

Penetration Testing

Team member name:

- Jin Zhang
- Jingyi Cui
- Yanjuan Li

Goal:

- Identify and test your application against at least 3 attack vectors that do not exploit UI vulnerabilities. - You will document your findings in a PDF (Google doc exported as PDF) and commit it to your Github repository. - Your report should be as detailed as possible.
- You will document attacks on your own web application with and without the AWS WAF in place.

WorkFlow:

- Software Installation
- Overall scan
- SQL
- SSL
- DNS

So, I am using KALI. Pretty Advanced Penetration Testing Tools package. It integrates many very good penetration testing tools into one system for ease of use.

Download it at <https://www.kali.org/>



 BY OFFENSIVE SECURITY	Blog		DRUG	WEAPONS	HACKING	UNCOMMON TACTICS	COMMUNITY	ABOUT US
	Follow us on Twitter	Follow @kaliops 20K followers	Follow @kaliattack 162K followers	Follow @kaliinfo 15K followers				
Download Kali Linux	Kali Linux Twitter Feed	    						
Download Kali Linux – our most advanced penetration testing platform we have ever made. Available in 32 bit, 64 bit, and ARM flavors, as well as a number of specialized builds for many popular hardware platforms. Kali can always be updated to the newest version without the need for a new download.	Whether our machine will run Linux, allowing us to work with ease.		Available on the Offensive Security Download Page	Available on the Offensive Security Download Page	Available on the Offensive Security Download Page	Available on the Offensive Security Download Page	Available on the Offensive Security Download Page	Apr 5, 2019
Kali Linux Kde 64 Bit	HTTP Torrent	3.6G	2019.1a	2948e1fec80edb8eb7d63c5b60daa0928c4ed97e9d0fc280fa503c661ecbd9fed				
Kali Linux 64 bit VMware VM				Available on the Offensive Security Download Page				
Kali Linux 32 bit VMware VM PAE				Available on the Offensive Security Download Page				
Kali Linux 64 bit Vbox				Available on the Offensive Security Download Page				
Kali Linux 32 bit Vbox				Available on the Offensive Security Download Page				

Kali Linux Weekly Builds

rate limited to 5 concurrent connections.

