While We Wait to Start…

- Please complete the survey: https://bit.ly/3mtkIqN

Please note, all survey results are anonymized (so we cannot identify you) - you may be asked to sign in, but this is only to confirm that you are a Coventry University Student & your details will not be recorded. If you wish to invoke your GDPR rights, please send me an email (ComSec@live.coventry.ac.uk).

This is really important to us, as lecturers & students are putting a lot of time into this. So please help us, help you!

- Jack, Martin & Tiago

Website Exploitation

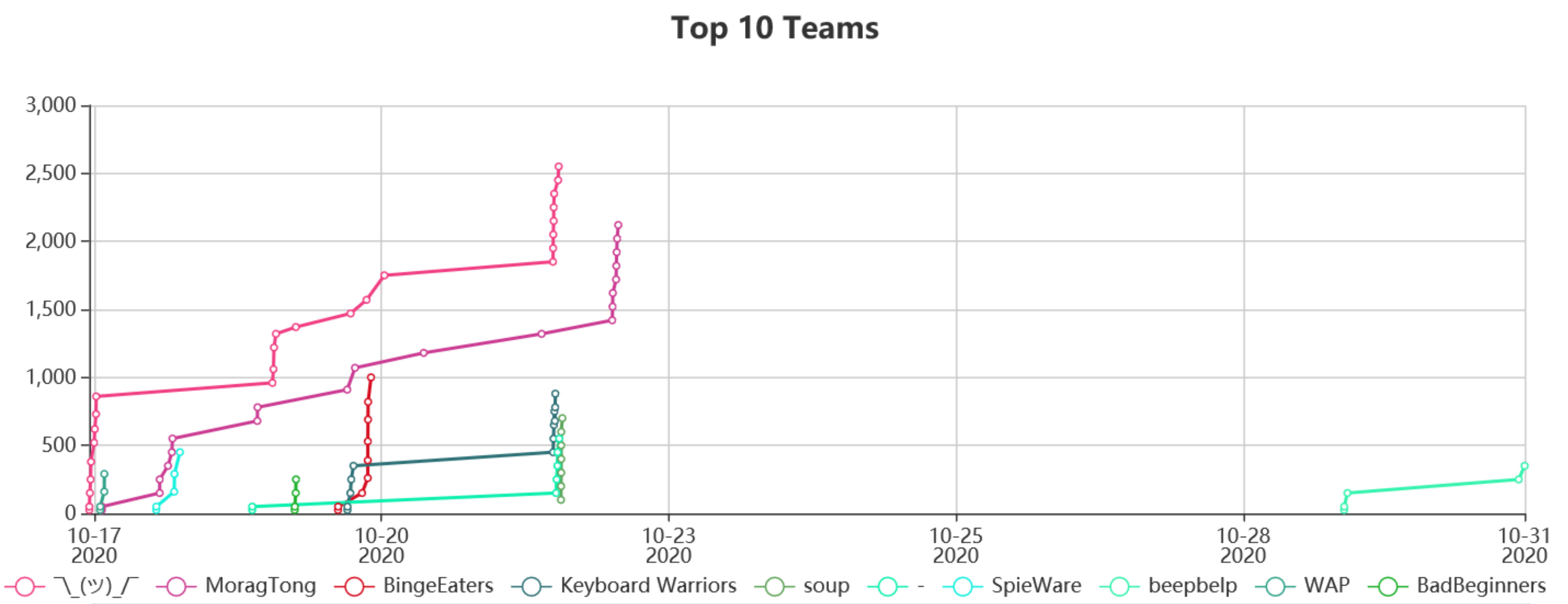
Coventry University ComSec

By Jack Orcherton

Remember to view our Legal/Terms of Use Statement

A Quick Catch Up

- Congratulations to Richie for staying at the top of the leader board!
- Check out our new website - cov-comsec.github.io/
- Complete the survey! bit.ly/3mtkIqN



Remember to keep on top of the latest CTFd challenges! (cueh-comsec.ctfd.io/). 1 new HOPR challenge!
Struggling to find a team to work with – drop us an email – Comsec@live.Coventry.ac.uk / contact us on Discord!

More ComSec?

- Can’t get enough of ComSec? Well join us every Thursday, 15:00 – 21:00.
- Informal sessions where we complete online challenges from HTB & THM
- May play KOTH

- **Note:** May be delayed start this week due to us having an exam. Will definitely be available from 17:00 onwards

Good Notes – Making Life Easier!

