Foundations of Security

Prepared by:
Chrevic Josef P. Dangan

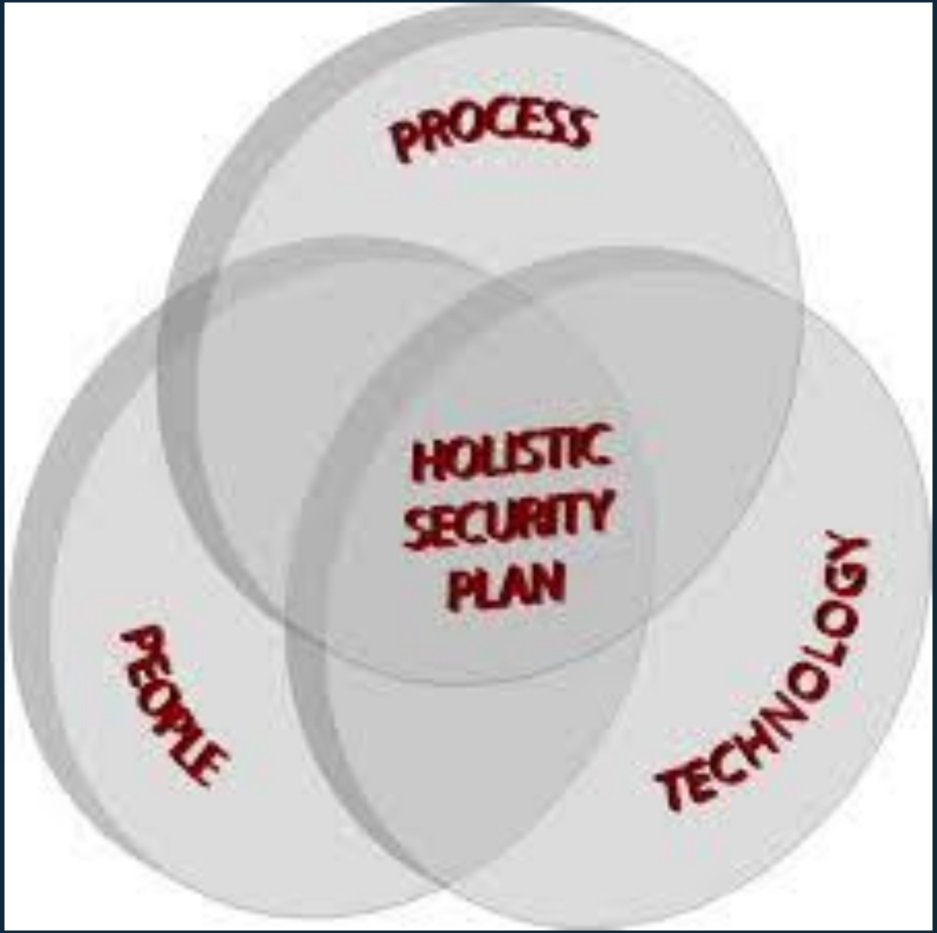
Today's Topics

- Security Goals
- Security Threats

What are the primary concerns in Software Engineering?

Security in Software Engineering

Holistic Security



Holistic Security

- Technological Security (Application, OS, Network)
- Physical Security (servers, dumpsites)
- Policies and Procedures
- People

Security Goals

- Authentication
- Authorization
- Confidentiality
- Data/message integrity
- Accountability
- Availability
- Non-repudiation

Authentication

- Act of verifying someone's identity
- Something You Know
- Something You Have
- Something You Are
- Two-Factor Authentication

Authorization

- Act of checking whether user has permission to conduct some action
- Access Control Lists (ACL)

Confidentiality

- Keep contents of a transient communication or data on temporary or persistent storage secret
- Encryption and Cryptography
- Public and Private keys
- HTTPS vs HTTP

Message / Data Integrity

- When Alice and Bob exchange messages, they don't want a third party such as Mallory to be able to modify the contents of their messages

Message / Data Integrity

- Man in the middle attack
- Integrity checks (e.g. Cyclic Redundancy Checks)

Accountability

- Ensure that you are able to determine who the attacker is in the case that something goes wrong
- Logging and audit trails
- Make sure logs can't be altered / deleted manually

Availability

- System can respond to its users' requests in reasonable timeframe
- Denial of Service Attack (DoS)
- Distributed Denial of Service Attack (DDoS)

