CS 290 Final Exam Your name here: ________________

This is an open-book, take-home exam. It is due at the end of our assigned exam period, during exam week. Print the exam, fill it out, and turn it in to a TA. You may turn it in early to a TA. You may not ask the professor or any TA for help.

You may consult the web and/or your classmates to discuss these questions. HOWEVER, YOU MUST 100% UNDERSTAND AND BE ABLE TO JUSTIFY EVERY ANSWER THAT YOU PUT DOWN. You may not just copy off of classmates. You may ask them for help. You may not ask them for an answer that you simply copy. The distinction is that the answers that you write must be 100% your own.

For each question, CIRCLE THE BEST ANSWER. It is possible that more than one answer might seem plausible. Circle the best answer. There is only one best answer for each question. Do not circle two or more answers. Do not skip any questions. No partial credit will be awarded if your circles are ambiguous.

1. Which of these is the best choice for controlling the appearance of your website?
    a. JS
    b. HTML
    c. CSS
    d. SQL
    e. PHP

2. Which of these is the best choice for controlling the client-side behavior of your website?
    a. JS
    b. HTML
    c. CSS
    d. SQL
    e. PHP

3. Which of these is the best choice for controlling the server-side behavior of your website?
    a. JS
    b. HTML
    c. CSS
    d. SQL
    e. PHP

4. Which of these is the best choice for controlling the storage of your website's data?
    a. JS
    b. HTML
    c. CSS
    d. SQL
    e. PHP

5. Which of these statements is most generally true?
    a. The font of a short headline on a website should be serif and set with a <font> tag
    b. The font of a short headline on a website should be serif and set with CSS
    c. The font of a short headline on a website should be sans-serif and set with a <font> tag
    d. The font of a short headline on a website should be sans-serif and set with CSS

6. What does the color #0000FF look like?
    a. Green
    b. Yellow
    c. Red
    d. Blue
    e. Black

7. A certain DIV has an ID of "rickAstley". Which CSS command will set the color of this DIV?
    a. .rickAstley { color: #00ff00; }
    b. #rickAstley { color: #00ff00; }
    c. rickAstley { color: #00ff00; }
    d. * rickAstley { color: #00ff00; }
    e. > rickAstley {color: #00ff00; }

8. What is the difference between a <main> tag and a <nav> tag?
    a. The <main> tag and the <nav> tag are displayed with different font sizes
    b. The <main> tag is displayed with italics, and the <nav> tag is not
    c. The <main> tag marks the main content of the page, and <nav> marks navigation
    d. The <main> tag is supported in HTML5, but the <nav> tag is not
    e. The <main> tag is not indexed by search engines, but the <nav> tag is indexed

9. Which of these situations would be a good opportunity to use a GET instead of a POST? Assume that your GET request does not have a cache-busting parameter.
    a. When deleting content from the website
    b. When uploading content to the website
    c. When displaying content that very rarely changes
    d. When displaying content that changes almost every second

10. Suppose your user clicks a link. Which of the following will definitely NOT happen?
    a. A POST might be sent to the server
    b. The page might be served out of the local cache on the user's computer
    c. The page might be served from a cache on a proxy server out on the web
    d. The webserver might respond with the contents of the page
    e. The webserver might respond with a 404 (page not found)

11. Suppose you want to reuse CSS in multiple web pages on your site. Which tag would you use?
    a. <style>
    b. <main>
    c. <css>
    d. <link>
    e. <iframe>

12. How should passwords be gathered from a user in an HTML form?
    a. Use an <input type=”text”> and send the data via POST
    b. Use an <input type=”text”> and send the data via GET
    c. Use an <input type=”hidden”> and send the data via POST
    d. Use an <input type=”hidden”> and send the data via GET
    e. Use an <input type=”password”> and send the data via POST
    f. Use an <input type=”password”> and send the data via GET

13. Which of the following does JavaScript support but PHP does NOT support?
    a. Loops
    b. Databases
    c. Associative arrays
    d. Conditionals
    e. Retrieving the user’s precise geolocation

