

Realtime  
publishers

"Leading the Conversation"

# The Essentials Series

# PCI Compliance

*sponsored by*



ALERTLOGIC

*by Rebecca Herold*

---

Article 1: Using PCI DSS–Compliant Log Management to Identify Insider Access Abuse.....	1
How the Insider Threat Impacts Business .....	1
PCI DSS Log Compliance Mitigates the Insider Threat.....	2
Using Logs to Protect Against the Insider Threat.....	3
A Practitioner’s Perspective.....	4
Be Prepared for Your QSA and Protect Against Insider Threats .....	5
Summary .....	6
Article 2: Using PCI DSS–Compliant Log Management to Identify Attacks from Outside the Enterprise .....	7
Outside Attacks Impact Business.....	7
PCI DSS Log Compliance Mitigates the Outsider Threat .....	8
Using Combinations of Logs to Protect Against Outside Attacks.....	8
A Practitioner’s Perspective.....	10
Be Prepared for Your QSA and Protect Against Outside Threats .....	11
Summary .....	12
Article 3: Addressing Application Vulnerabilities with PCI Log Management Compliance .....	13
Application Flaws Impact Business.....	13
PCI DSS Log Compliance Can Help Improve Application Security .....	14
1. Remote Code Execution Vulnerabilities.....	14
2. SQL Injection Vulnerabilities .....	14
3. Format String Vulnerabilities .....	15
4. Cross Site Scripting.....	15
5. Username Enumeration.....	15
An IT Security Expert Practitioner’s Perspective.....	16
Prepare for PCI DSS Compliance and Increase the Security of Applications.....	17

---

## Copyright Statement

© 2008 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at [info@realtimepublishers.com](mailto:info@realtimepublishers.com).

---

## Article 1: Using PCI DSS–Compliant Log Management to Identify Insider Access Abuse

Meeting the requirements for PCI DSS logging benefits businesses by putting into place logs that help to identify when authorized users may be doing things they should not be doing. There are literally thousands of types of logs that can be generated on corporate networks and appliances. Unfortunately, too few information security and IT practitioners understand that there are very important differences in how to use logs to identify insider threats from other types of threats. Too few know how to review the logs to identify when authorized users may be doing inappropriate activities with their access. The indicators found within logs for insider abuse are largely much different than indicators for other types of threats.

### How the Insider Threat Impacts Business


Think about how many people have authorized access to information resources within your organization. These “insiders” often include:

- Employees
- Contract workers
- Temporary workers
- Business partners
- Consultants
- External auditors
- Customers
- Former employees whose access has not been removed

Think about the sensitive information these insiders have been authorized to access. Think about all the bad things a malicious insider could do with this access. If there are gaps in security controls, malicious insiders can take advantage of those vulnerabilities to use the access privileges of authorized insiders.

---

The huge Société Générale fraud scandal is a good example of how insiders can exploit control gaps and have a devastating impact on the business. In early 2008, Jerome Kerviel, a Société Générale employee, was accused of stealing computer passwords, sending fake email messages, and illegally accessing the bank's computer system to exceed trading limits and cover up his actions. Kerviel allegedly bought futures contracts but did not follow requirements to offset them with countervailing buys. He reportedly did this by gaining unauthorized computer access, possibly through his co-workers' accounts or by exploiting control vulnerabilities, and forged documents that made it look like he had offset purchases, circumventing risk controls. His actions cost the company \$7.5 billion. It has been widely discussed that better controls, including effective log management and review procedures, could have prevented this unprecedented internal fraud of this magnitude.

 There is a 72% chance that the next successful network attack will come from an insider. - ICSA Labs

## PCI DSS Log Compliance Mitigates the Insider Threat

PCI DSS log management requirements mitigate the insider threat in multiple ways. The logs can be used to:

- Validate that proper controls are in place
- Validate policy compliance
- Determine when individuals are accessing data in ways that are beyond their authorized use of the data for business responsibilities
- Determine whether access is inappropriate based upon criteria such as:
  - Access to audit trails and associated modifications
  - Invalid logical access attempts
  - Use of identification and authentication mechanisms
  - Time stamps and clock synchronization changes
  - File integrity monitoring and change detection software for logs to ensure existing log data cannot be changed without generating alerts

---

## Using Logs to Protect Against the Insider Threat

Ben Rothke, CISSP, QSA, and Senior Security Consultant at BT INS, points out that, in his experience, database logs are the best indicators of the insider threat because they clearly show when authorized users have been snooping around in files that they have no reason to be accessing at particular times or in order to perform their business responsibilities.