Non-repudiation

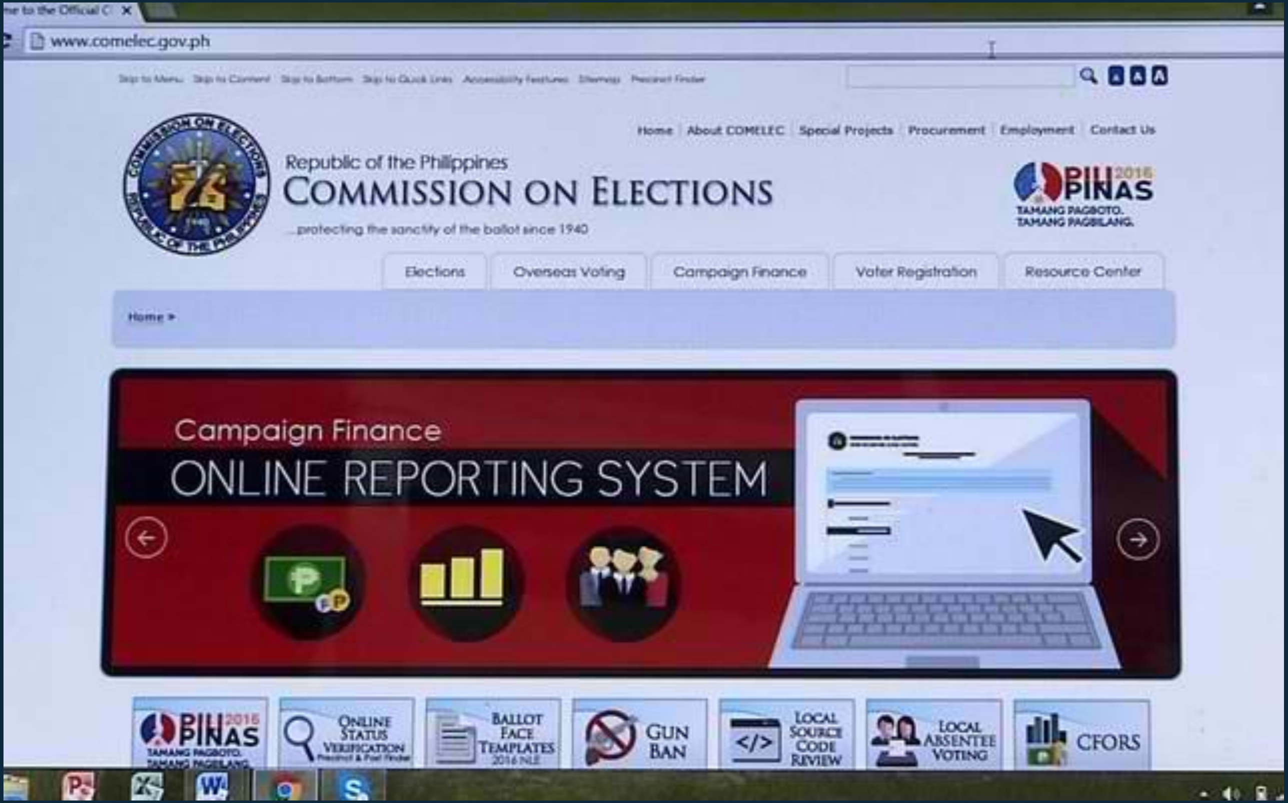
- Ensure undeniability of a transaction by any of the parties involved
- Trusted third party can be used to accomplish this
- Good in theory, expensive to implement

Security Threats

Defacement

- Form of online vandalism in which attackers replace legitimate pages of organization's web site with illegitimate ones

- Anonymous



Republic of the Philippines

COMMISSION ON ELECTIONS

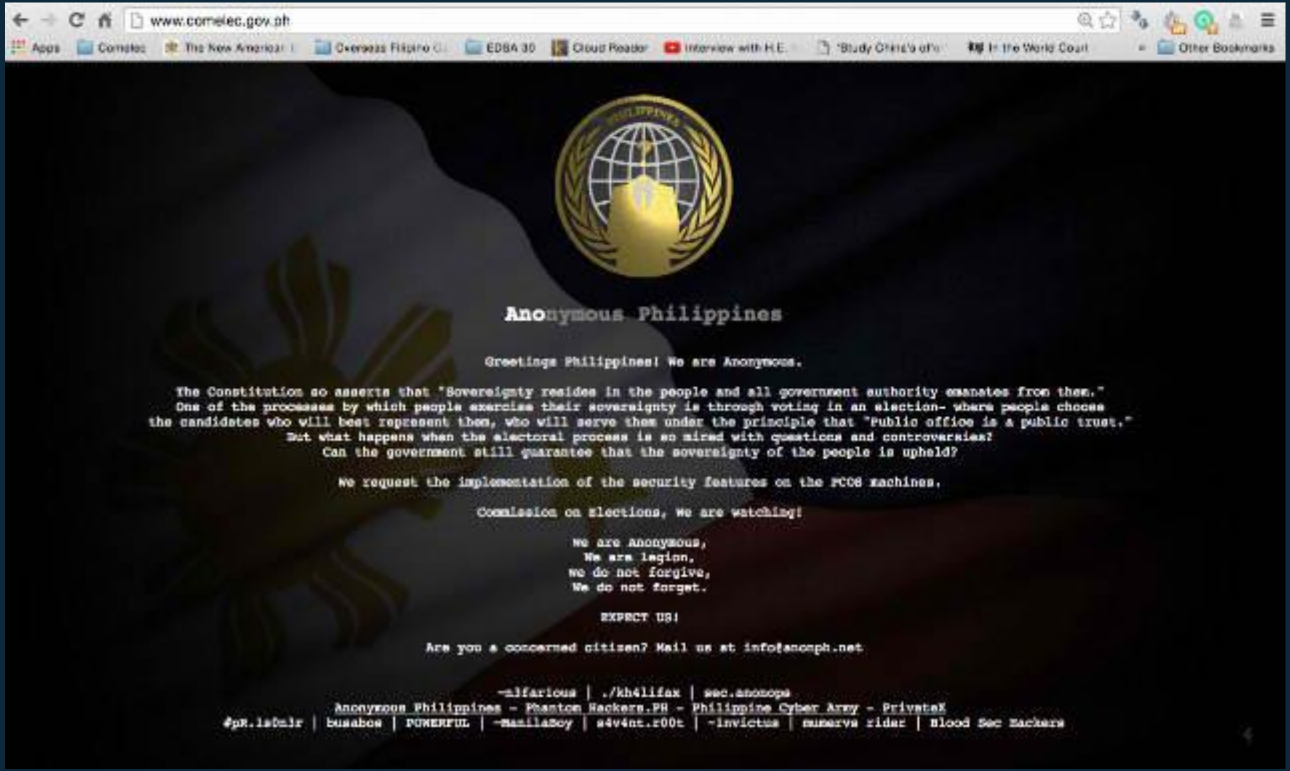
...protecting the sanctity of the ballot since 1940

Campaign Finance

ONLINE REPORTING SYSTEM

PILIPINAS 2016 TAMANG PAGBOTO. TAMANG PAGBILANG.
ONLINE STATUS VERIFICATION Precinct & Poll Finder
BALLOT FACE TEMPLATES 2016 NLE
GUN BAN
LOCAL SOURCE CODE REVIEW
LOCAL ABSENTEE VOTING
CFORS

COMELEC (before)



Anonymous Philippines

Greetings Philippines! We are Anonymous.

