```
┌──(someone㉿SALAMA)-[~]
└─$ nmap -sC -sV alamops.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-10 11:49 CEST
Nmap scan report for alamops.com (3.64.114.185)
Host is up (0.026s latency).
rDNS record for 3.64.114.185: ec2-3-64-114-185.eu-central-1.compute.amazonaws.com
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE  SERVICE  VERSION
22/tcp   open   ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 b0:8b:2c:1e:9a:45:21:c0:f7:e9:79:70:f0:95:66:44 (ECDSA)
|_  256 ef:98:f5:0c:f2:c5:b6:d4:cc:be:0d:ad:c0:a1:52:49 (ED25519)
80/tcp   open   http     nginx 1.24.0 (Ubuntu)
|_http-server-header: nginx/1.24.0 (Ubuntu)
|_http-title: Did not follow redirect to https://alamops.com/
113/tcp  closed ident
443/tcp  open   ssl/http nginx 1.24.0 (Ubuntu)
| ssl-cert: Subject: commonName=alamops.com
| Subject Alternative Name: DNS:alamops.com, DNS:www.alamops.com
| Not valid before: 2025-02-19T00:15:10
|_Not valid after:  2025-05-20T00:15:09
|_http-title: AlamOps - Expertos en Cloud Computing
|_http-server-header: nginx/1.24.0 (Ubuntu)
|_ssl-date: TLS randomness does not represent time
8008/tcp open   http?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 161.51 seconds

┌──(someone㉿SALAMA)-[~]
```

```
└─$ gobuster dir -u https://alamops.com -w wordlist.txt
Error: error on parsing arguments: wordlist file "wordlist.txt" does not exist: stat wordlist.txt: no such file or directory

┌──(someone㉿SALAMA)-[~]
└─$ mkdir wordlist.txt

┌──(someone㉿SALAMA)-[~]
└─$ ls -l
total 2668
-rw-r--r--  1 someone someone       0 Nov  9 23:57 explicacion.txt
-rw-r--r--  1 someone someone 2673967 Dec  7  2021 geckodriver-v0.30.0-linux64.tar.gz
-rw-r--r--  1 someone someone       0 Nov  9 23:45 gobuster_scan.txt
-rw-r--r--  1 someone someone    1235 Nov 10 00:17 informe_completo.txt
-rw-r--r--  1 someone someone   12901 Nov 10 00:18 informe_final.pdf
-rw-r--r--  1 someone someone     479 Nov 10 00:13 nikto_scan.txt
-rw-r--r--  1 root    root       2059 Nov 10 00:02 nmap_detailed_scan.txt
-rw-r--r--  1 someone someone      98 Nov 10 00:24 nmap_scan.txt
drwxr-xr-x  3 someone someone    4096 Nov 12 19:15 pacu
-rw-r--r--  1 someone someone    6807 Nov 10 21:05 reporte_wpscan.txt
drwxr-xr-x  8 someone someone    4096 Nov 12 19:21 ScoutSuite
drwxr-xr-x 10 someone someone    4096 Nov 10 20:28 spiderfoot
drwxr-xr-x  2 someone someone    4096 Apr 10 11:56 wordlist.txt

┌──(someone㉿SALAMA)-[~]
└─$ mkdir alamops.txt

┌──(someone㉿SALAMA)-[~]
└─$ ls -l
total 2672
```

```
drwxr-xr-x  2 someone someone    4096 Apr 10 11:57 alamops.txt
-rw-r--r--  1 someone someone       0 Nov  9 23:57 explicacion.txt
-rw-r--r--  1 someone someone 2673967 Dec  7  2021 geckodriver-v0.30.0-linux64.tar.gz
-rw-r--r--  1 someone someone       0 Nov  9 23:45 gobuster_scan.txt
-rw-r--r--  1 someone someone    1235 Nov 10 00:17 informe_completo.txt
-rw-r--r--  1 someone someone   12901 Nov 10 00:18 informe_final.pdf
-rw-r--r--  1 someone someone     479 Nov 10 00:13 nikto_scan.txt
-rw-r--r--  1 root    root       2059 Nov 10 00:02 nmap_detailed_scan.txt
-rw-r--r--  1 someone someone      98 Nov 10 00:24 nmap_scan.txt
drwxr-xr-x  3 someone someone    4096 Nov 12 19:15 pacu
-rw-r--r--  1 someone someone    6807 Nov 10 21:05 reporte_wpscan.txt
drwxr-xr-x  8 someone someone    4096 Nov 12 19:21 ScoutSuite
drwxr-xr-x 10 someone someone    4096 Nov 10 20:28 spiderfoot
drwxr-xr-x  2 someone someone    4096 Apr 10 11:56 wordlist.txt


┌──(someone㉿SALAMA)-[~]
└─$ gobuster dir -u https://alamops.com -w alamops.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://alamops.com
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                alamops.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
```

Error: the server returns a status code that matches the provided options for non existing urls. https://alamops.com/acea11b8-a210-414d-b2b6-f5670d9dc435 => 200 (Length: 1240). To continue please exclude the status code or the length

┌──(someone㉿SALAMA)-[~]

└─$ nikto -h https://alamops.com

- Nikto v2.5.0

+ Target IP: 3.64.114.185

+ Target Hostname: alamops.com

+ Target Port: 443

+ SSL Info: Subject: /CN=alamops.com

Altnames: alamops.com, www.alamops.com

Ciphers: TLS_AES_256_GCM_SHA384

Issuer: /C=US/O=Let's Encrypt/CN=E6

+ Start Time: 2025-04-10 11:59:37 (GMT2)

+ Server: nginx/1.24.0 (Ubuntu)

