iUnite Security

Overview of Security Measures within iUnite

Topic Overview

- Encryption & Database Security
- Security Before Page Loads
- Security During Page Loads
- Login & Form Security
- Scans, Alerts, & Monitoring

Encryption & Database Security

- What is encryption?
- How does it work?
- Types of encryption
- Encryption at Rest
- Minimalistic data access

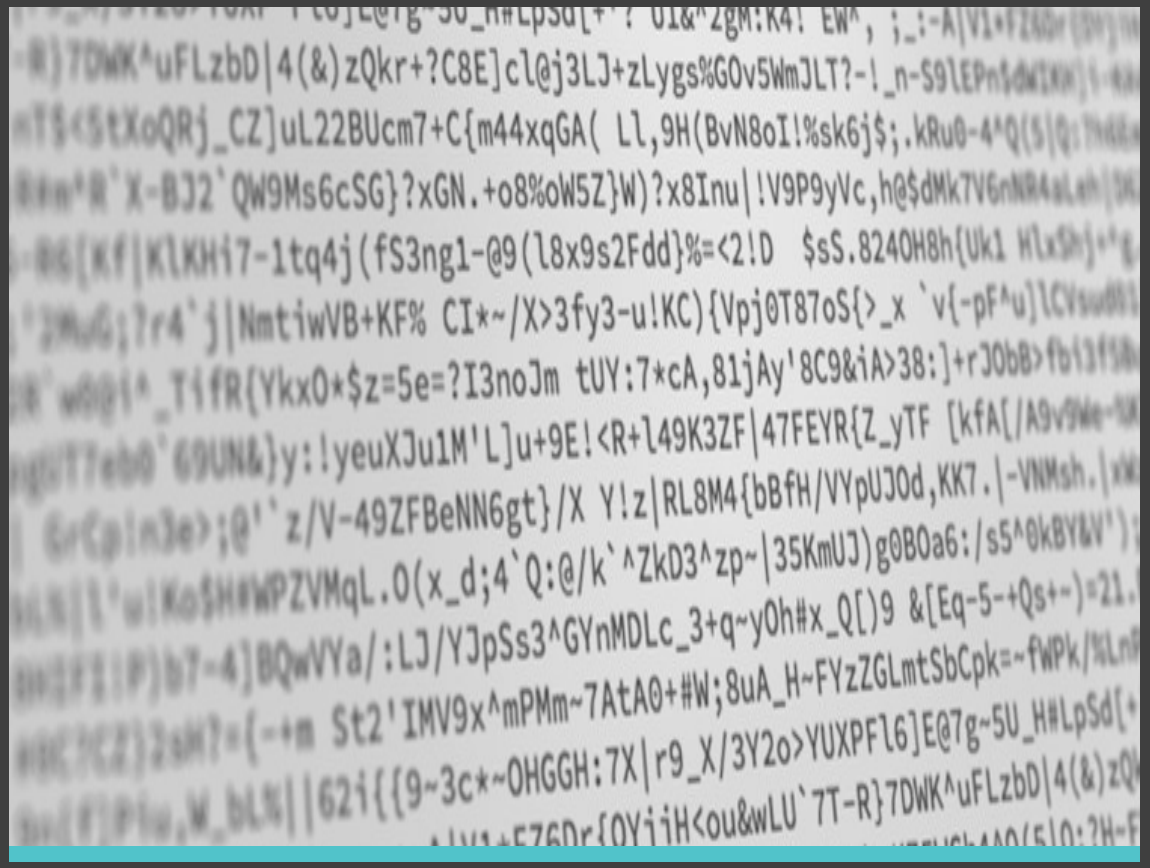
What is encryption?

Encryption & Database Security

Encryption is a process that takes readable text and makes it unreadable.

Example:

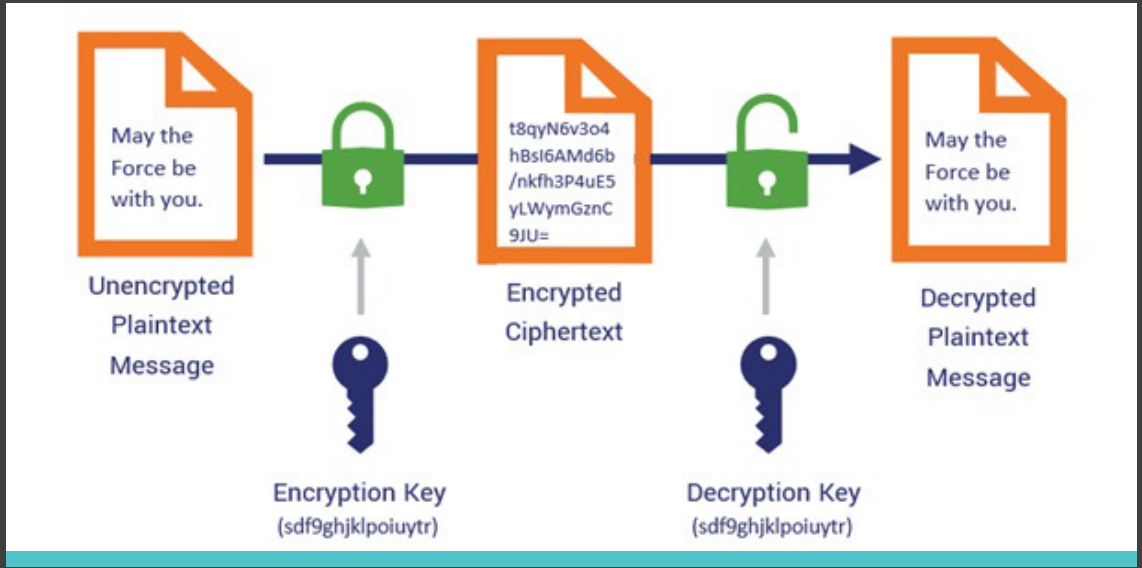
This is plain text. → dcd5d8dbabe2536a7eed30e61474005f3df4d7ba0a921fe3a12c6b0f62dc8741



How does it work?

