Java And Web Application Security

Exam

İsim Soyisim:

1. Kullanıcıdan Login, Register ve benzeri işlemleri yaparken form bilgilerinin alınabilmesi için form action’ında genel olarak GET veya POST yöntemi kullanılır. Bu tarz işlemlerde genel olarak POST önerilmesinin nedeni aşağıdakilerden hangisi olamaz.
2. Post işlemi dataları server side tarafında iletir bu yüzden daha güvenlidir.
3. Get işlemi ile yapılan gönderimler datayı üçüncü parti uygulamalar olmadan güvensiz olarak gönderir ve herkes bu datayı görebilir.
4. Post ile GET arasında çok önemli fark yoktur, post sadece büyük verileri göndermiş için kullanılır.
5. GET işlemi gönderimlerinde şifreler dahil her şey açık şekilde görülür ama Post her şeyi gizli gönderir. Bu yüzden tercih Post olmalıdır.
6. Cross Site Scripting (XSS) HTML kodlarının arasına istemci tabanlı kod gömülmesi yoluyla kullanıcının tarayıcısında istenen istemci tabanlı kodun çalıştırılabilmesi olarak tanımlanır. Bu bağlamda saldırıyı yapan kişinin ip adresinin tespit edilmesi gerekmektedir. Java da bu işlem ServletRequest nesnesi üzerinden getHeader fonksiyonu ile gerçekleşirken aşağıdaki hangi parametrelerden hangisi ip adresini tespit eder.
7. X-IP
8. X-FORWARDED-FOR
9. X-FOR-IP
10. X-CLIENT-IP
11. Gelen ve giden dataların zararlı kod içerip içermediği bilgisi geliştirici açısından çok önemlidir. Bu işlem için Java da Servlet nesnesinin çalışma prensibinde bazı değişiklikler yapmak gerekir. Bu değişiklik aşağıdaki hangi sınıfın miras alınması ile olur.
12. ServletRequest
13. ServletResponse
14. Filter
15. doFilter
16. Session fixation; Oturum sabitleme açığından faydalanarak bir saldırgan kullanıcının oturumunu kullanıcı adı ve şifre girmeksizin açmasına denir. Java da bu açığı bitirmek için kullanılacak fonksiyon aşağıdakilerinden hangisidir.
17. HttpSession->invalidate()
18. HttpSession->update()
19. HttpSession->remove()
20. HttpSession->refresh()
21. Kullanıcının daha önceki oturumu ile ilgili bilgi edinebilmek adına Cookie nesnesi kullanılır. Java da Cookie nesnesinin güvenliği ile ilgili aşağıdakilerden hangisi yanlıştır.
22. Cookie’ler içinde barındırdığı dataları sunucuda barındırdığı için güvenlidir. Herhangi bir önlem almaya gerek yoktur.
23. Cookie’ler kullanıcı tarayıcısında yaşadığı için açık şekilde görülür ve güvenliğin sağlanması gereklidir.
24. Cookie’ler belirli bir zaman içinde yaşarlar ve içindeki dataları süresi dolduğunda silerler.
25. Cookie’ler default halde güvenli değildir. Güvenliğin sağlanması gerekmektedir.
26. SQL Injection; Özellikle Web uygulamalarında bir çok işlem için kullanıcıdan alınan veri ile dinamik SQL cümlecikleri oluşturulur. Bu SQL cümlecikleri oluşturulurken araya sıkıştırılan herhangi bir meta-karakter SQL Injection’ a yol açar. Buda kullanıcının veritabanına hâkim olması demektir. Java 'da SQL Injection önlemi almak için veritabanına çıkarken aşağıdaki yöntemlerden hangisi en güvensizdir.
27. Statement
28. PreparedStatement
29. Hibernate
30. JPA
31. Rest API’ler güncel programcılık hayatımızda sıklıkla kullandığımız ortak veri paylaşım teknikleri sunar. Bir Rest API’ye bağlanırken URL açık şekilde olur ve bu url’le sahip olan herkes bu url’den bilgi istediğinde bulunabilir. Java da özellikle Spring uygulamaları yazarken bir Rest API güvenliği Spring’in hangi modülü ile sağlanır.
32. RestSecurity
33. HttpSecurity
34. Spring Security
35. Reset Policy
36. Rest Servisleri güvenliği için Client’ten oturum açılması istenerek Rest’in güvenliği sağlanır. Aşağıdaki yöntemlerden hangisi bir güvenlik yöntemidir?
37. Basic Authentication
38. Client Authentication
39. Authentication Server
40. Authentication Rest