1.3

Tuesday, September 19, 2023 4:14 PM

amplification attack or DRDoS

more powerful TCP SYN flood attack

Spoof victim IP and attempt to open connections w/ mult servers

Using once only tokens and timestamps prevents

- pass-the-hash
- replay attack

XSS - malicious cript hosted on attackers site or coded in link injected onto trusted site

XSRF - malicious script hosted on attacker's site, can exploit session in same

attacker's site, can exploit
started on another site in <u>same</u>
<u>browser</u>

Client side

Command injection - runs OS shell commands from browser, allows commands to operate outside of servers directory root

run as web "guest" used

Server-side request forgery - abuses functionality of services of backend servers to read and update internal resources

Privilege escalation can result in attackers gaining keys from mem or pagefiles directory traversal - when attacker gets access to file outside web server's root directory

transitive access - problem of authorizing a request for service that depends on intermediate service

API calls over HTTP are vulnerable to:

- key discovery
  - use keys to auth requests to web app
  - attacker can use to make API calls
- improper error handling
  - error messages over

exposing error messages over HTTP can give attackers info on systems

replay attack - attacker captures data like cookie file to enable connection, can use again to establish another connection

API attack - take advantage of unsecure comms with app services to perform DoS

clickjacking - attacker inserts invisible layer into trusted web page that can intercept/direct input

Reflected XSS - web app echoes

Reflected XSS - web app
user-supplied data w/out proper
sanitization

Stored XSS - attacker injects malicious
script directly into site that is
stored and served to users

DOM-based XSS - attacker manipulates
structure of HTML page
typically embedded in page itself

DLL injection - attempt to force
another app to load dll in mem
that can cause instability or leak
info

XML injection - same thing as SQL
but target against web servers using
XML apps

XML apps

XSRF is on attackers site abusing session started on another site

XSS is on attackers site or in link injected onto trusted site to compromise clients browsing trusted site

time of check to time of use race condition

LDAP injection - when attacker exploits client's unauth access to submit LDAP queries that could create/delete acc

uses port 389

reflected XSS is server-side input valid exploit that injects script into site

malicious code executes when user visits

Stored XSS server side that inserts code into backend