Annarita Giani, Postdoctoral Fellow in the Electrical Engineering and Computer Sciences Department, University of California at Berkeley, has done extensive systems log research and offers some good advice and insights into insider attacks.

*It is estimated that the majority of all computer security breaches are due to insider attacks. While some insider attackers use simple methodology, others rely on more sophisticated approaches, such as inserting a toolkit, an agent or scanning the network. Since the inside attackers have some authorization, they are able to compromise somebody else's account to launch the attack and be virtually invisible.*

*As organizations move to more automated environments, it becomes possible to detect signs of insider misuse much earlier than has previously been possible. In fact, information systems can be instrumented to record all uses of the system, down to the monitoring of individual keystrokes and mouse movements. A technologically adept malicious insider, however, may be aware of these countermeasures and take actions to neutralize them.*

*Many attacks can be detected using a combination of logs; log analysis of multiple log entries usually must be done to detect insider abuse. The first step is to build models of an insider attack. Once the models are built, compare them with the system logs. This can be done manually, but it becomes very difficult if the number of models is high. And in any case the amount of logs quickly becomes unmanageable.*

*Using only one source of data does not allow the detection of insider attacks. Finding nontrivial malicious activity depends greatly upon the ability to log and associate diverse information, malicious or suspicious traffic, and unexpected file modification.*

---

## A Practitioner's Perspective

A.B., an IT security expert practitioner with more than 25 years of experience within large multi-national companies (A.B.'s corporate rules do not allow him to have his name or his company's name published. However, his great expertise and vast experience offers some valuable lessons to readers.), offers some good points about how he has successfully used logs to identify the insider threat.

*Look for signs in the logs of unusual behavior. Those are the things that suggest something is amiss. For instance, something subtle would be a log entry showing an employee attempting to access customer data at 3:00am. But, she NEVER works those hours - that's suspicious. Maybe that is a bad guy using her username and password, or maybe the employee is trying to commit fraud.*

*Sometimes what you do \*NOT\* find in a log can be suspicious. For example, a server not logging when it should be could be a sign of an authorized user erasing log entries or disabling the system logs.*

*It is important for the IT personnel to become familiar with logs. How do you become familiar with logs? Simple; read them, even when you have a few spare minutes or are on a horribly boring conference call. It won't take long to start recognizing normal behavior as opposed to possible suspicious behavior. The secret is not to look for specific log entries, but to look for entries that stick out like a sore thumb.*

Annarita provides more advice based upon her research with real life incidents.

*It is common for malicious insiders to use an encrypted connection, such as a Virtual Private Network, to commit their crimes. Remote access is mostly used by attackers that have system privileges but do not have direct access to their computer at work, or by attackers who are no longer employed; they may have been fired, so they cannot enter in the building, but their access to the information system still exists. Remote access logs together with file access logs are very useful proofs of insider attacks that occur outside the facilities. Another method technical insiders often use is to spoof the source IP address to try and cover their identity.*

A large number of organizations fail to quickly remove remote access capabilities from individuals with whom they have terminated their business relationship. Many never remove the access at all! I know of dozens of cases in which vindictive ex-employees continued to use their remote access capabilities to do harm to their former employers.



Competent PCI DSS QSAs will closely review your personnel exit and termination policies and procedures, along with your user account logs, to ensure you consistently remove systems and information access as soon as possible following—and in some especially risky situations, before—the employee departure.

---

## ***Be Prepared for Your QSA and Protect Against Insider Threats***

Ben Rothke indicates the log management portion of the PCI DSS audits he performs is significant compared with the other PCI DSS requirement reviews. According to Ben, “Companies are finding that they can’t simply install an appliance and suddenly be PCI compliant. Logs require an organization to really understand their infrastructure. Far too many organizations have no idea about what and how much logs they are generating. PCI log requirements are a rude awaking for them.”

