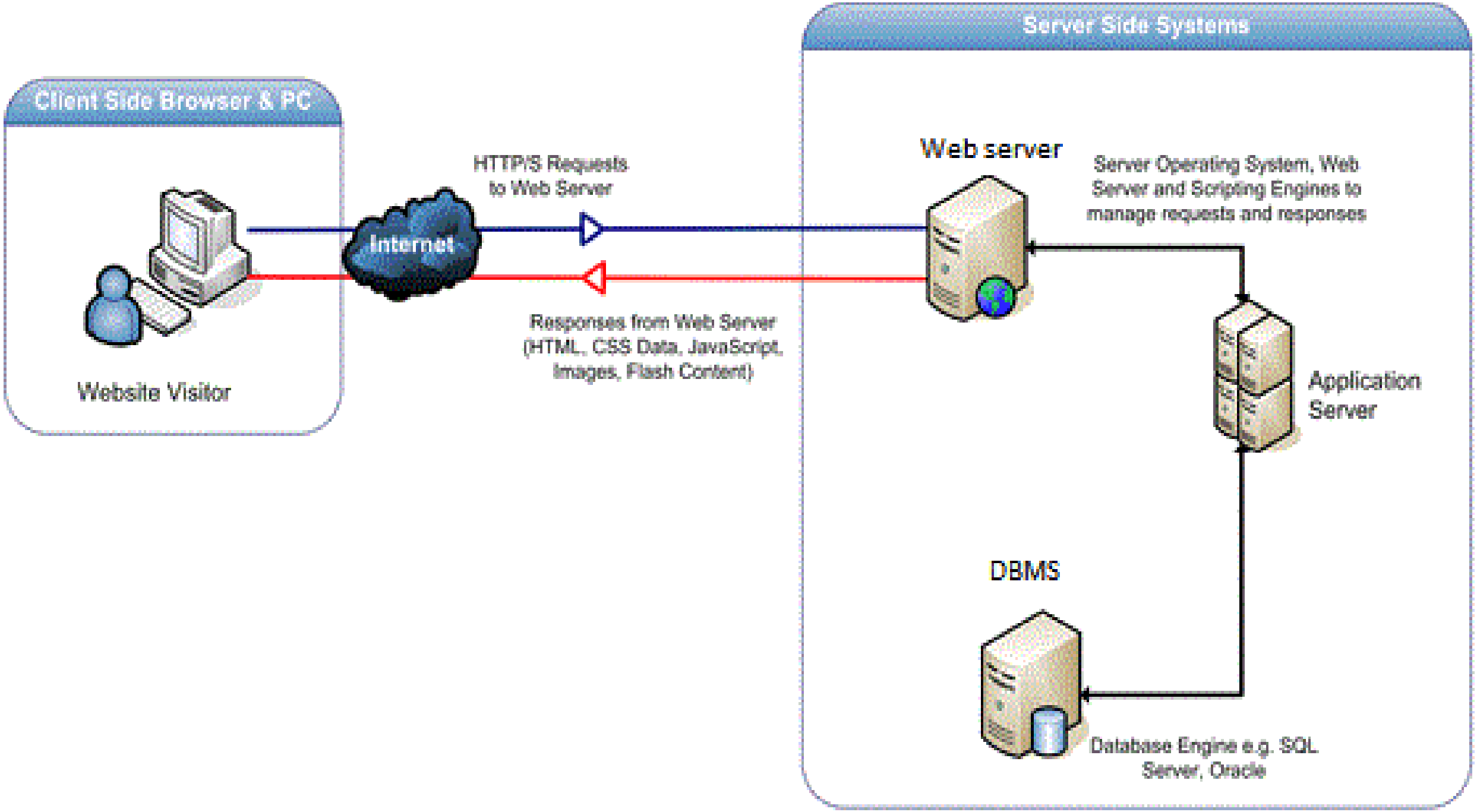
Web Application Security Testing

Pravesh Sharma

Research Associate, NCCS


Server Side Systems
Client Side Browser & PC
Web server
Server Operating System, Web Server and Scripting Engines to manage requests and responses
HTTP/S Requests to Web Server
Internet
Website Visitor
Responses from Web Server (HTML, CSS Data, JavaScript, Images, Flash Content)
Application Server
DBMS
Database Engine e.g. SQL Server, Oracle

What is Web Application Security Testing

- Process of testing web applications for vulnerabilities and ensuring they are secure from attacks.
- Essential to protect sensitive data, maintain integrity, and ensure compliance.

Security Testing Tools Overview

Why Use Security Testing Tools?

- Automated tools can find common vulnerabilities quickly and efficiently.
- Manual testing tools help penetration testers to explore deeper and complex vulnerabilities.

Popular Tools:

1. **TestSSL** – Tests SSL/TLS security.
2. **Nikto** – Web server vulnerability scanner.
3. **Burp Suite** – Comprehensive web application security testing.

What is TestSSL?

