



ASSIGNMENT 3

LNU Student Shop
Bad security in web applications

Paolo Molinaro
pm222py@student.lnu.se



TOOLS AND REQUIREMENTS

You work in pairs - choose your own partner and then request an instance from me

- VPN for working remotely
- Firefox + Web Dev Tools, or pick another that you are comfortable with
- Basic JS and HTML Knowledge, knowing how to do a little REST
- Password cracking tool -> John the ripper or any other
- 11-pages limit!

LNU STUDENT SHOP

- Platform of security challenges.
- Shop web application, deliberately made to be vulnerable.
- 13 tasks, 1 theoretical about XSS.
- You can add 3 extra tasks which you are free to pick.
 - Either as replacement task or bonus.
- There is an abundance of information on the web about this shop and how to exploit it.

LNU STUDENT SHOP

- Served on LNU's Cscloud.
- VPN for working remotely.
- You will get a personal URL.
- Progress is saved in cookies, do not delete them.
 - Unless you wish to start over...
- Progress is checked by us as well.
- For each vulnerability you exploit, you must write how it can be prevented.



OWASP

- Foundation focusing on web application security
- Efforts towards frameworks, standards and best-practices
- Software and web application domain
- OWASP Top 10 => vulnerability categories
- Match your challenges to these categories, mention which year they are from (if they appear).

ONLINE FINGERPRINT CANVAS

- A lot of information is exposed just by browsing the web.
- Change your fingerprint!
 - Moscow, Russia
 - Windows XP, AOL v.9
- Canvas element in HTML gives a relatively unique fingerprint.
- How does your browser handle it?
- How does the Tor browser handle it?



USEFUL LINKS

- [MyBrowserInfo](#)
- [Firefox Dev Tools](#)
- [Safari Dev Tools](#)
- [John The Ripper](#)
- [OWASP Top 10\(2013\)](#)
- [OWASP Top 10\(2017\)](#)
- [Student VPN Guide](#)