+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security

+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ /alamopscom.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /dump.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops.com.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /backup.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /com.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /com.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /dump.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /com.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /archive.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops_com.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /archive.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamopscom.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /3.64.114.185.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /archive.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /com.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops_com.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops.com.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /database.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /backup.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /com.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /dump.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops.com.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /com.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /3.64.114.185.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /database.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /site.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamopscom.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /archive.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops_com.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /backup.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /3.64.114.185.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops.com.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /database.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops_com.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /database.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /com.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /archive.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops_com.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /database.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /site.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /3.64.114.185.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops.com.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /dump.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /backup.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /site.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /database.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamopscom.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /com.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /dump.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /site.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops.com.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /backup.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops_com.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /database.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /3.64.114.185.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops_com.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamopscom.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /dump.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops.com.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /database.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops_com.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops.com.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /archive.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /dump.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /site.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /site.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /dump.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /backup.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamopscom.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops_com.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /com.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /com.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /dump.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /database.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /3.64.114.185.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamopscom.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops.com.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /site.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /3.64.114.185.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /archive.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /database.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamopscom.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /archive.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /3.64.114.185.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /site.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops.com.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamopscom.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /archive.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /3.64.114.185.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /backup.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /site.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /backup.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamopscom.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /backup.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /dump.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /alamops_com.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /archive.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /backup.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /site.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /3.64.114.185.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/

+ /css/: This might be interesting.

+ /js: This might be interesting.

+ 7866 requests: 0 error(s) and 116 item(s) reported on remote host

+ End Time: 2025-04-10 12:40:10 (GMT2) (2433 seconds)

+ 1 host(s) tested

****

┌──(someone㉿SALAMA)-[~]

└─$ whois alamops.com

Domain Name: ALAMOPS.COM

Registry Domain ID: 2923836650_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.godaddy.com

Registrar URL: http://www.godaddy.com

Updated Date: 2024-10-09T11:03:50Z

Creation Date: 2024-10-09T11:03:50Z

Registry Expiry Date: 2027-10-09T11:03:50Z

Registrar: GoDaddy.com, LLC

Registrar IANA ID: 146

Registrar Abuse Contact Email: abuse@godaddy.com

Registrar Abuse Contact Phone: 480-624-2505

Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited

Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited

Name Server: NS67.DOMAINCONTROL.COM

Name Server: NS68.DOMAINCONTROL.COM

DNSSEC: unsigned

URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

>>> Last update of whois database: 2025-04-10T09:50:29Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring

registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domain names or modify existing registrations; the Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. VeriSign does not guarantee its accuracy. By submitting a Whois query, you agree to abide by the following terms of use: You agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to VeriSign (or its computer systems). The compilation, repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of VeriSign. You agree not to use electronic processes that are automated and high-volume to access or query the Whois database except as reasonably necessary to register domain names or modify existing registrations. VeriSign reserves the right to restrict your access to the Whois database in its sole discretion to ensure operational stability. VeriSign may restrict or terminate your access to the Whois database for failure to abide by these terms of use. VeriSign reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.
Domain Name: alamops.com
Registry Domain ID: 2923836650_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.godaddy.com

Registrar URL: https://www.godaddy.com

Updated Date: 2024-10-09T06:03:50Z

Creation Date: 2024-10-09T06:03:50Z

Registrar Registration Expiration Date: 2027-10-09T06:03:50Z

Registrar: GoDaddy.com, LLC

Registrar IANA ID: 146

Registrar Abuse Contact Email: abuse@godaddy.com

Registrar Abuse Contact Phone: +1.4806242505

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited

Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited

Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited

Registry Registrant ID: Not Available From Registry

Registrant Name: Registration Private

Registrant Organization: Domains By Proxy, LLC

Registrant Street: DomainsByProxy.com

Registrant Street: 100 S. Mill Ave, Suite 1600

Registrant City: Tempe

Registrant State/Province: Arizona

Registrant Postal Code: 85281

Registrant Country: US

Registrant Phone: +1.4806242599

Registrant Phone Ext:

Registrant Fax:

Registrant Fax Ext:

Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=alamops.com

Registry Tech ID: Not Available From Registry

Tech Name: Registration Private

Tech Organization: Domains By Proxy, LLC

Tech Street: DomainsByProxy.com

Tech Street: 100 S. Mill Ave, Suite 1600

Tech City: Tempe

Tech State/Province: Arizona

Tech Postal Code: 85281

┌──(someone㉿SALAMA)-[~]

└─$ sqlmap -u "http://localhost/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=xyz" --batch --dbs

Command 'sqlmap' not found, but can be installed with:

sudo apt install sqlmap

┌──(someone㉿SALAMA)-[~]

└─$ sudo apt install sqlmap

[sudo] password for someone:

The following packages were automatically installed and are no longer required:

g++-13 libfmt9 libllvm16t64 libpython3.12-minimal python3-lib2to3

g++-13-x86-64-linux-gnu libgail-common libllvm17t64 libpython3.12-stdlib python3.11

gnome-accessibility-themes libgail18t64 libnl-3-200 libpython3.12t64 python3.11-dev

gnome-themes-extra libgfapi0 libnl-route-3-200 librados2 python3.11-minimal

gnome-themes-extra-data libgfrpc0 libnsl2 librdmacm1t64 python3.12

gtk2-engines-pixbuf libgfxdr0 libperl5.38t64 libssh-gcrypt-4 python3.12-dev

ibverbs-providers libglusterfs0 libpython3.11-dev libstdc++-13-dev python3.12-minimal

libassuan0 libgtk2.0-0t64 libpython3.11-minimal libutempter0 samba-vfs-modules

libboost-iostreams1.83.0 libgtk2.0-bin libpython3.11-stdlib openjdk-17-jre

libboost-thread1.83.0 libgtk2.0-common libpython3.11t64 openjdk-17-jre-headless

libcephfs2 libibverbs1 libpython3.12-dev perl-modules-5.38

Use 'sudo apt autoremove' to remove them.

