# Conclusions

Information security has been an important topic of debate since the inception of technology, and will remain an important topic in the foreseeable future. The risks associated with improperly secured systems range from economic harm to information theft, and the advent of the Internet has only increased this risk and its potential effects to unprecedented levels. Now more than ever, the importance of information security cannot be overstated.

In the particular case of enterprises, vulnerable systems might result in heavy financial damage and loss of reputation associated with the leaking of private information, which in some cases might even have legal repercussions. For blooming small and medium-sized enterprises this kind of mistake could prove fatal, and would severely hinder their possibilities of growing and becoming competitive in an ever-changing economy.

While this project has focused on vulnerabilities related to web applications in particular, that’s not to say other aspects of information security aren’t as important or should be disregarded. However, the fact that web applications are constantly exposed to the Internet make them an attractive target for attackers.

As mentioned in previous sections, statistics show that enterprises spend less in web application testing compared to other forms of computer security. This might denote an insufficient awareness of the importance of secure web applications, and information security in general.

## Recommendations

The web application scanner developed for this project should not be seen as a substitute for a proper penetration test from a professional. This scanner will fail to detect many kinds of vulnerabilities, some because the program is fairly simple, and some because certain types of vulnerabilities cannot be found by automated means at all. It can be seen as an inexpensive way to test the waters, but the only way to ensure a web application is secure is to actually contact a professional pen-tester.

It should also be noted that full invulnerability is unachievable, as there will always be new vectors of attack and unforeseeable circumstances. Still, good practices can be adopted to minimize risks, such as:

* Having a security plan detailing how to spend the security budget and what individuals are responsible for what is highly recommended. Vulnerabilities should be prioritized according to their potential for harm and ease of exploitation. If an enterprise has multiple web applications, they should also be prioritized accordingly.
* Cookies should be used safely. They should never store sensitive information, and should be encrypted if possible.
* URL encryption can help prevent a variety of different attacks, such as Cross-Site Request Forgery or path traversal.
* Data validation can help prevent some of the most widespread forms of attack such as XSS or injection.
* Usage of HTTPS over HTTP is recommended.

While these steps might be costly and might result in a more complex web infrastructure, the resulting web application will be less liable to being affected by an attack. All in all, while there is no easy solution to the issue of web application security, regular audits can prove to be a cost-effective method to keep possible risks under control.