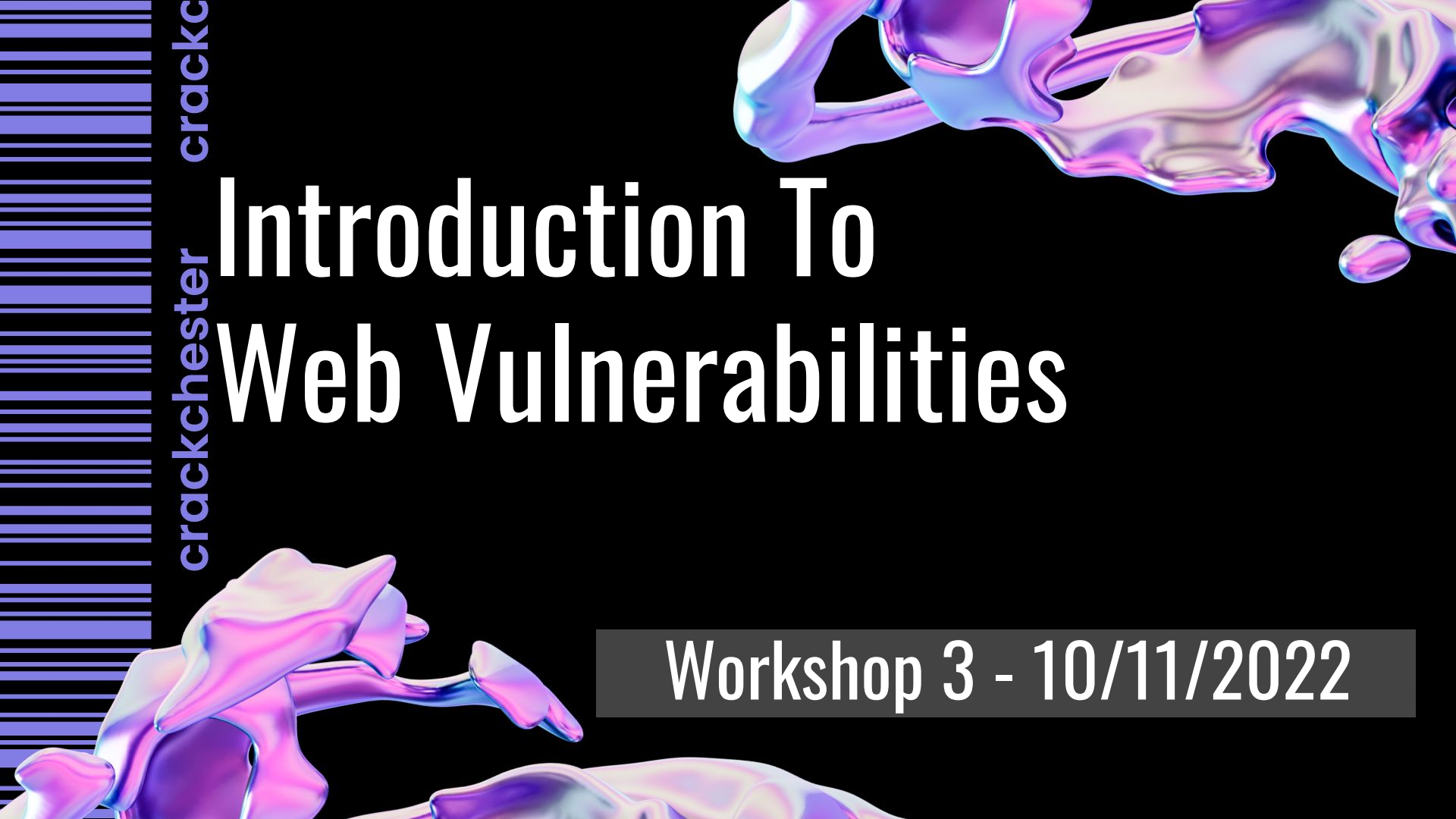
crackchester crackc
Introduction To
Web Vulnerabilities
Workshop 3 - 10/11/2022

Kali Linux

To save time in future workshops, and to provide you with a suitable toolkit, we recommend installing a kali linux VM. Kali linux is a debian distribution designed for penetration testing. If you don't have a VM framework, we recommend either VMware or Virtualbox, this will be the program you use to launch the Virtual Machine. After you have your VM software installed

1. Head to https://www.kali.org/get-kali/ and select Virtual Machines
2. Select your VM software and press the download button
3. Once this download is complete, extract the file
4. Launch your VM software and press Add, then select the Machine image we just extracted
5. Adjust the settings to suit your system
6. Once installed, boot up the VM
7. Login to Kali using the Username & Password: kali / kali

Unlike Most VMs Kali is a very specialised tool, for this reason we recommend that you don't use tools that you are not familiar with, as many of them can be unsafe if used incorrectly. If you want to learn more about kali and it's tools feel free to message the society discord and we'll try to get back to you!

Web Vulnerabilities

Using kali tools within web application analysis

Metasploitable for practising

Nmap (sudo apt-get install nmap)

SQLI

Works using data entry to manipulate database

Can be difficult to figure out

For number entry `105 OR 1=1` into `SELECT * FROM Users WHERE UserId = 105 OR 1=1;`

For text entry `" or ""="` into `SELECT * FROM Users WHERE Name ="" or ""=""`

There are tools that simplify the process

Damn Vulnerable Web Application(DVWA)

Install dvwa on kali `$ sudo apt install dvwa`

Starting the webpage `dvwa-start`

SQL Map

Sqlmap will scan for vulnerabilities

Navigate to 10.205.142.179, find the login page

SqlMap this url `sqlmap -u (url here)`

Fuzzing

Detecting hidden pages

Finding login/admin pages

Require a target and payload

Navigate to Documents

Clone payload from Github, using seclists

WFuzz

```
wfuzz -c -f sub-fighter.txt -Z
-w /usr/share/wordlists/wfuzz/general/big.txt --sc
200,202,204,301,302,307,403 http://10.205.142.179:42001/FUZZ
```

WPScan

Used for finding wordpress vulnerabilities

Announcements:

- Social Week after Reading Week

- Hoodie competition

Crackchester Open Positions:

Put yourself in the running for our new Podcast Officer position here!

Apply to join our Dev Team here!

Crackchester

Here’s a link to our link tree where you can find all our socials and our discord!


crackchester crackchester
chester
Demonstration