Installing:

sqlmap

Installing dependencies:

python3-magic

Summary:

Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 512

Download size: 6,933 kB

Space needed: 11.2 MB / 1,016 GB available

Continue? [Y/n] y

Get:1 http://kali.download/kali kali-last-snapshot/main amd64 python3-magic all 2:0.4.27-3 [14.6 kB]

Get:2 http://kali.download/kali kali-last-snapshot/main amd64 sqlmap all 1.9.2-1 [6,919 kB]

Fetched 6,933 kB in 4s (1,727 kB/s)

Selecting previously unselected package python3-magic.

(Reading database ... 178880 files and directories currently installed.)

Preparing to unpack .../python3-magic_2%3a0.4.27-3_all.deb ...

Unpacking python3-magic (2:0.4.27-3) ...

Selecting previously unselected package sqlmap.

Preparing to unpack .../sqlmap_1.9.2-1_all.deb ...

Unpacking sqlmap (1.9.2-1) ...

Setting up python3-magic (2:0.4.27-3) ...

Setting up sqlmap (1.9.2-1) ...

┌──(someone㉿SALAMA)-[~]

└─$ sqlmap -u "http://localhost/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=xyz" --batch --dbs

___

```
     __H__
 ___ ___["]_____ ___ ___  {1.9.2#stable}
|_ -| . ["]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 12:04:38 /2025-04-10/

[12:04:38] [INFO] testing connection to the target URL

[12:04:38] [CRITICAL] unable to connect to the target URL ('Connection refused'). sqlmap is going to retry the request(s)

[12:04:38] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you can try to rerun with switch '--random-agent' and/or proxy switches ('--proxy', '--proxy-file'...)

[12:04:38] [CRITICAL] unable to connect to the target URL ('Connection refused')

[*] ending @ 12:04:38 /2025-04-10/

┌──(someone㉿SALAMA)-[~]

└─$ gobuster dir -u http://alamops.com -w /usr/share/wordlists/dirb/alamops.txt

Error: error on parsing arguments: wordlist file "/usr/share/wordlists/dirb/alamops.txt" does not exist: stat /usr/share/wordlists/dirb/alamops.txt: no such file or directory

┌──(someone㉿SALAMA)-[~]

└─$ gobuster dir -u http://alamops.com -w /usr/share/wordlists/dirb/big.txt

Error: error on parsing arguments: wordlist file "/usr/share/wordlists/dirb/big.txt" does not exist: stat /usr/share/wordlists/dirb/big.txt: no such file or directory

```
┌──(someone㉿SALAMA)-[~]
└─$ ls -l
total 2672
drwxr-xr-x  2 someone someone    4096 Apr 10 11:57 alamops.txt
-rw-r--r--  1 someone someone       0 Nov  9 23:57 explicacion.txt
-rw-r--r--  1 someone someone 2673967 Dec  7  2021 geckodriver-v0.30.0-linux64.tar.gz
-rw-r--r--  1 someone someone       0 Nov  9 23:45 gobuster_scan.txt
-rw-r--r--  1 someone someone    1235 Nov 10 00:17 informe_completo.txt
-rw-r--r--  1 someone someone   12901 Nov 10 00:18 informe_final.pdf
-rw-r--r--  1 someone someone     479 Nov 10 00:13 nikto_scan.txt
-rw-r--r--  1 root    root       2059 Nov 10 00:02 nmap_detailed_scan.txt
-rw-r--r--  1 someone someone      98 Nov 10 00:24 nmap_scan.txt
drwxr-xr-x  3 someone someone    4096 Nov 12 19:15 pacu
-rw-r--r--  1 someone someone    6807 Nov 10 21:05 reporte_wpscan.txt
drwxr-xr-x  8 someone someone    4096 Nov 12 19:21 ScoutSuite
drwxr-xr-x 10 someone someone    4096 Nov 10 20:28 spiderfoot
drwxr-xr-x  2 someone someone    4096 Apr 10 11:56 wordlist.txt

┌──(someone㉿SALAMA)-[~]
└─$ cd alamops.txt

┌──(someone㉿SALAMA)-[~/alamops.txt]
└─$ gobuster dir -u http://alamops.com -w /usr/share/wordlists/dirb/alamops.txt
Error: error on parsing arguments: wordlist file "/usr/share/wordlists/dirb/alamops.txt" does not exist: stat /usr/share/wordlists/dirb/alamops.txt: no such file or directory

┌──(someone㉿SALAMA)-[~/alamops.txt]
└─$ gobuster dir -u http://alamops.com -w alamops.txt
Error: error on parsing arguments: wordlist file "alamops.txt" does not exist: stat alamops.txt: no such file or directory
```

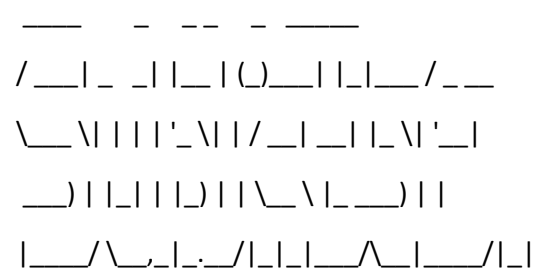
```
┌──(someone㉿SALAMA)-[~/alamops.txt]
└─$ gobuster dir -u http://alamops.com -w
Error: flag needs an argument: 'w' in -w

┌──(someone㉿SALAMA)-[~/alamops.txt]
└─$ gobuster dir -u http://alamops.com
Error: required flag(s) "wordlist" not set

┌──(someone㉿SALAMA)-[~/alamops.txt]
└─$ cd /usr/share/wordlists/dirb/
-bash: cd: /usr/share/wordlists/dirb/: No such file or directory

┌──(someone㉿SALAMA)-[~/alamops.txt]
└─$ mkdir /usr/share/wordlists/dirb/
mkdir: cannot create directory ‘/usr/share/wordlists/dirb/’: No such file or directory