Encryption & Database Security

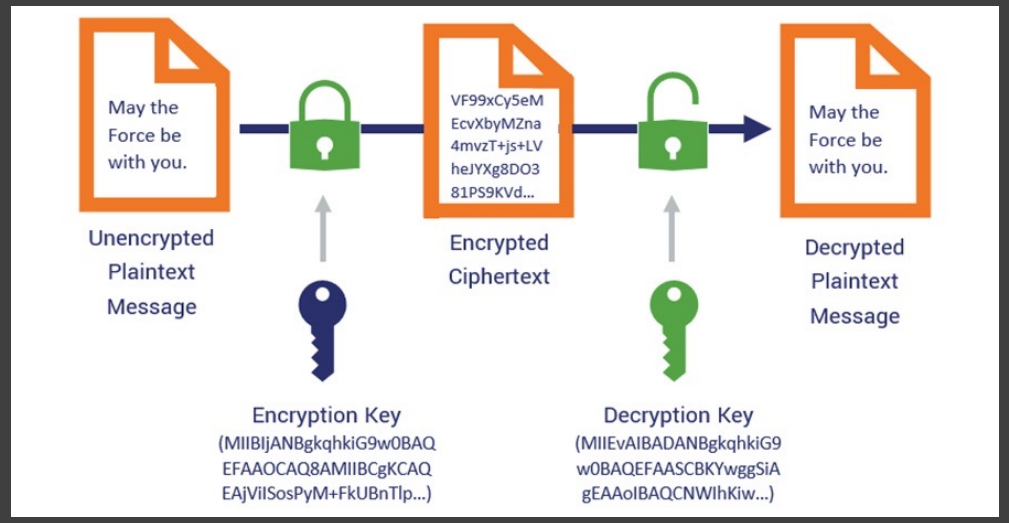
- Encryption function turns original data into unreadable “cipher text.”
- Cipher text is sent to intended recipient.
- Recipient has a “secret” encryption key used to turn the cipher text back into the original data.



Types of encryption.

