### Instructions for using prompts:

1. Choose a prompt sequence. Prompts used for requirements formalization are labeled as P35-P41. A post-processing prompt for explaining root causes of weaknesses (from formal Amalgam provenances to regular English) is also included.
2. Choose an LLM to use.
3. Replace each instance of [REQUIREMENTS] with the natural language requirements to be translated. Replace each instance of [#] with the number of requirements being analyzed.
4. Provide each prompt in order to the LLM. Prompt sequences are split up with one empty line between each individual prompt. For example, P35 contains three prompts: (1) The following text…, (2) Map each…, (3) Output.
5. Save all of the LLM’s output from the prompt sequence. This textual output will become the input to the helper program, *Alloy Statement Extractor*.
6. Once provenances are obtained from Amalgam, the optional post-processing prompt may be used to describe these formal provenances in natural language. For this prompt, replace [PROVENANCES] with the formal provenances you would like the LLM to explain.

### P35 (3 shot):

The following text contains statements in the Alloy specification language, along with a natural language sentence describing what they mean: Administrator\_Security\_Controls in Administrator.has The system's administrator has security controls. Attempts in Authentication.has\_restriction There is a restriction on the number of authentication attempts. Attempts in Recovery\_Mechanism.has\_restriction There is a restriction on the number of password/account recovery attempts. Authentication in Authentication.use\_of Authentication is used. Common in Password.has\_restriction Passwords must avoid the use of common strings such as "password", "admin", or similar. Compartmentalization in Access\_Controls.include Sensitive information is divided into isolated sections, each having its own security controls and access restrictions - isolated sections must be explicitly mentioned, not implied. Config\_File in Password.stored\_in Passwords are stored in a configuration file. Contextual\_String in Password.has\_restriction Passwords must not contain the username or user's information within them. Encrypted in Sensitive\_Data.stored\_as Sensitive data is stored in an encrypted state. Expiration\_Date in Password.has\_restriction Passwords expire. File\_Size in Log\_File.has\_restriction Log file size is limited to a maximum allowed size - log files must be explicitly mentioned or the requirement must specify ALL files. File\_Type in Input\_File.has\_restriction Certain file types or extensions are not allowed to be input into the system. GUI in Credentials.stored\_in The system stores credentials in cleartext directly within the GUI. GUI in Sensitive\_Data.stored\_in The system stores sensitive information in cleartext directly within the GUI. Input\_File in User\_Input.obtained\_as Users can or should input/upload a file into the system. Input\_Validation in Input\_File.has\_restriction Input files are validated. Input\_Validation in Other\_User\_Input.has\_restriction User input other than files is validated. IP\_Address in Authentication.uses The IP address is used for authentication. Least\_Privilege in Access\_Controls.include Users and applications only have access to the minimum resources and permissions they need to perform their designated tasks - this is explicitly mentioned, not implied. Length in Password.has\_restriction There is a restriction on password lengths. Log\_File in Credentials.stored\_in Credentials are stored in the log file. Log\_File in Sensitive\_Data.stored\_in Sensitive data is stored in the log file. Multi\_Factor\_Authentication in Authentication.is The system uses multi factor authentication. Multiple\_Security\_Questions in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to answer multiple security questions. Original\_Password in Reset.requires The original password needs to be provided for password resets. Other\_User\_Input in User\_Input.obtained\_as User input other than files is obtained. Password in Authentication.uses The system uses passwords for authentication. Privilege\_Separation in Access\_Controls.include Privilege separation is implemented in the system's access controls. Recovery\_Mechanism in Password.allows There is a password/account recovery mechanism. Reset in Password.requires Password resets are required. Reuse in Password.has\_restriction The user cannot reuse the same password as the old password for a password change. Security\_Event in Logging.use\_for Security events are logged. Sensitive\_Data in Sensitive\_Data.transport\_of The system sends or receives sensitive data, including, but not limited to: personally identifiable information, financial information, protected health information, intellectual property, and/or special category data. Sensitive\_Data in Sensitive\_Data.use\_of The system interacts with or stores sensitive data, including, but not limited to: personally identifiable information, financial information, protected health information, intellectual property, and/or special category data. Session\_Expiration in Session.has\_restriction The system implements session expiration. Strong\_Security\_Questions in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to answer strong security questions. Temporary\_Password in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to enter a temporary password to set a new password. Trust\_Boundary in Access\_Controls.include Trust boundaries are implemented in the system's access controls. Trust\_Zone in Access\_Controls.include Trust zones are implemented in the system's access controls. Verification in Where\_To\_Send.requires Password/account recovery requires the email address where recovery information is sent to be verified as belonging to the user. Where\_To\_Send in Recovery\_Mechanism.has\_restriction Password/account recovery requires an email address for where recovery information is sent to be collected from the user.

Map each of the following requirements to zero or more of the Alloy statements listed above. Only map an Alloy statement to a requirement if the statement can definitely be inferred from requirements. An example is: "The password should be at least 6 characters" maps to "Authentication in Authentication.use\_of, Password in Authentication.uses, Length in Password.has\_restriction." Another example is: "Passwords shall be strong" maps to "Authentication in Authentication.use\_of, Password in Authentication.uses" because it is possible to infer authentication use from password use, but it is not possible to infer other password strength techniques or restrictions due to the requirement being too vague. Another example is: “The user shall upload a document showing address and proof of residency” maps to “Input\_File in User\_Input.obtained\_as, Sensitive\_Data in Sensitive\_Data.transport\_of, Sensitive\_Data in Sensitive\_Data.use\_of” because uploading a document implies uploading a file and addresses are sensitive information. If the Alloy statement and requirements are negatives of each other, map the Alloy statement as NOT [Alloy statement]. Please map the [#] requirements below in the following text format “requirement number”, “Alloy mappings”, outputting 50 requirements per response: [REQUIREMENTS]

Output the next set of requirements.

