Vulnerabilities (27)

🟥🟥🟥🟥🟥 5 Reflected Cross-Site Scripting (XSS) Vulnerabilities port 32000/tcp

QID:	150001	CVSS Base:	7.5	PCI Severity:	🟥 HIGH
Category:	Web Application	CVSS Temporal:	6.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/26/2009				

THREAT:
XSS vulnerabilities occur when the Web application echoes user-supplied data in an HTML response sent to the Web browser. For example, a Web application might include the user's name as part of a welcome message or display a home address when confirming a shipping destination. If the user-supplied data contain characters that are interpreted as part of an HTML element instead of literal text, then an attacker can modify the HTML that is received by the victim's Web browser.

The XSS payload is echoed in HTML document returned by the request. An XSS payload may consist of HTML, JavaScript or other content that will be rendered by the browser. In order to exploit this vulnerability, a malicious user would need to trick a victim into visiting the URL with the XSS payload.

IMPACT:
XSS exploits pose a significant threat to a Web application, its users and user data. XSS exploits target the users of a Web application rather than the Web application itself. An exploit can lead to theft of the user's credentials and personal or financial information. Complex exploits and attack scenarios are possible via XSS because it enables an attacker to execute dynamic code. Consequently, any capability or feature available to the Web browser (for example HTML, JavaScript, Flash and Java applets) can be used to as a part of a compromise.

SOLUTION:
Filter all data collected from the client including user-supplied content and browser content such as Referrer and User-Agent headers.

Any data collected from the client and displayed in a Web page should be HTML-encoded to ensure the content is rendered as text instead of an HTML element or JavaScript.

RESULT:

```
url: http://72.165.128.12:32000/webmail/basic/./././././././././././././././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/./././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/././././././././././././././././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/./?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/./././././././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/minimizer/index.php?style=%22%27%3e%3cqss%20a%3dX3003689608Y1Z%3e
variants: 1
matched: /* SOUBOR "../'"><qss a=X3003689608Y1Z>" NENALEZEN */
```

```
url: http://72.165.128.12:32000/webmail/basic/./././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/./././././././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/./././././././././././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/./././././././././././././././?_n[p][main]=%22%3e%3cqss%3e&_
n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/./././././././././././././././././././././././././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/././././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/./././././././././././././././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/./././././././././././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/././././././././././././././././././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/./././././././././././././././././././././././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/././././././././././././././././././././././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/./././././././././././././././././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/./././././././././././././././././././././././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.16
5.128.12:32000/webmail/basic/./././././././././././././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/./././././././././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/./././././././././././././././././././././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/./././././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>

url: http://72.165.128.12:32000/webmail/basic/./././././././././././?_n[p][main]=%22%3e%3cqss%3e&_n[w]=main&tab=login
variants: 15
matched: GUI:Descriptor file missing:"><qss>
```