Weaver
Spring 2022

CS 161
Computer Security

Exam Prep 7

Q1 *To The Moon* (15 points)

ToTheMoon Bank has just created an online banking system. When a user wants to complete a transfer, they follow these steps:

1. The user logs in by making a POST request with their username and password.
2. The server sets a cookie with `name=auth_user` and `value=$token`, where `$token` is a session token specific to the user's login session.
3. The user initiates a transfer by making a GET request to `https://tothemoonbank.com/transfer?amount=$amount&to=$user`, replacing `$amount` and `$user` with the intended amount and recipient. Transfers use a parameterized SQL query.
4. The server runs the SQL query `SELECT username FROM users WHERE session_token = '$token'`, replacing `token` with the value of the cookie. The server does not use parameterized SQL or any input sanitization.

Q1.1 (4 points) Which of the following attacks are possible in this system? Select all that apply.

□ (A) SQL injection

□ (B) ROP attack

□ (C) CSRF attack

□ (D) Path traversal attack

□ (E) None of the above

□ (F) ——

Q1.2 (4 points) Mallory is a malicious user with an account on ToTheMoon Bank. Mallory creates a malicious link `https://tothemoonbank.com/transfer?amount=100&to=Mallory`.

Which of the following scenarios would cause Alice to send $100 to Mallory? Select all that apply.

□ (G) Alice clicks on the malicious link when Alice is not logged into the bank

□ (H) Alice clicks on the malicious link when Alice is logged into the bank

□ (I) Alice visits Mallory's website, which has an `img` tag loading the malicious link, when Alice is not logged into the bank

□ (J) Alice visits Mallory's website, which has an `img` tag loading the malicious link, when Alice is logged into the bank

□ (K) None of the above

□ (L) ——

Q1.3 (4 points) Suppose Step 4 is modified. To initiate a transfer, instead of making a GET request, the user makes a POST request to `https://tothemoonbank.com/transfer` with the amount and recipient in the POST body.

Which of the following scenarios would cause Alice to send $100 to Mallory? Select all that apply.

Clarification during exam: The malicious link in the answer choices should be `https://tothemoonbank.com/transfer?amount=100&to=Mallory`.

□ (A) Alice clicks on the malicious link when Alice is not logged into the bank

□ (B) Alice clicks on the malicious link when Alice is logged into the bank

□ (C) Alice visits Mallory's website, which has an `img` tag loading the malicious link, when Alice is not logged into the bank

□ (D) Alice visits Mallory's website, which has an `img` tag loading the malicious link, when Alice is logged into the bank

□ (E) None of the above

□ (F) ——

Q1.4 (3 points) Which user inputs might be vulnerable to SQL injection? Select all that apply.

□ (G) `amount` parameter

□ (H) `to` parameter

□ (I) Value of the `auth_user` cookie

□ (J) None of the above

□ (K) ——

□ (L) ——

Q2 *SQL Injection* **(20 points)**

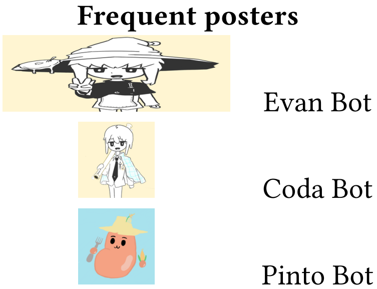
CS 161 students are using a modified version of Piazza to discuss project questions! In this version, the names and profile pictures of the students who answer questions frequently are listed on a side panel on the website.

The server stores a table of users with the following schema:

```
CREATE TABLE users (
    First TEXT,                  -- First name of the user.
    Last TEXT,                   -- Last name of the user.
    ProfilePicture TEXT,         -- URL of the image.
    FrequentPoster BOOLEAN,      -- Are they a frequent poster?
);
```

Q2.1 (3 points) Assume that you are a frequent poster. When playing around with your account, you notice that you can set your profile picture URL to the following, and your image on the frequent poster panel grows wider than everyone else's photos:

ProfilePicture URL: `https://cs161.org/evan.jpg" width="1000`



Frequent posters

Evan Bot

Coda Bot

Pinto Bot

What kind of vulnerability might this indicate on Piazza's website?

○ (A) Stored XSS

○ (B) Reflected XSS

○ (C) CSRF

○ (D) Path traversal attack

○ (E) Buffer overflow

○ (F) ——

Q2.2 (3 points) Provide a malicious image URL that causes the JavaScript `alert(1)` to run for any browser that loads the frequent poster panel. Assume all relevant defenses are disabled.