It is important for organizations preparing for a PCI DSS audit to know that QSAs typically examine the actual log records themselves to determine whether there is anything suspicious or unusual. Ben indicates that he not only takes and examines samples of data from the logs identified as being critical to financial transactions but also reviews the log management policies and procedures to ensure that the logs he reviews are in compliance with the policies and procedures.

The common log management problems Ben finds when performing PCI DSS reviews include:

- Completely misconfigured logs
- Default log settings left unchanged from installation
- Wrong items being logged
- No one reads the logs
- No one follows up on log issues
- Logs not correlated to any threats or vulnerabilities

 According to the CERT/Secret Service Insider Threat study, in 74% of incidents and frauds committed by insiders, the insiders’ identities were obtained using system logs (Source: "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," Carnegie Mellon CERT and U.S. Secret Service, 2004, <http://www.cert.org/archive/pdf/bankfin040820.pdf>).

The bottom line is that organizations must establish a well-documented log management program to not only meet PCI DSS log requirements but also help identify, and often prevent, damage that could occur from prolonged access from the insider threat.

---

The following list highlights just a few of the logs that are helpful for organizations to use to identify the insider threat and to be in compliance with PCI DSS:

- Remote access logs
- RADIUS authentication logs
- File access logs
- Database logs
- Application logs
- Email logs and application logs for authenticated email (POP, IMAP, etc.)
- IP address logs
- Authentication logs
- Windows system and Active Directory (AD) login/logout activity logs
- UNIX SSH login logs
- FTP server logs
- Logs indicating passively sniffed chat and IM login processes

Do not consider this a comprehensive list but rather a starting point to help you identify the logs to use within your organization. This type of documentation will also be important for ensuring PCI DSS compliance.

## Summary

History has taught us that most malicious insiders will attempt to take steps to conceal their actions. The insiders who know that the logs can be used to identify them will typically attempt to hide their fraudulent actions by modifying the logs, and it is not unusual for them to try to change the logs in such a way to implicate someone else for their devious actions. Sound log management practices not only help to fight this insider threat but also support PCI DSS compliance.

---

## Article 2: Using PCI DSS–Compliant Log Management to Identify Attacks from Outside the Enterprise

Meeting the PCI DSS requirements for logging benefits businesses by putting into place logs that help to reveal when unauthorized users from outside the network perimeter, and any enterprise system, have breached security. There are many indicators within logs that are typically overlooked but could be used to more effectively keep hackers from successfully attacking network resources and compromising sensitive data. By establishing log management practices to identify, mitigate, and prevent network attacks, information security and IT practitioners will also be providing actions to support PCI DSS compliance.

### Outside Attacks Impact Business

Network and database compromise by hackers and other malicious folks outside the organization can have a devastatingly negative impact on the business. Consider the following incidents that have recently occurred:

- Reported March 23, 2008—Hackers got into the Western Carolina University system and accessed personally identifiable information (PII) of alumni, including Social Security Numbers (SSNs), names, and addresses. The compromise was discovered while the school’s network administrators were searching for all the PII storage locations so that they could remove the PII from the unsecured servers. The compromised server, “normally used for sharing class notes and assignments,” had a history of being hacked “several times” in recent years. (Retrieved March 26, 2008 from <http://www.citizen-times.com/apps/pbcs.dll/article?AID=/20080323/NEWS01/80322062>.)
- Reported March 17, 2008—Hannaford Brothers supermarket chain reported that credit and debit card numbers were stolen during card authorization processing, possibly as the result of an application’s vulnerability, putting around 4.2 million of their customers at risk of fraud. Approximately 1800 cases of fraud related to this hacking incident had already occurred by March 17. (Retrieved March 26, 2008 from <http://www.wmur.com/news/15621249/detail.html>.)

Other organizations can help to prevent these and other types of outsider compromises, or catch them before damage is done, with effective log management practices targeted at identifying outsider attacks.

