ThreatFactor NSIA - Bug #287

Cookie Injection Vulnerability

12/03/2010 08:55 PM - Luke Murphey

Status:	Closed	**Start date:**	12/03/2010
Priority:	Immediate	**Due date:**	12/03/2010
Assignee:		**% Done:**	100%
Category:	Web Interface	**Estimated time:**	0.00 hour
Target version:	1.0.2		

Description

Optics for Vulnerability Management discovered a vulnerability in NSIA:

```
nc -v 127.0.0.1 8080
GET /<script>cross_site_scripting.nasl</script>.asp HTTP/1.1
Host:127.0.0.1
<pre>

This returns:
<pre>
<code class="html">
        <p>
                <form method="post" action="/<script>cross_site_scripting.nasl</script>.asp">
                        <input class="button" type="submit" value="Accept" name="BannerCheck">

                </form><p/>
</code>
</pre>
```

History

#1 - 12/03/2010 08:57 PM - Luke Murphey

- Subject changed from Cookie injection to Cookie Injection Vulnerability

#2 - 12/03/2010 09:00 PM - Luke Murphey

The following request will illustrate the problem more clearly: http://127.0.0.1:8080/"><script>alert('XSS')</script>

#3 - 12/03/2010 09:12 PM - Luke Murphey

Run the following regex search against FTL to find portions of templates that may need escaping:

```
[$][{][a-zA-Z0-9.()]+[^?][a-zA-Z0-9.()]+[}]
```

#4 - 12/03/2010 10:25 PM - Luke Murphey

- Status changed from New to Closed

- % Done changed from 0 to 100

Confirmed fixed by OSVM and manual test