14. What is the difference between the PHP *include* function and the PHP *require_once* function? (Note: This was not covered in class. Look this one up on the web.)
    a. The *include* function incorporates (includes) the content of some file X, and the *require_once* function just checks that the other file X actually exists
    b. The *include* function will terminate the web page if the needed file X does not exist; in contrast, the *require_once* function will just issue a warning message and keep going
    c. If *include(x)* is called multiple times, then the file will be incorporated multiple times; in contrast, *require_once(x)* guarantees that x is incorporated precisely once if X exists
    d. There is no difference between the two: *include* and *require_once* are identical

15. Which of the following does MySQL NOT support?
    a. Blobs (storing binary large objects in the database)
    b. Varchars (saving variable length character arrays in the database)
    c. Embedded PHP (running PHP inside the database)
    d. Auto-incremented columns

16. Which of the following is a valid reason to use PHP instead of other server-side languages (such as Java, C#, or JS)?
    a. PHP has far better performance than any of these other languages
    b. PHP has far higher security than any of these other languages
    c. These other languages are deprecated for web server use and unlikely to be supported at some point in the future
    d. Many hosts (especially those that are free) support PHP, but some do not support these other languages

17. US phone numbers have ten digits, with a hyphen after the third and sixth digits. Which of the following regular expressions is most appropriate for validating US phone number strings?
    a. “[0-9]*\-[0-9]*\-[0-9]*”
    b. “^[0-9]*\-[0-9]*\-[0-9]*$”
    c. “[0-9]{3}\-[0-9]{3}\-[0-9]{4}”
    d. “^[0-9]{3}\-[0-9]{3}\-[0-9]{4}$”

18. Which of the following is a good situation for using server-to-server http connections in PHP?
    a. Maybe you want to retrieve RSS from a server on another domain
    b. Maybe you want to retrieve data from your own database and convert it to JSON
    c. Maybe you need to retrieve the list of posts from a Facebook page via an <IFRAME> tag
    d. Maybe you need to retrieve a map from Google's API via a <script> tag

19. Which of these is a situation when you'd use an associative array, rather than an alternative?
    a. If you need to sort a list in PHP, then you'd use an associative array because there is no way to sort a regular array (i.e., a linear array indexed from 0)
    b. If you want to store and look up information in JS memory, based on some key that is a string (like "betty"), then you'd use an associative array instead of a linear array
    c. If you want to guarantee that certain data values are secure, then you would store them in a JavaScript associative array instead of a database
    d. If you want to improve the usability of your web site by reducing responsiveness, then you would store data in an associative array on the server, instead of in the database

20. What is the purpose of using nameless (anonymous) functions in JavaScript?
    a. To make it less likely that closure will occur
    b. To avoid polluting the namespace
    c. To improve the performance of functions
    d. To make the web page more usable
    e. To reduce the amount of traffic to the database

21. What is the purpose of *htmlspecialchars* in PHP?
    a. To prevent unintended characters from leaking into your SQL queries
    b. To reduce the risk of unintended characters from leaking into your HTML stream
    c. To avoid polluting the namespace
    d. To improve the performance of functions
    e. To improve the usability of your web page

22. Two web pages X and Y are nearly identical. Both of them retrieve a list of puppies from a database and output that list to the web. But page X outputs this list as JSON, and page Y outputs the list as HTML. Which of these statements is true?
    a. Page X is more likely than page Y to contain a security hole, due to the possibility that the puppy names contain unintended <script> tags in the JSON stream
    b. Page Y is more likely than page X to contain a security hole, due to the possibility that the puppy names contain unintended <script> tags in the HTML stream
    c. Page X is probably only accessible via a POST operation, but page Y probably can be accessed via GET or POST
    d. Page Y is probably only accessible via a POST operation, but page X probably can be accessed via GET or POST

23. Which of these is an important difference between JSON and XML?
    a. JSON can contain JS functions, but XML cannot
    b. JSON is susceptible to important security risks, and XML is not
    c. JSON is usually more concise and therefore offers better performance than XML
    d. JSON is older than XML and therefore is compatible with more legacy systems

