* **CONCLUSION:**

Damn Vulnerable Web App (DVWA) has shown me much the specialty of web application security and I trust that it very well may be utilized show web engineers and other moral hacking understudies/experts the equivalent.

DVWA can be utilized in various manners. By showing reasonable models and setting difficulties is utilized to show security in web application for the understudies. It is utilized as a learning instrument, DVWA is arranged everything viewed as basic as possible to set up and use.

We discovered a few weaknesses in the web application - DVWA. We exploit every single one of them and realized what sway every weakness has on the web application, and how to fix those weaknesses.

* **OPTIONS AVAIALBLE TO EXECUTE THE PROJECT:**
* **KALI LINUX**
* **DVWA**
* **BURPSUITE**
* **APACHE2**
* **MYSQL**
* **ADVANTAGES/DISADVANTAGES:**

|  |  |
| --- | --- |
| **ADVANTAGES** | **DISADVANTAGES** |
| [The network penetration testing](https://blog.eccouncil.org/what-is-web-application-penetration-testing-all-you-need-to-know/) process identifies such existing loopholes that you can close or keep an eye on. | Testing could be unethical |
| A [pen testing report](https://blog.eccouncil.org/4-ways-a-penetration-testing-report-helps-a-business/) is a very detailed analysis of all the threats that the IT infrastructure is exposed to. The upper management can prioritize the threats and fix them one by one. | Damages may occur if the penetration test isn’t done correctly. |
| Penetration testing helps in evading these fines and penalties, which is also essential for the business’ reputation. | This can be challenging if there is no trust between the tester and the client. |

**REFERENCES**

1. <https://www.youtube.com/watch?v=PaB17Cc0dUg>
2. <https://www.youtube.com/watch?v=yRkSL7xfiCM>
3. <https://portswigger.net/web-security>
4. <https://www.youtube.com/watch?v=MornGd0FQqw>
5. <https://techsphinx.com/hacking/hacking-for-beginners-command-injection-vulnerability/>
6. <https://owasp.org/www-project-top-ten/>
7. <https://link.springer.com/chapter/10.1007/978-981-13-6621-5_12>
8. <https://www.slideshare.net/BiagioBotticelli/system-and-enterprise-security-project-penetration-testing>
9. <https://phoenixnap.com/blog/vulnerability-assessment-scanning-tools>
10. <https://owasp.org/www-community/controls/>
11. <https://www.hacksplaining.com/prevention/command-execution>
12. <https://www.hacksplaining.com/prevention/>
13. <https://www.pivotpointsecurity.com/>
14. <https://www.esecurityplanet.com/threats/>
15. <https://www.wordfence.com/learn/how-to-prevent-file-upload-vulnerabilities/>
16. <https://blog.securelayer7.net/owasp-top-10-insufficient-attack-protection-7-captcha-bypass/>
17. <https://www.hacksplaining.com/prevention/session-fixation>
18. <https://www.acunetix.com/blog/articles/blind-sql-injection/>
19. <https://www.acunetix.com/blog/articles/non-persistent-xss/>
20. <https://www.acunetix.com/blog/articles/persistent-xss/>
21. <https://www.acunetix.com/blog/web-security-zone/unvalidated-redirects-and-forwards/>
22. <https://static1.squarespace.com/static/589316f3cd0f68e6bd715655/t/5d7ce2ed69433d1c3e3f7021/1568465657128/SAMPLE+Security+Testing+Findings.pdf>