قائمة الاسئلة

أمنية ويب - المستوى الثاني -قسم أمن سيبراني - - كلية الحاسوب وتكنولوجيا المعلومات - الفترة - درجة الامتحان (89)

أ. بكيل عزمان

1) A type of web application attack that tricks a user into executing an unwanted action on a web application that they are already authenticated with.
هجمة تستغل المستخدم المخول بعمل تغييرات لايريدها المستخدم

□□□

هجمة تستغل المستخدم المخول بعمل تغييرات لايريدها المستخدم

1) + CSRF
2) - XSS
3) - DoS
4) - broken access

2) An attack targets the user, but it requires the attacker to compromise the server first?
هجمة تستهدف المستخدم ولكنها تتطلب من الهاكر مهاجمة السرفر أولاً

□□□

هجمة تستهدف المستخدم ولكنها تتطلب من الهاكر مهاجمة السرفر أولاً

1) - CSRF
2) + XSS
3) - DoS
4) - broken access

3) Among the attacks that target the user and can be executed without the user's awareness are:
من الهجمات التي تستهدف المستخدم و يمكن تنفيذها دون دراية من المستخدم هي:

□□□

من الهجمات التي تستهدف المستخدم و يمكن تنفيذها دون دراية من المستخدم هي:

1) - XSS
2) - Clickjacking
3) - CSRF
4) + all of above

4) Django offers high-level protection against many common attacks. This is clearly demonstrated when trying to carry out an attack, as the built-in security features in Django must first be disabled to successfully conduct the test?
تتمتع الجانقو بتوفير حماية عالية ضد أغلب الهجمات المنتشرة ، ويتضح ذلك عند قيامنا بتجربة تنفيذ أي هجمة يتوجب عليها إيقاف الحماية المضمنة في الجانقو أولا لاتمام التجربة.

□□□

تتمتع الجانقو بتوفير حماية عالية ضد أغلب الهجمات المنتشرة ، ويتضح ذلك عند قيامنا بتجربة تنفيذ أي هجمة يتوجب عليها إيقاف الحماية المضمنة في الجانقو أولا لاتمام التجربة.

1) + TRUE.
2) - FALSE.

5) Most serious attacks on web applications revolve around automated Httprequests that the attacker uses?
تتمحور أغلب الهجمات الخطيرة على تتطبيقات الويب حول طلبات الأنشاء التلقائي التي يستخدمها المهاجم

□□□

تتمحور أغلب الهجمات الخطيرة على تتطبيقات الويب حول طلبات الأنشاء التلقائي التي يستخدمها المهاجم

1) + TRUE.

2) - FALSE.

6) The techniques used to create automated Httprequests in JavaScript:
التقنيات المستخدمة في إنشاء طلبات تلقائية في لغة الجافاسكربت

التقنيات المستخدمة في إنشاء طلبات تلقائية في لغة الجافاسكربت

1) - a) xmlhttprequest
2) - b) xmlhttprespone
3) - c) fetch
4) + d) a & c

7) Among the built-in defenses in modern web browsers against attacks that require the creation of automated requests are:
من الدفاعات المظمنة في متصفحات الويب الحديثة ضد الهجمات التي تتتطلب إنشاء طلب تلقائي

من الدفاعات المظمنة في متصفحات الويب الحديثة ضد الهجمات التي تتتطلب إنشاء طلب تلقائي

1) - Same-Origin Policy
2) - Content Security Policy (CSP)
3) - Cross-Origin Resource Sharing (CORS)
4) + all of above

8) Among the attacks that require the victim only to click on a link to open a web page are:
من الهجمات التي لا تتطلب من الضحية سوى الضغط على رابط لفتح صفحة ويب

من الهجمات التي لا تتطلب من الضحية سوى الضغط على رابط لفتح صفحة ويب

1) - a) csrf
2) - b) xss
3) - c) sql injection
4) + a & b

9) It is a unique, secret, and unpredictable value that is generated by the server-side application and shared with the client to mitigate some web app attacks
1) + CSRF Token
2) - password
3) - cookie
4) - session id

