# XML Attacks

Available XML Attack types In contact-us page ([**http://localhost:8080/contact-us.php**](http://localhost:8080/contact-us.php)) according to:

**A4:2017-XML External Entities (XXE)**

([OWASP Top Ten 2017 | A4:2017-XML External Entities (XXE) | OWASP Foundation](https://owasp.org/www-project-top-ten/2017/A4_2017-XML_External_Entities_(XXE)))

**A screenshot of a computer

AI-generated content may be incorrect.**

1. Disclosing files on the Server

A grey rectangular object with black text

AI-generated content may be incorrect.

It is still possible to read files using XML:  
A screenshot of a computer

AI-generated content may be incorrect.

1. Load xml on external websites

Loading external websites in xml format is still possible:  
A screenshot of a computer

AI-generated content may be incorrect. A black screen with colorful text

AI-generated content may be incorrect.

However it is not possible to open websites:  
A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. Load xml Files in the Private Networks

It is possible to load and read xml files in the private networks:  
A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect.

A screen shot of a computer program

AI-generated content may be incorrect.

1. Billion Laughs Attack

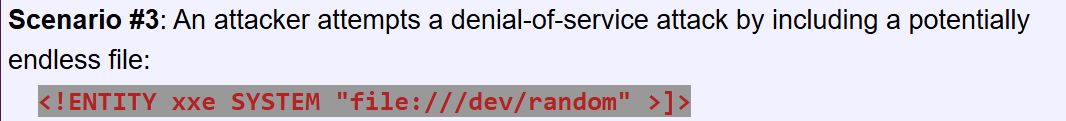
Billion Laughs Attack is not possible in PHP 8+, because libxml2 does not let loops in xml. I tried to deactivate or uninstall it, but I couldn't! PHP depends heavily on libxml2!A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. DOS Attack by trying reading a huge file:



Generate a random huge file in the web server cocker container using:  
# yes "XXE\_TEST\_DATA\_LINE" | head -c 5G > /tmp/hugefile.bin

Setting the max ram limit:  
A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

It was not possible to crash the docker container with a huge file!

1. Remote Code Execution

According to ([XML External Entity (XXE) Processing | OWASP Foundation](https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing))

A screenshot of a computer

AI-generated content may be incorrect.

expect:// “command” is not installed by default in PHP 8+

**There is no php-expect package for PHP 8+**

But you can still **add the expect CLI tool** (for use in shell scripts or PHP's shell\_exec())