

Web Logs and Security - Do You Know What's in Your Log Files?

Posted At : January 23, 2008 6:42 PM | Posted By : Mark Kruger

Related Categories: Coldfusion Security

So you have a new ecommerce application eh? You say you've done your homework. You are using a reputable gateway. You think you are PCI compliant. You are not storing Credit card numbers anywhere and you are using SSL (plus you have new snazzy haircut). Life is good. Hmmmm.... do you ever stay awake at night wondering if you forgot something? One of the things that you might have overlooked is the web log files. I'm sure you are aware of these files... the ones that your customer is always running reports on so he can marvel at the ip geocoding and exclaim "Well would you look at that" about the 4 people from Uzbekistan that visited the site yesterday. Web logs come in a number of flavors, but most of them are able to track the URL "query_string" variable in the log. Many of them are set up this way by default. This can be helpful to figure out traffic patterns. If you handle credit cards a certain way however, they can lead to the pit of despair. Take this example....

Credit Card Form 1

This form collects the information:

```
<pre>
<form action="process.cfm" method="get">
Name: <input type="text" name="ccname">
CC Number: <input type="text" name="ccnum">
exp: <input type="text" name="expNum">
<input type="submit" value="go">
</form>
</pre>
```

...and passes it to some kind of server side handler where it is vetted and used to create a transaction at the gateway. Does anyone see a problem? The form method is *GET*. If you fill this out with the following values:

- Frodo
- 411111111111111111
- 08/11

and submit it you will see a URL in the address bar that looks like

.../formscrip.cfm?ccname=Frodo&ccnum=411111111111111111&expnum=08%2F11.

If your web server is set up to collect the query string you can go and look at the log files and you will see an entry that looks vaguely like this IIS example:

```
date stuff ip stuff 443 GET /formscrip.cfm
ccname=joe&ccnum=411111111111111111&expNum=08%2F11 200 Mozilla/4.0+(...useragent
stuff)
```

See the easily recognizable CC number and expiration date? Very handy eh. This occurs whether your site is SSL secured or not. Please note, allowing CC Numbers to end up in the log files is a *bad thing*. Most admin types do not pay particular attention to securing the log files. Indeed, I have worked with some web hosts that zip them up

into a folder (like /weblogs) off of your web root for easy downloading.

The moral of the story is two-fold. First, know what is in your web logs! Find out what's being stored there. Take a gander at them periodically and just sort of blithely peruse them with an open mind (chanting might also help) to see what turns up. Secondly, handle CC data as a POST request. Post requests are *not* stored in log files and will not show up in your web logs.

Finally, whenever you are working with CC numbers take the time to test all the things that are happening on the web server from start to finish. Don't neglect background processes like web logging or database logging. The end game is to *know* everything that is going on so there are no surprises.