10) The goal of this type of attacks is to disrupt an organization’s network operations by denying access to its users
1) - Dotnet
2) - DDoS
3) - Dos
4) + all of above

11) A technique to protect our web apps from DoS attack?
1) + Blacklist IPs
2) - data sanitizing
3) - csrf_token
4) - all of above

12) A type of attacks that called redress or interface-based attack, where a malicious site wraps another site in an invisible frame.
1) - HTML Injection

2) - cross-site scripting
3) + Clickjacking
4) - none of above

13) The Django built-in app middleware that is responsible for protecting against clickjacking attack?
1) - SecurityMiddleware
2) - CsrfViewMiddleware
3) + XFrameOptionsMiddleware

14) The following SQL statement is free from injection? "SELECT * FROM members WHERE username = 'admin'--' "
1) - TRUE.
2) + FALSE.

15) the most active procedure for protect against injection attacks?
1) - denying of inputs
2) + sanitizing of inputs
3) - accepting of inputs
4) - none of above

16) A type of web application attack that does not target a specific user, but rather affects all users of that application?
نوع من الهجمات على تطبيقات الويب لا تستهدف مستخدم محدد. بل تشمل كل مستخدمين ذلك التطبيق.

□□□
نوع من الهجمات على تطبيقات الويب لا تستهدف مستخدم محدد. بل تشمل كل مستخدمين ذلك التطبيق.

1) + XSS
2) - Clickjacking
3) - CSRF
4) - all of above

17) Django framework escapes XSS injection using the below template tag?
1) + {%autoescape off %}
2) - {% csrf_token %}
3) - {% extends 'home' %}
4) - {% url 'page' %}

18) Some attacks target the operating system of the server on which the web application is hosted. What are some of these attacks?
هناك من الهجمات ما تستهدف نظام تشغيل الخادم المنصب عليه تطبيق الويب. من هذه الهجمات؟

□□□
هناك من الهجمات ما تستهدف نظام تشغيل الخادم المنصب عليه تطبيق الويب. من هذه الهجمات؟

1) - LDAP attack
2) + OS Command Injection
3) - authentication attack
4) - none of above

19) a process of verifying someone is who they say they are?
1) + authentication
2) - authorization
3) - parametrization
4) - none of above

20) a process of verifying that person has the right to do something?
1) - authentication
2) + authorization

3) - parameterization
4) - none of above

21) a process of verifying that user input has been treated strictly as data, separate from executable code.
1) - authentication
2) - authorization
3) + parameterization
4) - none of above

22) Authorization comes before authentication as it tries to check if the user is allowed to get access to resources based on their authorization level or not.
1) - TRUE.
2) + FALSE.

23) As a cybersecurity engineer, you should consider the authentication and authorization as a developer and as an admin
1) + TRUE.
2) - FALSE.

24) When considering the implementation of a multi-factor authentication system, the following must be taken into account:
عند التفكير في إنشاء نظام تحقق بأكثر من معامل واحد، لابد من مراعاة ما يلي:

□□□
عند التفكير في إنشاء نظام تحقق بأكثر من معامل واحد، لابد من مراعاة ما يلي:

1) - web application type
2) + user experience
3) - web application design
4) - all of above

25) fingerprint is a biometric authentication type that is based on some thing you have?
1) - TRUE.
2) + FALSE.

26) smartcard is a password-based authentication type that is based on some thing you have?
1) - TRUE.
2) + FALSE.