┌──(someone㉿SALAMA)-[~/alamops.txt]
└─$ sublist3r -d alamops.com
/usr/lib/python3/dist-packages/sublist3r.py:75: SyntaxWarning: invalid escape sequence '\_'
  print("""%s
/usr/lib/python3/dist-packages/sublist3r.py:287: SyntaxWarning: invalid escape sequence '\/'
  link_regx = re.compile('<cite.*?>(.*?)<\/cite>')
/usr/lib/python3/dist-packages/sublist3r.py:344: SyntaxWarning: invalid escape sequence '\/'
  link = re.sub("<(\/)?b>", "", link)
/usr/lib/python3/dist-packages/sublist3r.py:440: SyntaxWarning: invalid escape sequence '\/'
  link = re.sub('<(\/)?strong>|<span.*?>|<|>', '', link)
/usr/lib/python3/dist-packages/sublist3r.py:660: SyntaxWarning: invalid escape sequence '\/'
  tbl_regex = re.compile('<a name="hostanchor"><\/a>Host
Records.*?<table.*?>(.*?)</table>', re.S)
```

/usr/lib/python3/dist-packages/sublist3r.py:905: SyntaxWarning: invalid escape sequence '\-'

domain_check = re.compile("^(http|https)?[a-zA-Z0-9]+([\-\.]{1}[a-zA-Z0-9]+)*\.[a-zA-Z]{2,}$")

/usr/lib/python3/dist-packages/subbrute/subbrute.py:374: SyntaxWarning: invalid escape sequence '\.'

domain_match = re.compile("([a-zA-Z0-9_-]*\.[a-zA-Z0-9_-]*\.[a-zA-Z0-9_-]*)+")



Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for alamops.com

[-] Searching now in Baidu..

[-] Searching now in Yahoo..

[-] Searching now in Google..

[-] Searching now in Bing..

[-] Searching now in Ask..

[-] Searching now in Netcraft..

[-] Searching now in DNSdumpster..

[-] Searching now in Virustotal..

[-] Searching now in ThreatCrowd..

[-] Searching now in SSL Certificates..

[-] Searching now in PassiveDNS..

Process DNSdumpster-8:

Traceback (most recent call last):

File "/usr/lib/python3.13/multiprocessing/process.py", line 313, in _bootstrap

self.run()

~~~~~~~~^^
~~~~~~~~

```
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 269, in run
    domain_list = self.enumerate()
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 649, in enumerate
    token = self.get_csrftoken(resp)
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 644, in get_csrftoken
    token = csrf_regex.findall(resp)[0]
            ~~~~~~~~~~~~~~~~~~~~~~~~^^^
IndexError: list index out of range
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 7
www.alamops.com
api-dev.alamops.com
grafana.alamops.com
iac-dev.alamops.com
jenkins.alamops.com
pve.alamops.com
registry.alamops.com

┌──(someone㉿SALAMA)-[~/alamops.txt]
└─$ amass enum -d alamops.com
Command 'amass' not found, but can be installed with:
sudo apt install amass

┌──(someone㉿SALAMA)-[~/alamops.txt]
└─$ sudo apt install amass
[sudo] password for someone:
The following packages were automatically installed and are no longer required:
  g++-13                libfmt9          libllvm16t64          libpython3.12-minimal    python3-lib2to3
  g++-13-x86-64-linux-gnu  libgail-common  libllvm17t64          libpython3.12-stdlib
python3.11
```

gnome-accessibility-themes libgail18t64 libnl-3-200 libpython3.12t64 python3.11-dev

gnome-themes-extra libgfapi0 libnl-route-3-200 librados2 python3.11-minimal

gnome-themes-extra-data libgfrpc0 libnsl2 librdmacm1t64 python3.12

gtk2-engines-pixbuf libgfxdr0 libperl5.38t64 libssh-gcrypt-4 python3.12-dev

ibverbs-providers libglusterfs0 libpython3.11-dev libstdc++-13-dev python3.12-minimal

libassuan0 libgtk2.0-0t64 libpython3.11-minimal libutempter0 samba-vfs-modules

libboost-iostreams1.83.0 libgtk2.0-bin libpython3.11-stdlib openjdk-17-jre

libboost-thread1.83.0 libgtk2.0-common libpython3.11t64 openjdk-17-jre-headless

libcephfs2 libibverbs1 libpython3.12-dev perl-modules-5.38

Use 'sudo apt autoremove' to remove them.

Installing:

amass

Installing dependencies:

amass-common

Summary:

Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 512

Download size: 17.2 MB

Space needed: 46.1 MB / 1,016 GB available

Continue? [Y/n] y

Get:2 http://kali.download/kali kali-last-snapshot/main amd64 amass amd64 4.2.0-0kali1 [15.4 MB]

Get:1 http://mirror.es.cdn-perfprod.com/kali kali-last-snapshot/main amd64 amass-common all 4.2.0-0kali1 [1,803 kB]

Fetched 17.2 MB in 10s (1,773 kB/s)

Selecting previously unselected package amass-common.

(Reading database ... 179605 files and directories currently installed.)

Preparing to unpack .../amass-common_4.2.0-0kali1_all.deb ...

Unpacking amass-common (4.2.0-0kali1) ...

Selecting previously unselected package amass.

Preparing to unpack .../amass_4.2.0-0kali1_amd64.deb ...

Unpacking amass (4.2.0-0kali1) ...

Setting up amass-common (4.2.0-0kali1) ...

Setting up amass (4.2.0-0kali1) ...

┌──(someone㉿SALAMA)-[~/alamops.txt]

└─$ amass enum -d alamops.com

No assets were discovered

The enumeration has finished

┌──(someone㉿SALAMA)-[~/alamops.txt]

└─$ amass enum -d alamops.com

alamops.com (FQDN) --> ns_record --> ns68.domaincontrol.com (FQDN)

alamops.com (FQDN) --> ns_record --> ns67.domaincontrol.com (FQDN)

alamops.com (FQDN) --> mx_record --> alt1.aspmx.l.google.com (FQDN)

alamops.com (FQDN) --> mx_record --> alt3.aspmx.l.google.com (FQDN)

alamops.com (FQDN) --> mx_record --> alt2.aspmx.l.google.com (FQDN)

alamops.com (FQDN) --> mx_record --> aspmx.l.google.com (FQDN)

alamops.com (FQDN) --> mx_record --> alt4.aspmx.l.google.com (FQDN)

The enumeration has finished

┌──(someone㉿SALAMA)-[~/alamops.txt]

└─$ sqlmap -u "http://alamops.com/page.php?id=1" --batch --dbs

___