### P36 (4 shot):

The following text contains statements in the Alloy specification language, along with a natural language sentence describing what they mean: Administrator\_Security\_Controls in Administrator.has The system's administrator has security controls. Attempts in Authentication.has\_restriction There is a restriction on the number of authentication attempts. Attempts in Recovery\_Mechanism.has\_restriction There is a restriction on the number of password/account recovery attempts. Authentication in Authentication.use\_of Authentication is used. Common in Password.has\_restriction Passwords must avoid the use of common strings such as "password", "admin", or similar. Compartmentalization in Access\_Controls.include Sensitive information is divided into isolated sections, each having its own security controls and access restrictions - isolated sections must be explicitly mentioned, not implied. Config\_File in Password.stored\_in Passwords are stored in a configuration file. Contextual\_String in Password.has\_restriction Passwords must not contain the username or user's information within them. Encrypted in Sensitive\_Data.stored\_as Sensitive data is stored in an encrypted state. Expiration\_Date in Password.has\_restriction Passwords expire. File\_Size in Log\_File.has\_restriction Log file size is limited to a maximum allowed size - log files must be explicitly mentioned or the requirement must specify ALL files. File\_Type in Input\_File.has\_restriction Certain file types or extensions are not allowed to be input into the system. GUI in Credentials.stored\_in The system stores credentials in cleartext directly within the GUI. GUI in Sensitive\_Data.stored\_in The system stores sensitive information in cleartext directly within the GUI. Input\_File in User\_Input.obtained\_as Users can or should input/upload a file into the system. Input\_Validation in Input\_File.has\_restriction Input files are validated. Input\_Validation in Other\_User\_Input.has\_restriction User input other than files is validated. IP\_Address in Authentication.uses The IP address is used for authentication. Least\_Privilege in Access\_Controls.include Users and applications only have access to the minimum resources and permissions they need to perform their designated tasks - this is explicitly mentioned, not implied. Length in Password.has\_restriction There is a restriction on password lengths. Log\_File in Credentials.stored\_in Credentials are stored in the log file. Log\_File in Sensitive\_Data.stored\_in Sensitive data is stored in the log file. Multi\_Factor\_Authentication in Authentication.is The system uses multi factor authentication. Multiple\_Security\_Questions in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to answer multiple security questions. Original\_Password in Reset.requires The original password needs to be provided for password resets. Other\_User\_Input in User\_Input.obtained\_as User input other than files is obtained. Password in Authentication.uses The system uses passwords for authentication. Privilege\_Separation in Access\_Controls.include Privilege separation is implemented in the system's access controls. Recovery\_Mechanism in Password.allows There is a password/account recovery mechanism. Reset in Password.requires Password resets are required. Reuse in Password.has\_restriction The user cannot reuse the same password as the old password for a password change. Security\_Event in Logging.use\_for Security events are logged. Sensitive\_Data in Sensitive\_Data.transport\_of The system sends or receives sensitive data, including, but not limited to: personally identifiable information, financial information, protected health information, intellectual property, and/or special category data. Sensitive\_Data in Sensitive\_Data.use\_of The system interacts with or stores sensitive data, including, but not limited to: personally identifiable information, financial information, protected health information, intellectual property, and/or special category data. Session\_Expiration in Session.has\_restriction The system implements session expiration. Strong\_Security\_Questions in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to answer strong security questions. Temporary\_Password in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to enter a temporary password to set a new password. Trust\_Boundary in Access\_Controls.include Trust boundaries are implemented in the system's access controls. Trust\_Zone in Access\_Controls.include Trust zones are implemented in the system's access controls. Verification in Where\_To\_Send.requires Password/account recovery requires the email address where recovery information is sent to be verified as belonging to the user. Where\_To\_Send in Recovery\_Mechanism.has\_restriction Password/account recovery requires an email address for where recovery information is sent to be collected from the user.

Map each of the following requirements to zero or more of the Alloy statements listed above. Only map an Alloy statement to a requirement if the statement can definitely be inferred from requirements. An example is: "The password should be at least 6 characters" maps to "Authentication in Authentication.use\_of, Password in Authentication.uses, Length in Password.has\_restriction." Another example is: "Passwords shall be strong" maps to "Authentication in Authentication.use\_of, Password in Authentication.uses" because it is possible to infer authentication use from password use, but it is not possible to infer other password strength techniques or restrictions due to the requirement being too vague. Another example is: “The user shall upload a document showing address and proof of residency” maps to “Input\_File in User\_Input.obtained\_as, Sensitive\_Data in Sensitive\_Data.transport\_of, Sensitive\_Data in Sensitive\_Data.use\_of” because uploading a document implies uploading a file and addresses are sensitive information. Another example is: “The system shall require users to reset their password every six months.” maps to “Authentication in Authentication.use\_of, Expiration\_Date in Password.has\_restriction, Password in Authentication.uses, Reset in Password.requires” because there’s a requirement for passwords to be reset and passwords are used, but there aren’t any other password restrictions that can be inferred. If the Alloy statement and requirements are negatives of each other, map the Alloy statement as NOT [Alloy statement]. Please map the [#] requirements below in the following text format “requirement number”, “Alloy mappings”, outputting 50 requirements per response: [REQUIREMENTS]

Output the next set of requirements.