high
Certificates
hardware
tests
Linux
distribution

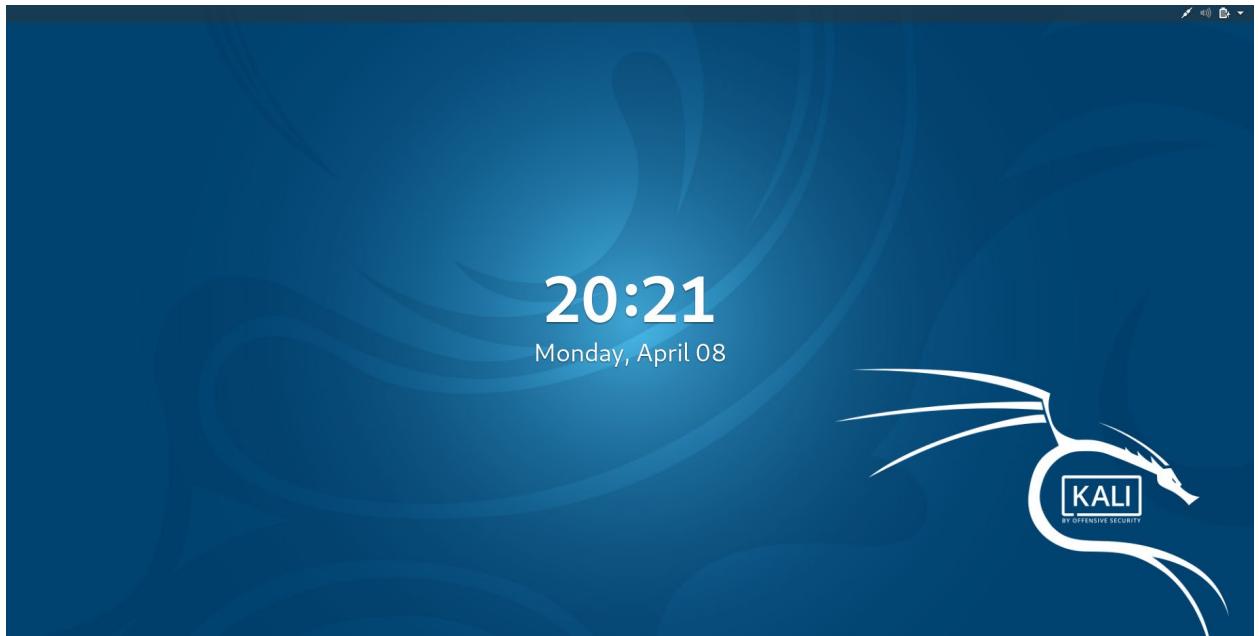
Kali Linux VMware Images

Kali Linux VirtualBox Images

Image Name	Torrent	Size	Version	SHA256Sum
Kali Linux Vm 64 Bit 7z	Torrent	2.5G	2019.1	e4c6999edccf27f97d4d014cdc66950b8b4148948abe8bb3a2c30bbc0915e95a
Kali Linux Vm 32 Bit 7z	Torrent	2.6G	2019.1	9d2c51b99da583c18fcdb3a47d001dbe1a9ed3013105d0557ed2594d033ce614

First for the very most, to install KALI Image. There are many editions of this platform. I choose **Kali Linux 64 bit Vbox**. This is like a VM with Linux OS.





First, I want to use **Nikto**: Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items. This is a multifunction powerful tool.

```

Applications ▾ Places ▾ Terminal ▾ Mon 21:18
cannyjin@kali: ~

File Edit View Search Terminal Help
-Help Extended help information
+host+ target host
+id+ Host authentication to use, format is id:pass or id:pass:realm
+list-plugins List all available plugins
+output+ Write output to this file
+nossal Disables using SSL
+no404 Disables 404 checks
+Plugins+ List of plugins to run (default: ALL)
+port+ Port to use (default 80)
+root+ Prepend root value to all requests, format is /directory
+ssl Force ssl mode on port
+Tuning+ Scan tuning
+timeout+ Timeout for requests (default 10 seconds)
+update Update databases and plugins from CIRT.net
+Version Print plugin and database versions
+vhost+ Virtual host (for Host header)
+ requires a value

Note: This is the short help output. Use -H for full help text.

cannyjin@kali: $ nikto -host csye6225-spring2019-zhangjin.me -Tuning 1
Nikto v2.1.6

+ No web server found on csye6225-spring2019-zhangjin.me:80
-----+ 0 host(s) tested
