16/17 Questions Answered
Saved at 3:45 PM

Homework 6

Q1 Project 3 (Web Security) Warmup

9 Points

This homework has instant feedback. When you click "Save Answer," if the answer is correct, you will see an explanation. You can resubmit as many times as you want.

In Project 3, you will be finding web security vulnerabilities in a poorly-designed website. This question will walk you through some strategies for analyzing a website for security flaws.

We recommend using Firefox or Chrome for this question (and for Project 3).

Q1.1

1 Point

Relevant lecture: Tuesday, March 2: Intro to Web (slides, Youtube , Kaltura, review videos, notes sections 1-3)

First, visit https://cs161.org/hw6 in your favorite browser. Examine the HTML for this page by right-clicking and choosing "View page source."

There is a secret hidden as an HTML comment. Enter the secret below.

bobbytables

EXPLANATION

bobbytables

✔ **Correct**

Save Answer Last saved on **Apr 20 at 3:43 PM**

Q1.2

1 Point

Relevant lecture: Tuesday, March 2: Intro to Web (slides, Youtube, Kaltura, review videos, notes sections 1-3)

Next, let's look at the HTML form. If you click "Submit," what type of HTTP request does this form send?

(The CS161 website can't generate custom responses to requests, so if you click Submit, you'll be sent to https://postman-echo.com, a dummy endpoint.)

○ HTTP GET

● HTTP POST

EXPLANATION

The `method="post"` attribute in the `form` tag tells us that this form will send an HTTP POST request.

✓ **Correct**

Save Answer Last saved on **Apr 20 at 3:43 PM**

Q1.3

1 Point

Relevant lecture: Thursday, March 4: CSRF (slides, Youtube , Kaltura, review videos, notes section 8)

This form implements CSRF protection using CSRF tokens. Assume that these tokens are high-entropy and randomly generated by the server each time.

```
<input type="hidden" name="csrf-token" value="5f4dcc3b5aa765d61d8327deb882cf9
```

Is this a good defense against CSRF attacks?

● Yes, because an attacker cannot guess the CSRF token value

○ Yes, because the `type=hidden` attribute means an attacker cannot see the CSRF token value

○ No, because the attacker can view the page source and see the CSRF token value

○ No, because CSRF tokens are a weak defense against CSRF attacks

EXPLANATION

Remember that in a CSRF attack, the attacker sends a malicious link to the victim. When the victim clicks on the malicious link, it generates a form that looks identical to the legitimate form, fills it out with malicious fields, and sends it to the server. The server has no way of distinguishing legitimate requests from the victim and malicious requests generated through a CSRF attack.

If the server implements CSRF tokens, then every time the victim makes a legitimate request for a blank form, the server will provide a random CSRF token as a hidden field in the form. The victim's browser must then send this token back to the server. Now, an attacker can't generate a form that looks identical to the legitimate form, because they don't know the victim's CSRF token.

The `type=hidden` attribute is only for aesthetic purposes. Websites don't want their users to see long random strings at the bottom of every form. Although anyone can view the page source to see their *own* CSRF token value (just like you did here), the attacker still has no way of viewing the victim's CSRF token value.

✓ **Correct**

Save Answer

Last saved on **Apr 20 at 3:43 PM**

Q1.4

1 Point

Relevant lecture: Tuesday, March 2: Intro to Web (slides, Youtube , Kaltura, review videos, notes sections 1-3)

Now, go back to https://cs161.org/hw6. Right-click and select "Inspect element" (Firefox) or "Inspect" (Chrome). You should see a panel appear with the HTML source of the page.

In the HTML, find the line `<a href="https://cs161.org">CS161 Home page</a>`. (You can use Ctrl+F in the Inspect panel if you're having trouble finding this line.)

Right-click this line of text and select "Edit as HTML." Change the link to `https://cs161.org/phishing`.

Now try clicking the link on the page. You've phished yourself!

If another student loads this website in another browser and clicks on the link, will they fall victim to your phishing attack?

○ Yes, because the HTML has been changed to link to the phishing page.

○ Yes, because the website has not implemented XSS protection.

● No, because you have not changed the server-side HTML.

○ No, because the website has implemented XSS protection.

