Scenario

A vulnerability was identified in a widely used product. Download the challenge attachment and review the code to identify it. Vulnerability Categories (Use this list to answer the related question. Example: Path Traversal): 1. Authentication Bypass 2. Buffer Overflow 3. Code Execution 4. Command Execution 5. Cryptographic flaw 6. Cross Origin Resource Sharing bypass 7. File Inclusion 8. Insecure Direct Object Reference 9. Insecure Deserialization 10. Path Traversal 11. Race Condition 12. Server-Side Request Forgery 13. Server-Side Template Injection 14. SQL Injection 15. XML External Entity

What is the technology affected?

Format: Technology Name

Based on the list of vulnerability categories in the challenge scenario, which one describes the identified vulnerability?

Format: Vulnerability Name

See the corresponding commit. How many lines of code were added when the vulnerability was introduced?

Format: Number of Lines Added

What HTTP header is required to exploit the vulnerability?

Format: HTTP-header