24. Suppose you create a web page that can send emails. Which of these is a good way to prevent spammers from hijacking your web page?
    a. Transmit the receiver (“to”) and email body to the server using JSON (via AJAX)
    b. Transmit the receiver (“to”) and email body to the server via a GET request
    c. Transmit the receiver (“to”) and email body to the server in XML format
    d. Write your server code in such a way that it accepts any “to” address
    e. Write your server code in such a way that it hardcodes the email body
    f. Write your server code in such a way that it hardcodes the “from” address

25. What is the single origin policy in JavaScript?
    a. A script can only be used (referenced) by single web page
    b. A script can only load data from the same web site that it was loaded from
    c. A script can only access its own web page once; it cannot access its page twice or more
    d. A script can only access its own web page; it cannot ask the server for more data

26. What effect, if any, would the single origin policy have on your PHP’s ability to send emails?
    a. Your PHP may only send emails to users on the same domain as the website
    b. Your PHP may send emails to any users, but it may not send text messages
    c. Your PHP may only make server-to-server connections to servers on the same domain
    d. The single origin policy only affects JavaScript, and it has no effect on PHP at all

27. Suppose that you have a PHP that sends out some emails, and you want your PHP to save a copy of every email in your database before it sends out that email. Which of the following is most likely to be true?
    a. Your database will probably have at least one blob (or clob) column
    b. Your database will definitely have at least one auto-increment column
    c. Your PHP code definitely does not use any prepared statements
    d. Your PHP code will probably need to send a regular expression to the database

28. What is the difference between cookies and sessions?
    a. Sessions are little pieces of data that flow back and forth between the client and server; cookies only exist on the client side
    b. Sessions are little pieces of data that flow back and forth between the client and server; cookies only exist on the server side
    c. Cookies are little pieces of data that flow back and forth between the client and server; sessions only exist on the client side
    d. Cookies are little pieces of data that flow back and forth between the client and server; sessions only exist on the server side

29. What is the relationship between cookies and sessions?
    a. Cookies are internally used by the web site to support sessions
    b. Sessions are internally used by the web site to support cookies
    c. Cookies are the means by which the server links sessions with CSS
    d. Sessions are the means by which the client links cookies with CSS

30. In AJAX with jQuery, which would you use to send a non-idempotent request?
    a. Invoke $.ajax and specify that the type is GET
    b. Invoke $.ajax and specify that the type is a content type (such as text/html)
    c. Invoke $.ajax and specify that the type is POST
    d. Invoke $.ajax and specify that the content is not a file upload
    e. Invoke $.ajax and specify that the type is null

31. Where should you validate?
    a. In your JS but not your PHP
    b. In your PHP but not your JS
    c. In your JS and in your PHP
    d. In your SQL but not in your JS or in your PHP
    e. In your SQL and in your JS but not in your PHP
    f. In your SQL and in your PHP but not in your JS

32. Suppose data is stored on the client side using one of the following methods. For which of these methods is the data automatically copied to the server as an http header?
    a. Local storage
    b. Cookies
    c. Associative arrays
    d. Web SQL Database
    e. indexedDB Database

33. What is the main benefit of having stateless servers in basic http?
    a. The users will be aware if the server is located on the internet or on an intranet
    b. All inputs and outputs are automatically encrypted
    c. Server replication is relatively easy
    d. Statelessness eliminates the risk of losing your cookies
    e. When http was invented, nobody had yet discovered how to create a stateful server

34. What is the main problem with having stateless servers in basic http?
    a. It is difficult to keep track of which requests belong to the same user
    b. It is completely impossible to replicate data across multiple servers
    c. The users can tell whether the server is located on the internet or on the intranet
    d. It is not possible to send data to a database from a stateless server
    e. Usability is very low in a stateless environment

35. What is the purpose of a foreign key in a database table?
    a. Foreign key constraints uniquely identify each row in the table
    b. Foreign key constraints improve the usability of the data
    c. Foreign key constraints help ensure that rows don’t reference non-existent values in other database tables
    d. Foreign key constraints indicate which users are “primary” administrators of the database, to help improve security
    e. Foreign key constraints store the password that your PHP uses to access the database

