Wist Kenya

Technical/demo slides...

Let the hunting begin...

root#whoami

Hilary Soita

Information security Analyst, Cellulant

Bug Bounty hunter

@bit3c0de

www.sylarsec.com

Affiliation: AfricaHackon

Top Vulnerabilities

- XSS
- SSTI
- SSRF
- SQLi
- XXE
- Open redirects
- Domain flyovers/takeovers

1. Discovery

- Subdomain scraping - sublist3r, amass,google, curl_them_all
- Content discovery - Seclist, robots disallowed, burp content discovery, dirb, dirsearch, arjun
- Platform identification - wappalyzer
- CMS - WPscan, CMSmap
- Port scanning - nmap, masscan, brutespray
- Visual identification - web screenshots
- CVE search - burp (vulners.com)

2. Exploitation:

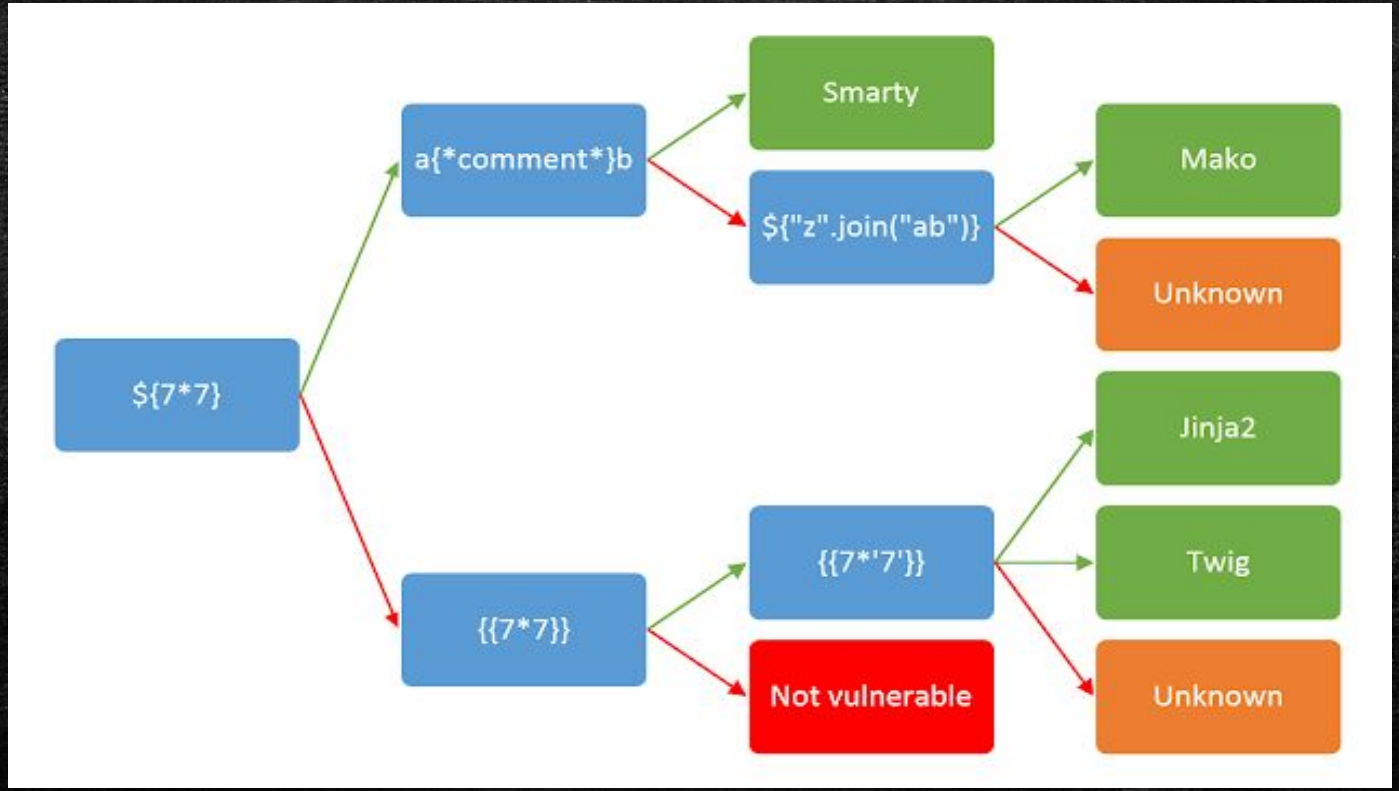
XSS (cross site scripting)

- Types:
  - Blind
  - Stored
  - Reflected
- Tools listing
  - XSS hunter
  - Sleepy
  - Knockxss
- Polyglots
- Test Environment - bwapp, dvwa.

SSTI (server side template injection)

- RCE for modern web apps using template engines like:
  - Flask
  - Jinja2
  - Twig
- Identification
  - Wappalyzer
  - Fuzzing
  - TPLmap (burp suite)
- Test Environment - XVWS

SSTI (identification)



SSRF (server side request forgery)

- Enables attackers to send requests made by the web application, often targeting internal systems behind a firewall.
  - Port scanning
  - Read local files using file:///
  - Attack internal web apps
  - Fingerprint intranet
- Test Environment - XVWS

Creative ways to use SSRF

- Port scanning (XSPA)
- Read files from server file://
- gopher://
- data://
- dict://

Filter evasion techniques

- Double encoding.
- Polyglots (XSS,SQLi)
- PHP wrapper filter evasions (LFI)
- Test Environment - Enovise VM

File upload vulnerabilities

- Bypassing extentions
- Bypassing content type.
- Adding image header

XXE (xml external entities)

- Happens due to poor parser configuration, enabling attackers to run commands on the system.
- Uses the SYSTEM command to expect an input and execute it from the user
  - Read files from the server
- Test environment: web for pentesters.iso

Shodan

- Search engine for servers and online devices.
- Some shodan dorks
  - hostname: find values that match the hostname
  - os: search based on operating system
  - port: find particular ports that are open
  - net: search based on an IP or /x CIDR
  - city: find devices in a particular city
  - country: find devices in a particular country
  - geo: you can pass it coordinates
  - before/after: find results within a timeframe
-
-

Leveraging on google

- Useful google dorks
  - inurl:download.php?file= site:ke
  - inurl:"upload.php" intitle:"upload a file"
  - filetype:inc intext:mysql_connect