Group A:
Alexandar Kraunsøe, Christian Lind, David Blum S., Kasper Pagh & Marco S. Blum.

It will be assumed that the group is a firm and that the codebase is intellectual property and the Database holds sensitive data

Attacker types:

Likely attackers (for us):
Script kiddies - Low threat, low profile
Black hat groups - Hight threat, high profile

Unlikely attackers (for us):
Government groups - Hight threat, political profile
White hats - Low threat, political profile

Security - threat model

Secure from what?

- The who/where

Our system is most likely to face attacks from either script kiddies or black hat groups. Our platform is a news site so Government groups does not have much value in hacking it, though they might profit from manipulating the information available on the site. White hats will likely not hack the system either as the system is not a high profile, and we do not host anything illegal, nor are we a fortune 500 company, so there is not much of a monetary reason to do so.

Script kiddies will certainly try out the open ports or other vulnerabilities.
Black hat groups is unlikely to target us as we are not a high profile target, so they can not get any political gain nor monetary gain from us.

What are you protecting?

- The what

We will mostly be protecting our database, as it contains sensitive information. However we cannot stop people from making scripts that manipulate the frontend, as in creating multiple accounts or downvoting specific subjects.

When are you secure?

- Vulnerabilities

Open ports, Our server is not, as of yet, protected behind a firewall - this is since we, accidentally, made it impossible to access our buildserver due to a misconfiguration of the servers firewall. This have made us hesitant to configure the production server firewall.
Github, public repositories can easily be snooped on, private repositories are more secure but github can still be hacked.
Personal Accounts, In case personal accounts are compromised and we use the same password for more than one platform.

Group A:
Alexandar Kraunsøe, Christian Lind, David Blum S., Kasper Pagh & Marco S. Blum.

DOS, We are potentially vulnerable to various DOS attacks[1]. This is since we have very little logic to determine whether incoming requests are malevolent in nature. This means we someone could use "*Slowloris*"[2]
Dockerhub, this have the same insecurities as github.
Physical Theft, as in stealing of computers or other property. If gained access to, they could get ahold of public and private keys for ssh, passwords for various platforms, sensitive information, blackmail material.
Jenkins, the hackers would then gain complete access to the CI chain, and could use that for various things.

- The how

We have not implemented much security as of yet, but we will try to implement so that only the frontend ip and Helges ip can be used to post to the backend. We could also use private repositories on github as we are currently hosting it in a public repository, which makes it highly likely that somebody will find our repository and use the knowledge it contains against us. We could update our passwords regularly so that they do not get stolen.

Risk Matrix

	Negligible	Marginal	Critical	Catastrophic
Certain	Open ports			
Likely				DB hacked
Possible		DB error	Github, DockerHub	
Unlikely	DOS		Jenkins	
Rare		Personal Accounts	Physical Theft	

Assessment of vulnerabilities of the ops group.

We have tried on multiple machines to get owtf to work, 7 to be exact, one with linux and the rest with windows. None have unfortunately worked. We are sorry we cannot fulfill this requirement.

[1] DOS stands for **D**enial **O**f **S**ervice. The most common type of DOS attack is the DDoS (**D**istributed **d**enial **o**f **s**ervice).
[2] https://en.wikipedia.org/wiki/Slowloris_(computer_security). A type of DoS attack, that relies on keeping a high number of requests open at any given point. This is achieved by sending a partial http requests very slowly.