



When web applications are set up, every action performed by the user should be logged. Logging is important because in the event of an incident, the attackers actions can be traced. Once their actions are traced, their risk and impact can be determined. Without logging, there would be no way to tell what actions an attacker performed if they gain access to particular web applications. The bigger impacts of these include:



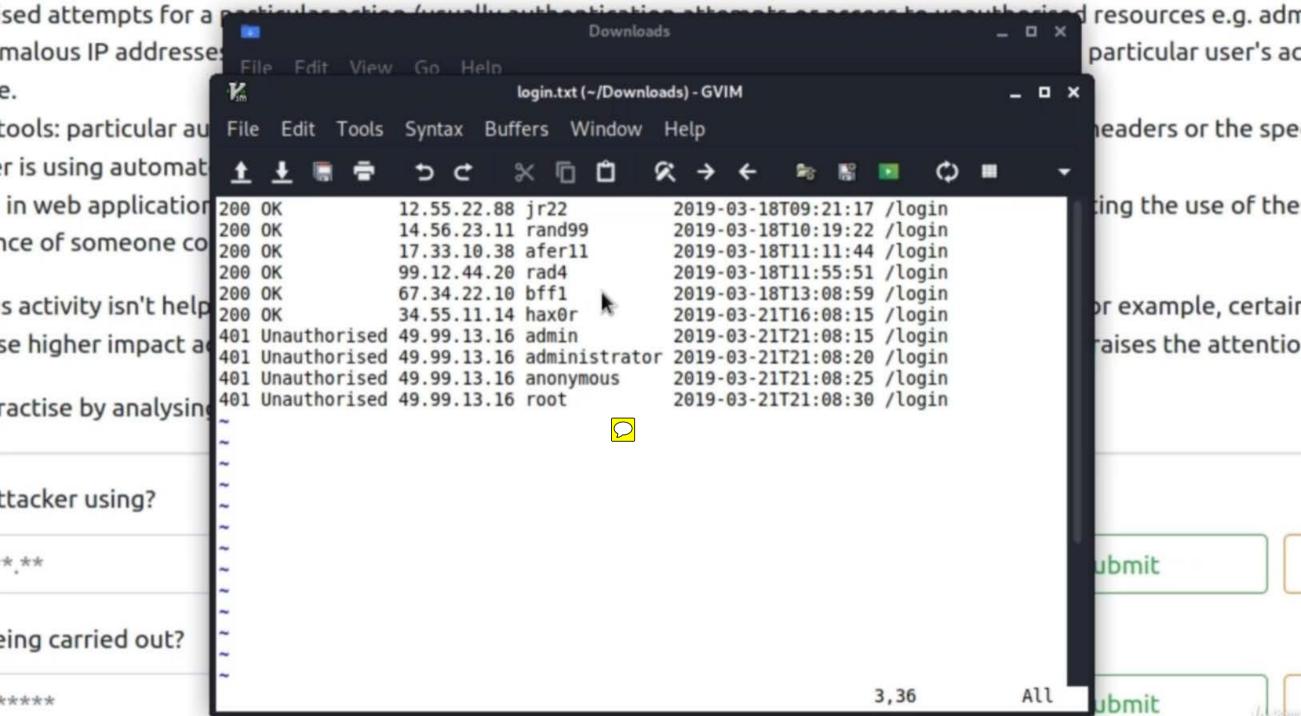
- regulatory damage: if an attacker has gained access to personally identifiable user information and there is no record of this, not only are users of the application affected, but the application owners may be subject to fines or more severe actions depending on regulations.
- risk of further attacks: without logging, the presence of an attacker may be undetected. This could allow an attacker to launch further attacks against web application owners by stealing credentials, attacking infrastructure and more.

The information stored in logs should include:

- HTTP status codes
- Time Stamps
- Usernames
- API endpoints/page locations
- IP addresses

These logs do have some sensitive information on them so its important to ensure that logs are stored securely and multiple copies of these logs are stored at different locations.

As you may have noticed, logging is more important after a breach or incident has occurred. The ideal case is having monitoring in place to detect any suspicious activity. The aim of detecting this suspicious activity is to either stop the attacker completely or reduce the impact they've made if their presence has been detected much later than anticipated. Common examples of suspicious activity includes:



Created by ben