- **Open-source tool** for testing SSL/TLS configurations on servers.
- Ensures **secure communication** between client and server by verifying encryption.
- Identifies weaknesses in **protocols, ciphers, and certificates**.
- Detects vulnerabilities like **Heartbleed, POODLE, and BEAST**.
- Useful in **web application security testing** to check if data exchange between the client and web server is secure.

Key Features of TestSSL

- **Protocol Testing**: Verifies SSL/TLS versions (e.g., SSL 2.0, TLS 1.3) used by the server.
- **Cipher Strength**: Detects weak or insecure ciphers.
- **Certificate Validation**: Checks the validity and configuration of SSL certificates.
- **Vulnerability Detection**: Finds known SSL/TLS issues like **Heartbleed**, **POODLE**, **LUCKY13** and **DROWN**.
- **Configuration Checks**: Ensures proper implementation of features like **Forward Secrecy (FS)** and **HSTS**.

```
┌──(dot㉿kali)-[~/testssl.sh]
└─$ ./testssl.sh https://10.220.102.62

###########################################################
    testssl.sh       3.2rc2 from https://testssl.sh/dev/
    (3c0ae46 2023-07-03 19:56:22)

      This program is free software. Distribution and
             modification under GPLv2 permitted.
      USAGE w/o ANY WARRANTY. USE IT AT YOUR OWN RISK!

       Please file bugs @ https://testssl.sh/bugs/

###########################################################

 Using "OpenSSL 1.0.2-bad (1.0.2k-dev)" [~183 ciphers]
 on kali:./bin/openssl.Linux.x86_64
 (built: "Sep  1 14:03:44 2022", platform: "linux-x86_64")


 Start 2023-07-25 10:56:38        -->> 10.220.102.62:443 (10.220.102.62) <<--

 rDNS (10.220.102.62):    --
 Service detected:        HTTP


 Testing protocols via sockets except NPN+ALPN

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      not offered
 TLS 1.1    not offered
 TLS 1.2    offered (OK)
 TLS 1.3    offered (OK): final
 NPN/SPDY   http/1.1 (advertised)
 ALPN/HTTP2 http/1.1 (offered)

 Testing cipher categories

 NULL ciphers (no encryption)                  not offered (OK)
 Anonymous NULL Ciphers (no authentication)    not offered (OK)
```



```
 NULL ciphers (no encryption)                  not offered (OK)
 Anonymous NULL Ciphers (no authentication)    not offered (OK)
 Export ciphers (w/o ADH+NULL)                 not offered (OK)
 LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)  not offered (OK)
 Triple DES Ciphers / IDEA                     not offered
 Obsoleted CBC ciphers (AES, ARIA etc.)        offered
 Strong encryption (AEAD ciphers) with no FS   offered (OK)
 Forward Secrecy strong encryption (AEAD ciphers) offered (OK)


 Testing server's cipher preferences

Hexcode  Cipher Suite Name (OpenSSL)       KeyExch.   Encryption  Bits     Cipher Suite Name (IANA/RFC)
-----------------------------------------------------------------------------------------------------
SSLv2
 -
SSLv3
 -
TLSv1
 -
TLSv1.1
 -
TLSv1.2 (no server order, thus listed by strength)
 xc030   ECDHE-RSA-AES256-GCM-SHA384       ECDH 521   AESGCM      256      TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 xc028   ECDHE-RSA-AES256-SHA384           ECDH 521   AES         256      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 xc014   ECDHE-RSA-AES256-SHA              ECDH 521   AES         256      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 x9d     AES256-GCM-SHA384                 RSA        AESGCM      256      TLS_RSA_WITH_AES_256_GCM_SHA384
 xc09d   AES256-CCM                        RSA        AESCCM      256      TLS_RSA_WITH_AES_256_CCM
 x3d     AES256-SHA256                     RSA        AES         256      TLS_RSA_WITH_AES_256_CBC_SHA256
 x35     AES256-SHA                        RSA        AES         256      TLS_RSA_WITH_AES_256_CBC_SHA
 xc02f   ECDHE-RSA-AES128-GCM-SHA256       ECDH 521   AESGCM      128      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc027   ECDHE-RSA-AES128-SHA256           ECDH 521   AES         128      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 xc013   ECDHE-RSA-AES128-SHA              ECDH 521   AES         128      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 xc09c   AES128-CCM                        RSA        AESCCM      128      TLS_RSA_WITH_AES_128_CCM
 x9c     AES128-GCM-SHA256                 RSA        AESGCM      128      TLS_RSA_WITH_AES_128_GCM_SHA256
 x3c     AES128-SHA256                     RSA        AES         128      TLS_RSA_WITH_AES_128_CBC_SHA256
 x2f     AES128-SHA                        RSA        AES         128      TLS_RSA_WITH_AES_128_CBC_SHA
TLSv1.3 (no server order, thus listed by strength)
 x1302   TLS_AES_256_GCM_SHA384            ECDH 256   AESGCM      256      TLS_AES_256_GCM_SHA384
 x1301   TLS_AES_128_GCM_SHA256            ECDH 256   AESGCM      128      TLS_AES_128_GCM_SHA256
 x1304   TLS_AES_128_CCM_SHA256            ECDH 256   AESCCM      128      TLS_AES_128_CCM_SHA256
```

```
x1304   TLS_AES_128_CCM_SHA256          ECDH 256   AESCCM      128      TLS_AES_128_CCM_SHA256

Has server cipher order?     no (NOT ok)
(limited sense as client will pick)

Testing robust forward secrecy (FS) -- omitting Null Authentication/Encryption, 3DES, RC4

FS is offered (OK)           TLS_AES_256_GCM_SHA384 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA TLS_AES_128_GCM_SHA256
                             TLS_AES_128_CCM_SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA
Elliptic curves offered:     prime256v1 secp384r1 secp521r1
TLS 1.2 sig_algs offered:    RSA+SHA224 RSA+SHA256 RSA+SHA384 RSA+SHA512 RSA-PSS-RSAE+SHA256 RSA-PSS-RSAE+SHA384 RSA-PSS-RSAE+SHA512
TLS 1.3 sig_algs offered:    RSA-PSS-RSAE+SHA256 RSA-PSS-RSAE+SHA384 RSA-PSS-RSAE+SHA512

Testing server defaults (Server Hello)

TLS extensions (standard)    "renegotiation info/#65281" "EC point formats/#11" "session ticket/#35" "next protocol/#13172" "supported versions/#43" "key share/#51"
                             "max fragment length/#1" "application layer protocol negotiation/#16" "encrypt-then-mac/#22" "extended master secret/#23"
Session Ticket RFC 5077 hint 300 seconds, session tickets keys seems to be rotated < daily
SSL Session ID support       yes
Session Resumption           Tickets: yes, ID: no
TLS clock skew               Random values, no fingerprinting possible
Certificate Compression      none
Client Authentication        none
Signature Algorithm          SHA256 with RSA