EXPLANATION

Changing HTML in your browser via "Inspect Element" only affects your local browser. If another user loads the same page, the server will send them an unedited version of the website. (You can check this for yourself by refreshing the page. The link should go back to the original `https://cs161.org`.

This phishing "attack" is unrelated to XSS, since we aren't adding any Javascript.

✓ **Correct**

Save Answer Last saved on **Apr 20 at 3:43 PM**

Q1.5

1 Point

Relevant lecture: Tuesday, March 2: Cookies (slides, Youtube, Kaltura, review videos, notes section 7)

Next, let's see how to view cookies.

In the Inspect Element panel, choose the "Storage" (Firefox) or "Application" (Chrome) tab.

How many cookies are set on this webpage?

○ 1

○ 2

● 3

○ 4

EXPLANATION

Each row of the table represents one cookie.

✓ **Correct**

Save Answer   Last saved on **Apr 20 at 3:43 PM**

Q1.6

1 Point

Find the cookie with `Name=session`.

What is the value of the cookie?

● 1612020

○ yes

○ session

○ tracking

○ .cs161.org

EXPLANATION

Look at the entry in the "Value" column corresponding to the `session` cookie.

✓ Correct

Save Answer Last saved on **Apr 20 at 3:44 PM**

Q1.7

1 Point

If you load the page https://cs161.org/calendar, will the cookie with `name=session` be sent to the server?

● Yes

○ No

EXPLANATION

The `session` cookie has domain `.cs161.org` and path `/`. The URL https://cs161.org/calendar has a domain ending with `.cs161.org` and a path starting with `/`, so the cookie will be sent.

✓ Correct

Save Answer Last saved on **Apr 20 at 3:44 PM**

Q1.8

1 Point

If you load the page http://cs161.org/hw6, will the cookie with `name=session` be sent to the server?

○ Yes

● No

EXPLANATION

This cookie has the Secure flag set to True, which means it will not be sent over insecure HTTP connections.

✓ Correct

Save Answer Last saved on **Apr 20 at 3:44 PM**

Q1.9

1 Point

You can also manually edit cookies in your browser.

Open the "Storage" tab in the Inspect Element panel. Make sure you can see all the cookies from the previous parts.

Now edit the `language=english` cookie by changing the value to your favorite language. Do not change the cookie name (`language`). The website supports `chinese`, `dutch`, `french`, `german`, `greek`, `italian`, `japanese`, `korean`, `portuguese`, `russian`, `spanish`, and `bot`. Cookies are case-sensitive, so be sure to use lowercase.

Once you've modified the cookie, refresh the page. Do you see the "Hello world" text translated into your chosen language?

● Yes, because your browser sent the modified cookie to the server.

○ Yes, because you changed your browser's global language settings.

○ No, because you have not changed the server-side HTML.

○ No, because websites cannot change their content based on cookie values.

EXPLANATION

Hopefully, you see the translated "Hello world" displayed. (If not, try clearing your browser cookies and repeating the steps.)

When you edit a cookie in your browser, your browser automatically attaches the modified cookie the next time you make a request. The CS161 server uses the value of the `language` cookie to decide what language should be displayed on the returned page.

Your browser's global language settings are unrelated to cookies (for example, if you go to Google, its language settings are unaffected by the `cs161.org` cookie). You are not changing the server-side HTML, but the server can dynamically change the content of the response HTML based on the value of the cookie.

✓ Correct

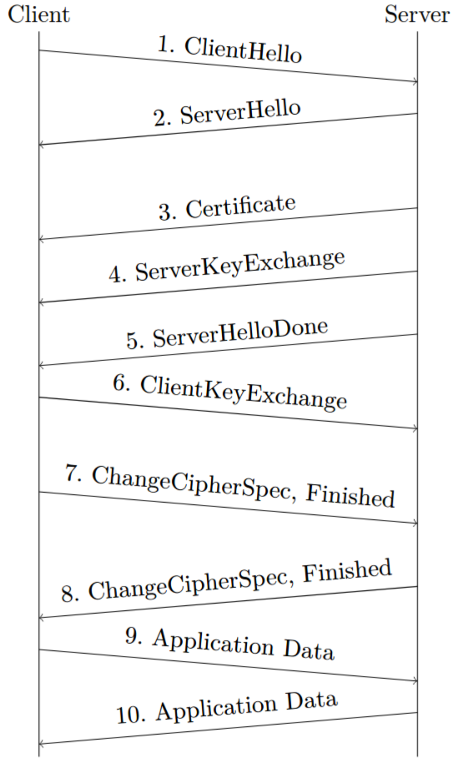
Save Answer Last saved on **Apr 20 at 3:44 PM**

