SbᴲD

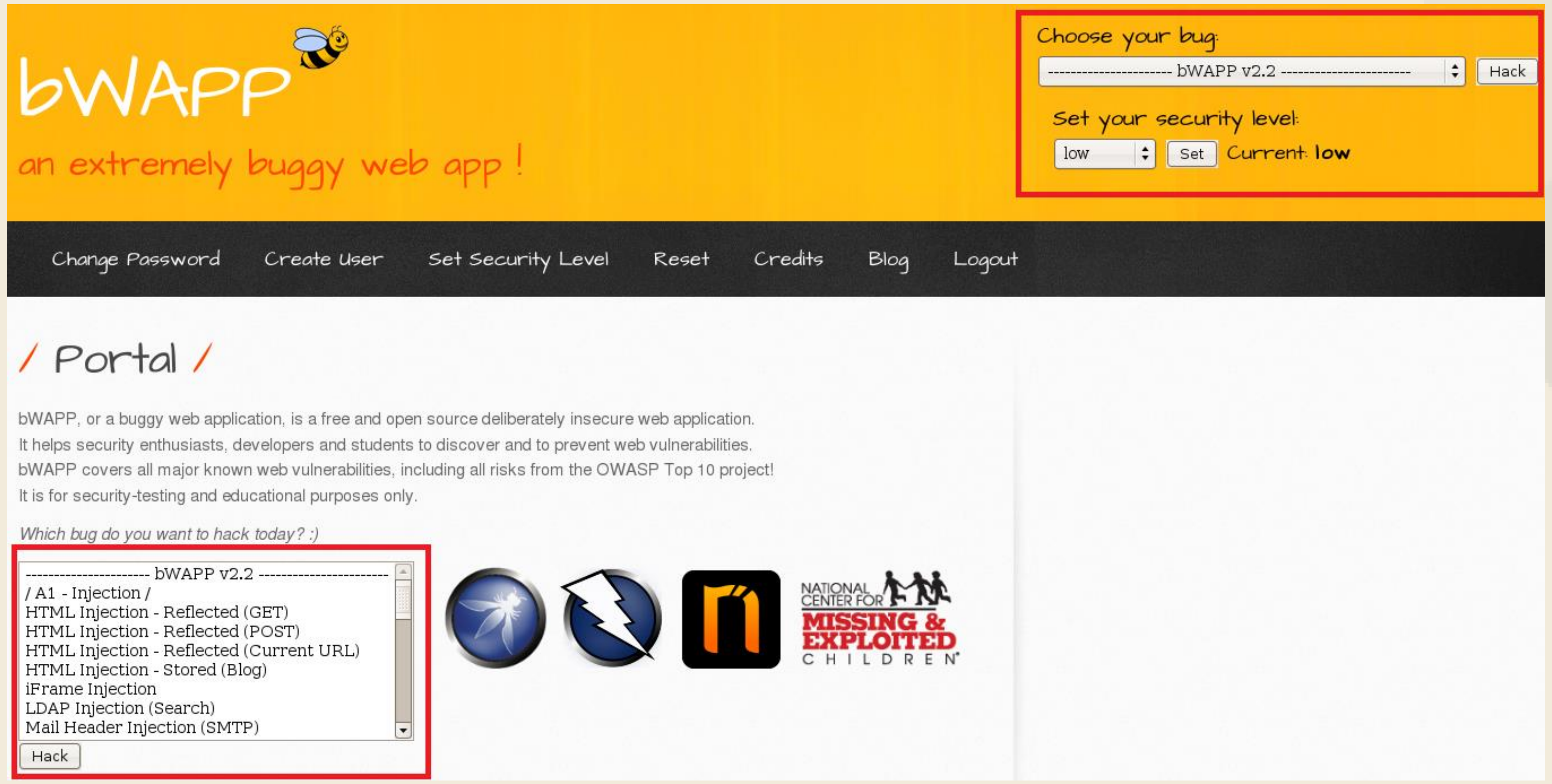
SECURITY
BY
DESIGN

DIY WEB HACKING

A hands-on web security awareness course

TOOLS

- Kali Linux – a hacker's toolbox
- bWAPP – a buggy web application



bWAPP

an extremely buggy web app !

Choose your bug: ---------------------- bWAPP v2.2 ---------------------- Hack

Set your security level: low Set Current: low

/ Portal /

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
It is for security-testing and educational purposes only.