```
     __H__
 ___ ___[,]_____ ___ ___  {1.9.2#stable}
|_ -| . ['']     | .'| . |
|___|_  [()]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 12:33:58 /2025-04-10/

[12:33:58] [INFO] testing connection to the target URL

got a 301 redirect to 'https://alamops.com/page.php?id=1'. Do you want to follow? [Y/n] Y

[12:33:59] [INFO] checking if the target is protected by some kind of WAF/IPS

[12:34:00] [INFO] testing if the target URL content is stable

[12:34:00] [WARNING] GET parameter 'id' does not appear to be dynamic

[12:34:00] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable

[12:34:00] [INFO] testing for SQL injection on GET parameter 'id'

[12:34:00] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'

[12:34:02] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'

[12:34:03] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'

[12:34:04] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'

[12:34:05] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'

[12:34:07] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'

[12:34:08] [INFO] testing 'Generic inline queries'

[12:34:08] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'

[12:34:08] [WARNING] time-based comparison requires larger statistical model, please wait. (done)

[12:34:09] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'

[12:34:11] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'

[12:34:12] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'

[12:34:13] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'

[12:34:15] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'

[12:34:16] [INFO] testing 'Oracle AND time-based blind'

it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] Y

[12:34:18] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'

[12:34:20] [WARNING] GET parameter 'id' does not seem to be injectable

[12:34:20] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 12:34:20 /2025-04-10/

┌──(someone㉿SALAMA)-[~/alamops.txt]

└─$ --cookie="PHPSESSID=abc123"

--level=5 --risk=3

--cookie=PHPSESSID=abc123: command not found

--level=5: command not found

┌──(someone㉿SALAMA)-[~/alamops.txt]

└─$ sqlmap -u "http://alamops.com/page.php?id=1" --batch --dbs --cookie="PHPSESSID=abc123"

--level=5 --risk=3

```
      ___
     __H__
 ___ ___[(]_____ ___ ___  {1.9.2#stable}
|_ -| . [)]     | .'| . |
|___|_  [,]_|_|_|_|__,|  _|
```

|_|V... |_| https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 12:38:13 /2025-04-10/

[12:38:13] [INFO] testing connection to the target URL

got a 301 redirect to 'https://alamops.com/page.php?id=1'. Do you want to follow? [Y/n] Y

[12:38:14] [INFO] testing if the target URL content is stable

[12:38:14] [WARNING] GET parameter 'id' does not appear to be dynamic

[12:38:14] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable

[12:38:14] [INFO] testing for SQL injection on GET parameter 'id'

[12:38:14] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'

[12:38:16] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'

[12:38:16] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'

[12:38:17] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'

[12:38:18] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'

[12:38:20] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'

[12:38:21] [INFO] testing 'Generic inline queries'

[12:38:21] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'

[12:38:21] [WARNING] time-based comparison requires larger statistical model, please wait. (done)

[12:38:22] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'

[12:38:23] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'

[12:38:24] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'

[12:38:25] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'

[12:38:27] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'

[12:38:28] [INFO] testing 'Oracle AND time-based blind'

it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] Y

[12:38:30] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'

[12:38:32] [WARNING] GET parameter 'id' does not seem to be injectable

[12:38:32] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 12:38:32 /2025-04-10/

--level=5: command not found

┌──(someone㉿SALAMA)-[~/alamops.txt]

└─$ xsser --url "http://alamops.com/page.php?q=test"

Command 'xsser' not found, but can be installed with:

sudo apt install xsser

┌──(someone㉿SALAMA)-[~/alamops.txt]

└─$ sudo apt install xsser

[sudo] password for someone:

The following packages were automatically installed and are no longer required:

g++-13 libfmt9 libllvm16t64 libpython3.12-minimal python3-lib2to3

g++-13-x86-64-linux-gnu libgail-common libllvm17t64 libpython3.12-stdlib python3.11

gnome-accessibility-themes libgail18t64 libnl-3-200 libpython3.12t64 python3.11-dev

gnome-themes-extra libgfapi0 libnl-route-3-200 librados2 python3.11-minimal

gnome-themes-extra-data libgfrpc0 libnsl2 librdmacm1t64 python3.12

gtk2-engines-pixbuf libgfxdr0 libperl5.38t64 libssh-gcrypt-4 python3.12-dev

ibverbs-providers libglusterfs0 libpython3.11-dev libstdc++-13-dev python3.12-minimal

libassuan0 libgtk2.0-0t64 libpython3.11-minimal libutempter0 samba-vfs-modules

libboost-iostreams1.83.0 libgtk2.0-bin libpython3.11-stdlib openjdk-17-jre

libboost-thread1.83.0 libgtk2.0-common libpython3.11t64 openjdk-17-jre-headless

libcephfs2 libibverbs1 libpython3.12-dev perl-modules-5.38

Use 'sudo apt autoremove' to remove them.

