Sjoerd’s vulnerability bingo

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| XXE XML External Entity | Old JavaScript outdated JavaScript library | HTTP plaintext HTTP usage | Directory listing directory listing enabled | CSRF cross site request forgery |
| unserialize user input is unserialized | File download arbitrary file download | IDOR insecure direct object references | Cookie flags session cookie without HttpOnly or Secure | X-Forwarded-For client IP set by header |
| Weak password weak passwords used | Version header server version in headers | GET/POST interchangable GET/POST | Git directory public version control directory | authentication missing authentication check |
| phpinfo phpinfo.php available | Admin interface open administrative interface | CORS insecure CORS configuration | RCE command injection | Clickjacking can be loaded in iframe |
| DoS denial of service | XSS stored cross site scripting | Technical errors error messages with technical details | Brute-force missing brute-force protection | Insecure hashes passwords not correctly hashed |