---

## PCI DSS Log Compliance Mitigates the Outsider Threat

PCI DSS log management requirements mitigate the threats from outside the organization in multiple ways. The logs can be used to:

- Determine individuals accessing data—in particular, cardholder data for PCI DSS—and identify access attempts from outside the network
- Identify intruder access to network files by examining logs for combinations of such things as
  - User identifiers and associated activities
  - Date and time of access to PII and sensitive data and resources
  - Type of access events and attempts to these resources
  - Affected data, system, and/or resource
  - Associated changes found in other logs
  - Time stamps and clock synchronization

Organizations can use file integrity monitoring and change detection software on logs to ensure existing log data cannot be changed without generating alerts. Outsiders often try to cover their tracks by removing logs that could point to their infiltration; the alerts will notify organizations as soon as the culprits try to remove evidence.

## Using Combinations of Logs to Protect Against Outside Attacks

Ben Rothke, CISSP, QSA, and Senior Security Consultant at BT INS, reveals that, in his experience, firewall and router logs are the best indicators of attempts of unauthorized access from outsiders. These logs can not only show the dates and times of the access attempts but also, and perhaps more significantly, the source of the attack. However, he indicates that it is common during his PCI DSS audits to find log management activities woefully lacking in checks for these activities.

---

Annarita Giani, Postdoctoral Fellow in the Electrical Engineering and Computer Sciences Department, University of California at Berkeley, has done extensive systems log research and offers some good advice and insights into using logs to identify and defend against attacks from outside the enterprise.

*Only a single log or alert does not provide enough information about an outside attack to be able to help defend against it. Attacks are more sophisticated nowadays, so more sophisticated approaches must be used to detect them.*

*Here is an example. Usually an outside attacker does not want to be recognized. Public web servers are easily accessible from the Internet, so they are often used as a stepping-stone to other attacks. By doing a scan on a web server, a hacker can discover and exploit a vulnerable PHP web application. Also, a remote shell open from the web server to the attacker on an unusual port can allow the attacker to escalate his privilege and install a rootkit. Now the stage is set, and not only can the real attack to a third machine take place, but the connection with the attacker will be hard to find. So the basic steps of the attack include:*

- 1. Privilege escalation*
- 2. Creation of a fake account*
- 3. Installation of a rootkit*
- 4. Replacing system libraries with some backdoor versions*

*While the logs for each of these steps separately do not represent the complete attack, their combined sequence is a sign of a remote shell through web application exploit. This is key; looking at more than one log to see what combinations of logs indicate outside attacks.*

*It is important to know that only one source of data does not allow the detection of outside attacks. Finding malicious activity depends enormously on the ability to associate, in a meaningful way, diverse information, malicious or suspicious traffic, together with unexpected file modification.*

Effective log management practices to defend against the outsider threat must involve more than just simple review of isolated log entries. By developing procedures to identify key combinations of log entries, organizations can help to prevent hacks that could have damaged the business and compromised PII; in addition, they are supporting PCI DSS log management compliance.

---

## A Practitioner's Perspective

A.B., an IT security expert practitioner with more than 25 years of experience within large multi-national companies (A.B.'s corporate rules do not allow him to have his name or his company's name published; however, his great expertise and vast experience offers some valuable lessons to readers), offers good points about how he has successfully used logs to help identify and prevent attacks originating from outside his organization.

*There aren't usually messages in the logs that immediately suggest exploitation of a particular vulnerability. For example, obvious signs of remote command execution don't usually exist in the logs. Instead, look for signs in the logs of unusual behavior. Those are the things that suggest something is amiss. For instance, seeing a server inexplicably rebooting in the logs could be a symptom of the server being compromised and the hacker attempting to cover his tracks. Or it could be a failed buffer overflow attack that corrupted the operating system's memory and caused the crash. Of course, there could be of a bunch of non-malicious explanations, too.*

*Another possibility is a log entry that shows an export of 1,000,000 credit card records. Is that normal? Probably not. That could be a hacker stealing credit card data. Even if the data is encrypted, the organization was hacked. Or, something even more subtle would be a log entry showing Rebecca Herold attempting to access customer data at 3:00am. But, you know she NEVER works those hours; that's suspicious. Maybe that is a bad guy using her username and password. Another example is the firewall logs showing users browsing to strange IP addresses. Perhaps that is a sign of a cross-site scripting or other web-based attack.*

*Sometimes what you do \*NOT\* find in a log can be suspicious. For example, a server not logging when it should be could be a sign of a hacker erasing log entries or disabling the system logs.*

*Something else that is important for log management is following through to investigate suspicious logs in a timely manner. The lawyers I work with during hacking incidents are emphatic that when you find something suspicious in logs, you \*MUST\* investigate it in a timely fashion. Ignoring suspicious behavior in logs is far worse than not logging at all. It is also important to document your investigations to show auditors that you are diligent about reacting to notable log entries.*

As you can see, A.B.'s experience supports Annarita's research as well as the practices Ben looks for as a QSA.

