NC STATE UNIVERSITY

Only Grey Box Testing Can Detect Input Validation and Error Message Information Leakage Vulnerabilities

Ben Smith and Laurie Williams, {ben_smith, laurie_williams}@ncsu.edu

Problem – Error message information leak and input validation vulnerabilities (in the CWE/SANS Top 25) relinquish information that makes the attacker's job significantly easier.

Objective – To asses the relative effectiveness of white box and grey box testing for protecting against these two vulnerability types.

Approach – Perform white box and grey box testing on four open source Java web applications and measure the number of vulnerabilities exposed by both grey box and white box testing.

Error Message Information Leak

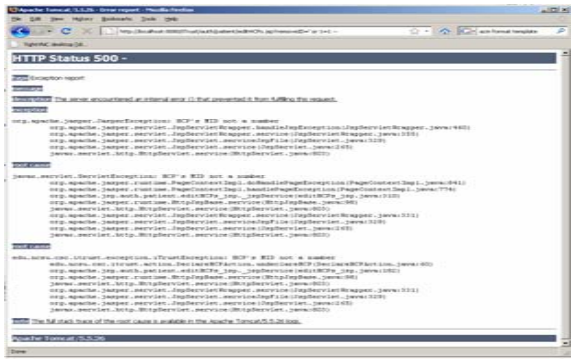


Figure 3. Example EMIL Vulnerability

Hotspot and Hotspot Variable Coverage

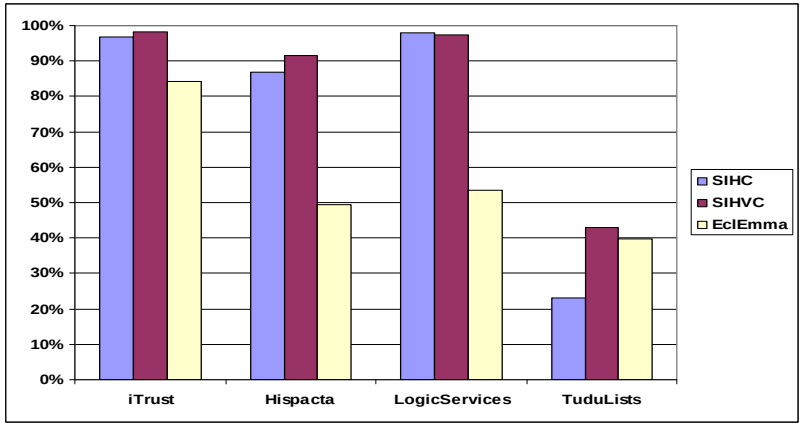


Figure 4. Coverage Measures Study Subjects

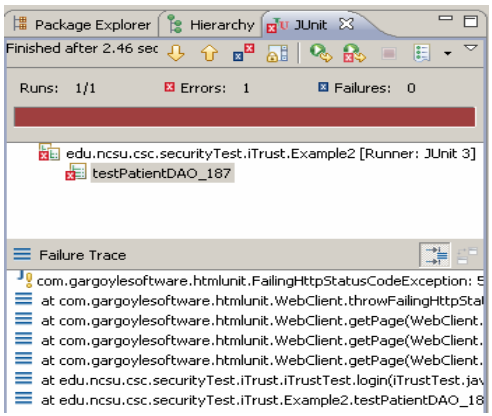
Now You See It

```
public void testPatientDAO_187() throws Exception
{

HtmlPage p = login("http://localhost:8080/" +
iTrust/auth/patient/editHCPs" +
".jsp?removeID=` UNION SELECT", "patient");

}
```

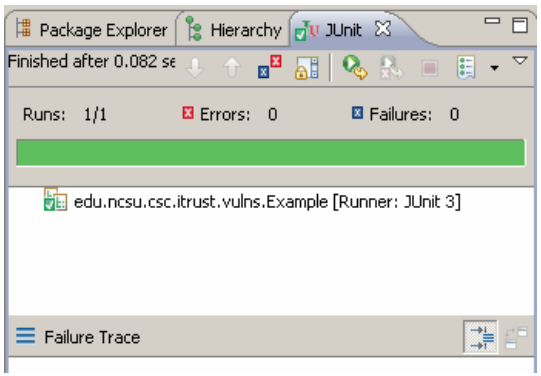
Figure 1. Grey Box Test Exposing Vulnerability



Now You Don't

```
public void testInvalidInputForRemoveHCP()
{
DeclareHCPAction action = new DeclareHCPAction()
//default constructor used for brevity
try
{
action.undeclareHCP("' UNION SELECT ");
fail("Exception should be thrown");
}
catch (iTrustException theException)
{
assertTrue("HCP's MID not a
number".equals(theException.getMessage());
}
}
```

Figure 2. White Box Test Not Exposing Vulnerability



Case Study Results

Project	iTrust	Hispacta	LogicServices	TuduLists
Hotspots	92	23	48	13
Covered	89	20	47	3
Hotspot Variables	213	36	76	49
Covered	209	33	74	21
Malicious Input Tests (initially)	0	0	0	0
New Grey Box Tests	149	29	80	14
Vulnerabilities by Grey Box	2	2	9	4
Vulnerabilities by White Box	0	0	0	0

Table 1. Results for the study subjects

Computer Science NC STATE UNIVERSITY

Real Research Group
Software Engineering @ NCSU