Vulnerability Assessment Report: 127.0.0.1

1. Network Scan Results (Nmap)

Port	Service	Version	State
3000	http		open
5000	upnp		open

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ No web server found on localhost:80
---------------------------------------------------------------------------
+ 0 host(s) tested
```

3. Crawled Website Endpoints

4. Vulnerability Intelligence (CVE Mapping)

Vulnerability: XSS
- CVE-2002-1315: Cross-site scripting (XSS) vulnerability in the Admin Server for iPlanet WebServer 4.x, up to SP11, allows remote attackers to execute web script or HTML as the iPlanet administrator by injecting the desired script into error logs, and possibly escalating privileges by using the XSS vulnerability in conjunction with another issue (CVE-2002-1316).
- CVE-2002-1316: importInfo in the Admin Server for iPlanet WebServer 4.x, up to SP11, allows the web administrator to execute arbitrary commands via shell metacharacters in the dir parameter, and possibly allows remote attackers to exploit this vulnerability via a separate XSS issue (CVE-2002-1315).
- CVE-2003-0292: Cross-site scripting (XSS) vulnerability in Inktomi Traffic-Server 5.5.1 allows remote attackers to insert arbitrary web script or HTML into an error page that appears to come from the domain that the client is visiting, aka "Man-in-the-Middle" XSS.

Vulnerability: Insecure Cookie
- CVE-2000-0970: IIS 4.0 and 5.0 .ASP pages send the same Session ID cookie for secure and insecure web sessions, which could allow remote attackers to hijack the secure web session of the user if that user moves to an insecure session, aka the "Session ID Cookie Marking" vulnerability.
- CVE-2002-1672: Webmin 0.92, when installed from an RPM, creates /var/webmin with insecure permissions (world readable), which could allow local users to read the root user's cookie-based authentication credentials and possibly hijack the root user's session using the credentials.
- CVE-2004-0869: Internet Explorer does not prevent cookies that are sent over an insecure channel (HTTP) from also being sent over a secure channel (HTTPS/SSL) in the same domain, which could allow remote attackers to steal cookies and conduct unauthorized activities, aka "Cross Security

Boundary Cookie Injection."
Vulnerability: Missing Security Headers
- CVE-2003-1016: Multiple content security gateway and antivirus products allow remote attackers to bypass content restrictions via MIME messages that use malformed quoting in MIME headers, parameters, and values, including (1) fields that should not be quoted, (2) duplicate quotes, or (3) missing leading or trailing quote characters, which may be interpreted differently by mail clients.
- CVE-2010-3541: Unspecified vulnerability in the Networking component in Oracle Java SE and Java for Business 6 Update 21, 5.0 Update 25, 1.4.2_27, and 1.3.1_28 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors. NOTE: the previous information was obtained from the October 2010 CPU. Oracle has not commented on claims from a reliable downstream vendor that this is related to missing validation of request headers in the HttpURLConnection class when they are set by applets, which allows remote attackers to bypass the intended security policy.
- CVE-2010-3573: Unspecified vulnerability in the Networking component in Oracle Java SE and Java for Business 6 Update 21 and 5.0 Update 25 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors. NOTE: the previous information was obtained from the October 2010 CPU. Oracle has not commented on claims from a reliable downstream vendor that this is related to missing validation of request headers in the HttpURLConnection class when they are set by applets, which allows remote attackers to bypass the intended security policy.

5. Attack Possibilities & Mitigation

XSS
Attack: Cross-Site Scripting (XSS), session hijacking
Mitigation: Input validation, output encoding, Content Security Policy
Insecure Cookie
Attack: Session hijacking
Mitigation: Enable HttpOnly and Secure cookie flags
Missing Security Headers
Attack: Clickjacking, XSS
Mitigation: Configure security headers (CSP, X-Frame-Options)