Cred.

IT Security

JavaScript

1. All scripts are minimised, uglified and concatenated to a single JavaScript file. This has two major benefits.
    a. The file size is reduced which increased download speed and reduces bandwidth requirements.
    b. The JavaScript file is totally unreadable. This prevent potential hackers learning the internal workings of the code.
2. A Request Verification Token is sent with every request ensuring that a session cannot be high jacked as the request needs to be paired with a UI verification token.

User Interface

1. Cross-site scripting (XSS) prevention with automatic data encoding. All potentially dangerous or malicious data entered by the end user, for example trying to save <script> tag to the database, is encoded to the safe a string equivalent &lt;script&gt;
2. Cross-site request forgery (CSRF/XSRF) prevention with anti-forgery form field meaning that a user's session cannot be high jacked by a potential hacker.
3. No Inline code in the UI means that potential hackers cannot get insight in to the underlying implementation of the code and platform.
4. No online registration. We do not allow users to register with Cred through an online registration form. Every user is added through Cred Hub ensuring that every user in the database is known to the Organisation to which they belong.
5. Data and user validation on ever post request. There are 4 levels of data and user validation on every request
    a. Every request must come from a valid authenticated user.
    b. Every request must be accompanied with a valid request token.
    c. Access to a resource on every request must be accompanied with the correct user role access.
    d. Every piece of data is validated before it is passed on to the service layer.
6. Framework details removed from response
    a. A lot of detail is returned in a response from a web server. This can give details of the framework used and hackers can use this to understand and exploited potential security loopholes in the framework. By removing this response information, you remove this potential loophole.
7. Cookies encrypted and can only be transported over SSL
    a. All cookies are configured to ensure that they cannot be read using scripts and must be transported over SSL
8. Sliding timeout set to 1 hour

   a. If a browser is left idol for an hour, Cred will automatically sign the user out. We use a sliding expiration property meaning the timeout is reset when in use so the user will not bed signed out while using Cred hub.

9. Max request set to 4mb reducing potential DOS attacks
   a. One of the ways that attackers perform DOS attacks on websites is to send huge requests to the server in an attempt to bring the server down. Azure has automatic DOS detection built in but we also reduce the max request length to 4mb thus reducing a possible DOS attach even further.
10. Failed login count.
    a. Every failed login attempt is counted and recorded. If this count reaches a predefined number, future login attempts are rejected for that user for a period of 15 minutes before the user can try again.
    b. No hint is given to the user if it is their Email/mobile number or password that is incorrect increasing the number of permutations required to login.
11. Error pages
    a. Custom error pages created for the following common server responses
       i. Errors
       ii. Not found
       iii. Access Denied
       iv. Forbidden
    b. A lot of potentially dangerous information can be displayed in an error messaged returned by the server. By creating custom error pages, we hide the details of these error from the end user.

Web Services (API)

1. Hosted in Microsoft Azure
   a. This provides all the security features inherited by default when using Microsoft Azure including physical security of the API along with malicious penetration and DOS attacks detection.
2. Service calls protected using API Key/Value pair
   a. All request must include a valid 32 character GUID when calling in to the API. Without this the call is rejected at source. The correct Key name must also be supplied.
3. All calls to the API are made over the secure communication protocol HTTPS
   a. All data must be transmitted securely with HTTP over SSL.
4. Restricted data transport. Cred only transfer data across HTTPS that is required for each request. For example, if a request is made to return an individual’s Name and phone number, no other information is retrieved from the database and transported across the network.
5. Data validation on ever post and get request
   a. Along with the API key/value pairing, all data must pass validation both of the data type and content before it is processed. If any validation fails, the request is rejected.

Database

1. Database held in Microsoft Azure data centre
    a. The Microsoft data centre is PCI compliant and although Cred does not store or transport any credit card or bank details, the database still benefits from the security that is required for PCI and is provided by Microsoft.
2. Guids as ID
    a. Guids are a 32 character unique identifiers that are virtually impossible to guess or cause a collision. Cred use Guids for all identifiers on all database table to ensure that an individual or organisations ID cannot be guessed. The Organisation ID is also stored against each table ensuring that data is never accidently shared. We do not return data without the Organisation ID being included in the request.
3. Password encryption.
    a. All passwords are stored using a hashing function and salting algorithm. The password once set cannot be read and cannot be retrieved. If someone forgets their password, the password must be reset as we cannot read it or send it.
4. Data masking
    a. As part of SQL Azure, we have implemented Data Masking on all sensitive data. For example, the first and last name, email address and mobile number of individuals are all masked with random characters. Unless a user has privileged admin access, if they write a SQL statement to retrieve sensitive data, they will be served with a masked version of the data that is not readable.
5. Transparent Data Encryption
    a. All of Cred's data is protected using Transparent Data Encryption (TDE). TDE helps protect against the threat of malicious activity by performing real-time encryption and decryption. So, all data at rest is encrypted at all times.
6. IP whitelist
    a. Only verified IP addresses can access the SQL Azure database. These IP addresses need to be approved by Cred and can only be set within the Azure management portal. All request from IP addresses not on this list are rejected.
7. Very long random password on database
    a. The database is protected with a very long random password. We also only have given access to one user so has eliminate the possibility of granting too much access to users.
8. Auditing configuration
    a. Database auditing is configured to ensure that all activity on the Cred database is recorded for auditing purposes.
9. Threat Detection configuration
    a. Database threat detection is configured on the Cred database. Azure constantly monitors the database for any suspicious or potentially malicious

activity and notifies the correct parties within Cred to ensure that the correct course of action is taken.

10. Automatic data backups
    a. All data is backed up at least one every day and stored for 90 days.
11. No unnecessary data stored in database
    a. Cred makes security and privacy of data as their number one priority. Care is taken to ensure that we only capture, transport and store data that is vital for Cred to operate. At this time we do not capture address information or full DOBs for individuals. If we ever need to capture sensitive data, that data will be protected with every defence possible both while it is at rest (using TDE and data masking) and in transport (using HTTP over SSL).