Which bug do you want to hack today? :)

---------------------- bWAPP v2.2 ----------------------
/ A1 - Injection /
HTML Injection - Reflected (GET)
HTML Injection - Reflected (POST)
HTML Injection - Reflected (Current URL)
HTML Injection - Stored (Blog)
iFrame Injection
LDAP Injection (Search)
Mail Header Injection (SMTP)

Hack

PREPARING YOUR ENVIRONMENT

- Download and install VMware Player (if you already have workstation pro, it is recommended to use that). You can also use Oracle Virtual Box but you need to “use existing hard drive” under New-> advanced setting, to launch .vmdk/.vmx files in Virtual Box. VMware seem to run it more seamlessly than virtual box.
- Download bwapp – recommended to download ‘bee-box’ which is a complete VM ready to launch.
- Use VM host (VMware/Virtual box) to launch bee-box. Credentials: bee/bug
- Download kali-linux . Credentials: kali/kali (all lower case, note that the username is also case-sensitive)
- Go to settings for both VMs (in VMware: Player -> Manage -> Virtual Machine Settings -> Network Adapter. Choose “Host-only network connection”). Note that you may need to reboot the bwapp VM to make the new configurations propagate to the web server if you already started your VM.
- Launch both VMs
- On the VMs, it is recommended to open keyboard settings and change keyboard layout to Danish (or which ever language layout your keyboard uses).
- On both VMs ensure they have two different IP addresses (use ‘ifconfig’ in the terminal), make note of the bwapp address, (you can try to ping from Kali to bwapp VM to make sure they can connect)
- On Kali, open a browser and connect to: http://[bwapp IP address]/bWAPP/login.php (The URL may be case sensitive)
- Set up Burp on the Kali VM as Proxy to intercept and modify traffic:
  - In Firefox settings on Kali, go to Proxy: Choose “manual proxy configuration”, for HTTP Proxy, enter: 127.0.0.1 and port: 8080, you can select to also use this proxy for HTTPS.
  - Run command “sudo burpsuite”, enter kali sudo creds (“kali”) and follow default steps to run a Burp project. Ignore the JRE and version warnings. Go to the tab “Proxy”, verify that the proxy settings match what you configured in firefox (127.0.0.1:8080) and under “Response interception rules” enable “intercept response based on the following rules:”, close configurations and then turn on interception, go to the firefox browser, and connect to the bwapp/login.php page again (refresh if you kept the window open), you should now see the traffic being intercepted in Burp, and have to “forward traffic using the “Forward”-button – this allows you to both view and to modify the traffic before it is sent to the bwapp server.
- Note: because bwapp is relatively old and intentionally vulnerable, modern browsers will often try to block you from accessing it. For example, because bwapp does not support TLS 1.2 and 1.1, and uses a self-signed certificate, you will likely encounter errors when trying to access it using https via FireFox on the Kali VM. To fix this, in FireFox type: about:config and change the value for security.tls.version.min to 1. You will still need to accept a warning and add an exception in your browser the first time you connect to bwapp via https.
- Verify that you can connect to bWAPP via HTTPS (see the note above)
- You are ready to hack