The Constitution so asserts that "Sovereignty resides in the people and all government authority emanates from them."
One of the processes by which people exercise their sovereignty is through voting in an election- where people choose
the candidates who will best represent them, who will serve them under the principle that "Public office is a public trust."
But what happens when the electoral process is so mired with questions and controversies?
Can the government still guarantee that the sovereignty of the people is upheld?

We request the implementation of the security features on the PCOS machines.

Commission on Elections, we are watching!

We are Anonymous,
We are legion,
We do not forgive,
We do not forget.

EXPECT US!

Are you a concerned citizen? Mail us at info@anonph.net

~n1farious | ./kh4lifax | sec.anonops
Anonymous Philippines - Phantom Hackers.PH - Philippine Cyber Army - PrivateX
#pR.is0n1r | busabos | POWERFUL | ~ManilaBoy | s4v4nt.r00t | ~invictus | minerva rider | Blood Sec Hackers

COMELEC (after)

Infiltration

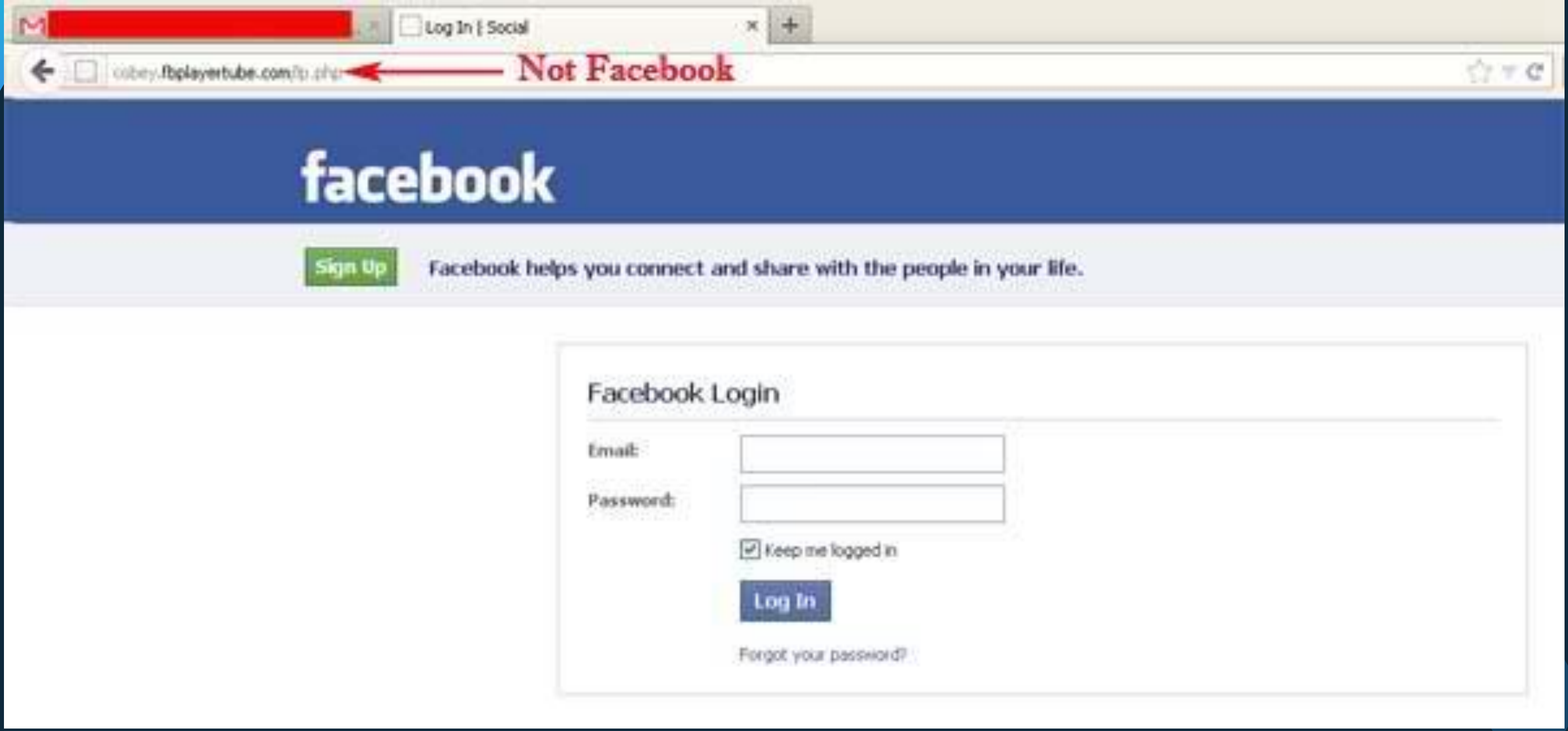
- Unauthorized party gains full access to resources of a computer system (CPUs, disk, network bandwidth)
- Done by buffer overflow, command injection, etc.

