**Databases Management (base from Gourd’s pdf)**

**Get txt on github(if needed):**

**DB(cyber).txt \*creates user ‘cyber’/rename to user.sql**

**DB(user).txt \*creates final ‘cyber’/rename to db.sql**

**Db(configurations).txt \*php source/rename to config.php**

**Db(functions).txt \*php source/rename to db.php**

**Db(testWeb).txt \*php source/rename to index.php**

sudo apt-get install mysql-server \*install mysql-server

mysql -uroot –p

CREATE DATABASE test; \*creates a database name test

USE test;

**\*creates a team table**

CREATE TABLE `teams` ( `id` smallint(5) unsigned NOT NULL AUTO\_INCREMENT, `name` varchar(50) NOT NULL DEFAULT '', `score` int(10) NOT NULL, PRIMARY KEY (`id`) ) ENGINE=InnoDB DEFAULT CHARSET=latin1;

DESCRIBE teams; \*what does it look like

**\*: means everything that’s being called from, ex) everything that’s underneath teams database**

SELECT \* FROM teams; \*what does it have

DROP DATABASE test; \*undo by removing the database

CREATE USER 'cyber'@'localhost' IDENTIFIED BY 'cyber'; \*create another users

CREATE DATABASE cyber;

GRANT ALL PRIVILEGES ON cyber.\* TO 'cyber'@'localhost';

**Logout and log into new users**

mysql –u<user> -p<password> <database> **\*new user format**

SHOW DATABASES;

SHOW TABLES;

CREATE TABLE `teams` ( `id` smallint(5) unsigned NOT NULL AUTO\_INCREMENT, `name` varchar(50) NOT NULL DEFAULT '', `score` int(10) NOT NULL, PRIMARY KEY (`id`) ) ENGINE=InnoDB DEFAULT CHARSET=latin1;

CREATE TABLE `acl` ( `id` smallint(5) unsigned NOT NULL AUTO\_INCREMENT, `team\_id` smallint(5) unsigned NOT NULL DEFAULT '0', `password` varchar(50) NOT NULL DEFAULT '', PRIMARY KEY (`id`), KEY `acl\_team\_id` (`team\_id`), CONSTRAINT `acl\_team\_id` FOREIGN KEY (`team\_id`) REFERENCES `teams` (`id`) ON DELETE CASCADE ON UPDATE CASCADE ) ENGINE=InnoDB DEFAULT CHARSET=latin1;

INSERT INTO `teams` VALUES (1,'GREED',0); \*add some data to the team table

INSERT INTO `teams` VALUES (2,'CHARITY',0);

SELECT \* FROM teams; \*what it contains

INSERT INTO `acl` VALUES (1,1,password('password')); \*add some data

INSERT INTO `acl` VALUES (2,2,password('123456'));

SELECT \* FROM acl; \*what is contains

**\*find pw(in hash) of GREED)**

SELECT `password` FROM acl WHERE `team\_id`=(SELECT `id` FROM teams WHERE `name`='GREED');

1. (SELECT `id` FROM teams WHERE `name`='GREED'); \*returns the ID 1
2. SELECT `password` FROM acl WHERE `team\_id`=1; \*uses this first value
   1. **SELECT `password` FROM acl,teams WHERE acl.`team\_id`=teams.`id` AND teams.`name`='GREED'; \*could do this too**
   2. **SELECT `password` FROM acl a,teams t WHERE a.`team\_id`=t.`id` AND t.`name`='GREED'; \*another shorthand**

**More SQL queries**

**note that % in SQL behaves very much like \* in bash**

SELECT `score` FROM teams WHERE `name` LIKE 'GRE%';

SELECT `score` FROM teams WHERE `name` LIKE 'gre%'; \*case insensitive

UPDATE teams SET `score`=`score`+100 WHERE `name` LIKE '%ree%'; \*gives points to name with that

SELECT \* FROM teams;

**PHP**

sudo apt-get install php libapache2-mod-php php-mysql \*install PHP

**to connect to the database, we'll need two configuration files**

**one for useful database functions: db.php**

**one to access the cyber database: config.php**

**to allow users to interact, we'll need a main HTML file: index.php**

**place the three files in /var/www/html**

**and remove index.html (if it already exists)**

**TRY IT OUT**

SELECT `name`,`score` FROM teams WHERE `name`='<whatever the user entered>’

SELECT `name`,`score` FROM teams WHERE `name`='GREED'

**Want to see the entire table and have no clue what the team names are**

SELECT `name`,`score` FROM teams WHERE `name`='name' or 'a'='a'

**\*note that ‘name’=’name’ is false but ‘a’=’a’ is true**

**Character ‘a’ is always = to character ‘a’**

**Entire WHERE clause will be true, causing SELECT caluse to performed the result**

**That ‘name’ and ‘score’ for all teams in the database**

SELECT `name`,`score` FROM teams WHERE `name`='blah'; delete from teams; -- '

**Nothing in blah so returns nothing**

**\*-- means that whatever follows is a comment**

DELETE FROM teams; \*deletes everything in teams tables

SELECT `name`,`score` FROM teams WHERE `name`='blah'; select \* from acl; -- '

SELECT \* FROM acl;

**Attacker is guessing, 1st SQL query does not perform cause WHERE clause is false**

**But 2nd 1 returns all tables in acl**

SELECT `name`,`score` FROM teams WHERE `name`='blah'; show tables; -- '

**\*listing of tables in cyber database returns**

SELECT `name`,`score` FROM teams WHERE `name`='blah'; show databases; -- '

**\*listing of databases accessible by user in cyber returns**

mysqldump -ucyber -p --skip-extended-insert --add-drop-database --add-drop-table --databases cyber

**export content of databases(do this outside of MySQL, at the terminal)**

mysqldump -ucyber -p --skip-extended-insert --add-drop-database --add-drop-table --databases cyber > db.sql

**save this file**

**let's drop the database to see how the file can be used to recreate it:**

mysql -ucyber -p

DROP DATABASE cyber;

SHOW DATABASES;

Exit

**and let's recreate it:**

mysql -ucyber -p < db.sql

mysql -ucyber -p cyber

SHOW TABLES;

SELECT \* FROM teams;

**the script user.sql is provided on the web site to facilitate creating the cyber user (the first time) execute it this way:**

mysql -uroot -p < user.sql