- Always make notes when hacking (otherwise you forget stuff or miss things)
- Many ways to make notes – make sure you pick the best for you:
  - Jack – OneNote or Markdown Files
  - Martin – Joplin
  - Tiago – Obsidian.md
- Keep them short and sweet – record program outputs like Nmap
- View Dan's example here.

Markdown Crash Course

- Same syntax as Discord/GitHub
- # Make a Heading
- ## Make a smaller header (can use up to six #)
- *make this italic*
- **make this bold**
- ***make this bold & italic***
- [Enter text](enter hyperlink)
- Inline embed `test`

```python
print(“Format this code like Python”)
```

What is Website Exploitation?

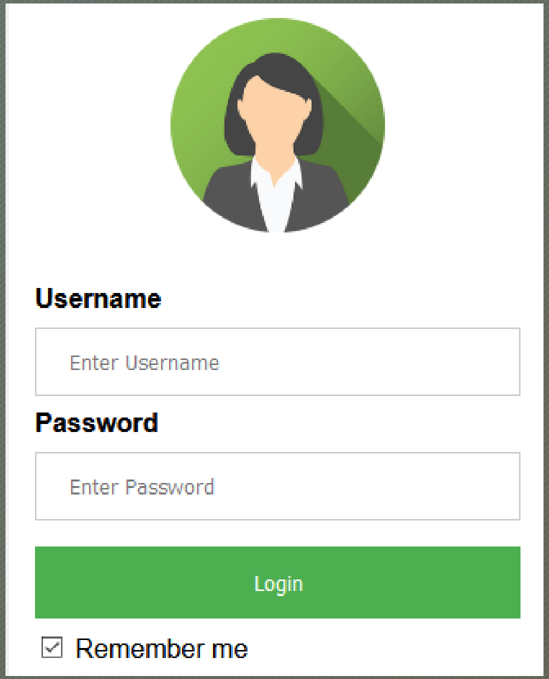
- The act of trying to gain access to a website. This can be achieved through many tactics.
- OWASP is a non-profit organisation that publishes the top 10 most prevalent types of exploitation:

1. Injection	6. Security Misconfigurations
2. Broken Authentication	7. Cross-Site Scripting (XSS)
3. Sensitive Data Exposure	8. Insecure Desacralisation
4. XML External Entities	9. Using Components with Known Vulnerabilities
5. Broken Access Control	10. Insufficient Logging & Monitoring

(OWASP, 2017)

Injection – a Big Topic

- Typically SQL injections – by entering malicious data in fields in order to receive data.



SELECT * FROM userTable WHERE name="?"

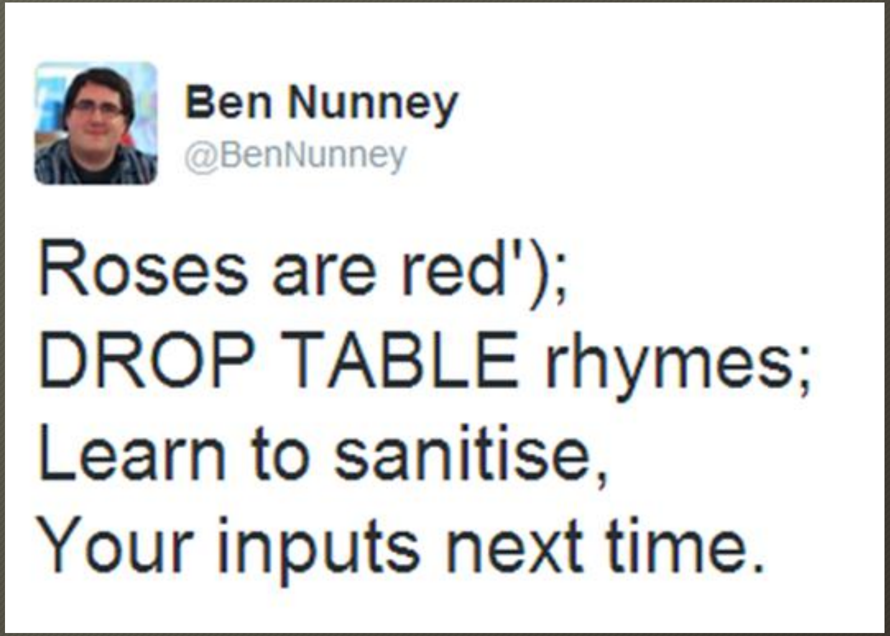
SELECT * FROM userTABLE WHERE name="Jack"

What malicious stuff can you do with this?

