| Attack: Application Exception - [OWASP 2013 A 5] | Ver: 1.2 | | Observations: 3 |
|---|---|---|---|
| Descr: Application Exceptions are vulnerabilities where unexpected inputs can trigger inappropriate exceptions, or error responses disclosing implementation information, such as a stack trace. The SmartAttack sends various unusual inputs and looks for text in responses evidencing poor error handling. | | | |
| Severity: Medium HARM: 96 Total HARM: 221 | Online Documentation for: Application Exception - [OWASP 2013 A 5] | | |

**Impact**

An attacker might gain administrative control of your web application by using vulnerabilities known to be in the servers or server-side technologies used. It is also be possible to gain remote access to restricted information via exploit of some vulnerability in your application.
An Application Exception vulnerability helps the attacker in formulating the correct attack depending on information disclosed in the error message. Such an error message may also disclose information about the deployment of the server, such as the database server used, server-side technology used, *etc*. Error messages often give an attacker useful information about how an application interacts with back-end components, and can reveal potential vulnerabilities within the application itself.
All Web applications use some server-side technology and back-end components which can be disclosed through error messages deliberately obtained by an attacker. For example, an error generated by a Web-based form for searching products in a shopping application may disclose the database or server-side technology it uses, their versions, *etc*. Or, errors generated by a Web-based banking application may expose further vulnerabilities such as Cross-Site Scripting present in the application.

## Application Exception - [OWASP 2013 A 5] Vulnerable Findings

**Assessment:** SI-OWASP2013, **Run:** 12/11/2014 3:44:25PM, **Traversal:** [Default Spider]

Application Exception - [OWASP 2013 A 5]

**1. Vulnerable (Medium, HARM: 96) at: http://asiloidflies.si.edu/biblio?f[author]=1**

Message: Application exception vulnerability found
Injectable request #: 15
Injected item: GET: f[author]
Injection value: [
Detection value: internal server error

Application Exception - [OWASP 2013 A 5]

**2. Vulnerable (Medium, HARM: 96) at: http://asiloidflies.si.edu/biblio?f[search]=testval&f[author]=108&f[type]=102&f[year]=2012&f[keyword]=67**

Message: Application exception vulnerability found
Injectable request #: 20
Injected item: GET: f[author]
Injection value: [
Detection value: internal server error

## Application Exception - [OWASP 2013 A 5] Warning Findings

**Assessment:** SI-OWASP2013, **Run:** 12/11/2014 3:44:25PM, **Traversal:** [Default Spider]

Application Exception - [OWASP 2013 A 5]

**1. Warning (Medium, HARM: 29) at: http://asiloidflies.si.edu/biblio?f[search]=testval&f[author]=108&f[type]=102&f[year]=2012&f[keyword]=67**

Message: Possible application exception vulnerability.
Server response status: 503
Service unavailable (server overloaded)
Injectable request #: 21
Injected item: GET+POST: f[author]
Injection value: [