Q2 TLS

5 Points

Relevant lecture: Tuesday, March 30: TLS (slides, Youtube , Kaltura, review videos, notes section 7)

This diagram of the TLS handshake from Discussion 10 might be helpful to reference throughout the question:



1. Client sends 256-bit random number R_b and supported ciphers

2. Server sends 256-bit random number R_s and chosen cipher

3. Server sends certificate

4. DH: Server sends $\{g, p, g^a \bmod p\}_{K^{-1}_{\text{server}}}$

5. Server signals end of handshake

6. DH: Client sends $g^b \bmod p$
   RSA: Client sends $\{PS\}_{K_{\text{server}}}$

Client and server derive cipher keys C_b, C_s and integrity keys I_b, I_s from R_b, R_s, PS

7. Client sends MAC(dialog, I_b)

8. Server sends MAC(dialog, I_s)

9. Client data takes the form $\{M_1, \text{MAC}(M_1, I_b)\}_{C_b}$

10. Server data takes the form $\{M_2, \text{MAC}(M_2, I_s)\}_{C_s}$

Q2.1

1 Point

Suppose that in TLS with RSA, in Step 1, the client always sends a public constant R_b, and in Step 2, the server always sends a public constant R_s. How does this affect the security of TLS?

○ An on-path attacker can learn all the symmetric cipher keys and integrity keys.

● An on-path attacker can perform a replay attack.

○ An on-path attacker cannot learn the symmetric keys or perform a replay attack.

EXPLANATION

An on-path attacker cannot learn the symmetric keys, because they do not know the pre-master secret used to generate the keys.

However, an on-path attacker can perform a replay attack without knowing the symmetric keys as follows: record the entire handshake and (encrypted) communication between the client and server. Then the attacker starts a new connection with the server, sending the (possibly encrypted) values from the previous connection each time. Because R_b and R_s are constant, and the attacker sends the same encrypted PS, the symmetric keys derived in this handshake are identical to the keys in the original connection. If the original communication said something like "Alice sends $10 to Mallory," now the attacker can *replay* that communication and make the server think Alice wants to send $10 to Mallory twice, even if the attacker cannot directly decrypt the communication.

✓ **Correct**

Save Answer

Last saved on **Apr 20 at 3:44 PM**

Q2.2

1 Point

Suppose that in TLS with RSA, in Step 1, the client sends a public constant R_b. (The server sends random R_s as normal in Step 2.) How does this affect the security of TLS?

○ An on-path attacker can learn all the symmetric cipher keys and integrity keys.

○ An on-path attacker can perform a replay attack.

● An on-path attacker cannot learn the symmetric keys or perform a replay attack.

EXPLANATION

Just like the previous part, an on-path attacker cannot learn the symmetric keys, because they do not know the pre-master secret used to generate the keys.

However, the replay attack from the previous part no longer works. Suppose the attacker tries to replay an entire communication. In step 2, R_s sent by the server is different from the R_s in the original connection. Since the symmetric keys are derived from R_b, R_s, and PS, even if the attacker replays the same R_b and PS, the symmetric keys will still be different the second time, and the attacker will be unable to replay the connection.

✓ Correct

Save Answer Last saved on **Apr 20 at 3:44 PM**

Q2.3

1 Point

Suppose that in TLS with RSA, in Step 6, the client uses the current time, with millisecond precision, as the pre-master secret. How does this affect the security of TLS?

● An on-path attacker can learn all the symmetric cipher keys and integrity keys.

○ An on-path attacker can perform a replay attack.

○ An on-path attacker cannot learn the symmetric keys or perform a replay attack.

EXPLANATION

An attacker can recover a low-entropy pre-master secret in a brute-force attack. The attacker also knows R_b and R_s, since those are sent in plaintext in Steps 1 and 2. Thus the attacker has all 3 values needed to generate the symmetric keys.