Hint: Recall that image tags are typically formatted as `<img src="image.png">`.

Q2.3 (4 points) Suppose your account is not frequent poster, but you still want to conduct an attack through the frequent posters panel!

When a user creates an account on Piazza, the server runs the following code:

```
query := fmt.Sprintf("
    INSERT INTO users (First, Last, ProfilePicture, FrequentPoster)
        VALUES ('%s', '%s', '%s', FALSE);
    ",
    first, last, profilePicture)
db.Exec(query)
```

Provide an input for `profilePicture` that would cause your malicious script to run the next time a user loads the frequent posters panel. You may reference `PAYLOAD` as your malicious image URL from earlier, and you may include `PAYLOAD` as part of a larger input.

Q2.4 (4 points) Instead of injecting a malicious script, you want to conduct a DoS attack on Piazza! Provide an input for `profilePicture` that would cause the SQL statement `DROP TABLE users` to be executed by the server.

Suppose that session cookies are used to authenticate to Piazza. This token is checked whenever the user sends a request to Piazza.

Clarification during exam: "Your malicious script" refers to your exploit in 7.2.

Q2.5 (3 points) Your malicious script submits a GET request to the Piazza website that marks "helpful!" on one of your comments. Does the same-origin policy defend against this attack?

○ (A) Yes, because the same-origin policy prevents the script from making the request

○ (B) Yes, because the script runs with the origin of the attacker's website

○ (C) No, because the same-origin policy does not block any requests from being made

○ (D) No, because the script runs with the origin of Piazza's website

○ (E) ——

○ (F) ——

Q2.6 (3 points) Your malicious script submits a GET request to the Piazza website that marks "helpful!" on one of your comments. Does enabling CSRF tokens defend against this attack?

○ (G) Yes, because the attacker does not know the value of the CSRF token

○ (H) Yes, because the script runs with the origin of the attacker's website

○ (I) No, because GET requests do not change the state of the server

○ (J) No, because the script runs with the origin of Piazza's website

○ (K) ——

○ (L) ——

Q3 *Hackerman Visits the Voting Booth* (21 points)

Your sketchy friend Jared asks you to use your CS 161 skills to help him rig some sort of election. He hands you a business card with credentials for a Russian supercomputer.

Armed with massive computing power, you show up to the Caltopia polling center. It has a Wi-Fi network secured with standard WPA2-PSK.

Q3.1 (5 points) You observe a WPA 4-way handshake. Which values from the handshake are needed to perform a brute-force search for the Wi-Fi password? Select all that apply.

□ (A) ANonce

□ (B) SNonce

□ (C) The router's MAC address

□ (D) The client's MAC address

□ (E) The MICs

□ (F) None of the above

Q3.2 (4 points) What can you do after successfully brute-forcing the Wi-Fi password? Select all that apply.

□ (G) Perform on-path network attacks against victims in the same Wi-Fi network

□ (H) Decrypt network traffic encrypted with the PTK of a user who joins the network after you

□ (I) Decrypt network traffic encrypted with the GTK

□ (J) Decrypt TLS network traffic

□ (K) None of the above

□ (L) ——

Q3.3 (3 points) Which defenses would stop your attack? Select all that apply.

□ (A) Changing the Wi-Fi password every day

□ (B) Using WPA2-Enterprise

□ (C) A modern NIDS system

□ (D) None of the above

□ (E) ——

□ (F) ——

You arrive at the New Blackwell City polling center. It also has a Wi-Fi network secured with standard WPA2-PSK.

You walk up to a poll worker, claim that you're a fellow poll worker, and ask for the Wi-Fi password. They write the password on a post-it note and give it to you.

Q3.4 (3 points) Which security principle is most closely related to your experience at this polling place?

○ (G) Consider Shannon's maxim

○ (H) Least privilege

○ (I) Security is economics

○ (J) Consider human factors

○ (K) Defense in depth

○ (L) Time of check to time of use

At the Campanile City polling center, you see a DHCP Discover message broadcast to everyone.

Assume your computer has IP address , and the network's router and DHCP server have IP address . Assume that there are no other machines on the network. Assume there are no reserved or private IP addresses.

You want to return a malicious DHCP Offer that would make you a MITM. What values of the assigned IP address and the gateway IP address could you use in your response?

Q3.5 (3 points) Assigned IP address:

Enter your answer in the text box on Exam Tool.

○ (A) —— ○ (B) —— ○ (C) —— ○ (D) —— ○ (E) —— ○ (F) ——

Q3.6 (3 points) Gateway IP address:

Enter your answer in the text box on Exam Tool.