### P37 (5 shot):

The following text contains statements in the Alloy specification language, along with a natural language sentence describing what they mean: Administrator\_Security\_Controls in Administrator.has The system's administrator has security controls. Attempts in Authentication.has\_restriction There is a restriction on the number of authentication attempts. Attempts in Recovery\_Mechanism.has\_restriction There is a restriction on the number of password/account recovery attempts. Authentication in Authentication.use\_of Authentication is used. Common in Password.has\_restriction Passwords must avoid the use of common strings such as "password", "admin", or similar. Compartmentalization in Access\_Controls.include Sensitive information is divided into isolated sections, each having its own security controls and access restrictions - isolated sections must be explicitly mentioned, not implied. Config\_File in Password.stored\_in Passwords are stored in a configuration file. Contextual\_String in Password.has\_restriction Passwords must not contain the username or user's information within them. Encrypted in Sensitive\_Data.stored\_as Sensitive data is stored in an encrypted state. Expiration\_Date in Password.has\_restriction Passwords expire. File\_Size in Log\_File.has\_restriction Log file size is limited to a maximum allowed size - log files must be explicitly mentioned or the requirement must specify ALL files. File\_Type in Input\_File.has\_restriction Certain file types or extensions are not allowed to be input into the system. GUI in Credentials.stored\_in The system stores credentials in cleartext directly within the GUI. GUI in Sensitive\_Data.stored\_in The system stores sensitive information in cleartext directly within the GUI. Input\_File in User\_Input.obtained\_as Users can or should input/upload a file into the system. Input\_Validation in Input\_File.has\_restriction Input files are validated. Input\_Validation in Other\_User\_Input.has\_restriction User input other than files is validated. IP\_Address in Authentication.uses The IP address is used for authentication. Least\_Privilege in Access\_Controls.include Users and applications only have access to the minimum resources and permissions they need to perform their designated tasks - this is explicitly mentioned, not implied. Length in Password.has\_restriction There is a restriction on password lengths. Log\_File in Credentials.stored\_in Credentials are stored in the log file. Log\_File in Sensitive\_Data.stored\_in Sensitive data is stored in the log file. Multi\_Factor\_Authentication in Authentication.is The system uses multi factor authentication. Multiple\_Security\_Questions in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to answer multiple security questions. Original\_Password in Reset.requires The original password needs to be provided for password resets. Other\_User\_Input in User\_Input.obtained\_as User input other than files is obtained. Password in Authentication.uses The system uses passwords for authentication. Privilege\_Separation in Access\_Controls.include Privilege separation is implemented in the system's access controls. Recovery\_Mechanism in Password.allows There is a password/account recovery mechanism. Reset in Password.requires Password resets are required. Reuse in Password.has\_restriction The user cannot reuse the same password as the old password for a password change. Security\_Event in Logging.use\_for Security events are logged. Sensitive\_Data in Sensitive\_Data.transport\_of The system sends or receives sensitive data, including, but not limited to: personally identifiable information, financial information, protected health information, intellectual property, and/or special category data. Sensitive\_Data in Sensitive\_Data.use\_of The system interacts with or stores sensitive data, including, but not limited to: personally identifiable information, financial information, protected health information, intellectual property, and/or special category data. Session\_Expiration in Session.has\_restriction The system implements session expiration. Strong\_Security\_Questions in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to answer strong security questions. Temporary\_Password in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to enter a temporary password to set a new password. Trust\_Boundary in Access\_Controls.include Trust boundaries are implemented in the system's access controls. Trust\_Zone in Access\_Controls.include Trust zones are implemented in the system's access controls. Verification in Where\_To\_Send.requires Password/account recovery requires the email address where recovery information is sent to be verified as belonging to the user. Where\_To\_Send in Recovery\_Mechanism.has\_restriction Password/account recovery requires an email address for where recovery information is sent to be collected from the user.

Map each of the following requirements to zero or more of the Alloy statements listed above. Only map an Alloy statement to a requirement if the statement can definitely be inferred from requirements. An example is: "The password should be at least 6 characters" maps to "Authentication in Authentication.use\_of, Password in Authentication.uses, Length in Password.has\_restriction." Another example is: "Passwords shall be strong" maps to "Authentication in Authentication.use\_of, Password in Authentication.uses" because it is possible to infer authentication use from password use, but it is not possible to infer other password strength techniques or restrictions due to the requirement being too vague. Another example is: “The user shall upload a document showing address and proof of residency” maps to “Input\_File in User\_Input.obtained\_as, Sensitive\_Data in Sensitive\_Data.transport\_of, Sensitive\_Data in Sensitive\_Data.use\_of” because uploading a document implies uploading a file and addresses are sensitive information. Another example is: “The system shall require users to reset their password every six months.” maps to “Authentication in Authentication.use\_of, Expiration\_Date in Password.has\_restriction, Password in Authentication.uses, Reset in Password.requires” because there’s a requirement for passwords to be reset and passwords are used, but there aren’t any other password restrictions that can be inferred. Another example is: “The user shall be able to access their health history and update their address” maps to “Other\_User\_Input in User\_Input.obtained\_as, Sensitive\_Data in Sensitive\_Data.use\_of” but not other mappings because health history and addresses are both considered sensitive data but it is not specified that it is being sent, and updating the address is a form of user input. If the Alloy statement and requirements are negatives of each other, map the Alloy statement as NOT [Alloy statement]. Please map the [#] requirements below in the following text format “requirement number”, “Alloy mappings”, outputting 50 requirements per response: [REQUIREMENTS]

Output the next set of requirements.