cannyjin@kali: $ nikto -host https://csye6225-spring2019-zhangjin.me/api/all/ -Tuning 1
Nikto v2.1.6

+ Target IP: 52.5.201.85
+ Target Hostname: csye6225-spring2019-zhangjin.me
+ Target Port: 443
-----+ SSL Info: Subject: /CN=csye6225-spring2019-zhangjin.me
          Ciphers: ECDHE-RSA-AES128-GCM-SHA256
          Issuer: /C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
+ Start Time: 2019-04-08 21:16:24 (GMT-4)
-----+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ 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
+ Server banner has changed from '' to 'awselb/2.0' which may suggest a WAF, load balancer or proxy is in place
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, OPTIONS

```

I want to use this tool to scan my app's vulnerable spot. To make a big picture, not to specify choose a vector.

Because in my perspective the most critical step of the penetration test is to scan the vulnerable spot. If you don't know that. How can you know where to attack. How do I choose a specific vector?

The result literally gives me the answer.

```

- Nikto v2.1.6
-----+ Target IP: 52.5.201.85
+ Target Hostname: csye6225-spring2019-zhangjin.me
+ Target Port: 443
-----+ SSL Info: Subject: /CN=csye6225-spring2019-zhangjin.me
          Ciphers: ECDHE-RSA-AES128-GCM-SHA256
          Issuer: /C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
+ Start Time: 2019-04-08 21:16:24 (GMT-4)
-----+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ 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
+ Server banner has changed from '' to 'awselb/2.0' which may suggest a WAF, load balancer or proxy is in place
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, OPTIONS

```

I would like to scan SQL and SSL and DNS.