✓ Correct

Save Answer Last saved on Apr 20 at 3:44 PM

Save Answer Last saved on **Apr 20 at 3:44 PM**

Q2.4

1 Point

Modern versions of TLS only support generating the pre-master secret with Diffie-Hellman. Why do we no longer support TLS with RSA?

○ Diffie-Hellman is faster than RSA

○ Pre-master secrets generated from Diffie-Hellman are harder to brute-force than pre-master secrets generated from RSA

● Diffie-Hellman keeps a communication secure even if someone compromises the keys later, while RSA does not

EXPLANATION

Diffie-Hellman TLS provides *forward secrecy*, while RSA does not. Suppose that an attacker records a server's (possibly encrypted) communications, and sometime in the future, they steal the server's secret key. In RSA TLS, the pre-master secret is encrypted with the server's public key and sent in the communication, so this attacker can now decrypt the pre-master secret, learn the symmetric keys, and decrypt old communications.

Diffie-Hellman avoids this problem, because only $g^a \mod p$ and $g^b \mod p$ are sent in the communication, and these values do not help the attacker learn the pre-master secret $g^{ab} \mod p$. The secret random values a and b are *ephemeral* (destroyed after every connection), so the attacker cannot learn past secret values, even if they compromise the server.

✓ Correct

Save Answer Last saved on **Apr 20 at 3:44 PM**

Q2.5

1 Point

Suppose that in TLS with Diffie-Hellman, in Step 4, the server does not send a signature along with $g, p, g^a \mod p$. How does this affect the security of TLS?

○ A MITM attacker can learn all the symmetric cipher keys and integrity keys.

○ A MITM attacker can perform a replay attack.

● A MITM attacker can impersonate the server.

○ A MITM attacker cannot do any of the above.

EXPLANATION

Without the signature in Step 4, the server in Diffie-Hellman TLS is never sending any proof that it owns the private key corresponding to the public key in the certificate. This allows a man-in-the-middle (MITM) attacker to pick their own secret m, send $g, p, g^m \bmod p$ to the client, and cause the client and attacker to derive shared symmetric keys. Without the signature, the client has no way of distinguishing the server from the attacker.

Note: In RSA, a signature is not needed because the server proves its ownership of the private key by decrypting the pre-master secret and using it to generate the symmetric keys.

✓ Correct

Save Answer Last saved on **Apr 20 at 3:44 PM**

Q3 Denial of Service (DoS)

2 Points

Relevant lecture: Thursday, April 1: Denial of Service (slides, Youtube , Kaltura, review videos)

Bob wants to prevent people from overwhelming his pet-photo website, and is considering the following solutions. For each of these proposals, choose whether it is effective at preventing all DoS attacks.

Q3.1

1 Point

Bob sees on the news that IP spoofing has been eradicated, and no one can spoof their IP anymore! He decides to limit the amount of data any given IP address can send or ask for, and simply terminates the connection for any single IP address that violates this.

○ Good solution

● Bad solution

EXPLANATION

An attacker can use a Distributed Denial of Service (DDoS) attack, executed by a botnet overwhelming the victim with large amounts of traffic coming from many sources.

✓ Correct

Save Answer Last saved on **Apr 20 at 3:44 PM**

Q3.2

1 Point

Bob installs a firewall. If his website starts receiving a huge amount of traffic, Bob's firewall will analyze each packet and drop any suspicious packets.

○ Good solution

● Bad solution

EXPLANATION

An attacker can perform a DoS attack and overwhelm Bob's firewall.

✓ Correct

Save Answer Last saved on **Apr 20 at 3:44 PM**

Q4 Feedback

0 Points

Optionally, feel free to include feedback. What's something we could do to make the class better? Or, what did you find most difficult or confusing from lectures or the rest of class, and what would you like to see explained better? If you have feedback, submit your comments here.

Your name will not be connected to any feedback you provide. (If you'd like a direct response, please ask over Piazza instead.) Anything you submit here will not affect your grade.

Enter your answer here

Save Answer Last saved on **Apr 20 at 3:45 PM**

Save All Answers

Submit & View Submission >