### P38 (5 shot, persona):

The following text contains statements in the Alloy specification language, along with a natural language sentence describing what they mean: Administrator\_Security\_Controls in Administrator.has The system's administrator has security controls. Attempts in Authentication.has\_restriction There is a restriction on the number of authentication attempts. Attempts in Recovery\_Mechanism.has\_restriction There is a restriction on the number of password/account recovery attempts. Authentication in Authentication.use\_of Authentication is used. Common in Password.has\_restriction Passwords must avoid the use of common strings such as "password", "admin", or similar. Compartmentalization in Access\_Controls.include Sensitive information is divided into isolated sections, each having its own security controls and access restrictions - isolated sections must be explicitly mentioned, not implied. Config\_File in Password.stored\_in Passwords are stored in a configuration file. Contextual\_String in Password.has\_restriction Passwords must not contain the username or user's information within them. Encrypted in Sensitive\_Data.stored\_as Sensitive data is stored in an encrypted state. Expiration\_Date in Password.has\_restriction Passwords expire. File\_Size in Log\_File.has\_restriction Log file size is limited to a maximum allowed size - log files must be explicitly mentioned or the requirement must specify ALL files. File\_Type in Input\_File.has\_restriction Certain file types or extensions are not allowed to be input into the system. GUI in Credentials.stored\_in The system stores credentials in cleartext directly within the GUI. GUI in Sensitive\_Data.stored\_in The system stores sensitive information in cleartext directly within the GUI. Input\_File in User\_Input.obtained\_as Users can or should input/upload a file into the system. Input\_Validation in Input\_File.has\_restriction Input files are validated. Input\_Validation in Other\_User\_Input.has\_restriction User input other than files is validated. IP\_Address in Authentication.uses The IP address is used for authentication. Least\_Privilege in Access\_Controls.include Users and applications only have access to the minimum resources and permissions they need to perform their designated tasks - this is explicitly mentioned, not implied. Length in Password.has\_restriction There is a restriction on password lengths. Log\_File in Credentials.stored\_in Credentials are stored in the log file. Log\_File in Sensitive\_Data.stored\_in Sensitive data is stored in the log file. Multi\_Factor\_Authentication in Authentication.is The system uses multi factor authentication. Multiple\_Security\_Questions in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to answer multiple security questions. Original\_Password in Reset.requires The original password needs to be provided for password resets. Other\_User\_Input in User\_Input.obtained\_as User input other than files is obtained. Password in Authentication.uses The system uses passwords for authentication. Privilege\_Separation in Access\_Controls.include Privilege separation is implemented in the system's access controls. Recovery\_Mechanism in Password.allows There is a password/account recovery mechanism. Reset in Password.requires Password resets are required. Reuse in Password.has\_restriction The user cannot reuse the same password as the old password for a password change. Security\_Event in Logging.use\_for Security events are logged. Sensitive\_Data in Sensitive\_Data.transport\_of The system sends or receives sensitive data, including, but not limited to: personally identifiable information, financial information, protected health information, intellectual property, and/or special category data. Sensitive\_Data in Sensitive\_Data.use\_of The system interacts with or stores sensitive data, including, but not limited to: personally identifiable information, financial information, protected health information, intellectual property, and/or special category data. Session\_Expiration in Session.has\_restriction The system implements session expiration. Strong\_Security\_Questions in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to answer strong security questions. Temporary\_Password in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to enter a temporary password to set a new password. Trust\_Boundary in Access\_Controls.include Trust boundaries are implemented in the system's access controls. Trust\_Zone in Access\_Controls.include Trust zones are implemented in the system's access controls. Verification in Where\_To\_Send.requires Password/account recovery requires the email address where recovery information is sent to be verified as belonging to the user. Where\_To\_Send in Recovery\_Mechanism.has\_restriction Password/account recovery requires an email address for where recovery information is sent to be collected from the user.

You are a security analyst reviewing security documentation for a system being designed. Map each of the following requirements to zero or more of the Alloy statements listed above. Only map an Alloy statement to a requirement if the statement can definitely be inferred from requirements. An example is: "The password should be at least 6 characters" maps to "Authentication in Authentication.use\_of, Password in Authentication.uses, Length in Password.has\_restriction." Another example is: "Passwords shall be strong" maps to "Authentication in Authentication.use\_of, Password in Authentication.uses" because it is possible to infer authentication use from password use, but it is not possible to infer other password strength techniques or restrictions due to the requirement being too vague. Another example is: “The user shall upload a document showing address and proof of residency” maps to “Input\_File in User\_Input.obtained\_as, Sensitive\_Data in Sensitive\_Data.transport\_of, Sensitive\_Data in Sensitive\_Data.use\_of” because uploading a document implies uploading a file and addresses are sensitive information. Another example is: “The system shall require users to reset their password every six months.” maps to “Authentication in Authentication.use\_of, Expiration\_Date in Password.has\_restriction, Password in Authentication.uses, Reset in Password.requires” because there’s a requirement for passwords to be reset and passwords are used, but there aren’t any other password restrictions that can be inferred. Another example is: “The user shall be able to access their health history and update their address” maps to “Other\_User\_Input in User\_Input.obtained\_as, Sensitive\_Data in Sensitive\_Data.use\_of” but not other mappings because health history and addresses are both considered sensitive data but it is not specified that it is being sent, and updating the address is a form of user input. If the Alloy statement and requirements are negatives of each other, map the Alloy statement as NOT [Alloy statement]. Please map the [#] requirements below in the following text format “requirement number”, “Alloy mappings”, outputting 50 requirements per response: [REQUIREMENTS]

Output the next set of requirements.