SQLMAP to test the vulnerability of the database of our web application.

It can scan the SQL. See App is injectable or not.

```
Kali-Linux-2019.1-vbox-amd64 [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
Applications ▾ Places ▾ Terminal ▾ Mon 19:22
cannyjin@kali: ~
```

File Edit View Search Terminal Help

```
General:
These options can be used to set some general working parameters
--batch           Never ask for user input, use the default behavior
--flush-session   Flush session files for current target

Miscellaneous:
--sqlmap-shell    Prompt for an interactive sqlmap shell
--wizard          Simple wizard interface for beginner users
cannyjin@kali:~$ sqlmap -u https://csye6225-spring2019-zhangjin.me/api/all/ --dbs:~$ sqlmap -u https://c
[+] [H] {1.3#stable}
[+] [I] http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It i
s the end user's responsibility to obey all applicable local, state and federal laws. Developers assume n
o liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 19:20:07 /2019-04-08/
[19:20:08] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/art
icle.php?id=1') and without providing any POST parameters through option '--data'
do you want to try URI injections in the target URL itself? [Y/n/q] y
[19:21:28] [INFO] testing connection to the target URL
[19:21:21] [INFO] checking if the target is protected by some kind of WAF/IPS
[19:21:21] [INFO] heuristics detected web page charset 'ascii'
[19:21:21] [CRITICAL] heuristics detected that the target is protected by some kind of WAF/IPS
do you want sqlmap to try to detect backend WAF/IPS? [y/N] y
```

```
Kali-Linux-2019.1-vbox-amd64 [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
Applications ▾ Places ▾ Terminal ▾ Mon 19:22
cannyjin@kali: ~
```

File Edit View Search Terminal Help

```
--flush-session   Flush session files for current target

Miscellaneous:
--sqlmap-shell    Prompt for an interactive sqlmap shell
--wizard          Simple wizard interface for beginner users
cannyjin@kali:~$ sqlmap -u https://csye6225-spring2019-zhangjin.me/api/all/ --dbs:~$ sqlmap -u https://c
[+] [H] {1.3#stable}
[+] [I] http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It i
s the end user's responsibility to obey all applicable local, state and federal laws. Developers assume n
o liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 19:20:07 /2019-04-08/
[19:20:08] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/art
icle.php?id=1') and without providing any POST parameters through option '--data'
do you want to try URI injections in the target URL itself? [Y/n/q] y
[19:21:28] [INFO] testing connection to the target URL
[19:21:21] [INFO] checking if the target is protected by some kind of WAF/IPS
[19:21:21] [INFO] heuristics detected web page charset 'ascii'
[19:21:21] [CRITICAL] heuristics detected that the target is protected by some kind of WAF/IPS
do you want sqlmap to try to detect backend WAF/IPS? [y/N] y
[19:22:14] [INFO] using WAF scripts to detect backend WAF/IPS protection
[19:22:15] [CRITICAL] WAF/IPS identified as 'Amazon Web Services Web Application Firewall (Amazon)'
are you sure that you want to continue with further target testing? [y/N] y
```

```

Applications Places Terminal Mon 19:23
cannyjin@kali:~>

File Edit View Search Terminal Help

[19:20:08] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/article.php?id=1') and without providing any POST parameters through option '--data'
do you want to try URL injections in the target URL itself? [Y/n/q] y
[19:21:20] [INFO] testing connection to the target URL
[19:21:21] [INFO] checking if the target is protected by some kind of WAF/IPS
[19:21:21] [INFO] heuristics detected web page charset 'ascii'
[19:21:21] [CRITICAL] heuristics detected that the target is protected by some kind of WAF/IPS
do you want to continue? [Y/n/q] y
[19:22:13] [WARNING] dropping timeout to 10 seconds (i.e. '--timeout=10')
[19:22:14] [INFO] using WAF scripts to detect backend WAF/IPS protection
[19:22:15] [CRITICAL] WAF/IPS identified as 'Amazon Web Services Web Application Firewall (Amazon)'
are you sure that you want to continue with further target testing? [y/N] y
[19:22:39] [WARNING] please consider usage of tamper scripts (option '--tamper')
[19:22:39] [INFO] testing if the target URL content is stable
[19:22:40] [INFO] testing if URI parameter '#1' is static
[19:22:40] [INFO] testing if URI parameter '#1' is dynamic
[19:22:40] [WARNING] URI parameter '#1' does not appear to be dynamic
[19:22:40] [INFO] heuristic (basic) test shows that URI parameter '#1*' might not be injectable
[19:22:40] [INFO] testing for SQL injection on URI parameter '#1'
[19:22:40] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[19:22:40] [WARNING] reflective value(s) found and filtering out
[19:22:41] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[19:22:41] [INFO] testing 'Boolean-based error-based - WHERE or HAVING clause (FLOOR)'
[19:22:41] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[19:22:42] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[19:22:42] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLEType)'
[19:22:42] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[19:22:42] [INFO] testing 'MySQL inline queries'
[19:22:42] [INFO] testing 'PostgreSQL inline queries'
[19:22:43] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IP)'
[19:22:43] [INFO] testing 'Oracle AND time-based blind'
[19:22:43] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[19:22:43] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[19:22:43] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[19:22:43] [INFO] testing 'Oracle stacked queries (DBMS PIPE RECEIVE_MESSAGE - comment)'
[19:22:43] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[19:22:44] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[19:22:44] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IP)'
[19:22:44] [INFO] testing 'Oracle AND time-based blind'
[19:22:44] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[19:22:45] [WARNING] URI parameter '#1*' does not seem to be injectable
[19:22:45] [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'
[19:22:49] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 57 times, 404 (Not Found) - 74 times

[*] ending @ 19:22:49 /2019-04-08/
cannyjin@kali:~$

