ECE568 Lecture 09:
Web Security & Cryptography 02

Wei Huang
Department of Electrical and Computer Engineering
University of Toronto

Lecture Outline

- SQL injection, DNS Rebinding
- Modular Arithmetic
- Diffie-Hellman
- RSA

SQL injection (Lab 4, Parts 6-8)

- Web server often takes input from HTTP requests and uses it in a SQL query to a backend database. For example, when authenticating a user:

```
set ok = execute(“SELECT * FROM UserTable
   WHERE username=’ ”  &  form(“user”)  &
   “ ’ AND password=’ ” & form(“pwd”) & “ ’ ” );

  If not ok.EOF
       login success
  else  fail;
```

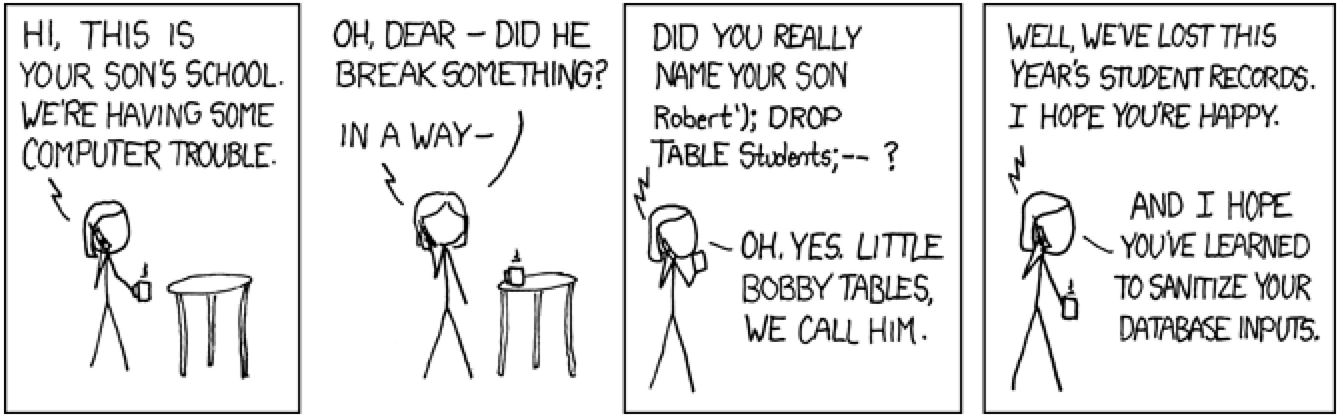
- Code takes `user` and `pwd` inputs from HTML form and does a query on the database to see if they are correct.

SQL injection

- In this case, the attacker is the person browsing the web page and the victim is the web site:
  - If attacker sets `user  = ' or 1 = 1 --` then the query becomes:

```
SELECT * FROM UserTable
WHERE username=' ' or 1 == 1 -- & …
```

  - Since 1 == 1 is always true, then the attacker can now login even if they do not know the user's password (the -- in SQL means to ignore everything afterwards).


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH, YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

DNS Rebinding attack

- To load balance, many web sites use very short DNS Time To Live (TTLs):
  - This means that the IP address for the web site changes frequently to spread load among the web servers in the server farm.
  - As a result, web browsers are used to querying the DNS for IP addresses often.

DNS Rebinding Attack

- Attacker can circumvent SOP by:
  1. Get the victim to visit the attacker's site. Attacker who controls the DNS for his site returns a DNS mapping with a short TTL and returns a web page with malicious javascript.
  2. The javascript again makes a query to the attacker's web site. The browser must make another DNS query, but this time the attacker's DNS returns **the IP address of a victim's web site**
  3. Now the browser believes that both the victim web site and attacker web site are in the same origin. Attacker's javascript can access victim's web site freely.
- Difficult to distinguish from IP address switching due to load balancer from this attack.
  – Current best defense is to check if both addresses are in the same subnet, but this is just a hack

Modular Arithmetics

Diffie Hellman

Public Key Cryptosystems

- Public Key (also called asymmetric) cryptosystems work as follows:
  - Every user has a public/private key pair. The private key and public key reveal nothing about each other.
  - Messages encrypted with one key can only be decrypted with the other key.
  - Users distribute the public key, and keep the private key in a safe place.
  - When someone wants to send a message, she encrypts the message with the intended recipient’s public key. Only the recipient should have the matching private key, so only the intended recipient can recover the original message.

RSA