Server key size              RSA 4096 bits (exponent is 65537)
Server key usage             --
Server extended key usage    --
Serial                       7A778D95BFB54285A5AE48B6264C16776F9E5F83 (OK: length 20)
Fingerprints                 SHA1 BBAAFE314E1A08C4D79E3D9F0548A168D2517BE0
                             SHA256 551295FEB8953E24E2EBCA9156FE204A8DEFE89413D23D5ADF32BB9231765BCA

Common Name (CN)             (no CN field in subject)
subjectAltName (SAN)         missing (NOT ok) -- Browsers are complaining
Trust (hostname)             certificate does not match supplied URI
Chain of trust               NOT ok (self signed)
EV cert (experimental)       no
Certificate Validity (UTC)   306 ⩾ 60 days (2023-05-27 09:44 ⟶ 2024-05-26 09:44)
ETS/"eTLS", visibility info  not present
Certificate Revocation List  --
OCSP URI                     --
                             NOT ok -- neither CRL nor OCSP URI provided
OCSP stapling                not offered
OCSP must staple extension   --
```

```
                           NOT ok -- neither CRL nor OCSP URI provided
 OCSP stapling             not offered
 OCSP must staple extension --
 DNS CAA RR (experimental) not offered
 Certificate Transparency  --
 Certificates provided     1
 Issuer                    (Default Company Ltd from IN)
 Intermediate Bad OCSP (exp.) Ok


 Testing HTTP header response @ "/"

 HTTP Status Code          200 OK
 HTTP clock skew           -66 sec from localtime
 Strict Transport Security not offered
 Public Key Pinning        --
 Server banner             nginx/1.20.1
 Application banner        --
 Cookie(s)                 (none issued at "/")
 Security headers          --
 Reverse Proxy banner      --


 Testing vulnerabilities

 Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
 CCS (CVE-2014-0224)                       not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK)
 ROBOT                                     not vulnerable (OK)
 Secure Renegotiation (RFC 5746)           supported (OK)
 Secure Client-Initiated Renegotiation     not vulnerable (OK)
 CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
 BREACH (CVE-2013-3587)                    no gzip/deflate/compress/br HTTP compression (OK)  - only supplied "/" tested
 POODLE, SSL (CVE-2014-3566)               not vulnerable (OK), no SSLv3 support
 TLS_FALLBACK_SCSV (RFC 7507)              No fallback possible (OK), no protocol below TLS 1.2 offered
 SWEET32 (CVE-2016-2183, CVE-2016-6329)    not vulnerable (OK)
 FREAK (CVE-2015-0204)                     not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)      not vulnerable on this host and port (OK)
                                           make sure you don't use this certificate elsewhere with SSLv2 enabled services, see
                                           https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=551295FEB8953E24E2EBCA9156FE204A8DEFE89413D23D5ADF32B
B9231765BCA
 LOGJAM (CVE-2015-4000), experimental      not vulnerable (OK): no DH EXPORT ciphers, no DH key detected with <= TLS 1.2
```

```
B9231765BCA
 LOGJAM (CVE-2015-4000), experimental      not vulnerable (OK): no DH EXPORT ciphers, no DH key detected with ⩽ TLS 1.2
 BEAST (CVE-2011-3389)                     not vulnerable (OK), no SSL3 or TLS1
 LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
 Winshock (CVE-2014-6321), experimental    not vulnerable (OK)
 RC4 (CVE-2013-2566, CVE-2015-2808)        no RC4 ciphers detected (OK)


 Running client simulations (HTTP) via sockets

 Browser                        Protocol  Cipher Suite Name (OpenSSL)       Forward Secrecy
--------------------------------------------------------------------------------------------
 Android 6.0                    TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       256 bit ECDH (P-256)
 Android 7.0 (native)           TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       256 bit ECDH (P-256)
 Android 8.1 (native)           TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       256 bit ECDH (P-256)
 Android 9.0 (native)           TLSv1.3   TLS_AES_128_GCM_SHA256            256 bit ECDH (P-256)
 Android 10.0 (native)          TLSv1.3   TLS_AES_128_GCM_SHA256            256 bit ECDH (P-256)
 Android 11 (native)            TLSv1.3   TLS_AES_128_GCM_SHA256            256 bit ECDH (P-256)
 Android 12 (native)            TLSv1.3   TLS_AES_128_GCM_SHA256            256 bit ECDH (P-256)
 Chrome 79 (Win 10)             TLSv1.3   TLS_AES_128_GCM_SHA256            256 bit ECDH (P-256)
 Chrome 101 (Win 10)            TLSv1.3   TLS_AES_128_GCM_SHA256            256 bit ECDH (P-256)
 Firefox 66 (Win 8.1/10)        TLSv1.3   TLS_AES_128_GCM_SHA256            256 bit ECDH (P-256)
 Firefox 100 (Win 10)           TLSv1.3   TLS_AES_128_GCM_SHA256            256 bit ECDH (P-256)
 IE 6 XP                        No connection
 IE 8 Win 7                     No connection
 IE 8 XP                        No connection
 IE 11 Win 7                    TLSv1.2   ECDHE-RSA-AES256-SHA384           256 bit ECDH (P-256)
 IE 11 Win 8.1                  TLSv1.2   ECDHE-RSA-AES256-SHA384           256 bit ECDH (P-256)
 IE 11 Win Phone 8.1            TLSv1.2   AES128-SHA256                     No FS
 IE 11 Win 10                   TLSv1.2   ECDHE-RSA-AES256-GCM-SHA384       256 bit ECDH (P-256)
 Edge 15 Win 10                 TLSv1.2   ECDHE-RSA-AES256-GCM-SHA384       256 bit ECDH (P-256)
 Edge 101 Win 10 21H2           TLSv1.3   TLS_AES_128_GCM_SHA256            256 bit ECDH (P-256)
 Safari 12.1 (iOS 12.2)         TLSv1.3   TLS_AES_128_GCM_SHA256            256 bit ECDH (P-256)
 Safari 13.0 (macOS 10.14.6)    TLSv1.3   TLS_AES_128_GCM_SHA256            256 bit ECDH (P-256)
 Safari 15.4 (macOS 12.3.1)     TLSv1.3   TLS_AES_128_GCM_SHA256            256 bit ECDH (P-256)
 Java 7u25                      No connection
 Java 8u161                     TLSv1.2   ECDHE-RSA-AES256-SHA384           256 bit ECDH (P-256)
 Java 11.0.2 (OpenJDK)          TLSv1.3   TLS_AES_128_GCM_SHA256            256 bit ECDH (P-256)
 Java 17.0.3 (OpenJDK)          TLSv1.3   TLS_AES_256_GCM_SHA384            256 bit ECDH (P-256)
 go 1.17.8                      TLSv1.3   TLS_AES_128_GCM_SHA256            256 bit ECDH (P-256)
 LibreSSL 2.8.3 (Apple)         TLSv1.2   ECDHE-RSA-AES256-GCM-SHA384       256 bit ECDH (P-256)
 OpenSSL 1.0.2e                 TLSv1.2   ECDHE-RSA-AES256-GCM-SHA384       256 bit ECDH (P-256)
```