```

I try to URI injections in the target URL which is my domain. <https://csye6225-spring2019-zhangjin.me/api/all/>

And is said [CRITICAL] heuristics detected that the target is protected by some kind of WAF/IPS

So, I try to detect backend WAF/IPS.

So, It identified as 'Amazon Web Services Web Application Firewall (Amazon)'

So, I go further target testing?

You can see the result in the screen shot.

```

[19:22:45] [INFO] testing generic UNION query (NULL) - 1 to 10 columns
[19:22:49] [WARNING] URI parameter '#1*' does not seem to be injectable
[19:22:49] [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'
[19:22:49] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 57 times, 404 (Not Found) - 74 times

[*] ending @ 19:22:49 /2019-04-08/
Preferred TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve P-256
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve P-256

```

Look like our firewall work well.

Next, I will try my teammate's Application that without firewall.

Now, try my teammate's domain that without firewall.

```
cannyjin@kali:~
```

```
File Edit View Search Terminal Help
Miscellaneous:
--sqlmap-shell    Prompt for an interactive sqlmap shell
--wizard          Simple wizard interface for beginner users
[!] to see full list of options run with 'hh'
cannyjin@kali:~$ sqlmap -u https://csye6225-spring2019-liyanj.me/api/all/ --dbs
      H
      |
      +-- [1] {1.3#stable}
      |   +-- [0]
      |   |   +-- [.]
      |   |   +-- [.]
      |   |   +-- [.]
      |   +-- [V] http://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 @ 16:16:35 /2019-04-09

[16:16:35] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/article.php?id=1') and without providing any POST parameters through option '--data'

[16:16:44] [INFO] testing connection to the target URL
[16:16:44] [INFO] checking if the target is protected by some kind of WAF/IPS
[16:16:44] [CRITICAL] heuristics detected that the target is protected by some kind of WAF/IPS
do you want sqlmap to try to detect backend WAF/IPS? [y/N] y
[16:16:50] [WARNING] dropping timeout to 10 seconds (i.e. '--timeout=10')
[16:16:50] [INFO] using WAF scripts to detect backend WAF/IPS protection
[16:16:50] [WARNING] WAF/IPS product hasn't been identified
[16:16:50] [INFO] testing if the target URL content is stable
[16:16:50] [INFO] target URL content is stable
[16:16:50] [INFO] testing if URI parameter '#1*' is dynamic
[16:16:51] [WARNING] URI parameter '#1*' does not appear to be dynamic
[16:16:51] [WARNING] heuristic (basic) test shows that URI parameter '#1*' might not be injectable
[16:16:51] [INFO] testing for SQL injection on URI parameter '#1*'
[16:16:51] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[16:16:51] [WARNING] reflective value(s) found and filtering out
[16:16:52] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[16:16:52] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[16:16:52] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'

[16:16:50] [INFO] testing if the target URL content is stable
[16:16:50] [INFO] target URL content is stable
[16:16:50] [INFO] testing if URI parameter '#1*' is dynamic
[16:16:51] [WARNING] URI parameter '#1*' does not appear to be dynamic
[16:16:51] [WARNING] heuristic (basic) test shows that URI parameter '#1*' might not be injectable
[16:16:51] [INFO] testing for SQL injection on URI parameter '#1*'
[16:16:51] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[16:16:51] [WARNING] reflective value(s) found and filtering out
[16:16:52] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[16:16:52] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[16:16:52] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[16:16:53] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[16:16:53] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLEType)'
[16:16:54] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[16:16:54] [INFO] testing 'MySQL inline queries'
[16:16:54] [INFO] testing 'PostgreSQL inline queries'
[16:16:54] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[16:16:54] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[16:16:54] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[16:16:55] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[16:16:55] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[16:16:55] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[16:16:56] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[16:16:56] [INFO] testing 'Oracle AND time-based blind'
[16:16:56] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[16:17:00] [WARNING] URI parameter '#1*' does not seem to be injectable
[16:17:00] [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'
[16:17:00] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 127 times, 405 (Method Not Allowed) - 1 times
```

```
cannyjin@kali:~
```

```
[16:16:44] [INFO] testing connection to the target URL
[16:16:44] [INFO] checking if the target is protected by some kind of WAF/IPS
[16:16:44] [CRITICAL] heuristics detected that the target is protected by some kind of WAF/IPS
do you want sqlMap to try to detect backend WAF/IPS? [y/N] y
[16:16:50] [WARNING] dropping timeout to 10 seconds (i.e. '--timeout=10')
[16:16:50] [INFO] using WAF scripts to detect backend WAF/IPS protection
[16:16:50] [WARNING] WAF/IPS product hasn't been identified
[16:16:50] [INFO] testing if the target URL content is stable
[16:16:50] [INFO] target URL content is stable
[16:16:50] [INFO] testing if URI parameter '#1*' is dynamic
[16:16:51] [WARNING] URI parameter '#1*' does not appear to be dynamic
[16:16:51] [WARNING] heuristic (basic) test shows that URI parameter '#1*' might not be injectable
[16:16:51] [INFO] testing for SQL injection on URI parameter '#1*'
[16:16:51] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[16:16:51] [WARNING] reflective value(s) found and filtering out
[16:16:52] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[16:16:52] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[16:16:52] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[16:16:53] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[16:16:53] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLEType)'
[16:16:54] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[16:16:54] [INFO] testing 'MySQL inline queries'
[16:16:54] [INFO] testing 'PostgreSQL inline queries'
[16:16:54] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[16:16:54] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[16:16:54] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[16:16:55] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[16:16:55] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[16:16:55] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[16:16:56] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[16:16:56] [INFO] testing 'Oracle AND time-based blind'
[16:16:56] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[16:17:00] [WARNING] URI parameter '#1*' does not seem to be injectable
[16:17:00] [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'
[16:17:00] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 127 times, 405 (Method Not Allowed) - 1 times
```

And the result seems to be the same.