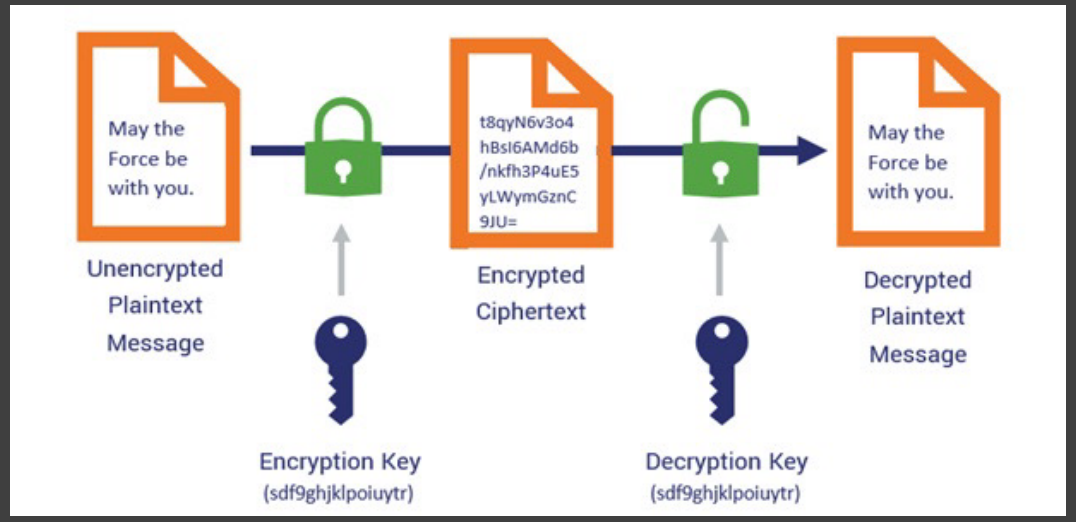
Encryption & Database Security

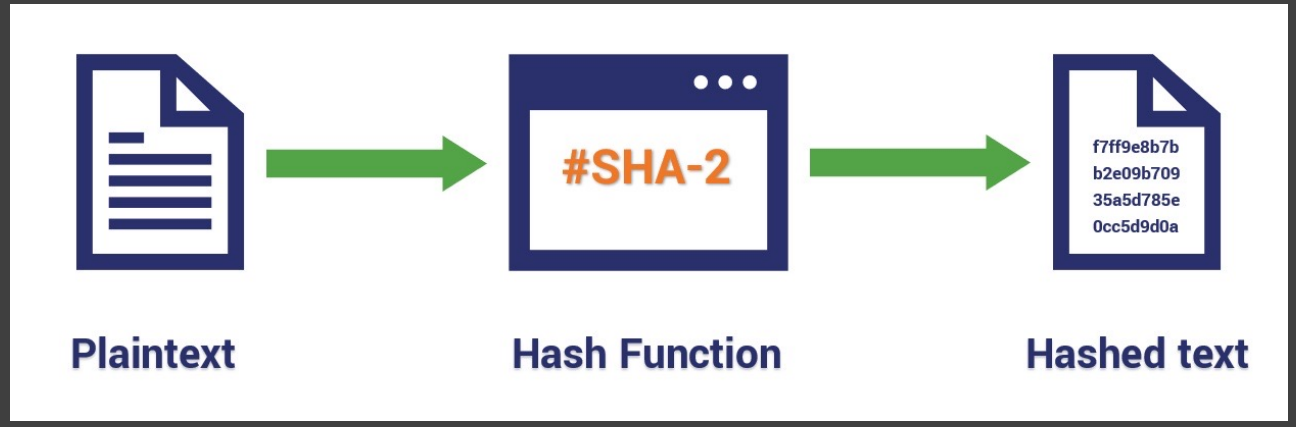
Symmetric Encryption



Hashing

Asymmetric Encryption

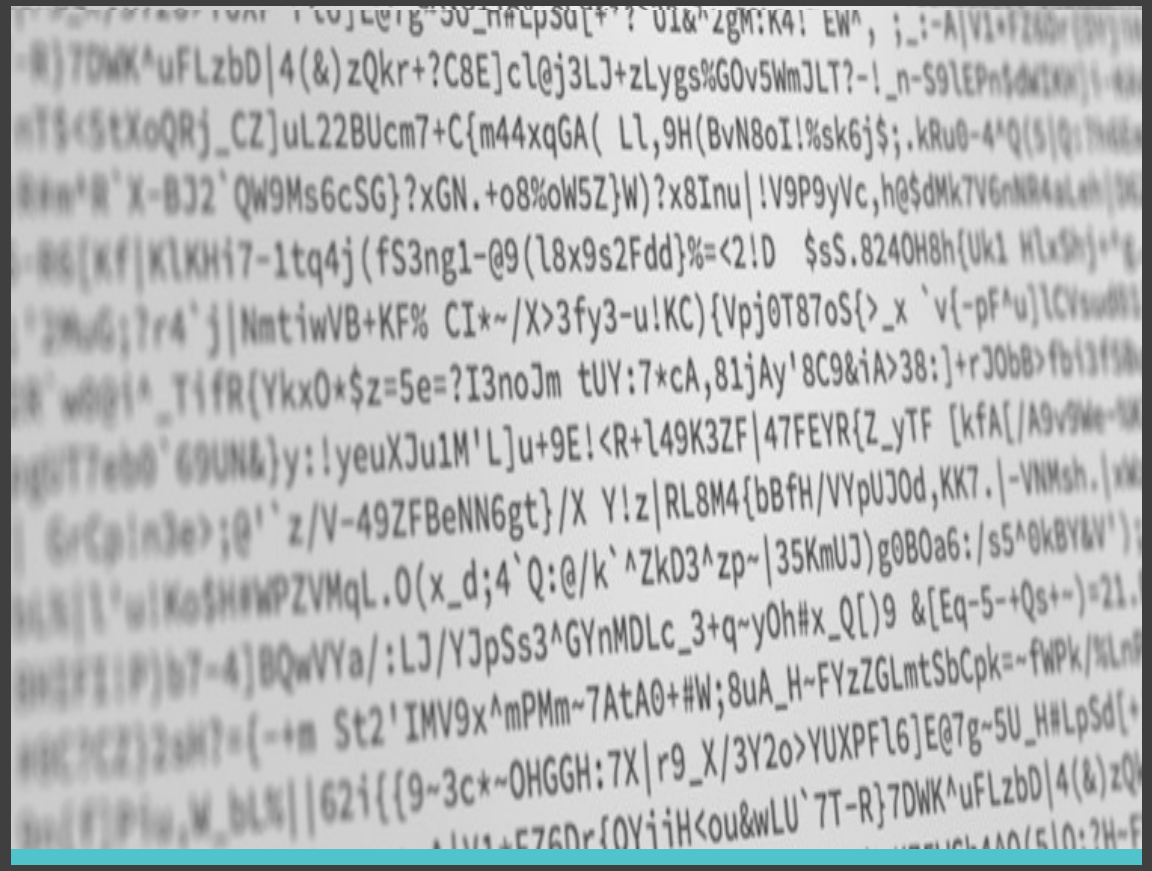




Encryption at Rest

Encryption & Database Security

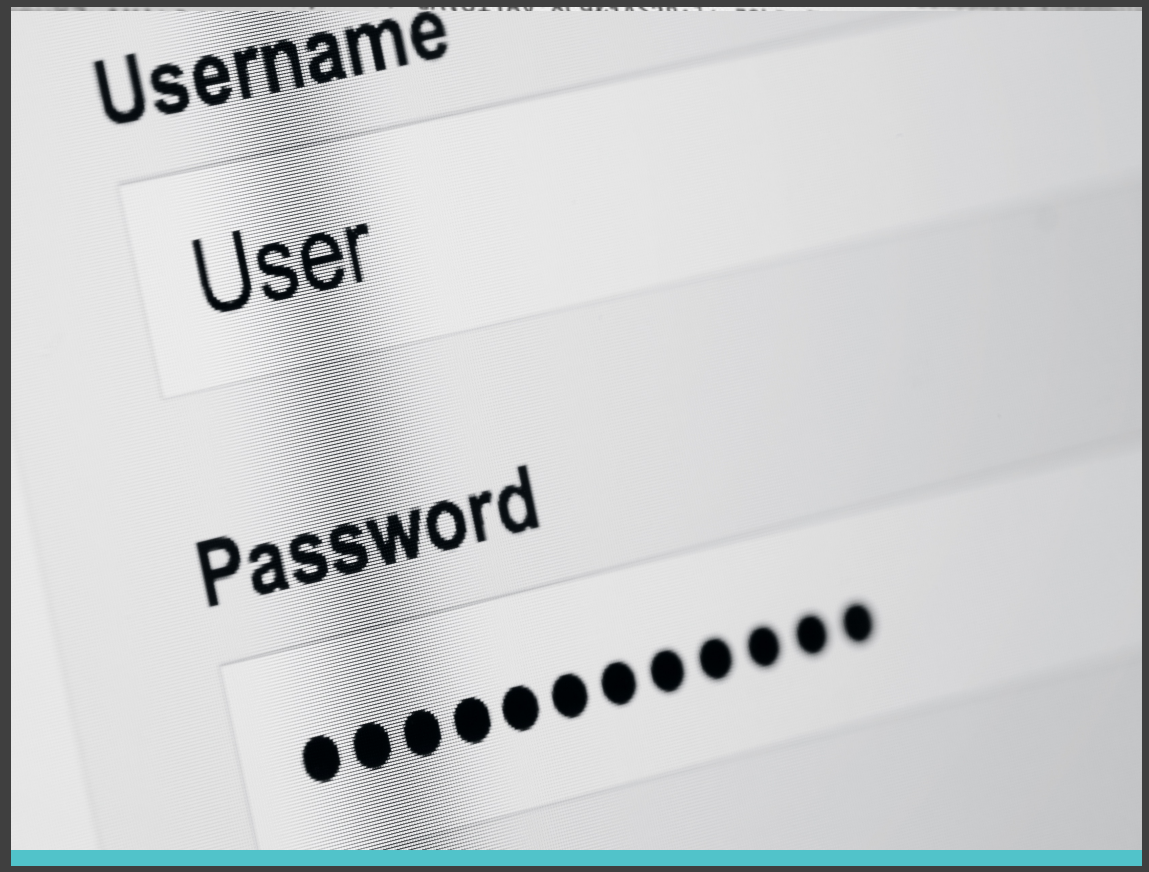
- Data is encrypted as it is stored within the database.
- Data is only decrypted as there are authenticated requests.
- Prevents physical data theft and digital data theft if the database is accessed outside of iUnite.



Minimalistic Data Access

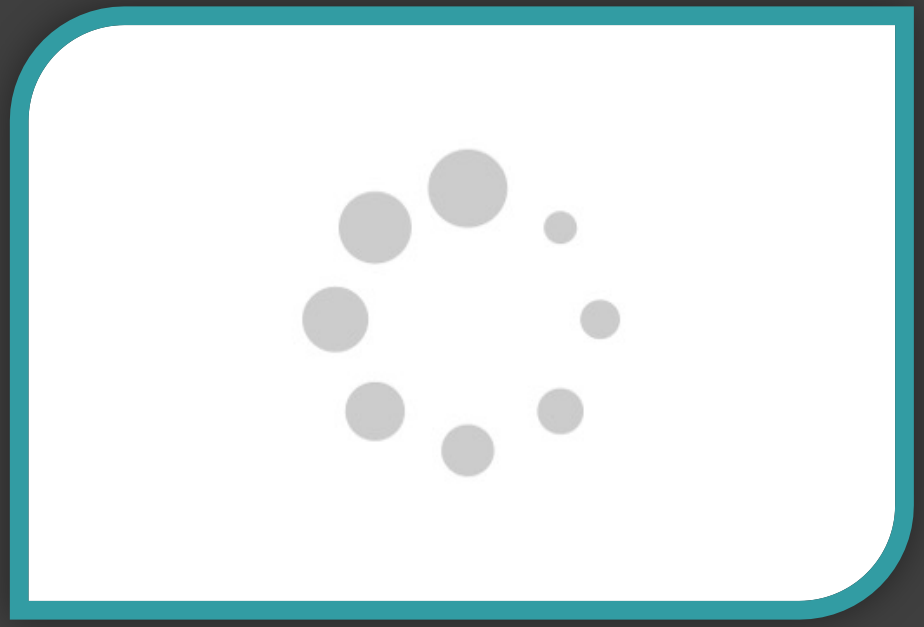
Encryption & Database Security

- Database server is separate from the web server.
- iUnite is granted access to the database with the fewest number of permissions possible.
- Database server can only be accessed with resources in the same account and region.



