcisecuritystandards.org/tech/download\\_the\\_pci\\_dss.htm](https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm)

(\*) **DISCLAIMER** The information provided does not constitute legal advice. The results of a vulnerability assessment will demonstrate potential vulnerabilities in your application that should be corrected in order to reduce the likelihood that your information will be compromised. As legal advice must be tailored to the specific application of each law, and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent counsel. IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.

# Compliance Scan Results

1 unique issues detected across 33 sections of the regulation:

Section	No. of Issues
1. Do not use vendor-supplied defaults for system passwords and other security parameters. (Requirement 2)	1
2. Always change the vendor-supplied defaults before you install a system on the network. (Requirement 2.1)	1
3. Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. (Requirement 2.2.2)	1
4. Configure system security parameters to prevent misuse. (Requirement 2.2.3)	1
5. Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems. (Requirement 2.2.4)	1
6. Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web based management and other non console administrative access. (Requirement 2.3)	-
7. This section applies to web applications that are used by hosting providers for hosting purposes – Hosting providers must protect each entity’s hosted environment and data. (Requirement 2.4)	-
8. Encrypt transmission of cardholder data across open, public networks. (Requirement 4)	-
9. Use strong cryptography and security protocols such as Secure Sockets Layer (SSL)/ transport layer security (TLS) and internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open public networks. (Requirement 4.1)	-
10. Develop and maintain secure systems and applications. (Requirement 6)	1
11. Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. (Requirement 6.1)	1

Section	No. of Issues
12. Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. (Requirement 6.2)	-
13. Develop software applications (internal and external, and including webbased administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging), and based on industry best practices. Incorporate information security throughout the software development life cycle. These processes must include the following: (Requirement 6.3)	1
14. Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers. (Requirement 6.3.1)	-
15. Removal of test data and accounts before production systems become active. (Requirement 6.4.4)	-
16. Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following: (Requirement 6.5)	1
17. Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws. (Requirement 6.5.1)	-
18. Buffer overflow (Requirement 6.5.2)	-
19. Insecure cryptographic storage (Requirement 6.5.3)	-
20. Insecure communications (Requirement 6.5.4)	-
21. Improper error handling (Requirement 6.5.5)	-
22. Cross site scripting (XSS) (Requirement 6.5.7)	-
23. Improper access control (Requirement 6.5.8)	-
24. Cross site request forgery (CSRF) (Requirement 6.5.9)	-

Section	No. of Issues
25. For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: 1. Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes. 2. Installing a web-application firewall in front of public-facing web applications (Requirement 6.6)	-
26. Restrict access to data by business need-to-know (Requirement 7)	-
27. Limit access to system components and cardholder data to only those individuals whose job requires such access. (Requirement 7.1)	-
28. Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities (Requirement 7.1.1)	-
29. Render all passwords unreadable during transmission and storage, on all system components using strong cryptography. (Requirement 8.4)	-
30. Ensure proper user identification and authentication management for non consumer users and administrators on all system components. (Requirement 8.5)	-
31. Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects. (Requirement 8.5.1)	-
32. Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators. (Requirement 8.5.16)	-
33. Regularly test security systems and processes. (Requirement 11)	-

# Unique Compliance-related Issues Detected

1 unique issues detected across 33 sections of the regulation:

ID	URL	Parameter/Cookie	Test Name	Sections
1	https://security2.bomgar.com/		SSL Certificate About to Expire	1, 2, 3, 4, 5, 10, 11, 13, 16

# Compliance-Related Issues and Section References

- 1) Do not use vendor-supplied defaults for system passwords and other security parameters.

(Requirement 2)

## 1 Issues

### SSL Certificate About to Expire

#### Security Risks

- It is possible to prevent the web application from serving other users (denial of service)
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

#### Causes:

- The web server or application server are configured in an insecure way

#### Remediation Tasks:

Update your SSL certificate, and make sure that all attributes are valid

#### Issues:

Issue ID	URL	Parameter/Cookie
1	https://security2.bomgar.com/	

- 2) Always change the vendor-supplied defaults before you install a system on the network.

(Requirement 2.1)

## 1 Issues

### SSL Certificate About to Expire

#### Security Risks

- It is possible to prevent the web application from serving other users (denial of service)
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

#### Causes:

- The web server or application server are configured in an insecure way

#### Remediation Tasks:

Update your SSL certificate, and make sure that all attributes are valid

#### Issues:

Issue ID	URL	Parameter/Cookie
----------	-----	------------------

**3) Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system.**

(Requirement 2.2.2)

**1 Issues**

**SSL Certificate About to Expire**

**Security Risks**

- It is possible to prevent the web application from serving other users (denial of service)
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

**Causes:**

- The web server or application server are configured in an insecure way

**Remediation Tasks:**

Update your SSL certificate, and make sure that all attributes are valid

**Issues:**

Issue ID	URL	Parameter/Cookie
1	https://security2.bomgar.com/	

---

**4) Configure system security parameters to prevent misuse.**

(Requirement 2.2.3)

**1 Issues**

**SSL Certificate About to Expire**

**Security Risks**

- It is possible to prevent the web application from serving other users (denial of service)
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