Upgrading:

curl libcurl3t64-gnutls libcurl4t64

Installing:

xsser

Installing dependencies:

geoip-database python3-cairocffi python3-geoip python3-legacy-cgi python3-ply python3-pycurl

libgeoip1t64 python3-cffi python3-geoip2 python3-maxminddb python3-pycparser python3-xcffib

Suggested packages:

geoip-bin python-cairocffi-doc python-maxmindb-doc python-ply-doc libcurl4-gnutls-dev python-pycurl-doc

Recommended packages:

python3-pygeoip

Summary:

Upgrading: 3, Installing: 13, Removing: 0, Not Upgrading: 509

Download size: 16.0 MB

Space needed: 39.2 MB / 1,016 GB available

Continue? [Y/n] y

Get:1 http://kali.download/kali kali-last-snapshot/main amd64 curl amd64 8.12.1-2 [256 kB]

Get:2 http://kali.download/kali kali-last-snapshot/main amd64 libcurl3t64-gnutls amd64 8.12.1-2 [365 kB]

Get:6 http://mirror.es.cdn-perfprod.com/kali kali-last-snapshot/main amd64 python3-ply all 3.11-7 [62.6 kB]

Get:3 http://kali.download/kali kali-last-snapshot/main amd64 geoip-database all 20241014-1 [2,921 kB]

Get:14 http://mirror.leitecastro.com/kali kali-last-snapshot/main amd64 python3-legacy-cgi all 2.6.1-2 [16.1 kB]

Get:4 http://kali.download/kali kali-last-snapshot/main amd64 libcurl4t64 amd64 8.12.1-2 [369 kB]

Get:5 http://http.kali.org/kali kali-last-snapshot/main amd64 libgeoip1t64 amd64 1.6.12-11.1+b1 [84.8 kB]

Get:7 http://kali.download/kali kali-last-snapshot/main amd64 python3-pycparser all 2.22-2 [78.0 kB]

Get:8 http://kali.download/kali kali-last-snapshot/main amd64 python3-cffi all 1.17.1-2 [89.4 kB]

Get:9 http://kali.download/kali kali-last-snapshot/main amd64 python3-xcffib all 1.5.0-1 [63.9 kB]

Get:10 http://kali.download/kali kali-last-snapshot/main amd64 python3-cairocffi all 1.7.1-3 [60.7 kB]

Get:11 http://http.kali.org/kali kali-last-snapshot/main amd64 python3-geoip amd64 1.3.2-6+b8 [20.9 kB]

Get:12 http://kali.download/kali kali-last-snapshot/main amd64 python3-maxminddb amd64 2.6.3-1 [31.4 kB]

Get:13 http://http.kali.org/kali kali-last-snapshot/main amd64 python3-geoip2 all 2.9.0+dfsg1-5 [22.8 kB]

Get:15 http://kali.download/kali kali-last-snapshot/main amd64 python3-pycurl amd64 7.45.4-1 [77.7 kB]

Get:16 http://kali.download/kali kali-last-snapshot/main amd64 xsser all 1.8.4-0kali3 [11.5 MB]

Fetched 16.0 MB in 10s (1,601 kB/s)

(Reading database ... 179628 files and directories currently installed.)

Preparing to unpack .../00-curl_8.12.1-2_amd64.deb ...

Unpacking curl (8.12.1-2) over (8.11.0-1) ...

Preparing to unpack .../01-libcurl3t64-gnutls_8.12.1-2_amd64.deb ...

Unpacking libcurl3t64-gnutls:amd64 (8.12.1-2) over (8.11.0-1) ...

Selecting previously unselected package geoip-database.

Preparing to unpack .../02-geoip-database_20241014-1_all.deb ...

Unpacking geoip-database (20241014-1) ...

Preparing to unpack .../03-libcurl4t64_8.12.1-2_amd64.deb ...

Unpacking libcurl4t64:amd64 (8.12.1-2) over (8.11.0-1) ...

Selecting previously unselected package libgeoip1t64:amd64.

Preparing to unpack .../04-libgeoip1t64_1.6.12-11.1+b1_amd64.deb ...

Unpacking libgeoip1t64:amd64 (1.6.12-11.1+b1) ...

Selecting previously unselected package python3-ply.

Preparing to unpack .../05-python3-ply_3.11-7_all.deb ...

Unpacking python3-ply (3.11-7) ...

Selecting previously unselected package python3-pycparser.

Preparing to unpack .../06-python3-pycparser_2.22-2_all.deb ...

Unpacking python3-pycparser (2.22-2) ...

Selecting previously unselected package python3-cffi.

Preparing to unpack .../07-python3-cffi_1.17.1-2_all.deb ...

Unpacking python3-cffi (1.17.1-2) ...

Selecting previously unselected package python3-xcffib.

Preparing to unpack .../08-python3-xcffib_1.5.0-1_all.deb ...

Unpacking python3-xcffib (1.5.0-1) ...

Selecting previously unselected package python3-cairocffi.

Preparing to unpack .../09-python3-cairocffi_1.7.1-3_all.deb ...

Unpacking python3-cairocffi (1.7.1-3) ...

Selecting previously unselected package python3-geoip:amd64.

Preparing to unpack .../10-python3-geoip_1.3.2-6+b8_amd64.deb ...

Unpacking python3-geoip:amd64 (1.3.2-6+b8) ...

Selecting previously unselected package python3-maxminddb.

Preparing to unpack .../11-python3-maxminddb_2.6.3-1_amd64.deb ...

Unpacking python3-maxminddb (2.6.3-1) ...

Selecting previously unselected package python3-geoip2.

Preparing to unpack .../12-python3-geoip2_2.9.0+dfsg1-5_all.deb ...

Unpacking python3-geoip2 (2.9.0+dfsg1-5) ...

Selecting previously unselected package python3-legacy-cgi.

Preparing to unpack .../13-python3-legacy-cgi_2.6.1-2_all.deb ...

Unpacking python3-legacy-cgi (2.6.1-2) ...

Selecting previously unselected package python3-pycurl.

Preparing to unpack .../14-python3-pycurl_7.45.4-1_amd64.deb ...

Unpacking python3-pycurl (7.45.4-1) ...

Selecting previously unselected package xsser.

Preparing to unpack .../15-xsser_1.8.4-0kali3_all.deb ...

Unpacking xsser (1.8.4-0kali3) ...

Setting up libcurl4t64:amd64 (8.12.1-2) ...

Setting up python3-ply (3.11-7) ...

Setting up libcurl3t64-gnutls:amd64 (8.12.1-2) ...

Setting up libgeoip1t64:amd64 (1.6.12-11.1+b1) ...

Setting up python3-pycparser (2.22-2) ...

Setting up python3-pycurl (7.45.4-1) ...

Setting up python3-legacy-cgi (2.6.1-2) ...