Defacement vs Infiltration

- Both show that there are security vulnerabilities
- Defacement could be just embarrassing
- Infiltration could be a real threat

Phishing

- Attack in which attacker sets up a spoofed web site that looks similar to a legitimate web site
- Attacker lures victims to spoofed web site and enter their login credentials
- Spam emails



[redacted]

Log In | Social

osbey.fbplayertube.com/lp.php

Not Facebook

facebook

Sign Up

Facebook helps you connect and share with the people in your life.

Facebook Login

Email:

Password:

☑ Keep me logged in

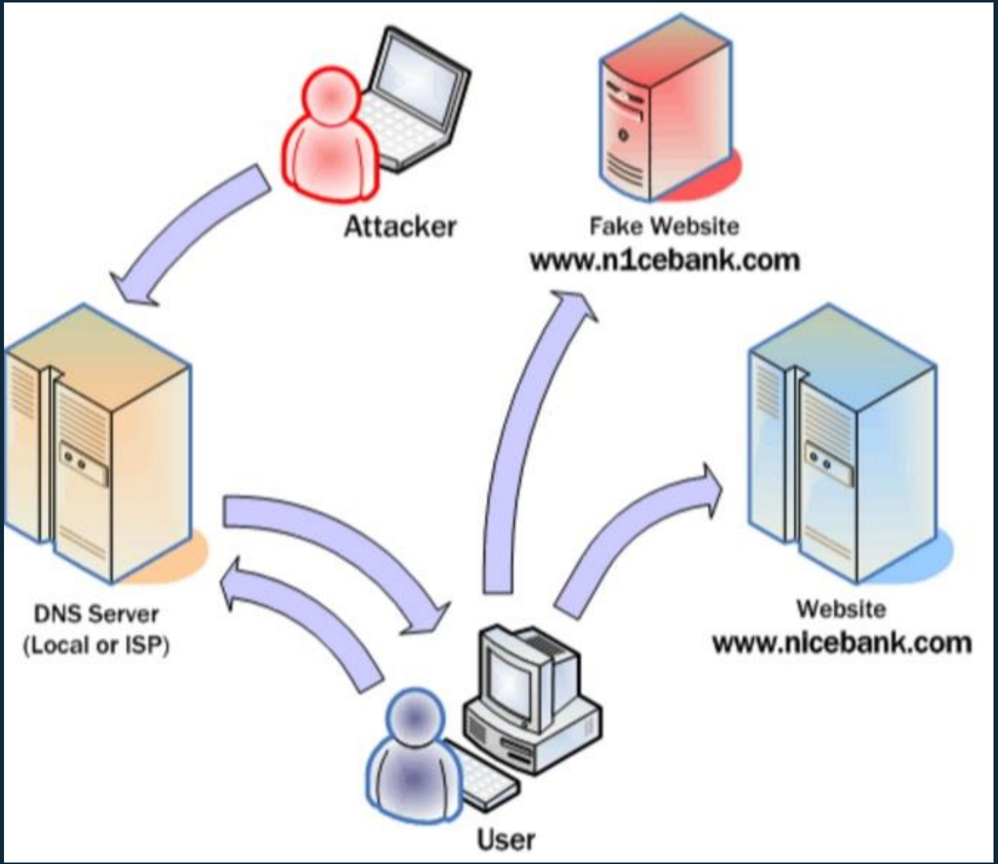
Log In

Forgot your password?

Phishing

Pharming

- User can be fooled into entering sensitive data into spoofed website
- Even if user correctly enters URL, attacker can redirect user to a malicious web site
- aka *DNS Cache Poisoning*


Attacker
Fake Website
www.n1cebank.com
DNS Server
(Local or ISP)
Website
www.nicebank.com
User

Pharming

Insider Threats

- Employees who abuse privileges to carry out malicious deeds
- Selling figures, financial reports to the black market, insider trading

Insider Threats

- "Inside job"
- Fooled employee (social engineering attack)

Click Fraud

- Pay-per-click advertising
- Click competitor's advertisements to max out their budget

Data Theft / Data Loss

- Banks, Social Security numbers
- Hard copy / soft copy

Worms

- Type of virus (program capable of making copies of itself and inserting copies into other programs)

- Uses network to copy itself onto other computers

More Malware

- ◇ **Rootkit**
  - set of impostor OS tools meant to replace the standard version to hide activities of attacker

More Malware

- ◇ **Trojan Horses**
  - software that claims to perform one function but performs and additional or different function than advertised once installed

More Malware

- **Spyware**
  - software that monitors activity of system and some or all of its users without their consent

More Malware

- ◇ **Keylogger**
  - type of spyware that monitors keyboard or mouse input
  - used to steal usernames, passwords, credit card numbers, bank account numbers, PINs

More Malware

- ◇ **Botnets**
  - network of software robots that attackers use to control large numbers of machines at once
  - used in DDoS

More Malware

◇ **Clickbot**

- software robot that clicks on ads to help attacker conduct click fraud
- also used in "Likes" contest

Cross-Site Request Forgery (XSRF)

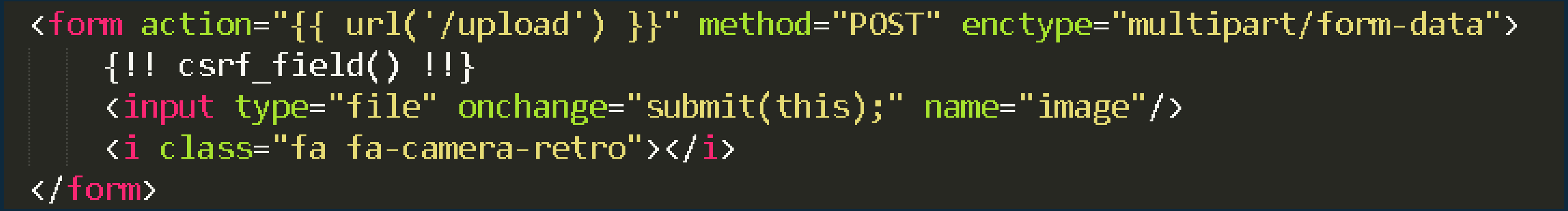
- aka *Session Riding*
- Unauthorized commands are transmitted from a user that the website trusts

XSRF Example

Eve: Hello Alice!