27) It is a process or technique used to verify the identity of a user requests access to the restricted data.
1) - authorization method
2) + authentication method
3) - multifactor authentication
4) - none of above

28) The most widely used authentication methodology to secure web application data at this time is:
منهجية االتحقق لأكثر استخدام لتأمين بيانات تطبيقات الويب هذه الفترة، هي :-

□□□
منهجية االتحقق لأكثر استخدام لتأمين بيانات تطبيقات الويب هذه الفترة، هي :-

1) - multifactor authentication
2) - password-based authentication
3) - One Time Passwords
4) + token-based authentication

29) The easiest authentication methodology for users is:
منهجية التحقق الأسهل بالنسبة للمستخدمين:-

□□□

منهجية التحقق الأسهل بالنسبة للمستخدمين:-

1) - SAML authentication
2) + OpenID authentication
3) - multifactor authentication
4) - passwordless-based authentication

30) An example of the passwordless-based authentication method:
من أمثلة تقنيات منهجية الباسوورد ليس :-

□□□

من أمثلة تقنيات منهجية الباسوورد ليس :-

1) + authenticator app
2) - token-based authentication
3) - cookie-based authentication
4) - HTTP digest authentication

31) there is no difference between cookie-based and session-based authentication?
1) - TRUE.
2) + FALSE.

32) SAML authentication method is used with single or multi web application, small or big web applications?
1) - TRUE.
2) + FALSE.

33) There is a direct relationship between the level of security and the complexity of the system, while the relationship between the level of security and the user experience is inverse?
هناك علاقة طردية بين درجة التأمين و تعقيدات النظام، بينما العلاقة بين درجة التأمين و تجربة المستخدم هي علاقة عكسية.

□□□

هناك علاقة طردية بين درجة التأمين و تعقيدات النظام، بينما العلاقة بين درجة التأمين و تجربة المستخدم هي علاقة عكسية.

1) + TRUE.
2) - FALSE.

34) Two methodologies, one is the oldest and another is the latest method of web app authentication methods?
منهجيتين تعتبر احدها هي الأقدم والأخرى هي الأحدث بين منهجيات التحقق من هوية المستخدمين على تطبيقات الويب.

□□□

منهجيتين تعتبر احدها هي الأقدم والأخرى هي الأحدث بين منهجيات التحقق من هوية المستخدمين على تطبيقات الويب.

1) - HTTP digest authentication & HTTP basic authentication
2) - password-based authentication & Multifactor authentication
3) - OpenID authentication & HTTP digest authentication
4) + HTTP basic authentication & Multifactor authentication

35) what is the appropriate authentication method for simple news web application?
المنهجية المناسبة للتحقق من هوية مستخدمين عاديين لموقع أخباري هي ؟

□□□

المنهجية المناسبة للتحقق من هوية مستخدمين عاديين لموقع أخباري هي ؟

1) - passwordless-based authentication
2) + password-based authentication
3) - multifactor authentication
4) - one Time Passwords

36) what is the appropriate authentication method for an e-commerce web application?
المنهجية المناسبة للتحقق من هوية مستخدمين مشتركين لموقع بيع وشراء هي ؟

المنهجية المناسبة للتحقق من هوية مستخدمين مشتركين لموقع بيع وشراء هي ؟

1) - openID authentication
2) - password-based authentication
3) + multifactor authentication
4) - biometric authentication

37) Problem(s) require thinking to avoid password-based auntication system?
1) - password reuse
2) - password forget
3) - password brute force
4) + all of above

38) token-based authentication method is considered a stateless method?
1) + TRUE.
2) - FALSE.

39) The client includes the JWT in the headers or request body for each subsequent request.
1) + TRUE.
2) - FALSE.

40) The token-based authentication method features scalability and flexibility, but on the other hand, it suffers from the potential for increased size.
1) + TRUE.
2) - FALSE.

41) SAML authentication is a suitable method to use when the target web application is:
1) - single web app
2) + Web application has multi sub web applications
3) - big web application
4) - e-commerce web application

42) SAML authentication and OpenID methods are forms of SSO (Single-Sign-On) method.
1) + TRUE.
2) - FALSE.

43) Token-based authentication method uses JWT data structure while SAML method uses XML data structure
1) + TRUE.
2) - FALSE.

44) Cost is one of the authentication methodology selection criteria?
1) + TRUE.
2) - FALSE.