---

## Be Prepared for Your QSA and Protect Against Outside Threats

Most outside attacks leave some kind of trail. The trick is in knowing how to find these intrusions among thousands, or even millions, of normal log entries. The key to success is to start with high-level queries of specific types of logs and associated activities, then work your way down to more specific conditions. Of course, this task would be too overwhelming without automation. Use log correlation tools to monitor network activity in real-time to identify when there is any suspicious or inappropriate access and usage occurring that originated from outside the network.

When creating your log management procedures to detect outside attacks, consider creating procedures to look for combinations of the following:

- Firewall logs that show unexpected or abnormal activities
- Router logs that show unexpected or abnormal activities
- Logs that reveal privilege escalation on certain accounts
- Logs that reveal creation of a fake account
- Logs that indicate installation of a rootkit
- Logs that show system libraries have been modified or replaced, possibly with some backdoor versions
- User identifiers/accounts and associated activities that do not make sense for the associated job responsibilities—Was a user on the network, or accessing a financial application, at an unusual or unexpected time? Were there an excessive number of failed login attempts?
- Logs showing date and time of access to PII and sensitive data and resources
- Logs for terminal services login attempts; check logins to all public terminal servers and check for successful logins from unrecognized IP addresses
- Logs specifying the type of access events and attempts to resources—specific to PCI DSS, what financial resources were accessed?
- Logs that indicate affected or modified data, in particular, financial data
- Logs that show access or changes to systems, particularly financial systems and associated resources
- Logs that show time stamp and clock synchronization tampering from outside sources

- 
- Logs that show connections from outside the enterprise lasted for lengths of time beyond what is normally expected
  - Logs showing source and destination IPs and ports—Who was talking to whom? And over what ports? Is anything unusual about the communications? Are the times of the connections out of the ordinary?
  - Logs showing protocols used—Was the connection a TCP, UDP, ICMP, or other protocol? Were any of them out of the ordinary?
  - Logs that show the number of packets sent and received—Was there abnormal packet activity in correlation to the connection that was made? Look at the packet payload size. How much data was involved in this connection? Is this unusual, unexpected, or abnormal?
  - Logs containing TCP flags—What TCP flags were in use by both client and server in the connection? What TCP flags are outside the boundaries of what would be expected as normal?

Do not consider this a comprehensive list but rather a starting point to help you identify the logs to use within your organization. These practices will not only help protect your business network but also support PCI DSS log management requirements.

## Summary

Keep in mind that when you are preparing for a PCI DSS audit, it is typical for the QSA to examine your log records along with your log management procedures. The QSA will look to determine whether your procedures are effective for identifying attacks from outside the enterprise, and she will determine whether you have been following your policies and procedures consistently and reacting appropriately to suspicious combinations of log entries that indicate possible outside attacks.



Sound log management practices not only help protect your business from attackers outside your network but also support PCI DSS compliance.

---

## Article 3: Addressing Application Vulnerabilities with PCI Log Management Compliance

Applications with significant and dangerous vulnerabilities continue to be pushed into production. More and more application vulnerabilities are being exploited, purposefully and accidentally, resulting in not only bad press for organizations but also costly incident response activities and personally identifiable information (PII) privacy breaches.

Meeting the PCI DSS requirements for logging can benefit businesses by putting into place logs that reveal vulnerabilities within applications that could have lead to information security incidents and privacy breaches if they were not discovered. Such vulnerabilities can also result in significant fines for PCI DSS non-compliance. Too many information security and IT practitioners do not clearly understand potential great negative impacts that poorly engineered and vulnerable applications can have upon the business.