Look here: <img src="http://bank.example.com/withdraw?account=Alice&amount=1000000&for=Eve">

csrf in Laravel



```
<form action="{{ url('/upload') }}" method="POST" enctype="multipart/form-data">
    {!! csrf_field() !!}
    <input type="file" onchange="submit(this);" name="image"/>
    <i class="fa fa-camera-retro"></i>
</form>
```

Solution

- Check Referer header

Cross-Site Scripting (XSS)

- Attackers inject client-side script into Web pages viewed by other users
- One of the more notorious web application vulnerabilities
- MySpace XSS Worm "Samy"

Cross-Site Scripting (XSS)

- Annoying to dangerous
- Used in Session Hijacking (stealing cookies)

Solution

- Input Validation
- Output Sanitization

SQL Injection

- Type of command injection
- Untrusted data is inserted into query

SQL Injection

- Specially crafted malicious input causes the query processor to misinterpret part of the supplied data

- One of the top 10 web application vulnerabilities

Client-Side Manipulation

- POST vs GET request in Form Sending
- Cookie Stealing

Others

- Replay Attacks
- Buffer Overflow
- IP Spoofing (related: Onion Routing)

Counter-Attacks

- Firewalls (allow web host to specify that they trust some host to connect to them on some ports while some are not trusted)
- Validations and Sanitation
- Fraud Checks

Things to Avoid

- ◇ Don't Roll Your Own Cryptography
- ◇ Don't hard code keys
- ◇ Don't neglect security

Final Thoughts on Security

"Security is a process, not a product."

–B.Schneier

"Better safe than sorry"

Final Thoughts on Security

- Build in security right from the start, not just at the end.
- Don't forget containment and recovery.
- Convenience / Less Complexity vs. Security

Wireshark

- HTTP vs HTTPS
- CRS and Facebook
- Can be used to steal passwords and sessions

Authentication

- Go to home.php without logging in
- Fix: Redirect to index.php if not logged in

SQL Injection

◇ Example #1

```
$username = blah' OR '1' = '1' -- '

WHERE username='blah' OR '1' = '1' -- ''
AND password=MD5('$password')

WHERE username='blah' OR '1' = '1'
```

SQL Injection

- Example #2

$username = roi' OR '1' = '1

WHERE username='roi' OR '1' = '1' AND password=MD5('$password')

WHERE username='roi' OR '1' = '1' AND password=MD5('$password')

Worse Things

- Good thing PHP's mysql interface doesn't support multiple SQL statements in one query

- SELECT * FROM users WHERE username='$username'

Worse Things

```
$username = '; DROP TABLE users; -- '

SELECT * FROM users WHERE
username=''; DROP TABLE users; -- ''
```

PHP Solutions

- mysql_escape_string (Deprecated)
- mysql_real_escape_string

Logic Error

Fix: Change mysql_num_rows($result) > 0

Change To: mysql_num_rows($result) == 1

Escaping Quotes

- A Little Less "Sixteen Candles", A Little More "Touch Me"
- Sugar We're Going Down

PHP Solutions

- mysql_real_escape_string
- stripslashes

More Robust Solutions

- PHP mysqli
- PHP Data Objects

mysqli

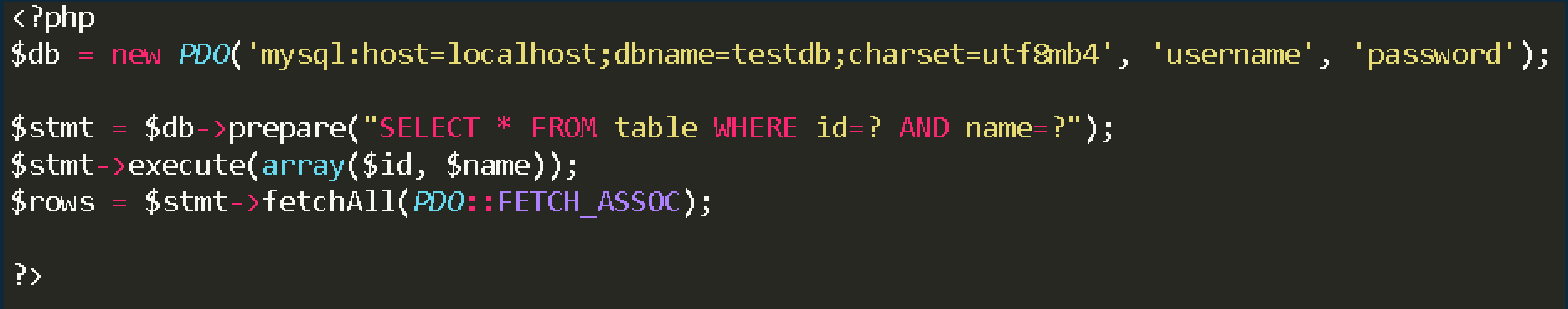
- MySQL improved
- Object-Oriented and Procedural Interfaces

mysqli Enhancements

- Object-oriented interface
- Prepared statements
- Multiple statements
- Transactions

PDO

- Database abstraction layer
- Consistent API for PHP application regardless of database server