45) Consideration(s) for selecting the right a user verification system are/is:
1) - business requirements
2) - application requirements
3) - security requirements
4) + all of above

46) the most basic model to build a Django authentication system is:
1) + AbstractUser model
2) - auth model
3) - CustomUser model
4) - none of above

47) Web application security discipline ultimate aims ultimately to keep web applications functioning smoothly and protecting business from cyber data theft.
1) + TRUE.
2) - FALSE.

48) The SDLC is King" means:
ما المقصود بهذه العبارة؟

□□□
ما المقصود بهذه العبارة؟

1) + integrating security into each phase of the SDLC
2) - start developing, then secure
3) - secure during development
4) - none of above

49) the first step to start securing a web application is :
1) - test to check vulnerabilities
2) + assessment and evaluation the situation
3) - review the source code
4) - stop all web app functions, then rerun one by one.

50) the top toolkit belong to cybersecurity engineer is:
1) + web application security framework
2) - web application security scanners
3) - web application security documentation
4) - web application security testing tools

51) the web application framework is:
1) - an instruction manual
2) - some of experts practices
3) - a set of guidelines
4) + all of above

52) among the web application security frameworks, which one emphasizes on recovery more than others?
1) - OWASP framework
2) - ISO framework
3) + NIST framework
4) - none of above

53) Which of the following web app security frameworks is known for publishing an annual list of the top attacks that happen within the year?
1) + OWASP framework
2) - ISO framework
3) - NIST framework
4) - PCI Software Security Framework

54) web application security testing process refers to :

□□□
ماذا يقصد بعملية اختبار حماية تطبيق الويب؟

1) - get solutions for threats
2) - solve app security issues
3) + detect app vulnerabilities
4) - all of above

55) The importance of documentation during security testing is equivalent to the testing itself.
للتوثيق أهمية بنفس أهمية فحص الحماية نفسها؟

□□□
للتوثيق أهمية بنفس أهمية فحص الحماية نفسها؟

1) + TRUE.

2) - FALSE.

56) Monitoring and auditing are ongoing processes that accompany a cybersecurity engineer throughout the performance of their duties at all times?
المراقبة والتدقيق عمليتان مستمرتان يصحبان الأمني طوال وقت أداء عمله؟

□□□
المراقبة والتدقيق عمليتان مستمرتان يصحبان الأمني طوال وقت أداء عمله؟

1) + TRUE.
2) - FALSE.

57) Security testing methodologies for web applications:
1) + code review
2) - ZAP tool
3) - risk management
4) - all of above

58) One of the methodologies for testing the security of web applications requires knowing and knowledge with a set of testing tools?
1) - code review
2) - manual inspection
3) - thread modeling
4) + penetration testing

59) In the absence of source code, what are the remaining available methods for a cybersecurity engineer to test the web app?
في حال غياب السورس كود فإن منهجية الاختبار المتاحة أمام الأمني هي:

□□□
في حال غياب السورس كود فإن منهجية الاختبار المتاحة أمام الأمني هي:

1) - code review
2) + penetration testing
3) - thread modeling
4) - none of above

60) It is a tool of theat modeling creation?
modeling thread أداة من أدوات إنشاء

□□□
modeling thread أداة من أدوات إنشاء

1) - Threat mitigation
2) - Threat SDLC
3) + Threat Dragon
4) - none of above

61) A testing method that tests a web app as a blackbox?
1) - code review
2) - manual inspection
3) - thread modeling
4) + penetration testing

62) No matter which security testing methodology is applied to a web application, its objective remains the following goal:
أي أختبار أمني على تطبيق ويب فإن هدفه هو ما يلي:-

□□□

أي أختبار أمني على تطبيق ويب فإن هدفه هو ما يلي:-

1) - risk assessment
2) - vulnerability remediation
3) - vulnerability exploitation
4) + none of above

63) During web application testing, it's essential to strike a balance between different testing methodologies. When code review phase, OWASP recommends with the following portion:
توصي OWASP بالنسبة التالية لاجراء اختبار الكود؟

□□□

توصي OWASP بالنسبة التالية لاجراء اختبار الكود؟

1) - 20%
2) + 30%
3) - 40%
4) - 50%

64) Which category of security testing tools is best suited for testing an application that is currently running?
ما الصنف المناسب من أدوات الأختبار الأمني التالية لأجراء اختبار لتطبيق قيد التشغيل.