Security Before Page Loads

- IP Address Check
- Web Application Firewall (WAF)
  - DDoS Protection
  - Bot Blocking
  - Virtual Patching & Hardening
  - Geo-blocking



IP Address Check

Security Before Page Loads

- All traffic must come through the firewall.
- Attempts to access iUnite.ca by bypassing the firewall will get a 403 error.
- IP is checked against known problem, block listed, and allow listed IP addresses.

Web Application Firewall (WAF)

Security Before Page Loads

01

DDoS Protection

Dedicated Denial of Service attacks aim to overload a server or otherwise prevent normal function through traffic volume.

02

Bot Blocking

Known malicious or other suspicious bots attempting to access a website are blocked and denied all access.

03

Virtual Patching & Hardening

Attacks based on known exploits of outdated software on a server are prevented in transit to the server.

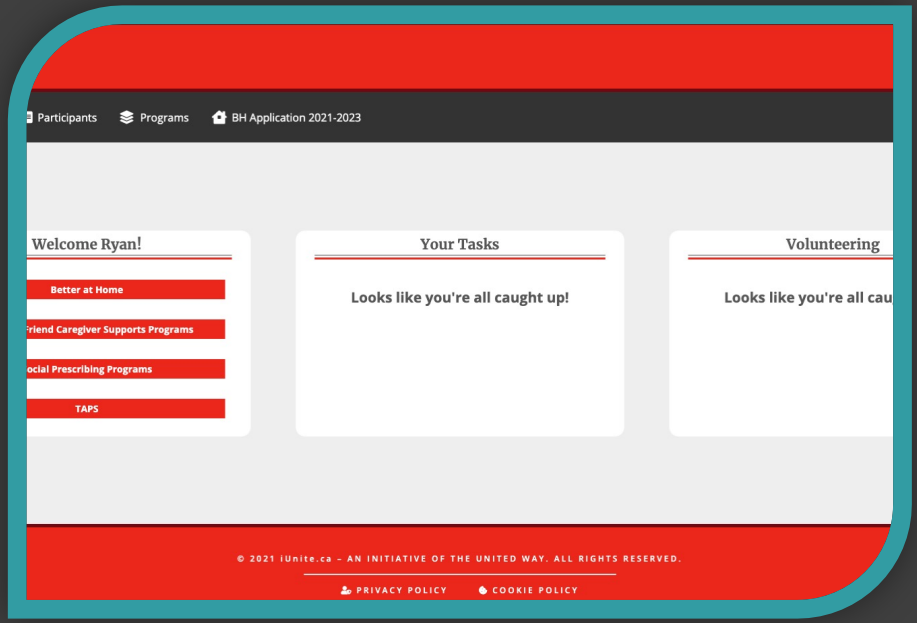
04

Geo-blocking

Block or allow traffic based on its originating location. iUnite blocks all traffic outside Canada.

Security During Page Loads

- Web Application Firewall (internal)
- Automatic logout
- Access Permissions
- Automatic redirects



Web Application Firewall (WAF)

Security During Page Loads

01

DDoS Protection

Dedicated Denial of Service attacks aim to overload a server or otherwise prevent normal function through traffic volume.

02

Bot Blocking

Known malicious or other suspicious bots attempting to access a website are blocked and denied all access.

03

Virtual Patching & Hardening

Attacks based on known exploits of outdated software on a server are prevented in transit to the server.