IE 11 Win 7	TLSv1.2	ECDHE-RSA-AES256-SHA384	256 bit ECDH (P-256)
IE 11 Win 8.1	TLSv1.2	ECDHE-RSA-AES256-SHA384	256 bit ECDH (P-256)
IE 11 Win Phone 8.1	TLSv1.2	AES128-SHA256	No FS
IE 11 Win 10	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384	256 bit ECDH (P-256)
Edge 15 Win 10	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384	256 bit ECDH (P-256)
Edge 101 Win 10 21H2	TLSv1.3	TLS_AES_128_GCM_SHA256	256 bit ECDH (P-256)
Safari 12.1 (iOS 12.2)	TLSv1.3	TLS_AES_128_GCM_SHA256	256 bit ECDH (P-256)
Safari 13.0 (macOS 10.14.6)	TLSv1.3	TLS_AES_128_GCM_SHA256	256 bit ECDH (P-256)
Safari 15.4 (macOS 12.3.1)	TLSv1.3	TLS_AES_128_GCM_SHA256	256 bit ECDH (P-256)
Java 7u25	No connection		
Java 8u161	TLSv1.2	ECDHE-RSA-AES256-SHA384	256 bit ECDH (P-256)
Java 11.0.2 (OpenJDK)	TLSv1.3	TLS_AES_128_GCM_SHA256	256 bit ECDH (P-256)
Java 17.0.3 (OpenJDK)	TLSv1.3	TLS_AES_256_GCM_SHA384	256 bit ECDH (P-256)
go 1.17.8	TLSv1.3	TLS_AES_128_GCM_SHA256	256 bit ECDH (P-256)
LibreSSL 2.8.3 (Apple)	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384	256 bit ECDH (P-256)
OpenSSL 1.0.2e	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384	256 bit ECDH (P-256)
OpenSSL 1.1.0l (Debian)	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384	256 bit ECDH (P-256)
OpenSSL 1.1.1d (Debian)	TLSv1.3	TLS_AES_256_GCM_SHA384	256 bit ECDH (P-256)
OpenSSL 3.0.3 (git)	TLSv1.3	TLS_AES_256_GCM_SHA384	256 bit ECDH (P-256)
Apple Mail (16.0)	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384	256 bit ECDH (P-256)
Thunderbird (91.9)	TLSv1.3	TLS_AES_128_GCM_SHA256	256 bit ECDH (P-256)