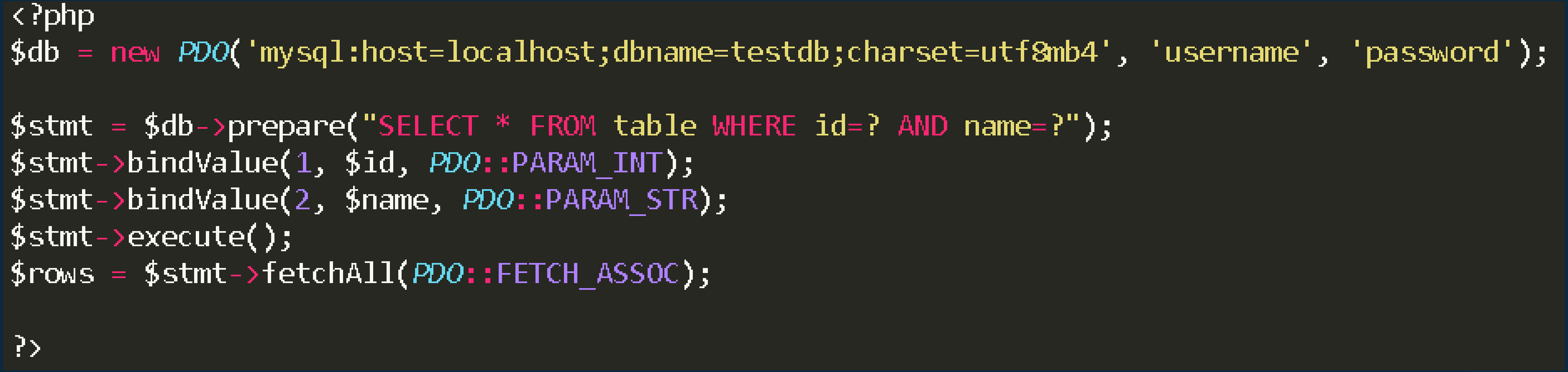


```php
<?php
$db = new PDO('mysql:host=localhost;dbname=testdb;charset=utf8mb4', 'username', 'password');

$stmt = $db->prepare("SELECT * FROM table WHERE id=? AND name=?");
$stmt->execute(array($id, $name));
$rows = $stmt->fetchAll(PDO::FETCH_ASSOC);

?>
```

PDO



```php
<?php
$db = new PDO('mysql:host=localhost;dbname=testdb;charset=utf8mb4', 'username', 'password');

$stmt = $db->prepare("SELECT * FROM table WHERE id=? AND name=?");
$stmt->bindValue(1, $id, PDO::PARAM_INT);
$stmt->bindValue(2, $name, PDO::PARAM_STR);
$stmt->execute();
$rows = $stmt->fetchAll(PDO::FETCH_ASSOC);

?>
```

PDO

Filters & Validations

- Type Checking (even in Dynamic PLs)
- Server-Side Validation (for Security)
- Client-Side Validation (for Convenience)
- Use both SS and CS Validation!

Frameworks & Good Practice

- Most frameworks already take care of usual security threats

- Always follow good practice, even when it's not needed

HTML Tags

- CMSC 126 Students: This is the new video tag: <video>

- I'm <b>bold</b>

- I'm <span style="font-size:100px">HUGE!</span>

XSS

```
<script>document.write("helloworld");
</script>

<script>alert("Annoying, isn't it?");</script>
```

XSS

```
<script>
window.onload = function(){
        document.open();
        document.write("You ar3 now
hack3d! Pawn3d!! Weep now!!!!");
        document.close();
};
</script>
```

PHP Solutions

- htmlspecialchars
- htmlentities
- htmlentities_decode

Other Solutions

- Disable JavaScript!

Bonus: Password Hashing

- password = MD5('$password')
- password = PASSWORD('$password')
- password = SHA1('$password')