04

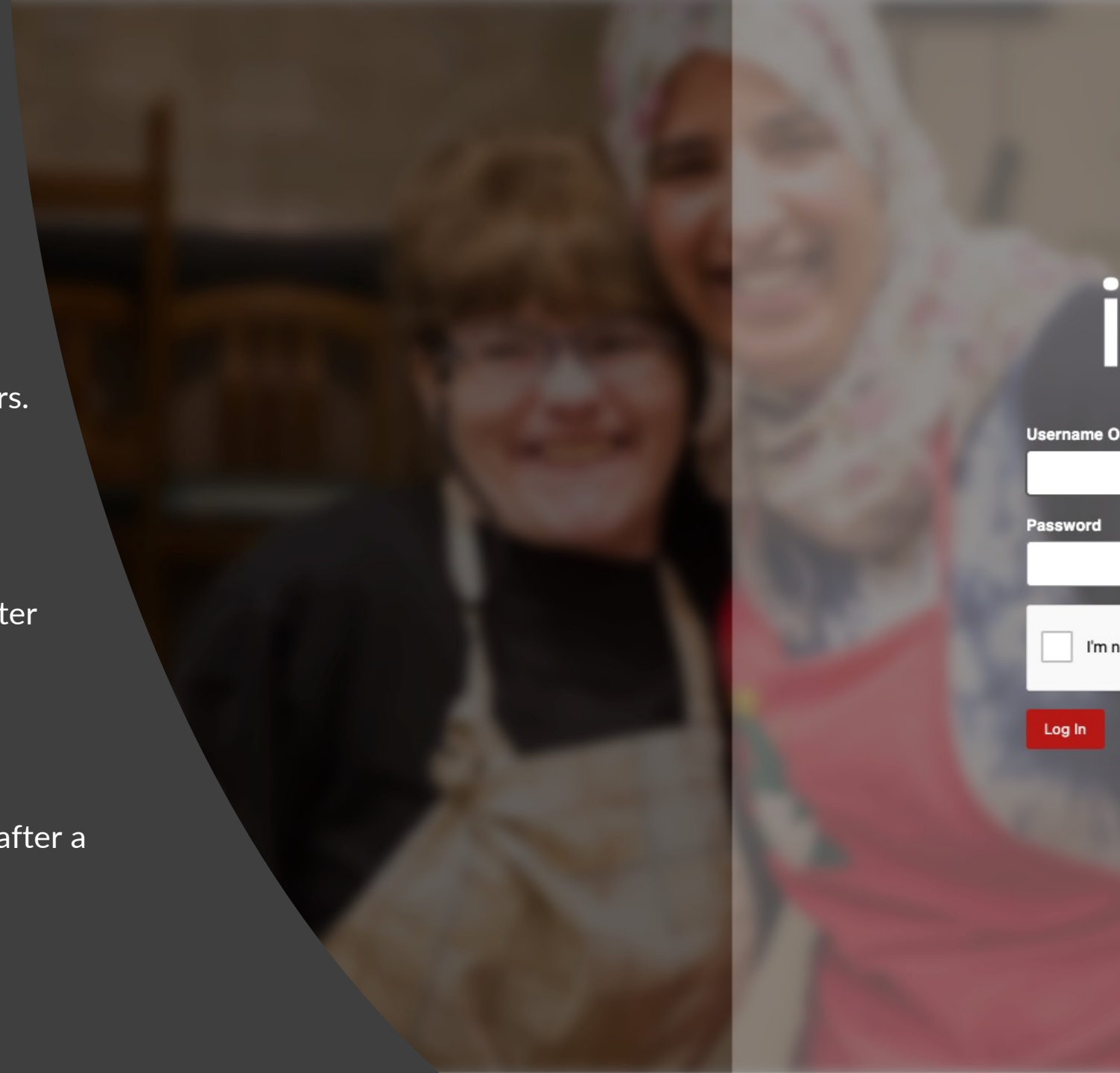
Geo-blocking

Block or allow traffic based on its originating location. iUnite blocks all traffic outside Canada.

Automatic logout

Security During Page Loads

- Each login expires after a max of 48 hours.
- When inactive, you can be logged out after 1 hour, depending on the current page.
- Users are redirected to the login screen after a login expires.



Access Permissions

Security During Page Loads

User Role

Check if the user's account has a sufficient role to access the page or data.

Data Access

Check if the user's can view/edit the field or data being displayed.

Page/Form Access

Check if the user can view/edit the current page and/or form being loaded.

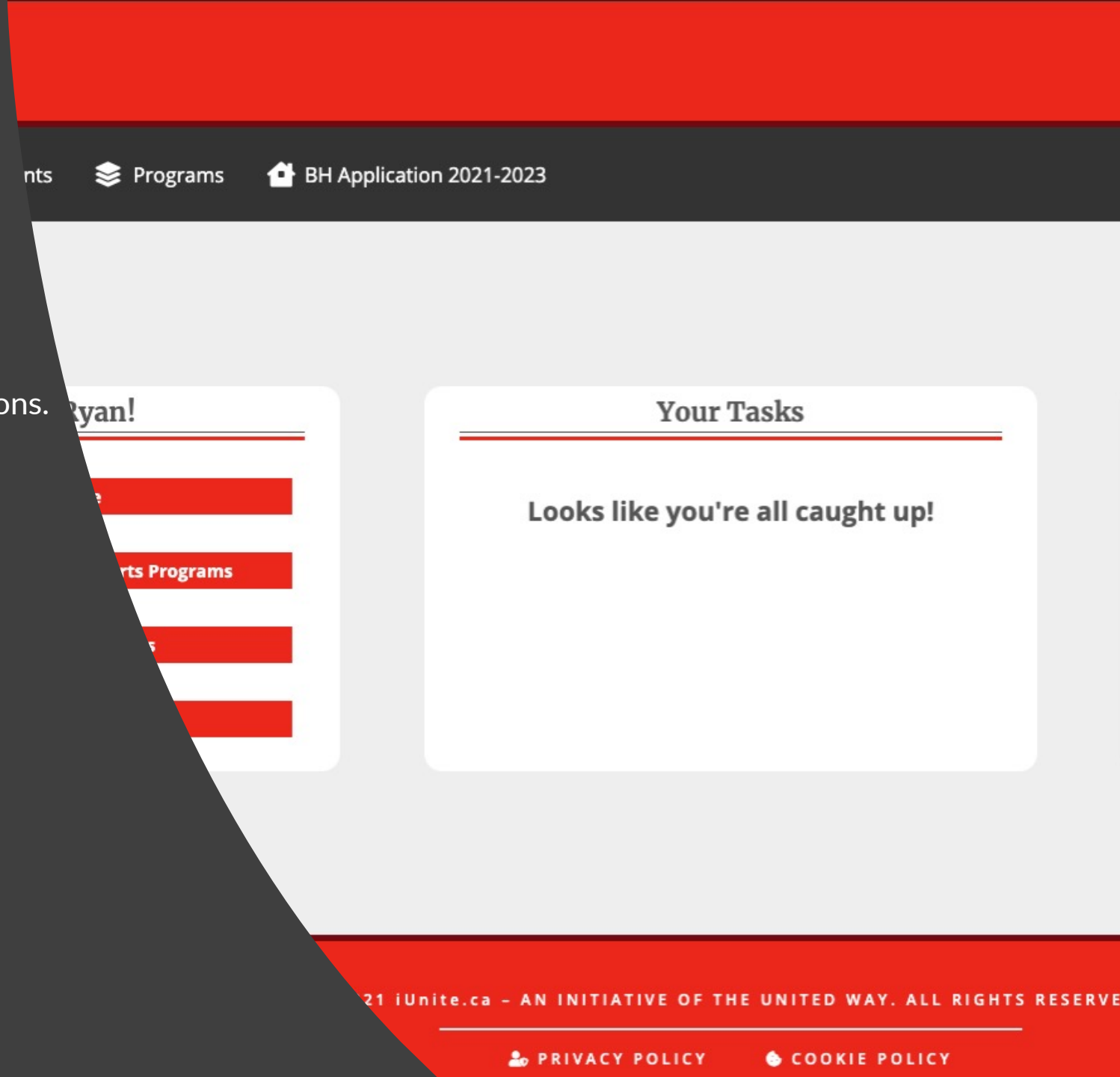
DB Table Access

Check if the user can read and/or write from a specific database table.

Automatic redirects

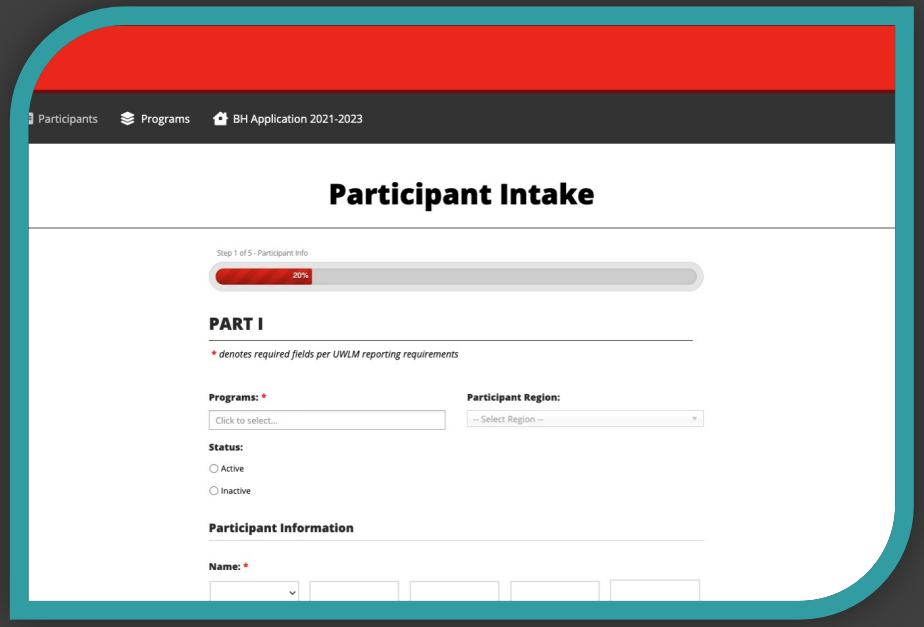
Security During Page Loads

- Redirects are based on account permissions.
- If still logged in, redirect to homepage.
- If logged out, redirect to login page.



