Research Paper on Security in the Software Development field

-Rares Petrisor-

# Topic of this research paper

This paper is created in order to assess what security concerns exist in the software world, what is the OWASP organization and why their opinion is relevant in this field and how to protect your applications against attackers. The Library and Field will be used in order to conduct this research and come to a conclusion to these questions.

## What does the term Security in Software Development refer to? Who are we protecting against?

As can be read on Wikipedia: “Security, as part of the software development process, is an ongoing process involving people and practices, and ensures application confidentiality, integrity, and availability”. This means that Security refers to the set of actions that the developers do in order to ensure confidentiality, integrity and availability for their product’s clients. Why are these protocols necessary? The malicious people that attempt to hinder these (the confidentiality, integrity and availability) are called attackers. They use several different exploits or faults in design in the technologies to gain access to systems they shouldn’t have.

## So how do we defend against these “attackers”?

Ever since technology has become more popular, so have these attackers trying to do malicious things. That is why, in 2001 the OWASP organization (or Open Web Application Security Project) has been born. They are an online community that produces “freely-available, articles, methodologies, documentation, tools and technologies in the field of the web”. This means that they are an authority in this field, working hard to gather information and help people defend themselves against the popular known techniques attackers use to breach/bypass security protocols using various exploits. That is why, they have created a top of the most common malicious attacks and gathered a lot of information about them, about how these work and about how developers should defend against them.

Here’s the list:

* Injection (<https://owasp.org/www-project-top-ten/2017/A1_2017-Injection.html>)
* Broken Authentication (<https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication.html>)
* Sensitive Data Exposure (<https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html>)
* XML External Entities (XXE) (<https://owasp.org/www-project-top-ten/2017/A4_2017-XML_External_Entities_(XXE).html>)
* Broken Access Control (<https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html>)
* Security Misconfiguration (<https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html>)
* Cross-Site Scripting (XSS) (<https://owasp.org/www-project-top-ten/2017/A7_2017-Cross-Site_Scripting_(XSS).html>)
* Insecure Deserialization (<https://owasp.org/www-project-top-ten/2017/A8_2017-Insecure_Deserialization.html>)
* Using Components with Known Vulnerabilities (<https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html>)
* Insufficient Logging&Monitoring (<https://owasp.org/www-project-top-ten/2017/A10_2017-Insufficient_Logging%2526Monitoring.html>)

## So which of these actually are relevant to my project?

After going through all of them and analyzing the data OWASP gives on them, I have come to the conclusion that the following exploits could be used against my system:

* Broken Authentication
* Sensitive Data Exposure

## Broken Authentication

This attack consists of attackers brute-forcing passwords, exploiting the fact that systems don’t reject the authentication attempts after several mistakes. The way to defend again this is implement a system that rejects these attempts after several mistaken attempts were requested in a row.

## Sensitive Data Exposure

This attack consists of attackers acting as a man in the middle and trying to intercept sensitive data (such as passwords). To defend against this, I am using a hashing system in the backend to ensure that the data is stored securely and even if it gets intercepted, unless it is hashed using exactly the same salt and algorithm it will not be recognized.

## Results

After having researched using OWASP’s resources, I have acquired information on common attacking techniques and implemented systems in place to defend against them. I have found out about the authority in web development security and researched their findings about several attacks and how they could damage the integrity, confidentiality or even availability of web based systems.

## Conclusion

Security is becoming more and more of a concern nowadays since more and more parts of out day to day life are getting tech involved in them (IOT field) and the last thing we as developers would want is the wrong people having access to them. That is why it is really important to be aware of these concerns and make sure to implement best practices recommended by security experts.