Rating (experimental)

Rating specs (not complete)	SSL Labs's 'SSL Server Rating Guide' (version 2009q from 2020-01-30)
Specification documentation	https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide
Protocol Support (weighted)	0 (0)
Key Exchange (weighted)	0 (0)
Cipher Strength (weighted)	0 (0)
Final Score	0
Overall Grade	T
Grade cap reasons	Grade capped to T. Issues with the chain of trust (self signed)
	Grade capped to M. Domain name mismatch
	Grade capped to A. HSTS is not offered

Done 2023-07-25 10:58:08 [94s] -->> 10.220.102.62:443 (10.220.102.62) <<--

```
┌──(dot㉿kali)-[~/testssl.sh]
└─$
```

What is Nikto?

- Nikto is an open-source web server scanner used to identify vulnerabilities and security risks in web applications.
- It is widely used by security professionals, penetration testers, and system administrators for scanning web servers.
- Nikto operates via the command line and is compatible with Windows, Linux, and other Unix-based operating systems.
- The tool is designed to detect various security vulnerabilities, including:
  - Outdated software versions.
  - Misconfigured servers.
  - Other potential security risks.
- Nikto conducts tests to identify common vulnerabilities such as:
  - Cross-site scripting (XSS).
  - SQL injection.
  - Other web application security vulnerabilities.