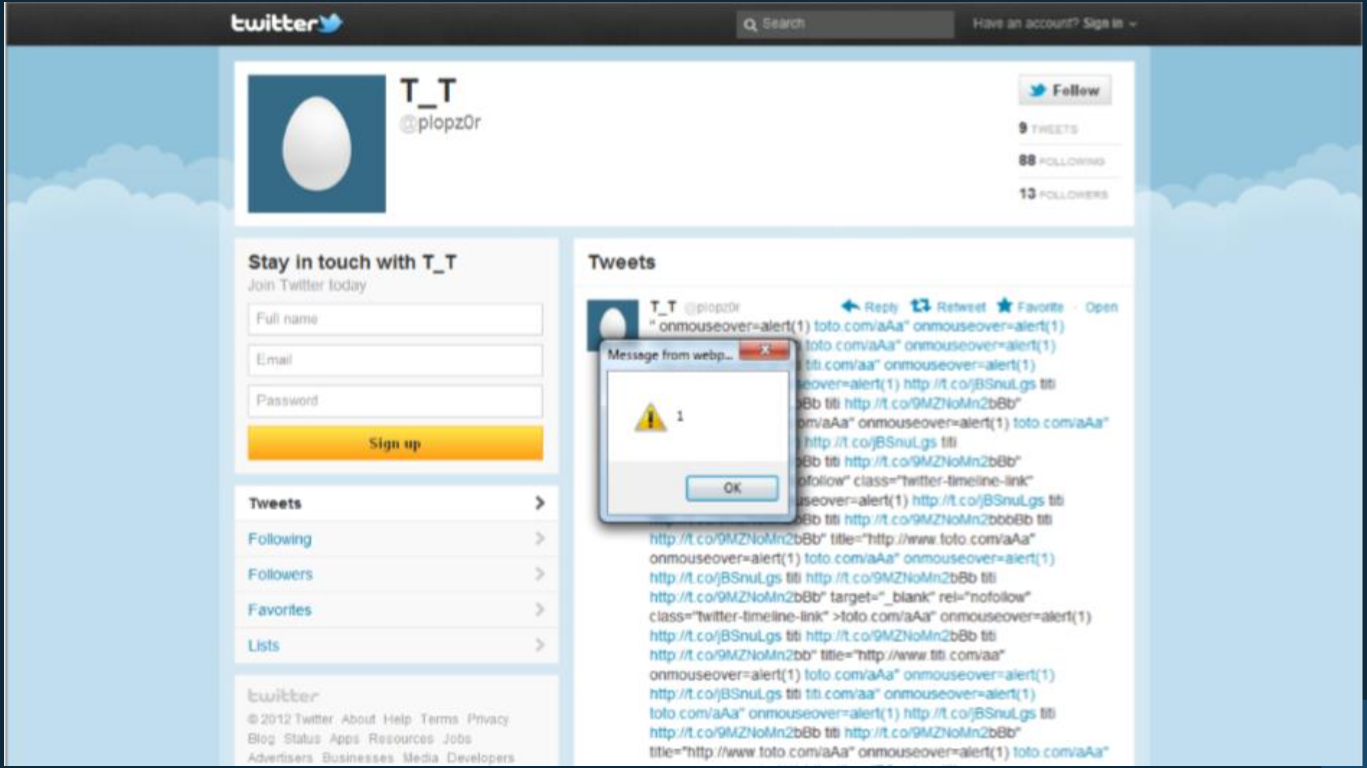
Reasons

- If we store the password as is, once the database is compromised, all the passwords can easily be seen

- Password Hashing makes it harder to guess the passwords even with a compromised database

Password Hashing

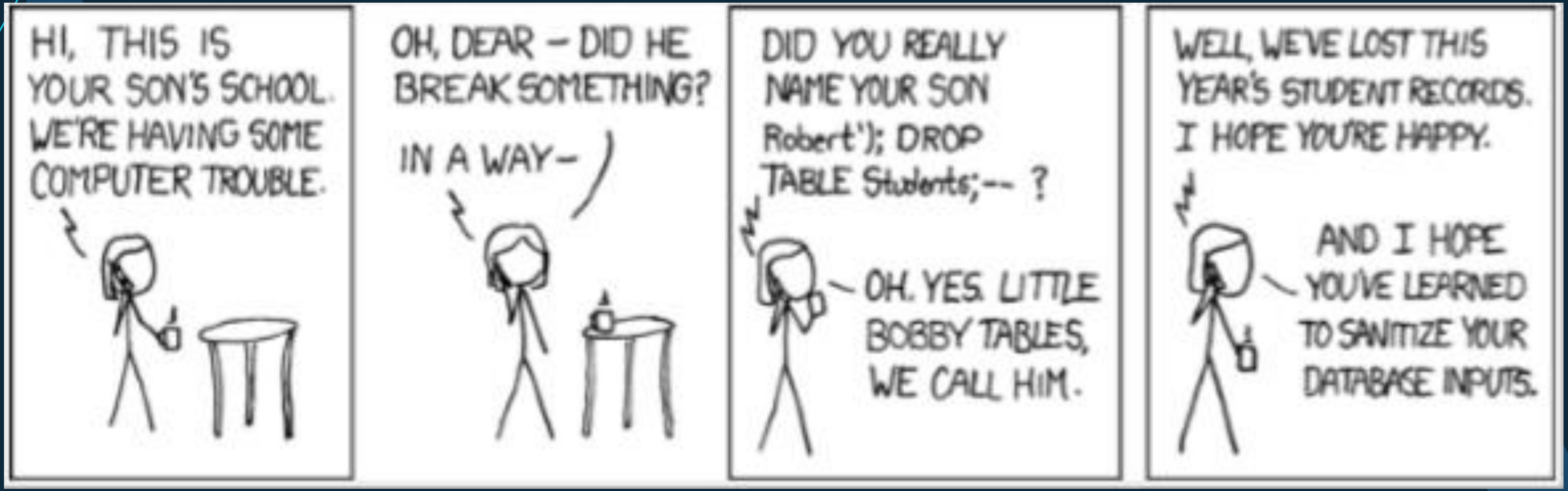
- Hashing is usually one-way; no decryption (Why?)
- Knowing which Hashing algo used won't help you (Why?)