Login & Form Security

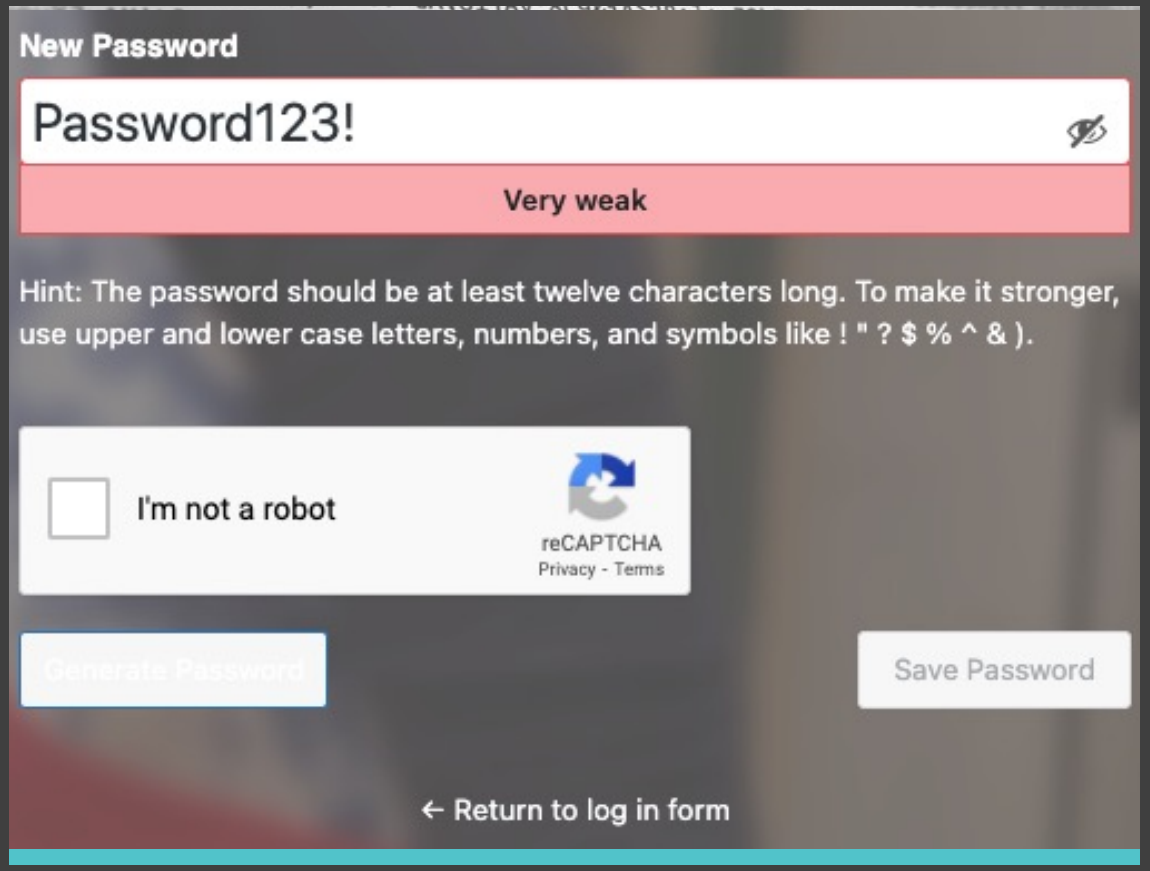
- Passwords
- Login Obscurity
- reCAPTCHA
- Two-Factor Authentication (2FA)
- Nonces
- Account Permissions
- Data Sanitization

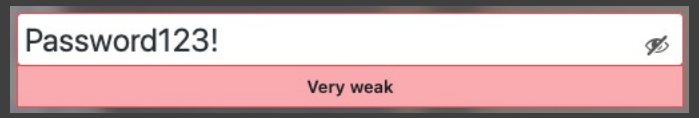


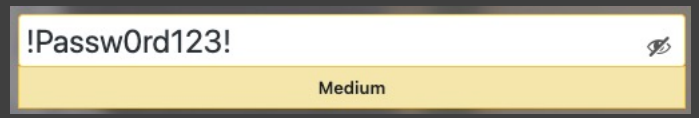
Passwords

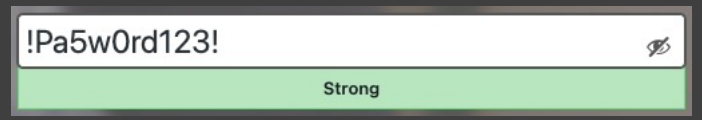
Login & Form Security

- Must be “Strong” to be allowed.
- Algorithm used looks for patterns, common groupings, and minor modifications to words (i.e. leet speak where some letters are replaced by numbers).
- Not strong enough alone for authentication.