36. Which of these is NOT a good way of validating data—in other words, which of these methods is most likely to allow invalid data of some sort to sneak through and cause harm?
    a. A user entered some strings, which your code validates with regular expressions
    b. A user uploaded a file, which your code checks to see if it's actually an image file
    c. Your web page displays an advertisement, which it incorporates from another server using <script src="http://www.anotherserver.com/something/something"></script>
    d. Your server reads a string from another server, which your code verifies that it can parse as XML
    e. Your server reads some strings from your own database, which your code escapes with htmlspecial chars before sending to the browser

37. When is the most absolutely essential important time to validate (or escape) a piece of data?
    a. Just before your code accepts that data from the user
    b. Just after your code accepts that data from the user
    c. Just before your code uses that data
    d. Just after your code uses that data

38. For which of the following reasons, or all of them, is it important to validate even the data that your code reads from your own database?
    a. It's possible that some member of your company intentionally slipped bad data into the database
    b. It's possible that some other web page has a security hole that inadvertently allows bad data to slip into the database
    c. It's possible that some portions of the database were purchased from another organization and therefore might still contain old, unvalidated data
    d. All of the above
    e. None of the above

39. Which strings never need to be validated?
    a. Strings received from users
    b. Strings received in your PHP through AJAX transmissions from your own web page
    c. Strings received in your PHP from other servers
    d. Strings that are hardcoded in your PHP

40. When you store usernames and passwords in a database, why is it most important for you to hash all of the passwords with salt?
    a. Hashing a password with salt improves its usability by making it more readable
    b. Hashing a password with salt improves its performance by making it shorter
    c. Hashing a password with salt improves its performance by eliminating redundant characters
    d. Hashing a password with salt improves its security by making it harder for an adversary who steals the database to figure out the password
    e. Hashing a password with salt improves its security by ensuring that users only select passwords that are hard to guess

41. Suppose that you implement a login form. What role does the SESSION play in your code?
    a. Usually, after the user logs in, your code will store the user's identifier in the session (for example, a user id number, or perhaps the user's username)
    b. Usually, before the user logs in, your code will store the user's password in the session
    c. Usually, just after the user logs out, your code will show the contents of the user's session on the screen
    d. Usually, just before the user logs out, your code will store the contents of the user's session in the database

42. Which of the following are risks of using a 3rd party login system, rather than implementing your own? For example, what are the potential downsides of using Google's login for your site?
    a. The 3rd party could hypothetically pretend to be one of the users and get into your site as a result (e.g., Google could hack your site)
    b. Dependence on the 3rd party could lead to reduced usability (e.g., due to user confusion about "why am I on Google's site all of a sudden?")
    c. Both of the above
    d. Neither of the above

43. Which of the following are potential downsides of using OSU's ONID authentication service for controlling access to your site?
    a. OSU could hypothetically pretend to be one of the users and get into your site
    b. OSU only allows sites hosted on OSU domains to authenticate users with ONID (unless if you establish a separate agreement with the OSU administrators)
    c. Both of the above
    d. Neither of the above

44. Suppose that you wanted to do a file upload, and you didn't want the user to see that ugly <input type="file"> widget. What could you do instead? (Note: We didn't cover this in class; look it up on the web.)
    a. You could use an ActiveX library, which is supported in pretty much all browsers and provides a lot more control over the appearance of file upload widgets
    b. You could use a Java applet, which is supported in pretty much all browsers and provides a lot more control over the appearance of file upload widgets
    c. You could use a client-side PHP script, which is supported in pretty much all browsers and provides a lot more control over the appearance of file upload widgets
    d. You could use a jQuery UI library, which is supported in pretty much all browsers and provides a lot more control over the appearance of file upload widgets
    e. None of the above: the basic <input type="file"> widget is your only choice

45. Which of the following is the best explanation of what learnability means?
    a. How easy it is for people to remember how to use your web site
    b. How easy it is for people to figure out how to use your web site
    c. How easy it is for people to explain how to use your web site
    d. The number of actions required to use your web site
    e. The number of icons displayed by your web site
    f. The overall aesthetics of your web site