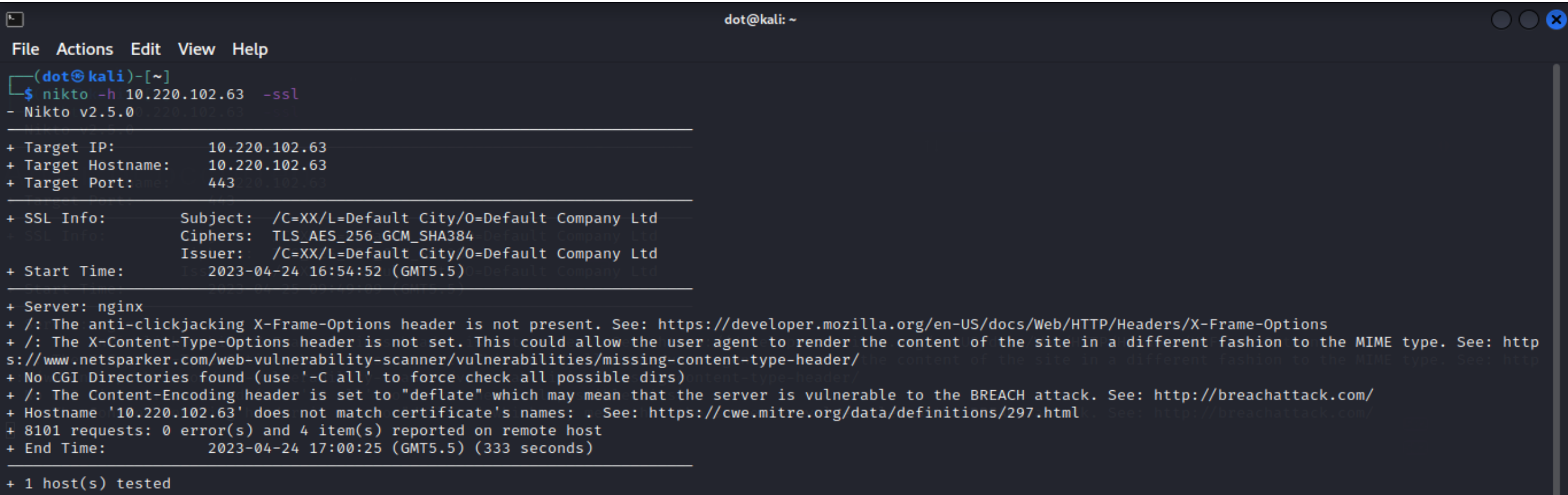
Functionality of Nikto

- Identifies outdated software, default files, insecure server configurations, and common vulnerabilities like XSS, SQL injection.
- *Identify installed software (via headers, favicons, and files)*
- *Guess subdomains*
- *Includes support for SSL (HTTPS) websites*
- *Saves reports in plain text, XML, HTML or CSV*
- *Report unusual headers*
- *Check for server configuration items like multiple index files, HTTP server options, and so on*

```
# nikto -h 192.168.18.132 -p 80,443

---------------------------------------------------------------------------
+ No web server found on 192.168.18.132:443
---------------------------------------------------------------------------
+ Target IP:          192.168.18.132
+ Target Hostname:    192.168.18.132
+ Target Port:        80
+ Start Time:         2013-02-24 12:27:27 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.2.19). Apache 1.3.42
(final release) and 2.0.64 are also current.
+ PHP/5.2.4-2ubuntu5.10 appears to be outdated (current is at least 5.3.6)
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ OSVDB-3233: /phpinfo.php: Contains PHP configuration information
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-40478: /tikiwiki/tiki-graph_formula.php?w=1&h=1&s=1&min=1&max=2&f[]=x.tan.phpinfo
()&t=png&title=http://cirt.net/rfiinc.txt?: TikiWiki contains a vulnerability which allow
s remote attackers to execute arbitrary PHP code.
+ 6474 items checked: 2 error(s) and 9 item(s) reported on remote host
+ End Time:           2013-02-24 12:28:20 (GMT-5) (53 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@bt:/pentest/web/nikto#
```


dot@kali: ~
File Actions Edit View Help
(dot㉿kali)-[~]
$ nikto -h 10.220.102.62 -p 80
- Nikto v2.5.0
+ Target IP: 10.220.102.62
+ Target Hostname: 10.220.102.62
+ Target Port: 80
+ Start Time: 2023-07-25 13:40:51 (GMT5.5)
+ Server: nginx/1.20.1
+ /: 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 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)
+ /backup.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html


dot@kali: ~
File Actions Edit View Help
(dot㉿kali)-[~]
$ nikto -h 10.220.102.63 -ssl
- Nikto v2.5.0
+ Target IP: 10.220.102.63
+ Target Hostname: 10.220.102.63
+ Target Port: 443
+ SSL Info: Subject: /C=XX/L=Default City/O=Default Company Ltd
Ciphers: TLS_AES_256_GCM_SHA384
Issuer: /C=XX/L=Default City/O=Default Company Ltd
+ Start Time: 2023-04-24 16:54:52 (GMT5.5)
+ Server: nginx
+ /: 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 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)
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ Hostname '10.220.102.63' does not match certificate's names: . See: https://cwe.mitre.org/data/definitions/297.html
+ 8101 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time: 2023-04-24 17:00:25 (GMT5.5) (333 seconds)
+ 1 host(s) tested

What is Burp Suite

- **Burp Suite** is a Java application that can be used to penetrate web application**.** It includes modules like Proxy, Repeater, Scanner, and Intruder to identify and address security vulnerabilities. Its customizable and modular design enhances efficiency in finding and fixing web application issues.
- **Developer:**
- **PortSwigger:** Burp Suite is developed by PortSwigger, a cybersecurity company renowned for its focus on web application security.