### P39 (5 shot, CoT):

The following text contains statements in the Alloy specification language, along with a natural language sentence describing what they mean: Administrator\_Security\_Controls in Administrator.has The system's administrator has security controls. Attempts in Authentication.has\_restriction There is a restriction on the number of authentication attempts. Attempts in Recovery\_Mechanism.has\_restriction There is a restriction on the number of password/account recovery attempts. Authentication in Authentication.use\_of Authentication is used. Common in Password.has\_restriction Passwords must avoid the use of common strings such as "password", "admin", or similar. Compartmentalization in Access\_Controls.include Sensitive information is divided into isolated sections, each having its own security controls and access restrictions - isolated sections must be explicitly mentioned, not implied. Config\_File in Password.stored\_in Passwords are stored in a configuration file. Contextual\_String in Password.has\_restriction Passwords must not contain the username or user's information within them. Encrypted in Sensitive\_Data.stored\_as Sensitive data is stored in an encrypted state. Expiration\_Date in Password.has\_restriction Passwords expire. File\_Size in Log\_File.has\_restriction Log file size is limited to a maximum allowed size - log files must be explicitly mentioned or the requirement must specify ALL files. File\_Type in Input\_File.has\_restriction Certain file types or extensions are not allowed to be input into the system. GUI in Credentials.stored\_in The system stores credentials in cleartext directly within the GUI. GUI in Sensitive\_Data.stored\_in The system stores sensitive information in cleartext directly within the GUI. Input\_File in User\_Input.obtained\_as Users can or should input/upload a file into the system. Input\_Validation in Input\_File.has\_restriction Input files are validated. Input\_Validation in Other\_User\_Input.has\_restriction User input other than files is validated. IP\_Address in Authentication.uses The IP address is used for authentication. Least\_Privilege in Access\_Controls.include Users and applications only have access to the minimum resources and permissions they need to perform their designated tasks - this is explicitly mentioned, not implied. Length in Password.has\_restriction There is a restriction on password lengths. Log\_File in Credentials.stored\_in Credentials are stored in the log file. Log\_File in Sensitive\_Data.stored\_in Sensitive data is stored in the log file. Multi\_Factor\_Authentication in Authentication.is The system uses multi factor authentication. Multiple\_Security\_Questions in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to answer multiple security questions. Original\_Password in Reset.requires The original password needs to be provided for password resets. Other\_User\_Input in User\_Input.obtained\_as User input other than files is obtained. Password in Authentication.uses The system uses passwords for authentication. Privilege\_Separation in Access\_Controls.include Privilege separation is implemented in the system's access controls. Recovery\_Mechanism in Password.allows There is a password/account recovery mechanism. Reset in Password.requires Password resets are required. Reuse in Password.has\_restriction The user cannot reuse the same password as the old password for a password change. Security\_Event in Logging.use\_for Security events are logged. Sensitive\_Data in Sensitive\_Data.transport\_of The system sends or receives sensitive data, including, but not limited to: personally identifiable information, financial information, protected health information, intellectual property, and/or special category data. Sensitive\_Data in Sensitive\_Data.use\_of The system interacts with or stores sensitive data, including, but not limited to: personally identifiable information, financial information, protected health information, intellectual property, and/or special category data. Session\_Expiration in Session.has\_restriction The system implements session expiration. Strong\_Security\_Questions in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to answer strong security questions. Temporary\_Password in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to enter a temporary password to set a new password. Trust\_Boundary in Access\_Controls.include Trust boundaries are implemented in the system's access controls. Trust\_Zone in Access\_Controls.include Trust zones are implemented in the system's access controls. Verification in Where\_To\_Send.requires Password/account recovery requires the email address where recovery information is sent to be verified as belonging to the user. Where\_To\_Send in Recovery\_Mechanism.has\_restriction Password/account recovery requires an email address for where recovery information is sent to be collected from the user.

Map each of the following requirements to zero or more of the Alloy statements listed above. Only map an Alloy statement to a requirement if the statement can definitely be inferred from requirements. An example is: "The password should be at least 6 characters" maps to "Authentication in Authentication.use\_of, Password in Authentication.uses, Length in Password.has\_restriction." Another example is: "Passwords shall be strong" maps to "Authentication in Authentication.use\_of, Password in Authentication.uses" because it is possible to infer authentication use from password use, but it is not possible to infer other password strength techniques or restrictions due to the requirement being too vague. Another example is: “The user shall upload a document showing address and proof of residency” maps to “Input\_File in User\_Input.obtained\_as, Sensitive\_Data in Sensitive\_Data.transport\_of, Sensitive\_Data in Sensitive\_Data.use\_of” because uploading a document implies uploading a file and addresses are sensitive information. Another example is: “The system shall require users to reset their password every six months.” maps to “Authentication in Authentication.use\_of, Expiration\_Date in Password.has\_restriction, Password in Authentication.uses, Reset in Password.requires” because there’s a requirement for passwords to be reset and passwords are used, but there aren’t any other password restrictions that can be inferred. Another example is: “The user shall be able to access their health history and update their address” maps to “Other\_User\_Input in User\_Input.obtained\_as, Sensitive\_Data in Sensitive\_Data.use\_of” but not other mappings because health history and addresses are both considered sensitive data but it is not specified that it is being sent, and updating the address is a form of user input. If the Alloy statement and requirements are negatives of each other, map the Alloy statement as NOT [Alloy statement]. For each requirement and its possible Alloy mappings, ask yourself: Can this Alloy statement be directly and unambiguously inferred from the text of the requirement? Is the requirement too generic, underspecified, or ambiguous to support a specific mapping? What semantic or functional relationship justifies this mapping? If the requirement contradicts the Alloy statement, should it be mapped as a NOT? After reasoning through these questions, generate only the final mappings. Please map the [#] requirements below in the following text format “requirement number”, “Alloy mappings”, outputting 50 requirements per response: [REQUIREMENTS]

Output the next set of requirements.

