

Week 4 - Vulnerable Components

Why are Vulnerable Components important to the security of our application?

Vulnerable components have security flaws which are not under our control. Also, they can be easily and quickly exploited when the component is popular. Attackers can search through projects that use these components and exploit.

We can and should use automated tools which detect vulnerable components in security databases, as OSAWAP. One tool is OSAWAP Dependency Check

Exploiting CVE-2013-7285 (XStream)

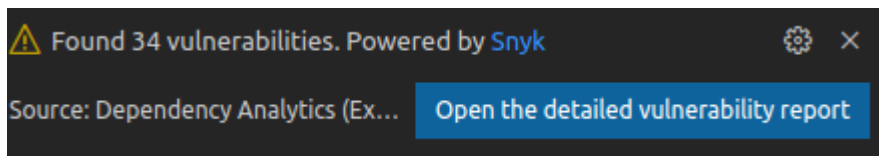
WebGoat Sends an XML document to add contacts to a contacts database.

```
<contact>
  <id>1</id>
  <firstName>Bruce</firstName>
  <lastName>Mayhew</lastName>
  <email>webgoat@owasp.org</email>
</contact>
```

For this example, we will let you enter the xml directly versus intercepting the request and modifying the data. You provide the XML representation of a contact and We convert it to a Contact object using `XStream.fromXML(xml)`.

Enter the contact's xml representation:

Go!



Patch

```
<dependency>
  <groupId>com.thoughtworks.xstream</groupId>
  <artifactId>xstream</artifactId>
  <version>1.4.18</version>
</dependency>
```