Burp Suite Editions

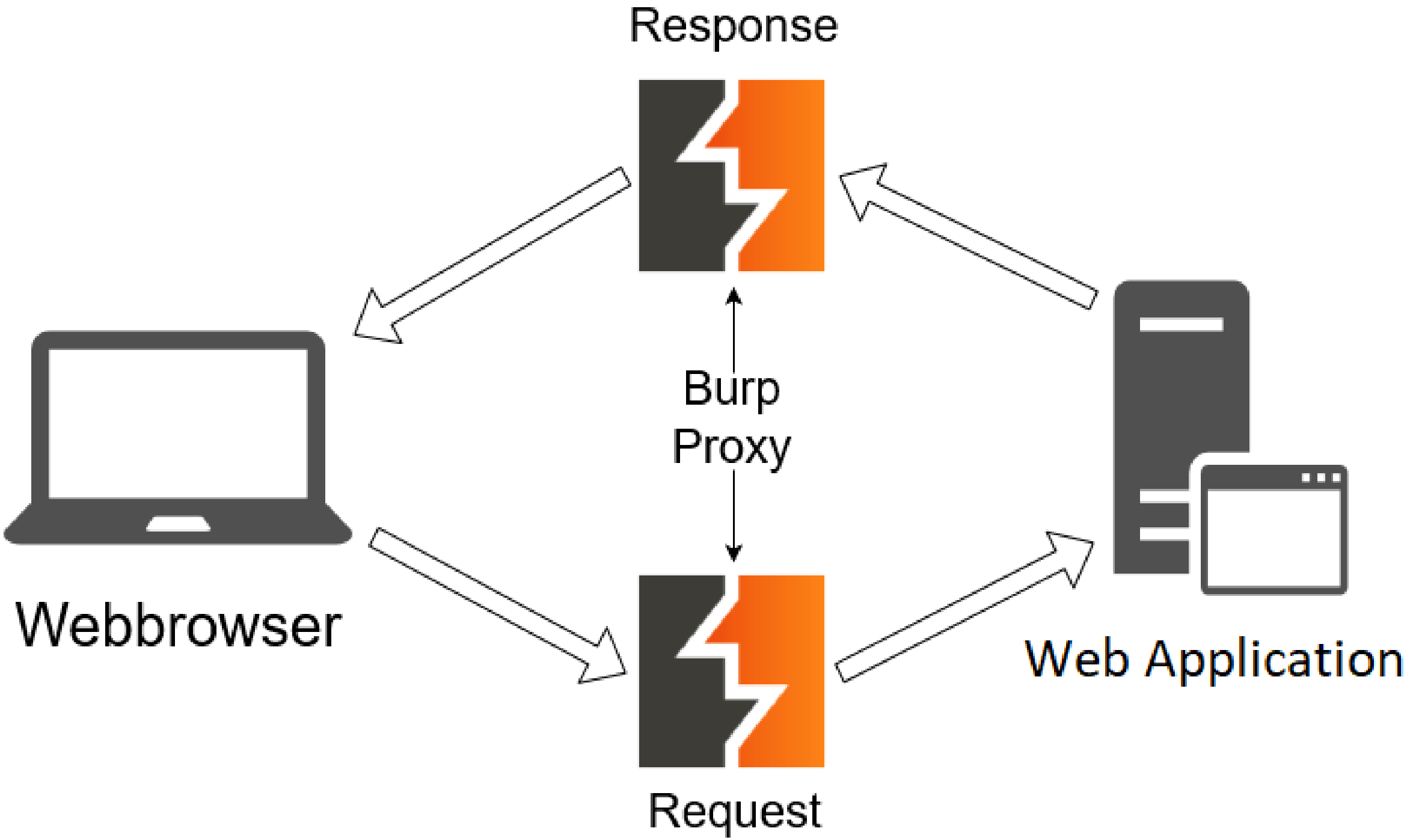
Burp Suite Community Edition	Burp Suite Professional Edition	Burp Suite Enterprise Edition
Free	Paid (License-based subscription)	Paid (Enterprise-level subscription)
Features: Proxy, Intruder, Repeater, Sequencer etc	***Features:*** All Community Edition Features + automated scanning +Collaboration Tools	***Features:*** All Professional Edition Features +Centralized Management

Key Features

1. **Vulnerability Detection:** Burp Suite helps discover and analyze security issues, such as SQL injection, cross-site scripting (XSS), and more.
2. **Traffic Manipulation:** It enables users to intercept and modify HTTP requests and responses, allowing for in-depth analysis and testing.
3. **Automation:** Burp Suite Professional provides automated scanning capabilities to identify common security flaws in web applications efficiently.

Overview of Burp Suite components

- Burp Suite is a comprehensive web application security testing tool that consists of several key components, each serving a specific purpose in the testing process. Here's an overview of the main components of Burp Suite:
- **1. Proxy:**
- **Purpose:** Allows interception and modification of HTTP/S traffic between the browser and the target application.
- **Functionality:**
  - Intercept and modify requests and responses in real-time.
  - Analyze and manipulate traffic for security testing.


Response
Burp
Proxy
Webbrowser
Web Application
Request

Overview of Burp Suite components

- **2. Repeater:**
- **Purpose:** Allows manual sending and modification of individual HTTP requests.
- **Functionality:**
  - Send requests to the server and analyze the corresponding responses.
  - Facilitates manual testing by allowing users to repeat requests with variations.
  - Useful for understanding how the server responds to different inputs.

Overview of Burp Suite components

- **3. Intruder:**
- **Purpose:** Performs automated attacks on web applications with customizable payloads.
- **Functionality:**
  - Automates tasks like brute force attacks, fuzzing, and payload-based testing.
  - Allows customization of attack parameters and payloads.
  - Analyzes server responses to identify potential vulnerabilities.