### P40 (5 shot, self-reflection):

The following text contains statements in the Alloy specification language, along with a natural language sentence describing what they mean: Administrator\_Security\_Controls in Administrator.has The system's administrator has security controls. Attempts in Authentication.has\_restriction There is a restriction on the number of authentication attempts. Attempts in Recovery\_Mechanism.has\_restriction There is a restriction on the number of password/account recovery attempts. Authentication in Authentication.use\_of Authentication is used. Common in Password.has\_restriction Passwords must avoid the use of common strings such as "password", "admin", or similar. Compartmentalization in Access\_Controls.include Sensitive information is divided into isolated sections, each having its own security controls and access restrictions - isolated sections must be explicitly mentioned, not implied. Config\_File in Password.stored\_in Passwords are stored in a configuration file. Contextual\_String in Password.has\_restriction Passwords must not contain the username or user's information within them. Encrypted in Sensitive\_Data.stored\_as Sensitive data is stored in an encrypted state. Expiration\_Date in Password.has\_restriction Passwords expire. File\_Size in Log\_File.has\_restriction Log file size is limited to a maximum allowed size - log files must be explicitly mentioned or the requirement must specify ALL files. File\_Type in Input\_File.has\_restriction Certain file types or extensions are not allowed to be input into the system. GUI in Credentials.stored\_in The system stores credentials in cleartext directly within the GUI. GUI in Sensitive\_Data.stored\_in The system stores sensitive information in cleartext directly within the GUI. Input\_File in User\_Input.obtained\_as Users can or should input/upload a file into the system. Input\_Validation in Input\_File.has\_restriction Input files are validated. Input\_Validation in Other\_User\_Input.has\_restriction User input other than files is validated. IP\_Address in Authentication.uses The IP address is used for authentication. Least\_Privilege in Access\_Controls.include Users and applications only have access to the minimum resources and permissions they need to perform their designated tasks - this is explicitly mentioned, not implied. Length in Password.has\_restriction There is a restriction on password lengths. Log\_File in Credentials.stored\_in Credentials are stored in the log file. Log\_File in Sensitive\_Data.stored\_in Sensitive data is stored in the log file. Multi\_Factor\_Authentication in Authentication.is The system uses multi factor authentication. Multiple\_Security\_Questions in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to answer multiple security questions. Original\_Password in Reset.requires The original password needs to be provided for password resets. Other\_User\_Input in User\_Input.obtained\_as User input other than files is obtained. Password in Authentication.uses The system uses passwords for authentication. Privilege\_Separation in Access\_Controls.include Privilege separation is implemented in the system's access controls. Recovery\_Mechanism in Password.allows There is a password/account recovery mechanism. Reset in Password.requires Password resets are required. Reuse in Password.has\_restriction The user cannot reuse the same password as the old password for a password change. Security\_Event in Logging.use\_for Security events are logged. Sensitive\_Data in Sensitive\_Data.transport\_of The system sends or receives sensitive data, including, but not limited to: personally identifiable information, financial information, protected health information, intellectual property, and/or special category data. Sensitive\_Data in Sensitive\_Data.use\_of The system interacts with or stores sensitive data, including, but not limited to: personally identifiable information, financial information, protected health information, intellectual property, and/or special category data. Session\_Expiration in Session.has\_restriction The system implements session expiration. Strong\_Security\_Questions in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to answer strong security questions. Temporary\_Password in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to enter a temporary password to set a new password. Trust\_Boundary in Access\_Controls.include Trust boundaries are implemented in the system's access controls. Trust\_Zone in Access\_Controls.include Trust zones are implemented in the system's access controls. Verification in Where\_To\_Send.requires Password/account recovery requires the email address where recovery information is sent to be verified as belonging to the user. Where\_To\_Send in Recovery\_Mechanism.has\_restriction Password/account recovery requires an email address for where recovery information is sent to be collected from the user.

Map each of the following requirements to zero or more of the Alloy statements listed above. Only map an Alloy statement to a requirement if the statement can definitely be inferred from requirements. An example is: "The password should be at least 6 characters" maps to "Authentication in Authentication.use\_of, Password in Authentication.uses, Length in Password.has\_restriction." Another example is: "Passwords shall be strong" maps to "Authentication in Authentication.use\_of, Password in Authentication.uses" because it is possible to infer authentication use from password use, but it is not possible to infer other password strength techniques or restrictions due to the requirement being too vague. Another example is: “The user shall upload a document showing address and proof of residency” maps to “Input\_File in User\_Input.obtained\_as, Sensitive\_Data in Sensitive\_Data.transport\_of, Sensitive\_Data in Sensitive\_Data.use\_of” because uploading a document implies uploading a file and addresses are sensitive information. Another example is: “The system shall require users to reset their password every six months.” maps to “Authentication in Authentication.use\_of, Expiration\_Date in Password.has\_restriction, Password in Authentication.uses, Reset in Password.requires” because there’s a requirement for passwords to be reset and passwords are used, but there aren’t any other password restrictions that can be inferred. Another example is: “The user shall be able to access their health history and update their address” maps to “Other\_User\_Input in User\_Input.obtained\_as, Sensitive\_Data in Sensitive\_Data.use\_of” but not other mappings because health history and addresses are both considered sensitive data but it is not specified that it is being sent, and updating the address is a form of user input. If the Alloy statement and requirements are negatives of each other, map the Alloy statement as NOT [Alloy statement]. Please map the [#] requirements below in the following text format “requirement number”, “Alloy mappings”, outputting 50 requirements per response: [REQUIREMENTS]

Output the next set of requirements.