□□□

ما الصنف المناسب من أدوات الأختبار الأمني التالية لأجراء اختبار لتطبيق قيد التشغيل.

1) - SAST
2) + DAST
3) - SCA
4) - IAST

65) They simulate cyber-attacks to identify vulnerability in applications?
1) - Endpoint Protection Platforms
2) - Software Composition Analysis tools
3) + Automatic Penetration Testing tools
4) - Identity and Access Management tools

66) The suitable method for performing security testing on web applications?
1) - manual review
2) - penetration testing
3) - CI/CD integration testing
4) + balanced approach

67) the most popular testing tools for web application security testing?
1) - OWASP ZAP
2) - Burp Suite
3) - AP
4) + all of above

68) The protection process of web applications is a continous process?
1) + TRUE.
2) - FALSE.

69) Cookies were invented to solve the problem how to remember information about the user?
1) + TRUE.
2) - FALSE.

70) Httprequest is a stateless, but by cookies aid it can stateful?
ولكن يمكن التغلب على ذلك بستخدام الكويز

□□□

ولكن يمكن التغلب على ذلك بستخدام الكويز

1) + TRUE.
2) - FALSE.

71) the correct Django statement to set cookie?
1) - response.cookie('mycake','cakes')
2) + response.set_cookie('mycake','cakes')
3) - request.set_cookie('mycake','cakes')
4) - response.setCookie('mycake','cakes')

72) They are the mechanism used by Django for keeping track of the "state" between the site and a particular browser.
1) - Cookies
2) - tokens
3) + sessions
4) - HTTP protocol

73) Django provides full support for anonymous sessions?
1) + TRUE.
2) - FALSE.

74) Django provides a session framework that lets developers store data on the client side?
1) - TRUE.
2) + FALSE.

75) Each HttpRequest object has a session attribute, which is a dictionary-like object
1) + TRUE.
2) - FALSE.

76) Django statement: request.session["user30"]='new value' - used to:
1) - a) update session value
2) - b) delete session value
3) - c) create new session
4) + d) a & c

77) You can read the session for a user from any view of the application views?
1) + TRUE.
2) - FALSE.

78) The static files in Django applications are all web app files except python files?
1) - TRUE.
2) + FALSE.

79) STATICFILES_DIRS & STATIC_URL are essential methods to configure static files in the Django applications
1) - TRUE.
2) + FALSE.

80) It is a Django built-in command to compile static files into a folder.
1) - whitenoise
2) + collectstatic
3) - STATICFILES_STORAGE
4) - all of above

81) Django runs through each URL pattern, in order, and stops at the first one that matches the requested URL?
1) + TRUE.
2) - FALSE.

82) To allow a value to pass through URL as a variable in Django URLConfig we use:
1) - <myvar>
2) - <int:myvar>

3) - <slag:myvar>
4) + all of above

83) Django redirect method returns an HttpResponseRedirect object?
1) + TRUE.
2) - FALSE.

84) Django reverse method is used to dynamic update URL?
1) + TRUE.
2) - FALSE.

85) The Django reverse function allows retrieving url details from the url's.py file through the name value?
1) + TRUE.
2) - FALSE.

86) The Django reverse method in views is similar to url tag in Django template?
1) + TRUE.
2) - FALSE.

87) The data structure of the returned database query is:
1) - dictionary
2) + queryset
3) - dictionary-like
4) - list

88) A QuerySet is a set of database queries used to retrieve statistics from a database?
1) + TRUE.
2) - FALSE.

89) they are basic queryset methods?
1) - filter
2) - values
3) - get
4) + all of above