### Application Flaws Impact Business

Early in my career, I was a systems analyst and applications programmer. I followed a stringent applications testing procedure as part of the company's change management policy when moving new and updated programs into the production environment. During this testing, we checked not only input and output but also the logs to ensure the application was communicating with only the other databases, common modules, applications, and other systems resources as intended. The logs were of great value to our testing activities.

For example, one time while our team was testing changes for a payment processing application, the immediate outputs on the screens for the corresponding inputs all looked valid. However, upon checking the logs of the application following the test run, we saw that the application was actually applying the payments to the wrong database—a mirror of the production database that was created to serve as a backup but was not to be used during the actual payment processing cycle. The net result of this error was that the payments in that backup database were overwritten at the end of the application processing cycle by the valid customer database, negating the customer payments. If this had not been caught, and the application had gone into production, we would likely have had a very large number of angry customers contacting the company upon receiving bills for amounts that they had already paid! Many of the customers would likely have taken their business elsewhere.

It is very easy to make application errors, especially if there is a tight timeline for putting the application into production; application testing often gets shortchanged as a result. Following log management procedures to verify the application has executed as intended helps to keep errors from being put into production and facilitates catching errors in production applications as soon as possible, helping to keep mistakes and vulnerability exploits from negatively impacting business.

---

## PCI DSS Log Compliance Can Help Improve Application Security

PCI DSS log management requirements can be used to mitigate the possibility of putting buggy applications into production and catch vulnerabilities within applications already in production. For example, log management procedures can be used to

- Troubleshoot problems and bugs in applications using the logs
- Analyze data flows and identify data leaks and vulnerabilities
- Identify inappropriate links to other systems components that may put PII at risk
- Determine inappropriate storage points that put PII at risk
- Identify erroneous storage of prohibited data, such as PII

There are many ways in which logs can be used to improve applications security while helping to support compliance with PCI DSS log management requirements. Kevin Beaver, founder and principal information security consultant of Principle Logic, LLC, talked with me about five such methods.

### **1. Remote Code Execution Vulnerabilities**

Coding errors, or poor quality code, can create vulnerabilities that could allow an attacker to run arbitrary, system-level code on the vulnerable server and access sensitive information. A couple of examples of code that, in the past, have contained such vulnerabilities include Invision Board and the PayPal cart. How can logs point to a remote code execution vulnerability within an application?

According to Kevin, “Server logs could certainly point out that at least a connection was made and when it happened. More specifically, application and/or database logs could point out that certain system calls were made, certain data was accessed, or specific data was added, modified, or transferred.”

### **2. SQL Injection Vulnerabilities**

SQL injection vulnerabilities within applications can allow an attacker to retrieve information from a Web server’s database. Depending upon how the application is engineered, the attack can vary from basic information disclosure to remote code execution and even possibly total system compromise. Could logs indicate whether an application is vulnerable to SQL injection, and if so, how?

Kevin answers, “Sure, all you’d have to do is look for specific SQL commands such as SELECT, CONNECT, and UNION being submitted to the server or application. You may also have log entries for SQL errors that are being generated and displayed back to the user of the application.”

---

### **3. Format String Vulnerabilities**

It can be a great challenge to secure applications that interact with Web-based customers, such as e-commerce applications—especially when so many of those trying to use the application may in fact have malicious intent. Applications written in C can be a particular challenge to secure because of the security that is often traded to gain efficiency. Something that often results is format string vulnerability.

Since the discovery of the format string vulnerability, many hackers have exploited it to gain root access to these vulnerable systems. An application that does not adequately filter user input, such as the format string parameter in certain Perl or C functions that perform formatting (such as C's `printf()` command), will create the ability for a malicious attacker to perform a Denial of Service (DoS) attack, read confidential data, or perhaps even write to sensitive data bases. Could logs indicate whether an application has format string vulnerabilities?

Kevin replies, “Yes, potentially; if the application has logging capabilities. As with the remote code problems mentioned earlier, you may at least be able to see basic connections being made from the application.”

### **4. Cross Site Scripting**

Poorly engineered applications may be vulnerable to cross site scripting (XSS). This attack is typically accomplished when the victim executes a malicious URL that appears to be legitimate, and then goes to that URL only to have malicious code executed in their browser. Examples of products that have been vulnerable to this type of exploit in the past include Yahoo Mail and Google search, just to name a couple.