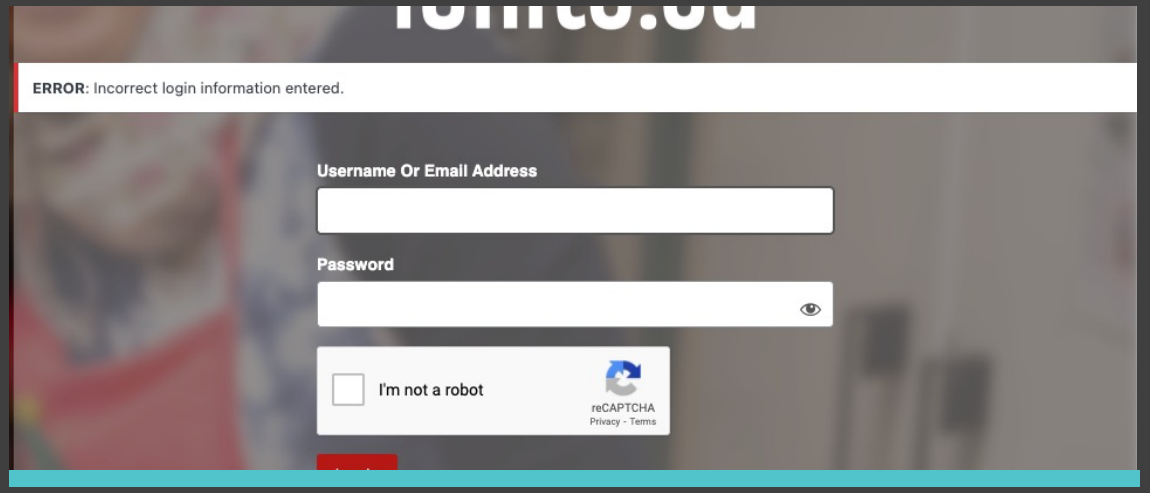




Login Obscurity

Login & Form Security

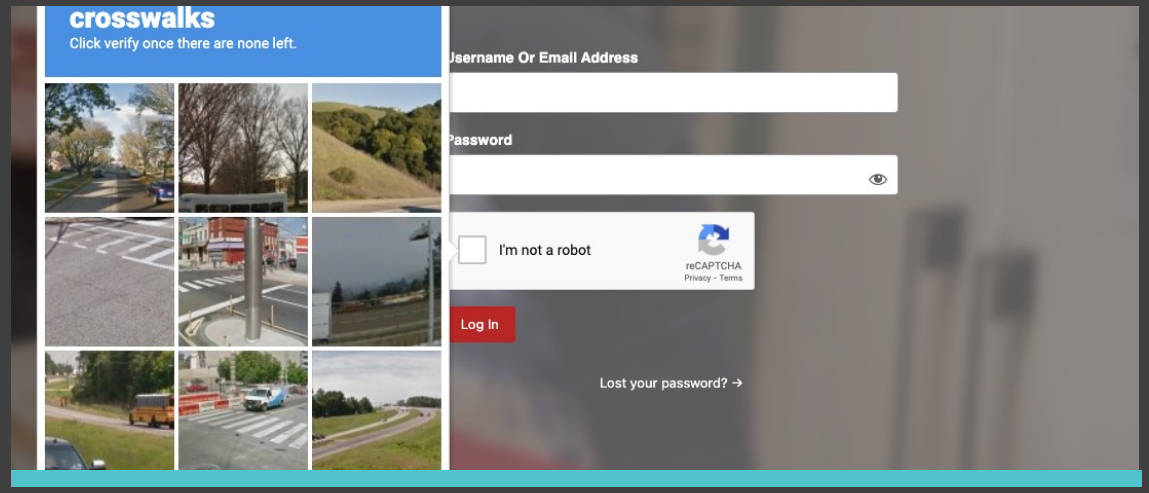
- Shows the same error messages regardless if login attempt is a real account or not.
- Password reset does not confirm if an email was sent or not, to avoid confirming account emails or usernames.
- Makes it harder to hack a password if guessing at emails and usernames.



reCAPTCHA

Login & Form Security

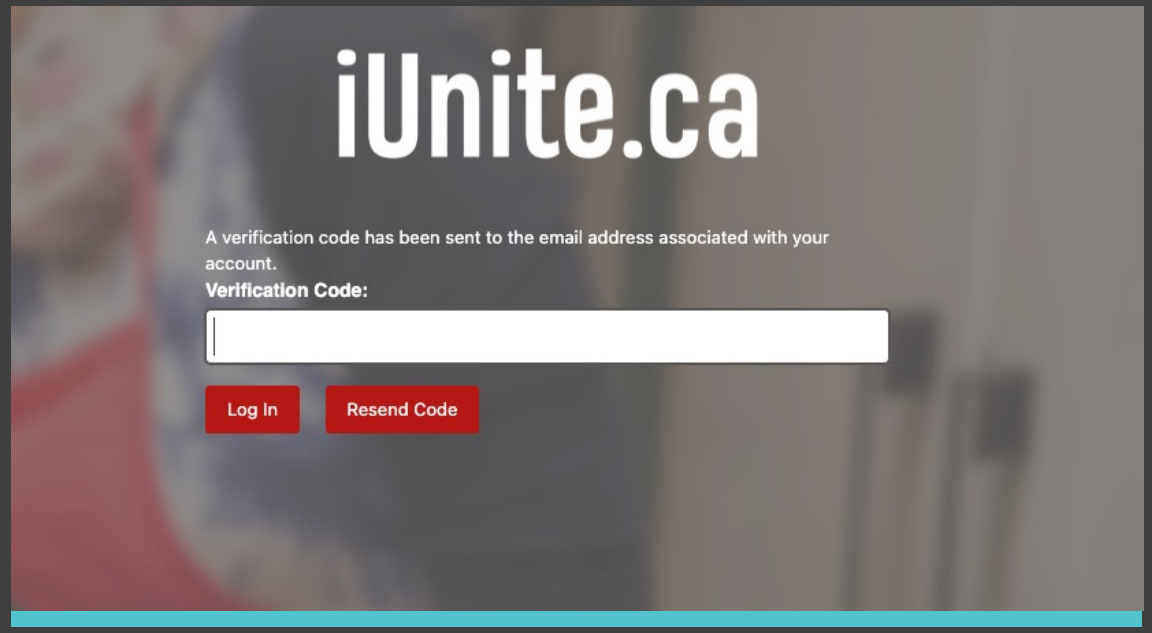
- Two types: invisible and checkbox
- Assesses how pieces of a website are regularly used to weed out suspicious users and bots.
- Based on how user behaves on a website, a risk score between 0 (bad traffic) and 1 (good traffic) is created.



Two-Factor Authentication (2FA)

Login & Form Security

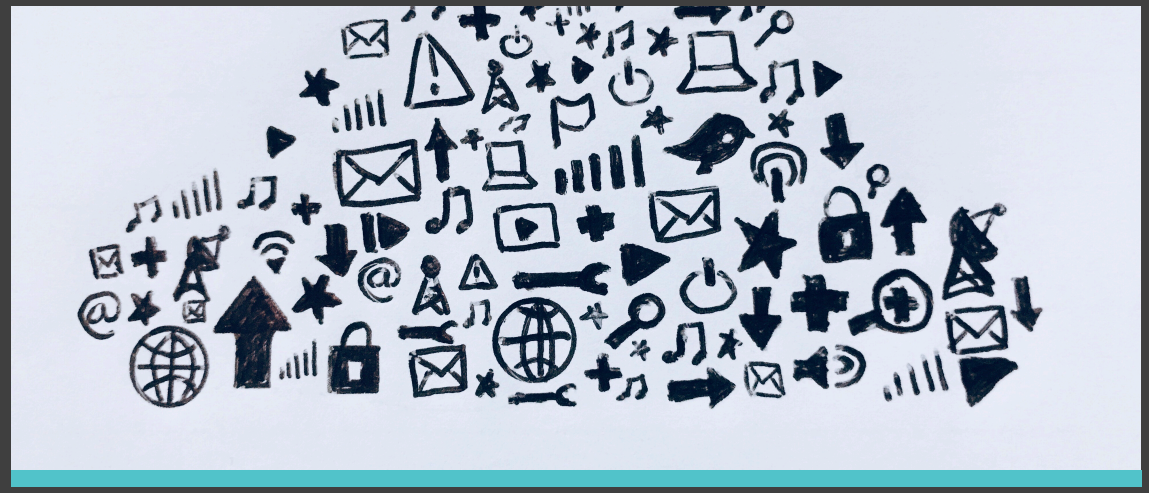
- Email code sent is unique for that account and time sensitive (5 minutes).
- To hack into an account, hacker would need to have a username or email, current password, and access to the email account.
- Future options:
  - SMS/Text
  - Time Based One-Time Password (TOTP)
  - One-Touch Sign-on
  - Magic Link
  - Single Sign On (SSO)