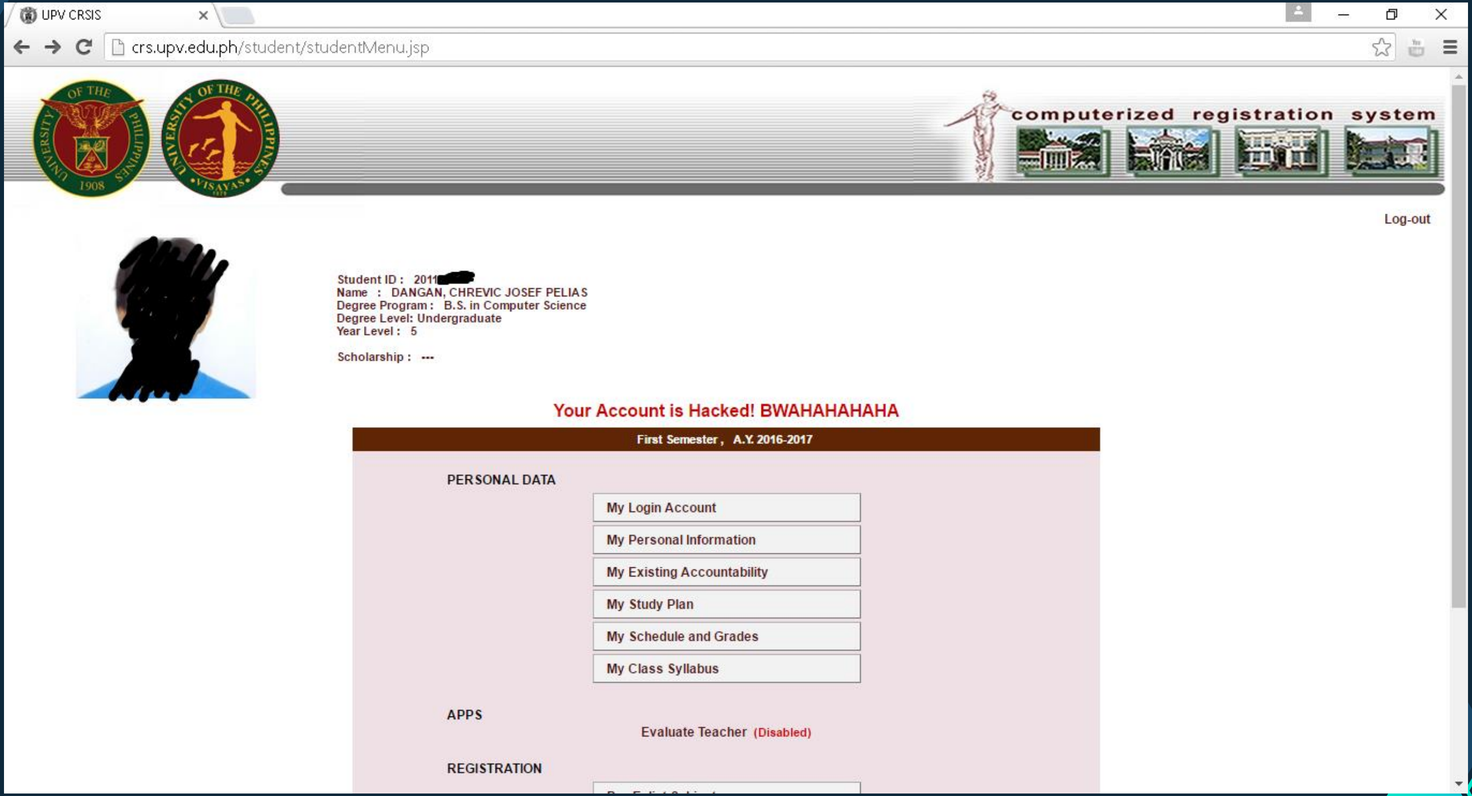
```
" onmouseover=alert(1) toto.com/aAa" onmouseover=alert(1)
toto.com/aAa" onmouseover=alert(1)
titi.com/aa" onmouseover=alert(1)
eover=alert(1) http://t.co/jBSnuLgs titi
Bb titi http://t.co/9MZNoMn2bBb"
m/aAa" onmouseover=alert(1) toto.com/aAa"
http://t.co/jBSnuLgs titi
Bb titi http://t.co/9MZNoMn2bBb"
ofollow" class="twitter-timeline-link"
seover=alert(1) http://t.co/jBSnuLgs titi
Bb titi http://t.co/9MZNoMn2bbbBb titi
http://t.co/9MZNoMn2bBb" title="http://www.toto.com/aAa"
onmouseover=alert(1) toto.com/aAa" onmouseover=alert(1)
http://t.co/jBSnuLgs titi http://t.co/9MZNoMn2bBb titi
http://t.co/9MZNoMn2bBb" target="_blank" rel="nofollow"
class="twitter-timeline-link" >toto.com/aAa" onmouseover=alert(1)
http://t.co/jBSnuLgs titi http://t.co/9MZNoMn2bBb titi
http://t.co/9MZNoMn2bb" title="http://www.titi.com/aa"
onmouseover=alert(1) toto.com/aAa" onmouseover=alert(1)
http://t.co/jBSnuLgs titi titi.com/aa" onmouseover=alert(1)
toto.com/aAa" onmouseover=alert(1) http://t.co/jBSnuLgs titi
http://t.co/9MZNoMn2bBb titi http://t.co/9MZNoMn2bBb"
title="http://www.toto.com/aAa" onmouseover=alert(1) toto.com/aAa"
```

```
1
```

Casualties


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.

Casualties



UPV CRSIS
crs.upv.edu.ph/student/studentMenu.jsp
computerized registration system
Log-out

[redacted]

Student ID : 2011[redacted]
Name : DANGAN, CHREVIC JOSEF PELIAS
Degree Program : B.S. in Computer Science
Degree Level: Undergraduate
Year Level : 5

Scholarship : ---

Your Account is Hacked! BWAHAHAHAHA

First Semester , A.Y. 2016-2017

PERSONAL DATA

- My Login Account
- My Personal Information
- My Existing Accountability
- My Study Plan
- My Schedule and Grades
- My Class Syllabus

APPS

Evaluate Teacher (Disabled)

REGISTRATION

Casualties

Two Hacker Hats

- ◇ **WHITE HAT**
  - 'good hackers' : improve security

- ◇ **BLACK HAT**
  - 'bad hackers' : exploit vulnerabilities

Types

End of Third Long Exam Topics

End of CMSC129

Any questions?

References

Foundations of Security, N.Daswani et al, 2007

Important Dates

3rd Long Exam:

May 11 (Wed), 5:30PM onwards CL2

Final Lessons

- Don't *memorize*; understand!
- Experience is the best teacher
- Do pet projects
- Don't stop learning new technologies
- Evolve or die (gracefully)

Whenever you feel you can't..

- Remember: CJDi
- Calmly, Just Do it.