SSLScan This queries SSL/TLS services, such as HTTPS, in order to determine the ciphers that are supported.

I want to see our cipher is secure enough or not.

```
1.11.12-static
OpenSSL 1.0.2-chacha (1.0.2g-dev)

Command:
  ssllscan [Options] [host:port | host]

Options:
--targets=<file>      A file containing a list of hosts to check.
--sni-name=<name>      Hostname for SNI
--ipv4, -4              Only use IPv4
--ipv6, -6              Only use IPv6
--show-certificate     Show full certificate information
--no-check-certificate Don't warn about weak certificate algorithm or keys
--show-client-cas      Show trusted CAs for TLS client auth
--show-ciphers          Show supported client ciphers
--show-cipher-ids      Show cipher ids
--show-times            Show handshake times in milliseconds
--ssl2                  Only check SSLv2 ciphers
--ssl3                  Only check SSLv3 ciphers
--tls10                 Only check TLSv1.0 ciphers
--tls11                 Only check TLSv1.1 ciphers
--tls12                 Only check TLSv1.2 ciphers
--talsall                Only check TLS ciphers (all versions)
--ocsp                  Request OCSP response from server
--pk=<file>             A file containing the private key or a PKCS#12 file
--pkpass=<password>    The password for the private key or PKCS#12 file
--certs=<file>          A file containing PEM/ASN1 formatted client certificates
--no-ciphersuites       Do not check for supported ciphersuites
--no-fallback           Do not check for TLS Fallback SCSV
--no-renegotiation     Do not check for TLS renegotiation
--no-compression        Do not check for TLS compression (CRIME)
--no-heartbleed         Do not check for OpenSSL Heartbleed (CVE-2014-0160)
--starttls-ftp          STARTTLS setup for FTP
--starttls-imap         STARTTLS setup for IMAP
--starttls-irc          STARTTLS setup for IRC
--starttls-ldap          STARTTLS setup for LDAP
--starttls-pop3         STARTTLS setup for POP3
--starttls-smtp         STARTTLS setup for SMTP

OpenSSL 1.0.2-chacha (1.0.2g-dev)

Connected to 18.214.77.145

Testing SSL server csye6225-spring2019-zhangjin.me on port 443 using SNI name csye6225-spring2019-zhangjin.me

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve P-256 DHE 256
Accepted  TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve P-256 DHE 256
Accepted  TLSv1.2 128 bits ECDHE-RSA-AES128-SHA Curve P-256 DHE 256
Accepted  TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-256 DHE 256
Accepted  TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve P-256 DHE 256
Accepted  TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
Accepted  TLSv1.2 128 bits AES128-GCM-SHA256
Accepted  TLSv1.2 128 bits AES128-SHA256
Accepted  TLSv1.2 128 bits AES128-SHA
Accepted  TLSv1.2 256 bits AES256-GCM-SHA384
Accepted  TLSv1.2 256 bits AES256-SHA256
Accepted  TLSv1.2 256 bits AES256-SHA
Preferred TLSv1.1 128 bits ECDHE-RSA-AES128-SHA Curve P-256 DHE 256
Accepted  TLSv1.1 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
Accepted  TLSv1.1 128 bits AES128-SHA
Accepted  TLSv1.1 256 bits AES256-SHA
Preferred TLSv1.0 128 bits ECDHE-RSA-AES128-SHA Curve P-256 DHE 256
Accepted  TLSv1.0 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
Accepted  TLSv1.0 128 bits AES128-SHA
Accepted  TLSv1.0 256 bits AES256-SHA

  SSL Certificate:
```

```
SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048

Subject: csye6225-spring2019-zhangjin.me
AltNames: DNS:csye6225-spring2019-zhangjin.me
Issuer: Amazon

Not valid before: Apr 6 00:00:00 2019 GMT
Not valid after: May 6 12:00:00 2020 GMT
```

As you can see I got a lot of results.

I got the cipher Algorithm, you can google it to check this **sha256WithRSAEncryption** Algorithm is secure or not.