Overview of Burp Suite components

- **4. Sequencer :**
- **Purpose:** Assesses the randomness and predictability of data sequences.
- **Functionality:**
  - Calculates entropy using Shannon entropy formula.

$$H = -\sum_{i=1}^{n} p(i) \cdot \log_2(p(i))$$

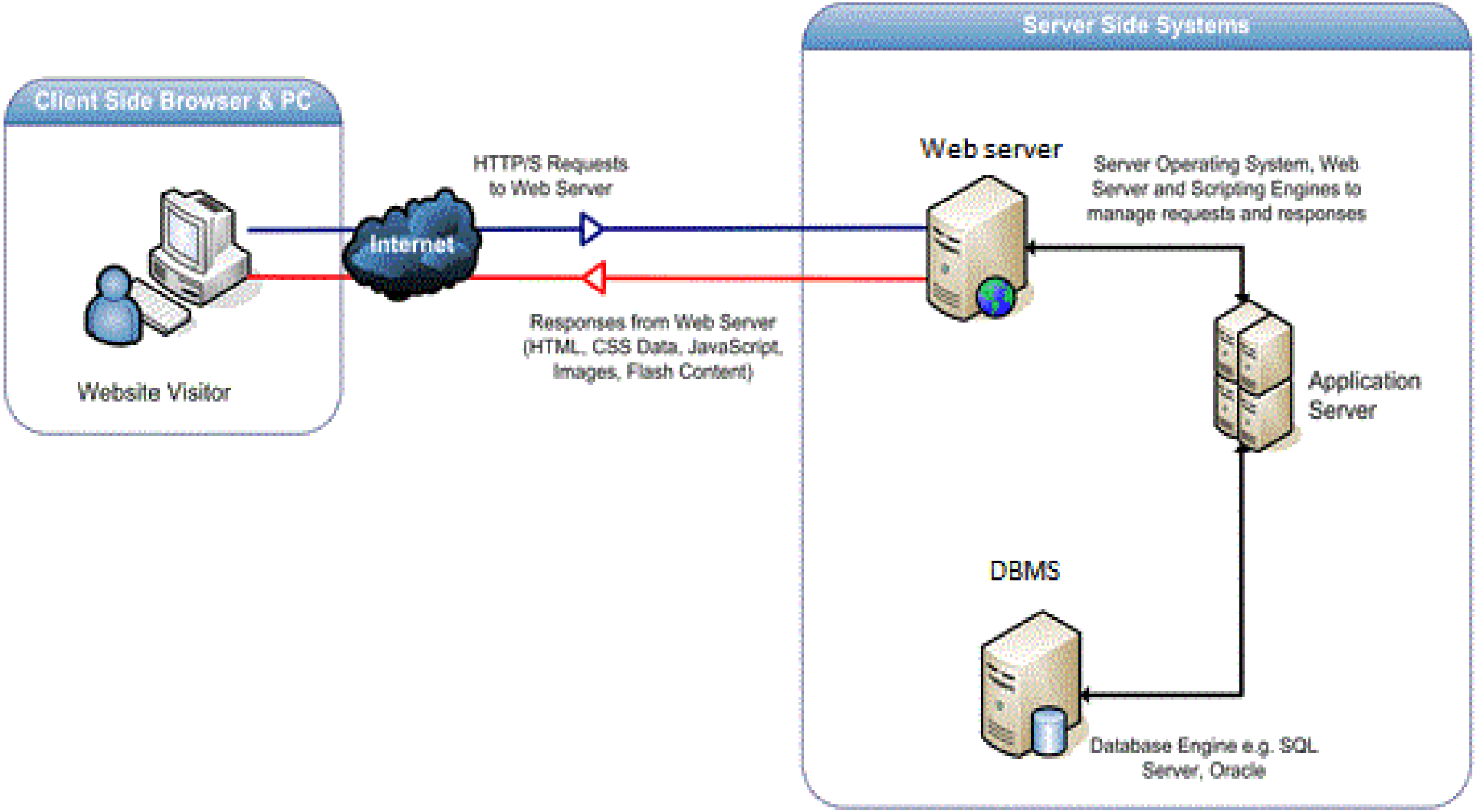
Where:

H is the Shannon entropy.

n is the number of unique symbols in the sequence.

p(i) is the probability of occurrence of the ith symbol.

Entropy, in the context of Burp Suite Sequencer, refers to the measure of randomness or disorder in a sequence of data


Server Side Systems
Client Side Browser & PC
Web server
Server Operating System, Web Server and Scripting Engines to manage requests and responses
HTTP/S Requests to Web Server
Internet
Website Visitor
Responses from Web Server (HTML, CSS Data, JavaScript, Images, Flash Content)
Application Server
DBMS
Database Engine e.g. SQL Server, Oracle

How These Tools Work Together

Integrating the Tools in Testing:

- **TestSSL** ensures that the SSL/TLS configuration is secure, preventing communication-based vulnerabilities.
- **Nikto** scans the web server for common misconfigurations and vulnerable components.
- **Burp Suite** performs both automated and manual testing for deeper penetration testing, focusing on input validation and session management.

Testing Workflow:

- Run **TestSSL** to verify secure SSL/TLS configurations.
- Use **Nikto** to scan the web server for known vulnerabilities.
- Run **Burp Suite** to test for web application vulnerabilities like SQL Injection, XSS, and more.

Thank You