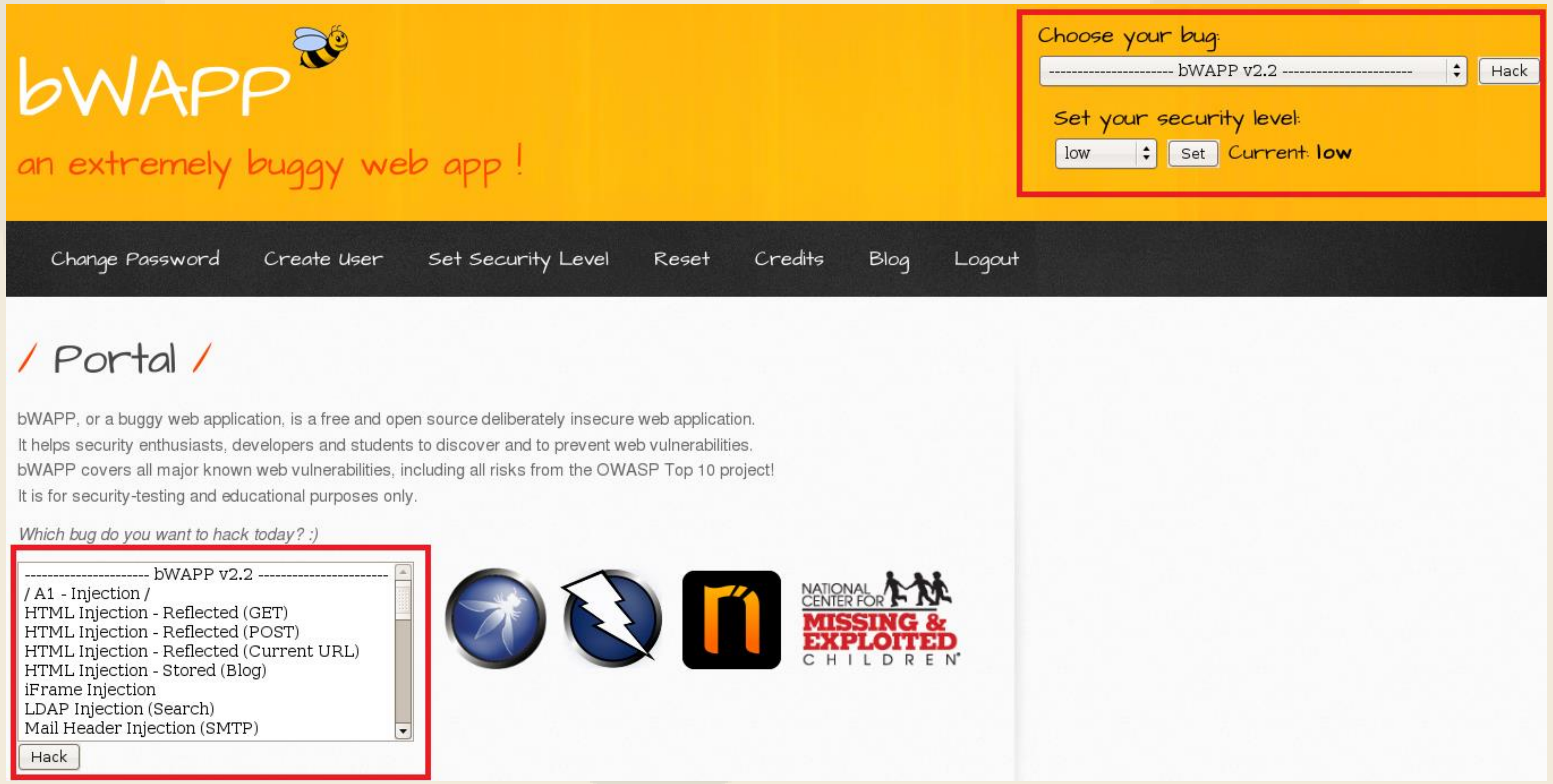
NOTES REGARDING EXERCISES

- The bWAPP site is VERY buggy - modern browsers will detect and block quite a few of the flaws - you may need to exempt the site to have its certificate trusted by your browser to enable HTTPS, allow for weak crypto ciphers etc.
- Unless otherwise specified, all actions/exercises should be performed from your Kali VM with the bWAPP VM running idle in the background. This simulates the view of an attacker, who only has remote access - you will see what the attacker sees and can access only the resources that the web application exposes to the kali VM.
- We use a free version of Burp Suite - it times out and closes from time to time, it is not a bug but a feature (to make you pay them)

Disclaimer: You should NOT under any circumstances use these techniques against a system that you have not expressly been granted permission to attack. (even typing ‘ in an input-field on a webpage could be perceived as an attempt at an injection attack and lead to legislative action)

HOW TO DO EXERCISES

- All exercises are done from Kali against the bWAPP Virtual Machine
- Many exercises requires using the browser to connect to bWAPP but we will also use other tools from Kali, such as wireshark, nmap, Burp etc.
- To get started with the exercises, open a browser and connect to the BWAPP portal (like you did when setting up the VMs)
- Authenticate to the portal using credentials: bee/bug
- You will see a scroll-box menu with a list of exercises.
- Scroll to the exercise you are instructed to and click “hack”.
- You can also access exercises using the drop-down menu at the top right corner.
- This is also the place where you set the security level.
- The security level should normally be set to 1, but you may free-style exercises that are more difficult by increasing the security level



/ Portal /

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
It is for security-testing and educational purposes only.

Which bug do you want to hack today? :)

---------------------- bWAPP v2.2 ----------------------
/ A1 - Injection /
HTML Injection - Reflected (GET)
HTML Injection - Reflected (POST)
HTML Injection - Reflected (Current URL)
HTML Injection - Stored (Blog)
iFrame Injection
LDAP Injection (Search)
Mail Header Injection (SMTP)