46. What is a good way to improve the memorability of your site?
    a. Make sure that all text on the site is bold and in a very large font
    b. Move functionality around on the screen, on a regular basis, to keep it “fresh”
    c. Change the rules of the site (e.g., when users need to authenticate), to keep it “fresh”
    d. Use colored icons with memorable shapes to make it easy to find functionality
    e. Provide a “welcome” splash screen that displays a detailed tutorial video
    f. Use http tags to cache the content of the site on the user’s computer

47. What is a good way to improve the overall usability of your site?
    a. Include as many features as possible
    b. Change the rules of the site (e.g., when users need to authenticate), to keep it “fresh”
    c. Put up a splash screen to impress the users as they arrive
    d. Avoid using <main> and <nav> tags, which can confuse search engines
    e. Perform all long operations synchronously
    f. Perform all long operations asynchronously

48. Under what conditions would you want to AVOID using paper prototyping?
    a. When you do not own a copy of PhotoShop or similar image-editing software
    b. When your site is extremely important, and any usability problem could be costly
    c. When your site isn’t going to have a user interface; for example, maybe it is a search engine that indexes the web and only returns search results in JSON format
    d. All of the above
    e. None of the above

49. Which of the following is the best explanation of what accessibility is?
    a. Accessibility means that a site is usable to the largest population practically possible
    b. Accessibility means that the site shows no text: all information is provided via mp3 files
    c. Accessibility means eliminating all requirements for authentication
    d. Accessibility means that the website cannot have any JavaScript
    e. Accessibility means that the site is, aesthetically speaking, awesome
    f. Accessibility means ensuring that the site is always online, all day every day

50. Which of the following is NOT a good way to choose mutually harmonious colors?
    a. Use just black and white, plus a third color for emphasis
    b. Use three colors equally spaced but near each other (analogic)
    c. Use two colors opposite from one another on the color wheel (complementary colors)
    d. Use three or four colors spaced equally around the color wheel (triads and tetrads)
    e. Use every primary and complementary color (universal)

51. Which of the following refers to the total time between when an operation is initiated and when the operation completes?
    a. Latency
    b. Responsiveness
    c. Scalability
    d. Security rating
    e. Throughput
    f. Reliability

52. Under what conditions would you use $(“#something”) as part of your code?
    a. There is exactly one item on the page that you want to modify
    b. There are exactly two items on the page that you want to modify
    c. There are items on the page that you want to modify, but you’re unsure how many
    d. All of the above

53. Which of these is NOT true about jQuery?
    a. jQuery can insert and remove elements from the DOM
    b. jQuery can change the appearance of elements in the DOM
    c. jQuery works even when JavaScript is turned off in the browser
    d. jQuery supports sending and receiving JSON
    e. jQuery supports a range of plug-ins, including some for data validation

54. Where is it ok to cache information, when trying to improve scalability?
    a. Cache information in the server if feasible; never cache in the client (JS or browser)
    b. Cache information in the client (JS or browser) if feasible; never cache at the server
    c. Cache information in both the client (JS or browser) and the server if feasible
    d. Never cache information in the client (JS or browser) or the server

55. What is a key benefit of using jQuery, compared to using just JavaScript?
    a. jQuery improves the scalability of your code
    b. jQuery improves the security of your code
    c. jQuery improves the usability of your page
    d. jQuery improves the likelihood your code will work on many browsers

56. What is a key benefit of caching?
    a. Caching eliminates the need to recompute results
    b. Caching requires no storage to store values
    c. Caching reduces the risk that users will receive 404 (page not found) errors
    d. Caching eliminates the risk of security holes
    e. All of the above
    f. None of the above

57. When should you AVOID caching information?
    a. When the information is used repeatedly
    b. When the information is expensive to compute or retrieve
    c. When the information changes very frequently and thus requires recomputing
    d. When the information is small and requires little memory to store

