**Project Ideas for Information Security**

1. Malicious PDF Detection using Metadata and Structural Features

<https://personal.utdallas.edu/~muratk/courses/dmsec_files/Malicious_PDF_Detection_ACSAC_12.pdf>

1. Exploiting Machine Learning to Subvert Your Spam Filter

<https://people.eecs.berkeley.edu/~tygar/papers/SML/Spam_filter.pdf>

1. EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis

<http://www.covert.io/research-papers/security/Exposure%20-%20Finding%20malicious%20domains%20using%20passive%20dns%20analysis.pdf>

1. eXpose: A Character-Level Convolutional Neural Network with Embeddings For Detecting Malicious URLs, File Paths and Registry Keys

<https://arxiv.org/pdf/1702.08568.pdf>

1. Password Hunting with Machine Learning in Active Directory URL:https://blog.hunniccyber.com/password-hunting-with-ml-in-active-directory/
2. Vulnerablity testing/ Penetration testing

**Resources to get Started with Vulnerablity testing/ penetration Testing**

1. Owasp top 10 - <https://owasp.org/www-project-top-ten/>
2. GitHub profile of a top hunter where he lists some blog posts and materials required for a beginner <https://github.com/nahamsec/Resources-for-Beginner-Bug-Bounty-Hunters>
3. Commonly used tools for bug bounty: <https://github.com/vavkamil/awesome-bugbounty-tools>

Book - Web Hacking 101 How to Make Money Hacking Ethically by Peter Yaworski (A popular book by one of the best hunter which is beginner friendly)

1. What is bug bounty?

==============================

https://whatis.techtarget.com/definition/bug-bounty-program

https://hacken.io/research/education/what-is-bug-bounty-bug-bounty/

https://www.process.st/bug-bounties/

<https://techbeacon.com/security/why-every-organization-needs-bug-bounty-program>

e ) Top Bug bounty platforms

===========================

<https://geekflare.com/bug-bounty-platforms/>

1. Bug bounty programs

===========================

https://hackerone.com/bug-bounty-programs

<https://www.bugcrowd.com/bug-bounty-list/>

1. How does one become a bug bounty hunter and methodology used?

============================================

https://www.quora.com/How-does-one-become-a-bug-bounty-hunter

https://medium.com/inbughunters/getting-started-in-bug-bounty-7052da28445a

https://www.bugcrowd.com/blog/getting-started-bug-bounty-hunter-methodology/

<https://medium.com/@infosecsanyam/bug-bounty-methodology-ttp-tactics-techniques-and-procedures-v-2-0-2ccd9d7eb2e2>

Links for Penetration Testing Notes:

<https://github.com/AnasAboureada/Penetration-Testing-Study-Notes>

<https://github.com/adon90/pentest_compilation>

https://github.com/dostoevskylabs/dostoevsky-pentest-notes