Review each of the [#] initial Alloy mappings you produced. For each mapping, carefully evaluate whether it is accurate, necessary, and well-justified. If any mapping is incorrect, unnecessary, or based on vague or overly broad inferences, revise or remove it. If the requirement clearly implies a mapping that was omitted, add it. In particular: Remove or revise mappings that assume too much from ambiguous language. Replace or simplify mappings that are too specific for vague requirements. Add missing mappings that are clearly and confidently supported by the requirement. Then output **o**nly the revised set of final mappings, 50 requirements per response. Do not include the original mappings in your output — only the updated versions.

Output the next set of requirements.

### P41 (5 shot, distractor):

The following text contains statements in the Alloy specification language, along with a natural language sentence describing what they mean: Administrator\_Security\_Controls in Administrator.has The system's administrator has security controls.

Attempts in Authentication.has\_restriction There is a restriction on the number of authentication attempts.

Attempts in Recovery\_Mechanism.has\_restriction There is a restriction on the number of password/account recovery attempts.

Authentication in Authentication.use\_of Authentication is used.

Authentication\_Attempts in Logging.record Authentication attempts are logged or recorded.

Common in Password.has\_restriction Passwords must avoid the use of common strings such as "password", "admin", or similar.

Compartmentalization in Access\_Controls.include Sensitive information is divided into isolated sections, each having its own security controls and access restrictions - isolated sections must be explicitly mentioned, not implied.

Config\_File in Password.stored\_in Passwords are stored in a configuration file.

Contextual\_String in Password.has\_restriction Passwords must not contain the username or user's information within them.

Data\_Recovery in Data\_Recovery.use It is possible to recover lost data.

Deactivate in Session.ability The system can deactivate or log out a user from a session.

Encrypted in Sensitive\_Data.stored\_as Sensitive data is stored in an encrypted state.

Expiration\_Date in Password.has\_restriction Passwords expire.

File\_Size in Log\_File.has\_restriction Log file size is limited to a maximum allowed size - log files must be explicitly mentioned or the requirement must specify ALL files.

File\_Type in Input\_File.has\_restriction Certain file types or extensions are not allowed to be input into the system.

GUI in Credentials.stored\_in The system stores credentials in cleartext directly within the GUI.

GUI in Sensitive\_Data.stored\_in The system stores sensitive information in cleartext directly within the GUI.

Input\_File in User\_Input.obtained\_as Users can or should input/upload a file into the system.

Input\_Validation in Input\_File.has\_restriction Input files are validated.

Input\_Validation in Other\_User\_Input.has\_restriction User input other than files is validated.

IP\_Address in Authentication.uses The IP address is used for authentication.

Least\_Privilege in Access\_Controls.include Users and applications only have access to the minimum resources and permissions they need to perform their designated tasks - this is explicitly mentioned, not implied.

Length in Password.has\_restriction There is a restriction on password lengths.

Log\_File in Credentials.stored\_in Credentials are stored in the log file.

Log\_File in Sensitive\_Data.stored\_in Sensitive data is stored in the log file.

Multi\_Factor\_Authentication in Authentication.is The system uses multi factor authentication.

Multiple\_Security\_Questions in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to answer multiple security questions.

Original\_Password in Reset.requires The original password needs to be provided for password resets.

Other\_User\_Input in User\_Input.obtained\_as User input other than files is obtained.

Password in Authentication.uses The system uses passwords for authentication.

Password\_Restrictions in Strong.are Passwords requirements or restrictions are strong.

Privileges in Permission.used Permissions or privileges are used.

Privilege\_Separation in Access\_Controls.include Privilege separation is implemented in the system's access controls.

Recovery\_Mechanism in Password.allows There is a password/account recovery mechanism.

Reset in Password.requires Password resets are required.

Reuse in Password.has\_restriction The user cannot reuse the same password as the old password for a password change.

Security\_Event in Logging.use\_for Security events are logged.

Sensitive\_Data in Sensitive\_Data.transport\_of The system sends or receives sensitive data, including, but not limited to: personally identifiable information, financial information, protected health information, intellectual property, and/or special category data.

Sensitive\_Data in Sensitive\_Data.use\_of The system interacts with or stores sensitive data, including, but not limited to: personally identifiable information, financial information, protected health information, intellectual property, and/or special category data.

Session\_Expiration in Session.has\_restriction The system implements session expiration.

Single\_Sign\_On in Single\_Sign\_On.used Single sign on (SSO) is used.

Size\_Restriction in Files.have Files have a maximum size restriction.

Strong\_Security\_Questions in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to answer strong security questions.

Temporary\_Password in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to enter a temporary password to set a new password.

Trust\_Boundary in Access\_Controls.include Trust boundaries are implemented in the system's access controls.

Trust\_Zone in Access\_Controls.include Trust zones are implemented in the system's access controls.

Unauthorized\_Access in Protected.is The account or data is protected against unauthorized access.

Verification in Where\_To\_Send.requires Password/account recovery requires the email address where recovery information is sent to be verified as belonging to the user.

Where\_To\_Send in Recovery\_Mechanism.has\_restriction Password/account recovery requires an email address for where recovery information is sent to be collected from the user.