Setting up curl (8.12.1-2) ...

Setting up geoip-database (20241014-1) ...

Setting up python3-maxminddb (2.6.3-1) ...

Setting up python3-geoip2 (2.9.0+dfsg1-5) ...

Setting up python3-cffi (1.17.1-2) ...

Setting up python3-xcffib (1.5.0-1) ...

Setting up python3-geoip:amd64 (1.3.2-6+b8) ...

Setting up python3-cairocffi (1.7.1-3) ...

Setting up xsser (1.8.4-0kali3) ...

Processing triggers for libc-bin (2.40-3) ...

┌──(someone㉿SALAMA)-[~/alamops.txt]

└─$ xsser --url "http://alamops.com/page.php?q=test"

==

XSSer v1.8[4]: "The HiV€!" - (https://xsser.03c8.net) - 2010/2021 -> by psy

==

Testing [XSS from URL]...

==

==============================

[Error] XSSer cannot find a correct place to start an attack. Aborting!...

[Info] This is because you aren't providing:

At least one -payloader- using a keyword: 'XSS' (for hex.hash) or 'X1S' (for int.hash):

- ex (GET): xsser -u 'https://target.com' -g '/path/profile.php?username=bob&surname=XSS&age=X1S&job=XSS'

- ex (POST): xsser -u 'https://target.com/login.php' -p 'username=bob&password=XSS&captcha=X1S'

Any extra attack(s) (Xsa, Xsr, Coo, Dorker, Crawler...):

- ex (GET+Cookie): xsser -u 'https://target.com' -g '/path/id.php?=2' --Coo

- ex (POST+XSA+XSR+Cookie): xsser -u 'https://target.com/login.php' -p 'username=admin&password=admin' --Xsa --Xsr --Coo

- ex (Dorker): xsser -d 'news.php?id=' --Da

- ex (Crawler): xsser -u 'https://target.com' -c 100 --Cl

Or a mixture:

- ex (GET+Manual): xsser -u 'https://target.com' -g '/users/profile.php?user=XSS&salary=X1S' --payload='<script>alert(XSS);</script>'

- ex (POST+Manual): xsser -u 'https://target.com/login.asp' -p 'username=bob&password=XSS' --payload='}}%%&//<sc&ri/pt>(XSS)--;>'

- ex (GET+Cookie): xsser -u 'https://target.com' -g '/login.asp?user=bob&password=XSS' --Coo

- ex (POST+XSR+XSA): xsser -u 'https://target.com/login.asp' -p 'username=bob&password=XSS' --Xsr --Xsa

==========

┌──(someone㉿SALAMA)-[~/alamops.txt]

└─$ curl http://target.com/robots.txt

┌──(someone㉿SALAMA)-[~/alamops.txt]

└─$ curl http://target.com/alamops.txt

┌──(someone㉿SALAMA)-[~/alamops.txt]

└─$ chmod +x Pentesting_Web_Script.sh

chmod: cannot access 'Pentesting_Web_Script.sh': No such file or directory

┌──(someone㉿SALAMA)-[~/alamops.txt]

└─$ chmod +x

chmod: missing operand after ‘+x’

Try 'chmod --help' for more information.

┌──(someone㉿SALAMA)-[~/alamops.txt]

└─$ --help

--help: command not found

┌──(someone㉿SALAMA)-[~/alamops.txt]

└─$ help

GNU bash, version 5.2.32(1)-release (x86_64-pc-linux-gnu)

These shell commands are defined internally. Type `help' to see this list.

Type `help name' to find out more about the function `name'.

Use `info bash' to find out more about the shell in general.

Use `man -k' or `info' to find out more about commands not in this list.

A star (*) next to a name means that the command is disabled.

job_spec [&] history [-c] [-d offset] [n] or history -anrw [filename] or hi>

((expression)) if COMMANDS; then COMMANDS; [elif COMMANDS; then COMMANDS;].>

. filename [arguments] jobs [-lnprs] [jobspec ...] or jobs -x command [args]

: kill [-s sigspec | -n signum | -sigspec] pid | jobspec ... or >

[arg...] let arg [arg ...]

[[expression]] local [option] name[=value] ...

alias [-p] [name[=value] ...] logout [n]

bg [job_spec ...] mapfile [-d delim] [-n count] [-O origin] [-s count] [-t] [-u >

bind [-lpsvPSVX] [-m keymap] [-f filename] [-q name] [-u name] > popd [-n] [+N | -N]

break [n] printf [-v var] format [arguments]

builtin [shell-builtin [arg ...]] pushd [-n] [+N | -N | dir]

caller [expr] pwd [-LP]

case WORD in [PATTERN [| PATTERN]...) COMMANDS ;;]... esac read [-ers] [-a array] [-d delim] [-i text] [-n nchars] [-N nc>

cd [-L|[-P [-e]] [-@]] [dir] readarray [-d delim] [-n count] [-O origin] [-s count] [-t] [->

command [-pVv] command [arg ...] readonly [-aAf] [name[=value] ...] or readonly -p

compgen [-abcdefgjksuv] [-o option] [-A action] [-G globpat] [-> return [n]

complete [-abcdefgjksuv] [-pr] [-DEI] [-o option] [-A action] [> select NAME [in WORDS ... ;] do COMMANDS; done

compopt [-o|+o option] [-DEI] [name ...] set [-abefhkmnptuvxBCEHPT] [-o option-name] [--] [-] [arg ...]

continue [n] shift [n]

coproc [NAME] command [redirections] shopt [-pqsu] [-o] [optname ...]

declare [-aAfFgiIlnrtux] [name[=value] ...] or declare -p [-aAf> source filename [arguments]

dirs [-clpv] [+N] [-N] suspend [-f]

disown [-h] [-ar] [jobspec ... | pid ...] test [expr]

echo [-neE] [arg ...] time [-p] pipeline

enable [-a] [-dnps] [-f filename] [name ...] times

eval [arg ...] trap [-lp] [[arg] signal_spec ...]