Nonces

Login & Form Security

- Number used once to verify the form submission is from the same user that loaded the page.
- Nonces is a grouping of random characters randomly generated (i.e. 39a650fbec)
- Same nonce could possibly be used twice or more eventually but would not be the same for multiple accounts at the same time (holds for 12 hours).



Access Permissions

Login & Form Security

User Role

Check if the user's account has a sufficient role to access the page or data.

Data Access

Check if the user's can view/edit the field or data being displayed.

Page/Form Access

Check if the user can view/edit the current page and/or form being loaded.

DB Table Access

Check if the user can read and/or write from a specific database table.

Data Sanitization

Login & Form Security

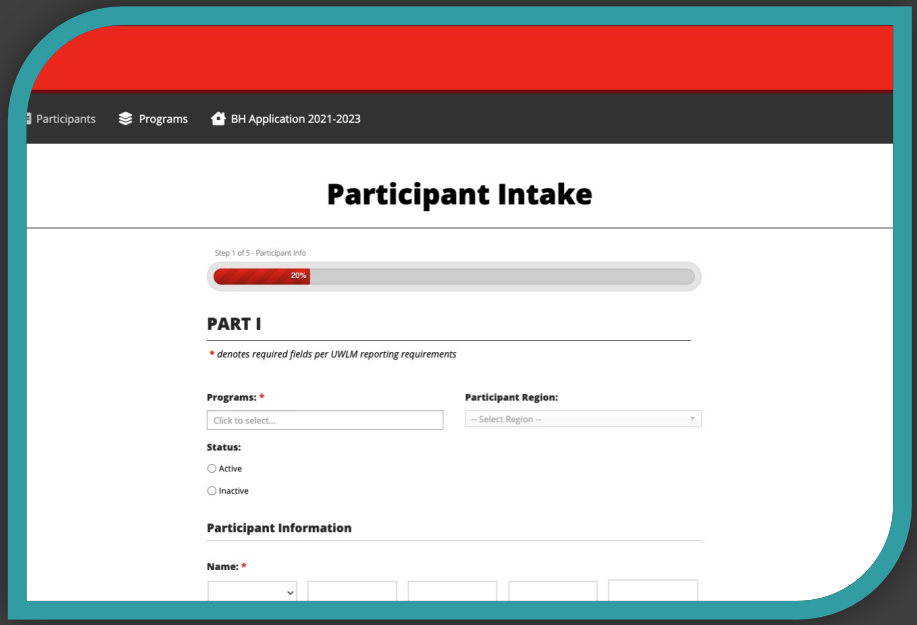
- Converts all submitted data to strings (text).
- Checks for and removes code snippets. These are typically in the format of:

  <script> var code = something; </script>

- Files are scanned during upload for potential malicious code, suspicious file data, and file type mismatches (i.e. uploaded as a .pdf, but is really a .exe file).

Scans, Alerts, & Monitoring

- Scans
- Alerts
- Monitoring



Scans

Scans, Alerts, & Monitoring

Malware & Hack Scanning

Looks for malicious code and unusual content within files and the database.

DNS Scanning

Checks for any changes to the domain's DNS records. Changes here can change where the domain goes.

File integrity

Checks for file changes against previous scans and/or repositories.

Alerts

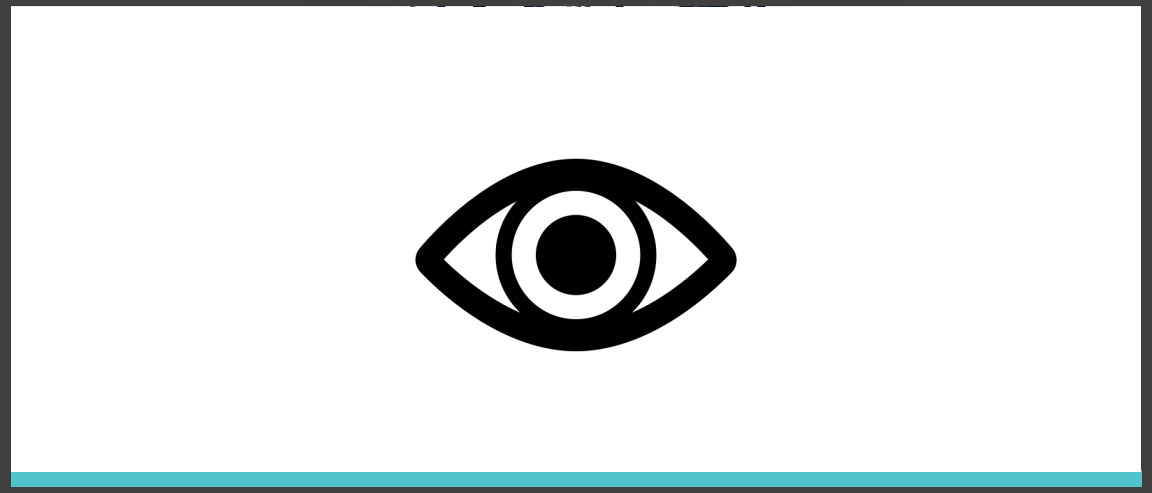
Scans, Alerts, & Monitoring

- User account changes (add, edit, delete, failed logins)
- Website changes (software activated/deactivated, odd files, file changes, DNS changes)
- Security events (blocked actions, unauthorized form submissions, blocked users/traffic)

Monitoring

Scans, Alerts, & Monitoring

- Blacklist monitoring
- Security Logging:
  - Logins
  - Failed login attempts
  - Form submissions/Actions taken
  - User account changes (add/edit/delete)
  - Password reset attempts



Questions

If you have any additional questions after this webinar, please contact us.

help@iunite.ca