Door-Unlocker

Description

Door-Unlocker is a service that provides authorized users with access to private spaces. This document details the comprehensive security policy and measures taken to ensure user safety, protect user data, maintain expected system behavior, and prevent malicious activities.

Active precautions

Focus

- Code of conduct
- Session management
- User data
- System integrity

Code of conduct

Keeping the space safe is a task that both the users and administrators must engage in considering any bad actors in the system would be capable of compromising its integrity. As such, in order to use the service, users must accept and agree to the details and procedures outlined in this document.

Do

- Remain vigilant for unusual occurrences, verifying the authenticity of the site by its certificates and potential warnings. These occurrences can indicate attacks on the service.
- Be aware that you are considered responsible for any individuals you let into the space, which includes holding the door open for those behind you as you enter the space
- Know that there will be additional security measures in place to further reinforce desired user behavior such as video monitoring and the usage of facial recognition software

Do not

Users are encouraged to avoid behaviors that may falsely flag and deactivate their account which includes, but is not limited to;

- Spam the server
- Log in too many times
- Attempt to use the unlocking functionality away from the space’s premises
- Share your account credentials with others

Note that both spamming the server and or logging in repeatedly will get your account deactivated to protect the server against DDoS and brute force attacks.

Session management

Careful Cookie Handling

Managing sessions will largely depend on careful cookie handling and all active sessions will be managed by the database until they expire or close. During transactions, cookies will be chained meaning they are frequently changed, which, alongside the use of http only, secure and same site cookie attributes, makes them near impossible for third parties to obtain or use in potential replay attacks.

Restricted HTTP verbs

Furthermore, the communication verbs track and trace are both disabled. Any and all anomalies detected which include the use of expired credentials, invalid requests, invalid redirections and the use of old cookies will alert the system. Note the only external requests that users should expect will occur during the zero authentication process during login.

User data

Handling

Protecting user data is equally as important to the Door-Unlocker service. As such, all user data will be obscured and encrypted using modern day techniques such as data salting and peppering which combines user data with randomly generated data before it is stored, as a hash value. These practices will be applied to both user and log data which will be regularly backed up and encrypted.

In case of attacks

That is, in the event data is stolen from any database it should be difficult to use, thus adding additional layers of security against data breaches especially considering only the minimum amount of user data will ever be stored.

Transparency

Lastly, any and all privacy concerns are taken into consideration and users can request copies of their data whenever they like.

System integrity

Arguably most important to the Door-Unlocker service is establishing system integrity in which a multifaceted approach is used to achieve this goal.

Background checks

First, administrators should conduct background checks on new members to validate their authenticity and trustworthiness before they can start using the system.

Strong passwords

Secondly, by using a zero authentication scheme, users will need to use their accounts that already exist with other services. These external services will be considered based on their password strength requirements ultimately leading to a more safe system with passwords that are more difficult to obtain.

Injection attacks

Thirdly, all system requests will be validated to prevent injection attacks in all its forms, including cross-site scripting and SQL injection. Using frontend frameworks to prevent cross site scripting, prepared statements from database libraries to prevent SQL injections and backend logic to ensure appropriate data constraints.

SSL encryption

Fourthly, SSL encryption is implemented to encrypt exchanges between users and the server. This has the added effects of protecting users against DNS poisoning attacks and man in the middle attacks therefore ensuring users are sent to the correct sites and ensuring the message authenticity.

Physical security

Fifthly, physical security is also a priority, as the server's physical location is critical to ensure hardware integrity which is why all hardware will be secured, requiring a key to access these resources. Keyloggers will be installed to record any and all changes made to the server, and video surveillance will be recorded at all times for review and storage on a weekly basis.

Ultimately, these measures help prevent breaches caused by manual overrides, service alteration as well as the addition of untested, potentially malicious or unsafe software and or hardware.

Network security

Sixthly, service hardware will only be connected to private networks connected strictly using ethernet cables to prevent packet sniffing where only preset authorized devices will be permitted. All other traffic and use of other ports will be non-permissible.

System monitoring

Seventhly, to enhance transparency, debuggability and accountability, extensive logging of all user actions and systems events are conducted at both the server and application levels. This ensures that any suspicious activities or anomalies are promptly identified and addressed, and

that all administrative actions are closely monitored in the event any administrator’s account is compromised.

In such a case, knowing what actions they take is critical to reverse potential unauthorized changes after removing the account from the system and the subsequent attacker.

Problem resolution

Communication

In the event issues arise, users can trust that proper measures will be taken to communicate service availability, data breaches, potential threats to the system as well as incoming changes to minimize risk and damage. That is, all of which will be communicated on the associated service’s social media account.

Disciplinary action

Suspicious activity should be reported immediately. Users who fail to do so, or disobey any of the rules outlined in this policy risk termination. Illegal activities will warrant law enforcement, should the need arise.

Serious issues

In the event a serious issue arises, services may experience temporary downtime soon after. If it can be handled swiftly services would return shortly after, otherwise, for more complex or persistent issues, a different strategic approach will be taken. The site will be taken offline, users will be notified, the system's data will be falsified to be used as a honeypot to further study any of the issues at hand until a better understanding and solution can be reached.

Final note

Lastly, this security policy can be found on the website's help page, where it will be annually reviewed and updated to accommodate any and all changes in technology, regulations, and threats.