- Bypass Authentication "or 1=1 --
- View, modify/delete records "; drop table [name] --

Making Life Easier – SQL Map

- Our time is precious (and we don’t want to waste it typing in random commands)
- Lets automate using SQL map
- General command: sqlmap –a –u ‘http://example.com’
  - Runs all scripts against an URL
- Demo Time !

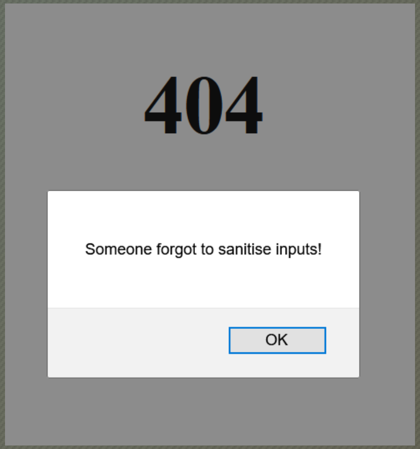


Ben Nunney
@BenNunney

Roses are red');
DROP TABLE rhymes;
Learn to sanitise,
Your inputs next time.

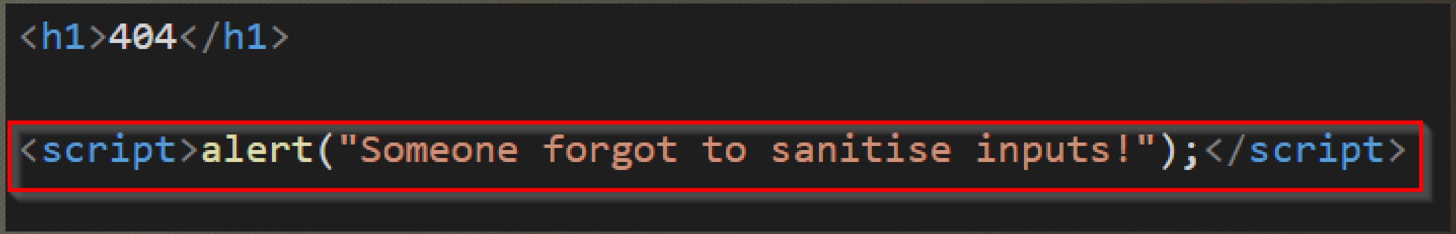
Cross Site Scripting (XSS)

- When clients are able to inject html commands into an input field.
- Problem with this is that they can use the script HTML tags they can add JavaScript
- Commonly web forums are susceptible to this sort of attack
- Easiest way to test – try adding an alert box



404

Someone forgot to sanitise inputs!



```
<h1>404</h1>

<script>alert("Someone forgot to sanitise inputs!");</script>
```

It’s just a pop up!

- With JavaScript you are able to do more evil things:
  - Steal cookies & send them to a remote server (could lead to session hijacking)
  - Deface websites (E.g. create tech support scam pop-ups)
  - Preform actions on behalf of the user (such as transactions)
  - Create iframes – this can allow you to embed different webpages into another. One use of this could be to spoof a login page (so instead of logging in they send credentials to your server) – great for phishing!
  - Capture keystrokes
  - Read all the data on a victims webpage (could reveal sensitive information).

To find out how to do the above, click here!

Sensitive Data Exposure

- When websites accidently expose/leak sensitive data
- Could be in transit – using HTTP/unencrypted communication
- Having public S3 buckets/insecure databases
- Leaving keys in Git repositories / view previous website archives
- Using unprotected passwords
- Leaving API keys/admin credentials in code comments

This Week’s Challenge

- Let’s use DVWA – this can be run locally or on THM (need an account)
- Connect to the THM VPN
- Open up the DVWA room & deploy
- Start hacking the SQL & XSS challenges
- Enter flags you find on CTFd

Go Further

- Read into the other OWASP Top 10
- Complete TryHackMe OWASP Top 10
- OWASP Juiceshop
- Mutillidae
- Look at previous website breaches (and how they were achieved), (Bugcrowd and Hackerone reports are a great source)

See you next Wednesday @ 18:30

Any feedback or questions?

Thank You!

Ensure you complete the survey: https://bit.ly/3mtkIqN