CompTIA PenTest+: Application-based Attacks

Study online at https://quizlet.com/_g034fq

Which example best describes a business logic vulnerability?	A conditional statement misses a rule that allows validation bypass
Which IP address is commonly used to attack the vulnerable server itself in a SSRF attack?	127.0.0.1
Which data format is most commonly associated with REST APIs?	JSON
Which penetration testing tool is published by OWASP and used to automate web app security testing?	ZAP
If a directory is unintentionally set to execute permissions under the web root, how could an attacker exploit this over the web?	By using a file upload feature form to upload an executable script
Which operation should be performed on LDAP search inputs before using?	Escape special characters
What user file might get exposed to brute-force attacks via directory traversal vulnerabilities?	/etc/shadow
Select the two main types of XSS attack.	Reflected Stored
Which cookie setting is used to help prevent CSRF attacks?	SameSite
Which Ruby application is used to generate world lists from crawled web sites?	CeWL
Which type of SQLi attack relies on Boolean values or time-based results to determine success?	Blind
Which command is used to get network connection information on Windows or Linux?	netstat -an
Which flags can be set to make cookies safer?	Secure HttpOnly