**Causes:**

- The web server or application server are configured in an insecure way

**Remediation Tasks:**

Update your SSL certificate, and make sure that all attributes are valid

**Issues:**

Issue ID	URL	Parameter/Cookie
1	https://security2.bomgar.com/	

- 5) **Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems.**

(Requirement 2.2.4)

**1 Issues**

**SSL Certificate About to Expire**

**Security Risks**

- It is possible to prevent the web application from serving other users (denial of service)
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

**Causes:**

- The web server or application server are configured in an insecure way

**Remediation Tasks:**

Update your SSL certificate, and make sure that all attributes are valid

**Issues:**

Issue ID	URL	Parameter/Cookie
1	https://security2.bomgar.com/	

- 6) **Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web based management and other non console administrative access.**

(Requirement 2.3)

**No issues.**

- 7) **This section applies to web applications that are used by hosting providers for hosting purposes – Hosting providers must protect each entity’s hosted environment and data.**

(Requirement 2.4)

**No issues.**

8) **Encrypt transmission of cardholder data across open, public networks.**

(Requirement 4)

No issues.

9) **Use strong cryptography and security protocols such as Secure Sockets Layer (SSL)/ transport layer security (TLS) and internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open public networks.**

(Requirement 4.1)

No issues.

10) **Develop and maintain secure systems and applications.**

(Requirement 6)

**1 Issues**

#### **SSL Certificate About to Expire**

##### **Security Risks**

- It is possible to prevent the web application from serving other users (denial of service)
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

##### **Causes:**

- The web server or application server are configured in an insecure way

##### **Remediation Tasks:**

Update your SSL certificate, and make sure that all attributes are valid

##### **Issues:**

Issue ID	URL	Parameter/Cookie
1	https://security2.bomgar.com/	

11) **Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.**

(Requirement 6.1)

**1 Issues**

## SSL Certificate About to Expire

### Security Risks

- It is possible to prevent the web application from serving other users (denial of service)
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

### Causes:

- The web server or application server are configured in an insecure way

### Remediation Tasks:

Update your SSL certificate, and make sure that all attributes are valid

### Issues:

Issue ID	URL	Parameter/Cookie
1	https://security2.bomgar.com/	

- 12) **Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.**

(Requirement 6.2)

**No issues.**

- 13) **Develop software applications (internal and external, and including webbased administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging), and based on industry best practices. Incorporate information security throughout the software development life cycle. These processes must include the following:**

(Requirement 6.3)

**1 Issues**

## SSL Certificate About to Expire

### Security Risks

- It is possible to prevent the web application from serving other users (denial of service)
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

### Causes:

- The web server or application server are configured in an insecure way

### Remediation Tasks:

Update your SSL certificate, and make sure that all attributes are valid

### Issues:

Issue ID	URL	Parameter/Cookie
1	https://security2.bomgar.com/	

- 14) **Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers.**

(Requirement 6.3.1)

**No issues.**

- 15) **Removal of test data and accounts before production systems become active.**

(Requirement 6.4.4)

**No issues.**

- 16) **Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following:**

(Requirement 6.5)

**1 Issues**

## SSL Certificate About to Expire

### Security Risks

- It is possible to prevent the web application from serving other users (denial of service)
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

### Causes:

- The web server or application server are configured in an insecure way

### Remediation Tasks:

Update your SSL certificate, and make sure that all attributes are valid

### Issues:

Issue ID	URL	Parameter/Cookie
1	https://security2.bomgar.com/	

- 17) **Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.**

(Requirement 6.5.1)

**No issues.**

- 18) **Buffer overflow**

(Requirement 6.5.2)

**No issues.**

- 19) **Insecure cryptographic storage**

(Requirement 6.5.3)

**No issues.**

- 20) **Insecure communications**

(Requirement 6.5.4)

**No issues.**

**21) Improper error handling**

(Requirement 6.5.5)

**No issues.**

**22) Cross site scripting (XSS)**

(Requirement 6.5.7)

**No issues.**

**23) Improper access control**

(Requirement 6.5.8)

**No issues.**

**24) Cross site request forgery (CSRF)**

(Requirement 6.5.9)

**No issues.**

**25) For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: 1. Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes. 2. Installing a web-application firewall in front of public-facing web applications**

(Requirement 6.6)

**No issues.**

**26) Restrict access to data by business need-to-know**

(Requirement 7)

**No issues.**

**27) Limit access to system components and cardholder data to only those individuals whose job requires such access.**

(Requirement 7.1)

**No issues.**

**28) Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities**

(Requirement 7.1.1)

**No issues.**

**29) Render all passwords unreadable during transmission and storage, on all system components using strong cryptography.**

(Requirement 8.4)

**No issues.**

**30) Ensure proper user identification and authentication management for non consumer users and administrators on all system components.**

(Requirement 8.5)

**No issues.**

**31) Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects.**

(Requirement 8.5.1)

**No issues.**

**32) Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators.**

(Requirement 8.5.16)

**No issues.**

**33) Regularly test security systems and processes.**

(Requirement 11)

**No issues.**