exec [-cl] [-a name] [command [argument ...]] [redirection ...> true

exit [n] type [-afptP] name [name ...]

export [-fn] [name[=value] ...] or export -p typeset [-aAfFgiIlnrtux] name[=value] ... or typeset -p [-aAfF>

false ulimit [-SHabcdefiklmnpqrstuvxPRT] [limit]

fc [-e ename] [-lnr] [first] [last] or fc -s [pat=rep] [command> umask [-p] [-S] [mode]

fg [job_spec] unalias [-a] name [name ...]

for NAME [in WORDS ...] ; do COMMANDS; done unset [-f] [-v] [-n] [name ...]

for ((exp1; exp2; exp3)); do COMMANDS; done until COMMANDS; do COMMANDS-2; done

function name { COMMANDS ; } or name () { COMMANDS ; } variables - Names and meanings of some shell variables

getopts optstring name [arg ...] wait [-fn] [-p var] [id ...]

hash [-lr] [-p pathname] [-dt] [name ...] while COMMANDS; do COMMANDS-2; done

help [-dms] [pattern ...] { COMMANDS ; }

┌──(someone㉿SALAMA)-[~/alamops.txt]

└─$ ./Pentesting_Web_Script.sh

-bash: ./Pentesting_Web_Script.sh: No such file or directory

```
┌──(someone㉿SALAMA)-[~/alamops.txt]
└─$ nano REPORT.md

┌──(someone㉿SALAMA)-[~/alamops.txt]
└─$ ls
'REPORT alamOps.md'

┌──(someone㉿SALAMA)-[~/alamops.txt]
└─$ mv REPORT.md ~/Escritorio/
mv: cannot stat 'REPORT.md': No such file or directory

┌──(someone㉿SALAMA)-[~/alamops.txt]
└─$ mv REPORT alamOps.md ~/Escritorio/
mv: target '/home/someone/Escritorio/': No such file or directory

┌──(someone㉿SALAMA)-[~/alamops.txt]
└─$ wafw00f https://alamops.com
Command 'wafw00f' not found, but can be installed with:
sudo apt install wafw00f

┌──(someone㉿SALAMA)-[~/alamops.txt]
└─$ sudo apt install wafw00f
[sudo] password for someone:
The following packages were automatically installed and are no longer required:
  g++-13                libfmt9          libllvm16t64          libpython3.12-minimal    python3-lib2to3
  g++-13-x86-64-linux-gnu  libgail-common  libllvm17t64          libpython3.12-stdlib
python3.11
  gnome-accessibility-themes  libgail18t64  libnl-3-200          libpython3.12t64
python3.11-dev
```

```
  gnome-themes-extra          libgfapi0          libnl-route-3-200      librados2              python3.11-
minimal
  gnome-themes-extra-data     libgfrpc0          libnsl2                librdmacm1t64          python3.12
  gtk2-engines-pixbuf         libgfxdr0          libperl5.38t64         libssh-gcrypt-4        python3.12-dev
  ibverbs-providers           libglusterfs0      libpython3.11-dev      libstdc++-13-dev
python3.12-minimal
  libassuan0                  libgtk2.0-0t64     libpython3.11-minimal  libutempter0           samba-vfs-
modules
  libboost-iostreams1.83.0    libgtk2.0-bin      libpython3.11-stdlib   openjdk-17-jre
  libboost-thread1.83.0       libgtk2.0-common   libpython3.11t64       openjdk-17-jre-headless
  libcephfs2                  libibverbs1        libpython3.12-dev      perl-modules-5.38
Use 'sudo apt autoremove' to remove them.

Installing:
  wafw00f

Installing dependencies:
  python3-pluginbase

Summary:
  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 509
  Download size: 52.5 kB
  Space needed: 306 kB / 1,016 GB available

Continue? [Y/n] y
Get:1 http://kali.download/kali kali-last-snapshot/main amd64 python3-pluginbase all 1.0.1-1
[13.5 kB]
Get:2 http://kali.download/kali kali-last-snapshot/main amd64 wafw00f all 2.3.1-1 [39.0 kB]
Fetched 52.5 kB in 1s (60.8 kB/s)
Selecting previously unselected package python3-pluginbase.
(Reading database ... 180101 files and directories currently installed.)
Preparing to unpack .../python3-pluginbase_1.0.1-1_all.deb ...
```

```
Unpacking python3-pluginbase (1.0.1-1) ...
Selecting previously unselected package wafw00f.
Preparing to unpack .../wafw00f_2.3.1-1_all.deb ...
Unpacking wafw00f (2.3.1-1) ...
Setting up python3-pluginbase (1.0.1-1) ...
Setting up wafw00f (2.3.1-1) ...

┌──(someone㉿SALAMA)-[~/alamops.txt]
└─$ wafw00f https://alamops.com

              ?           ,.   (   .     )       .     "
     __       ??        ("     )  )'    ,'       )  . (`     '`
  (___()'`;   ???         .; )  ' (( (" )    ;(,     ((  (  ;)  "  )")
  /,___ /`              _".,  ,._'_.,)_(..,( . )_  _' )_') (. _..( ' )
  \\  \\             |____|____|____|____|____|____|____|____|____|

                        ~ WAFW00F : v2.3.1 ~
                ~ Sniffing Web Application Firewalls since 2014 ~

[*] Checking https://alamops.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7

┌──(someone㉿SALAMA)-[~/alamops.txt]
└─$ curl -I https://alamops.com | grep -i 'set-cookie'
 % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
 0  1240    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
```

```
┌──(someone㉿SALAMA)-[~/alamops.txt]
└─$ curl -s -D - https://alamops.com -o /dev/null
HTTP/1.1 200 OK
Server: nginx/1.24.0 (Ubuntu)
Date: Thu, 10 Apr 2025 12:11:47 GMT
Content-Type: text/html
Content-Length: 1240
Connection: keep-alive
Last-Modified: Thursday, 10-Apr-2025 12:11:47 UTC
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate, max-age=0
Accept-Ranges: bytes
```