A screenshot of a Google search results page. The search query "sha256withrsaencryption vulnerability" is entered into the search bar. The results are filtered under the "All" tab. There are approximately 20,000 results found in 0.41 seconds. The first result is a link to "SHA1 vs SHA256 - KeyCDN Support" from <https://www.keycdn.com/support/sha1-vs-sha256>. Below the link, a snippet of text from the page states: "Oct 4, 2018 - To compare the differences that exist between the SHA1 vs **SHA256** ... Additionally, SHA1 has also been deemed quite **vulnerable** to collision ...". The second result is a link to "All about SHA1, SHA2 and SHA256 hash algorithms" from <https://www.tbs-certificates.co.uk/FAQ/en/sha256.html>. Below the link, a snippet of text from the page states: "Nov 2, 2018 - **SHA256**, provided by TBS INTERNET since 2008, will in the coming few ... SHA0 (obsolete because **vulnerable**), SHA1 (the most popular one), ...". The third result is a link to "Is using "SHA-256 with RSA-2048 Encryption" a secure certificate ..." from <https://security.stackexchange.com/.../is-using-sha-256-with-rsa-2048-encryption-a-se...>. Below the link, a snippet of text from the page states: "May 4, 2016 - The only viable attacks would require finding a **weakness** in the hash algorithm itself, and it's not necessarily the case that SHA-512 would be ...". Below this, there are several smaller links to related questions on Stack Exchange, such as "How to bypass PHP strings == comparison for **sha256** ...", "decryption - Why can't **SHA256** be decrypted ...", "OpenSSL check if a SSL certificate is SHA-1 or ...", and "**sha256** - What is the relationship between "SHA-2 ...". A "More results from security.stackexchange.com" link is also present.

People also ask

Nmap I use it to discovery the network for our Web to see there is any security issue.



```
Kali-Linux-2019.1-vbox-amd64 [正在运行] - Oracle VM VirtualBox
File Edit View Search Terminal Help
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V Print version number
-h Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -A -p 192.168.0.0/16 10.0.0.0/8
nmap -v -sR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
cannyjin@kali:~$ nmap
Address      Hwtype   Flags Mask   Iface
gateway     ether    52:54:00:12:35:02 C      eth0
cannyjin@kali:~$ nmap https://csye6225-spring2019-zhangjin.me/api/all/
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-08 21:50 EDT
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.07 seconds
WARNING: No targets were specified, so 0 hosts scanned.
Nmap version 7.70 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.3 openssl-1.1.1a libbz2-1.2.11 libpcre-8.39 nmap-libpcap-1.7.3 nmap-libdnet-1.12 ipv6
Completed without errors
Available service engines: espell poll select
cannyjin@kali:~$ nmap 100.27.35.148
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-08 21:51 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.10 seconds
cannyjin@kali:~$ nmap csye6225-spring2019-zhangjin.me
bash: /tmp/nmap: Permission denied
cannyjin@kali:~$ nmap 100.27.35.148
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-08 22:01 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.09 seconds
cannyjin@kali:~$ nmap 104.233
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-08 22:02 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.09 seconds
cannyjin@kali:~$ nmap -Pn 104.233
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-08 22:32 EDT
Nmap scan report for ec2-18-207-104-233.compute-1.amazonaws.com (18.207.104.233)
Host is up (0.026s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 7.68 seconds
cannyjin@kali:~$
```

I was trying to get the network of my application.

I got nothing, as the screenshot show. First, I was confused. Maybe is the VPC, private cloud that makes me cannot be got the info of network.

But when I got this:

```
cannyjin@kali:~$ nmap 18.207.104.233
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-08 22:32 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.09 seconds
cannyjin@kali:~$ nmap -Pn 18.207.104.233
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-08 22:32 EDT
Nmap scan report for ec2-18-207-104-233.compute-1.amazonaws.com (18.207.104.233)
Host is up (0.026s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 7.68 seconds
```

I realize is the SSH did this. So, looks like the network is pretty security I think.

I think SSL has nothing to do with firewall. I skip the section about testing the app without firewall.