Map each of the following requirements to zero or more of the Alloy statements listed above. Only map an Alloy statement to a requirement if the statement can definitely be inferred from requirements. An example is: "The password should be at least 6 characters" maps to "Authentication in Authentication.use\_of, Password in Authentication.uses, Length in Password.has\_restriction." Another example is: "Passwords shall be strong" maps to "Authentication in Authentication.use\_of, Password in Authentication.uses" because it is possible to infer authentication use from password use, but it is not possible to infer other password strength techniques or restrictions due to the requirement being too vague. Another example is: “The user shall upload a document showing address and proof of residency” maps to “Input\_File in User\_Input.obtained\_as, Sensitive\_Data in Sensitive\_Data.transport\_of, Sensitive\_Data in Sensitive\_Data.use\_of” because uploading a document implies uploading a file and addresses are sensitive information. Another example is: “The system shall require users to reset their password every six months.” maps to “Authentication in Authentication.use\_of, Expiration\_Date in Password.has\_restriction, Password in Authentication.uses, Reset in Password.requires” because there’s a requirement for passwords to be reset and passwords are used, but there aren’t any other password restrictions that can be inferred. Another example is: “The user shall be able to access their health history and update their address” maps to “Other\_User\_Input in User\_Input.obtained\_as, Sensitive\_Data in Sensitive\_Data.use\_of” but not other mappings because health history and addresses are both considered sensitive data but it is not specified that it is being sent, and updating the address is a form of user input. If the Alloy statement and requirements are negatives of each other, map the Alloy statement as NOT [Alloy statement]. Please map the [#] requirements below in the following text format “requirement number”, “Alloy mappings”, outputting 50 requirements per response: [REQUIREMENTS]

Output the next set of requirements.

### Optional post-processing provenance explanation prompt:

Given these Alloy criteria and their descriptions ( Administrator\_Security\_Controls in Administrator.has The system's administrator has security controls. Attempts in Authentication.has\_restriction There is a restriction on the number of authentication attempts. Attempts in Recovery\_Mechanism.has\_restriction There is a restriction on the number of password/account recovery attempts. Authentication in Authentication.use\_of Authentication is used. Common in Password.has\_restriction Passwords must avoid the use of common strings such as "password", "admin", or similar. Compartmentalization in Access\_Controls.include Sensitive information is divided into isolated sections, each having its own security controls and access restrictions - isolated sections must be explicitly mentioned, not implied. Config\_File in Password.stored\_in Passwords are stored in a configuration file. Contextual\_String in Password.has\_restriction Passwords must not contain the username or user's information within them. Encrypted in Sensitive\_Data.stored\_as Sensitive data is stored in an encrypted state. Expiration\_Date in Password.has\_restriction Passwords expire. File\_Size in Log\_File.has\_restriction Log file size is limited to a maximum allowed size - log files must be explicitly mentioned or the requirement must specify ALL files. File\_Type in Input\_File.has\_restriction Certain file types or extensions are not allowed to be input into the system. GUI in Credentials.stored\_in The system stores credentials in cleartext directly within the GUI. GUI in Sensitive\_Data.stored\_in The system stores sensitive information in cleartext directly within the GUI. Input\_File in User\_Input.obtained\_as Users can or should input/upload a file into the system. Input\_Validation in Input\_File.has\_restriction Input files are validated. Input\_Validation in Other\_User\_Input.has\_restriction User input other than files is validated. IP\_Address in Authentication.uses The IP address is used for authentication. Least\_Privilege in Access\_Controls.include Users and applications only have access to the minimum resources and permissions they need to perform their designated tasks - this is explicitly mentioned, not implied. Length in Password.has\_restriction There is a restriction on password lengths. Log\_File in Credentials.stored\_in Credentials are stored in the log file. Log\_File in Sensitive\_Data.stored\_in Sensitive data is stored in the log file. Multi\_Factor\_Authentication in Authentication.is The system uses multi factor authentication. Multiple\_Security\_Questions in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to answer multiple security questions. Original\_Password in Reset.requires The original password needs to be provided for password resets. Other\_User\_Input in User\_Input.obtained\_as User input other than files is obtained. Password in Authentication.uses The system uses passwords for authentication. Privilege\_Separation in Access\_Controls.include Privilege separation is implemented in the system's access controls. Recovery\_Mechanism in Password.allows There is a password/account recovery mechanism. Reset in Password.requires Password resets are required. Reuse in Password.has\_restriction The user cannot reuse the same password as the old password for a password change. Security\_Event in Logging.use\_for Security events are logged. Sensitive\_Data in Sensitive\_Data.transport\_of The system sends or receives sensitive data, including, but not limited to: personally identifiable information, financial information, protected health information, intellectual property, and/or special category data. Sensitive\_Data in Sensitive\_Data.use\_of The system interacts with or stores sensitive data, including, but not limited to: personally identifiable information, financial information, protected health information, intellectual property, and/or special category data. Session\_Expiration in Session.has\_restriction The system implements session expiration. Strong\_Security\_Questions in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to answer strong security questions. Temporary\_Password in Recovery\_Mechanism.has\_restriction Password/account recovery requires the user to enter a temporary password to set a new password. Trust\_Boundary in Access\_Controls.include Trust boundaries are implemented in the system's access controls. Trust\_Zone in Access\_Controls.include Trust zones are implemented in the system's access controls. Verification in Where\_To\_Send.requires Password/account recovery requires the email address where recovery information is sent to be verified as belonging to the user. Where\_To\_Send in Recovery\_Mechanism.has\_restriction Password/account recovery requires an email address for where recovery information is sent to be collected from the user. ) I will give you a list of provenances of why various weaknesses occur in a software. Can you explain what are the inherent problems in the software requirements?

[PROVENANCES]