I asked Kevin whether logs could indicate if an application has format string vulnerabilities. “Yes, definitely. An application could be coded to log anything that’s out of the ordinary. That said, if developers are writing logging capabilities such as this, then they’ve hopefully addressed the basic XSS problems to begin with! You can also set up Web servers and other systems to trigger on suspect input such as `<script>` tags.”

### **5. Username Enumeration**

Sometimes applications are coded in such a way that they allow for username enumeration. Applications can be prone to username enumeration exploits because of the inadequate ways in which they verify end user-supplied application input. Attackers may exploit this weakness to determine valid usernames. This can assist attackers in brute-force password cracking or other types of attacks.

Username enumeration can be exploited when the back-end validation code tells the attacker whether the supplied username correct or not. The attacker can then try different usernames until the attacker finds valid ones by noting the different error messages.

Kevin has recent experience with this type of exploit. “I just came across this very vulnerability in a Web application. Detection of this vulnerability is as simple as looking for large numbers of ‘incorrect user’ and ‘incorrect password’ errors and distinguishing between the two to determine that something’s going on. This could be done at the server or the application level depending on how the site and/or application works.”

---

## An IT Security Expert Practitioner's Perspective

A.B., an IT security expert practitioner with more than 25 years of experience within large multi-national companies (A.B.'s corporate rules do not allow him to have his name or his company's name published; however, his great expertise and vast experience offers some valuable lessons to readers), offers some good points and examples about how he has successfully used logs to help identify vulnerabilities within applications.

*Consider this scenario: The log file of a web server that is a front end to a database shows that a remote user has accessed files that are outside of the web server's environment. For example if the web server's environment is under the directory tree (e.g., c:/applications/database/webserver/) and you see users in the application log fetching files from the root level of the c: drive (e.g., "c:/"), then something is very wrong. The developers should consider that they did not do an adequate job of URL input validation.*

*Here's another example; a programming pet peeve of mine. Suppose a log file shows that a hacker was able to subvert an application's input validation routine. The command he used is in the log file. Analysis of the log shows that the hacker abused a character that was supposed to cause an illegal input error message. When the developers look at the program, they discover that the abused character was not in the list of illegal input characters, an easy mistake to make after long hours of programming. But here's my pet peeve: The programmers took the wrong approach in error checking. By scanning the input characters for illegal characters, they take the risk of not checking for **ALL** of the illegal characters (which is what happened). Instead, it is best to ensure that all characters in the input are legal (e.g., scan for legal characters). If the program finds a character that is not legal, then the application should signal an error message. With this approach, if a legal character is erroneously programmed as illegal (e.g., an apostrophe), Mr. BigBoss will complain. Better an annoyed legitimate user than a successful hacker.*

*Another example is a log file showing the mysterious creation of a privileged account on a web server. There is a possibility that a hacker was able to craft input to break out of the web environment to the command line. If the web server was running under a privileged account, he could have created an administrator account. Until recently SQL, by default, allowed SQL commands to execute DOS commands. A bonehead idea from a security point of view. I think Microsoft reconsidered that idea and fixed this vulnerability.*

---

## Prepare for PCI DSS Compliance and Increase the Security of Applications

Kevin indicated the following are significant application vulnerabilities that he often runs across, “Username and password enumeration is a biggie; it is common to find these vulnerabilities within e-commerce applications. Another one is basic URL manipulation and hidden field manipulation. Both of these types of vulnerabilities can be detected in Web logs and help prevent malicious unauthorized use of the application.”

Creating effective log management practices supports PCI DSS compliance and helps to protect the business against using applications that contain vulnerabilities such as those described, in addition to others. When creating your log management procedures to detect application vulnerabilities, include checks to look for the following:

- Remote code execution, especially for Web applications that process credit cards
- Username and password enumeration vulnerabilities
- Incorrect database updates
- SQL injection vulnerabilities
- Format and input string validation vulnerabilities
- Cross site scripting
- Applications inappropriately running under privileged accounts
- Multiple application sessions using the same username

Do not consider this a comprehensive list but rather a starting point to help you identify which application logs to use within your organization. These practices will not only help protect your business, they will also help to support PCI DSS log management requirements.