58. How is indexing related to caching?
    a. Indexing is often a good way to organize and find information in a cache (e.g., to retrieve values from an associative array)
    b. Caching is often a good way to ensure that information is kept secure before it is indexed (e.g., by recording its primary keys in content-addressable storage)
    c. Indexing is a useful way of validating data before you cache it
    d. Caching is a useful way of validating data before you index it

59. Which of the following is true about most database systems?
    a. Most databases will automatically create an index based on your primary key
    b. Most database systems lack support for indexing
    c. Most database systems will automatically delete your data once you add it to the index
    d. Most databases will automatically create an index based on all mediumblob columns
    e. In most databases, creating an index will speed up “insert” operations but slow down “read” (or “select”) operations

60. Suppose that somebody steals a copy of all the social security numbers in your system. Which is violated?
    a. Confidentiality
    b. Availability
    c. Integrity
    d. Compatibility with HTML5 standards

61. Suppose your site is susceptible to a denial-of-service attack. Which of the following is threatened?
    a. Confidentiality
    b. Availability
    c. Integrity
    d. Compatibility with HTML5 standards

62. Suppose that your site has a URL where anybody can issue a GET request to retrieve a JSON – formatted list of puppies from your database. This page is very very slow. Which of the following is most likely to suffer as a result?
    a. Confidentiality
    b. Availability
    c. Integrity
    d. Compatibility with HTML5 standards

63. Consider again that puppy JSON feed mentioned in the last question above. What could you do to improve your site and definitely eliminate the problem mentioned in the question above?
    a. Require all incoming requests to use POST
    b. Require incoming requests to include a specially-formatted cookie
    c. Only allow requests from certain IP addresses; ignore all other requests
    d. All of the above: any of these three strategies would definitely solve the problem
    e. None of the above: none of these strategies would definitely solve the problem

64. How can you prevent most man-in-the-middle attacks?
    a. Require all users to authenticate (with a login form) before you send them any data
    b. Disable autocomplete on all form fields
    c. Install an SSL certificate and use https instead of http
    d. Replicate your server onto as many machines as possible
    e. Be sure to use htmlspecialchars() in your PHP when sending data to the client

65. Which of the following is the best explanation of what injection attacks are?
    a. Inserting something into your code that does not belong there
    b. Accessing your server before it finishes booting up
    c. Storing data in the database without encrypting it
    d. Tricking the user's browser into trashing your site

66. Which of the following attacks is most likely to harm the largest number of users in the worst possible way?
    a. Somebody steals your database
    b. SQL injection attack
    c. HTML injection attack
    d. Cross-site scripting attack
    e. Cross-site request forgery
    f. It’s hard to tell: any of the above could be the worst, depending on the details

67. How can you prevent an injection attack from succeeding?
    a. Escape all values before you use them
    b. Require the browser to transmit all data via POST
    c. Avoid server-to-server requests
    d. Use https instead of http
    e. Cache values whenever possible
    f. None of the above: None of these will definitely prevent an attack from succeeding

68. How can you prevent a cross-site scripting (XSS) attack from succeeding?
    a. Escape all values before you use them
    b. Require the browser to transmit all data via POST
    c. Avoid server-to-server requests
    d. Use https instead of http
    e. Cache values whenever possible
    f. None of the above: None of these will definitely prevent an attack from succeeding

69. How can you prevent a cross-site request forgery (CSRF) attack from succeeding?
    a. Escape all values before you use them
    b. Require the browser to transmit all data via POST
    c. Avoid server-to-server requests
    d. Use https instead of http
    e. Cache values whenever possible
    f. None of the above: None of these will definitely prevent an attack from succeeding

70. Which of these sentences is a true statement about how one specific technology can be used to improve security, usability and scalability?
    a. AJAX can be used to prevent CSRF, to improve responsiveness, and to reduce latency.
    b. CSS can be used to conceal CSRF, to improve aesthetics, and to implement caching.
    c. Hashing can be used to encrypt passwords, to track usability, and to raise throughput.
    d. IFRAMES can be used to detect XSS, to improve accessibility, and to duplicate indexes.