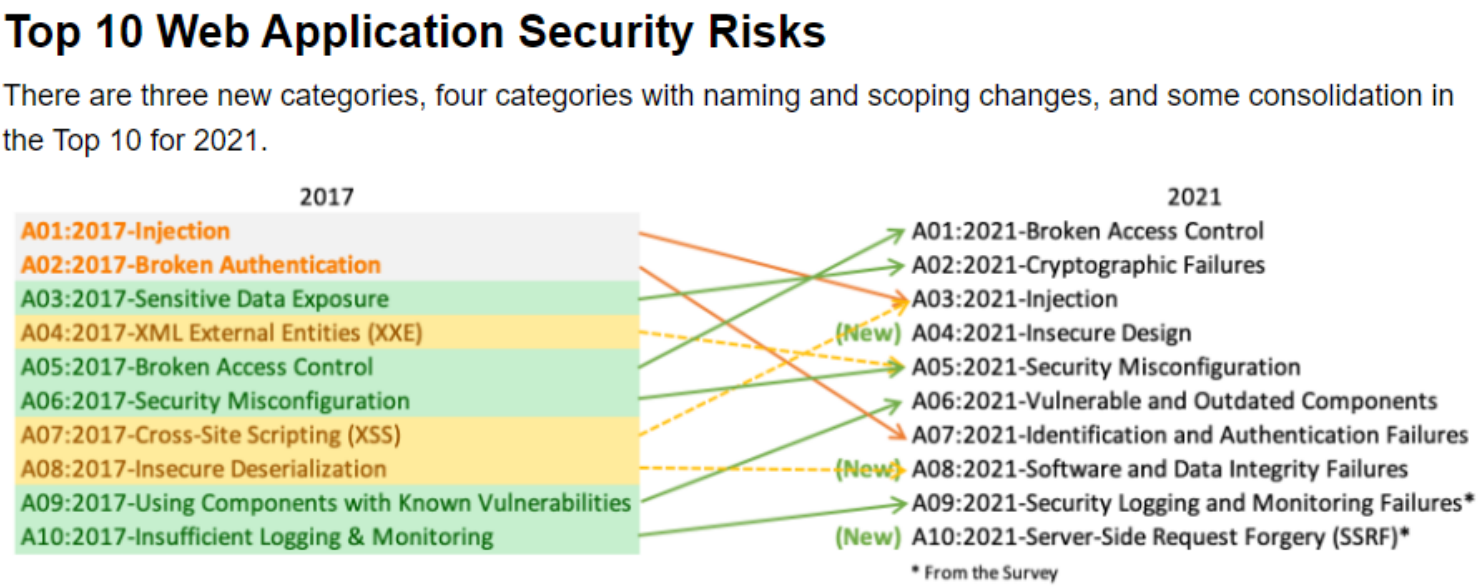
# *Vulnerability Analisys*

### Vulnerability Scan

### TOP 10 Web Application Security Risks



## Top 10 Web Application Security Risks

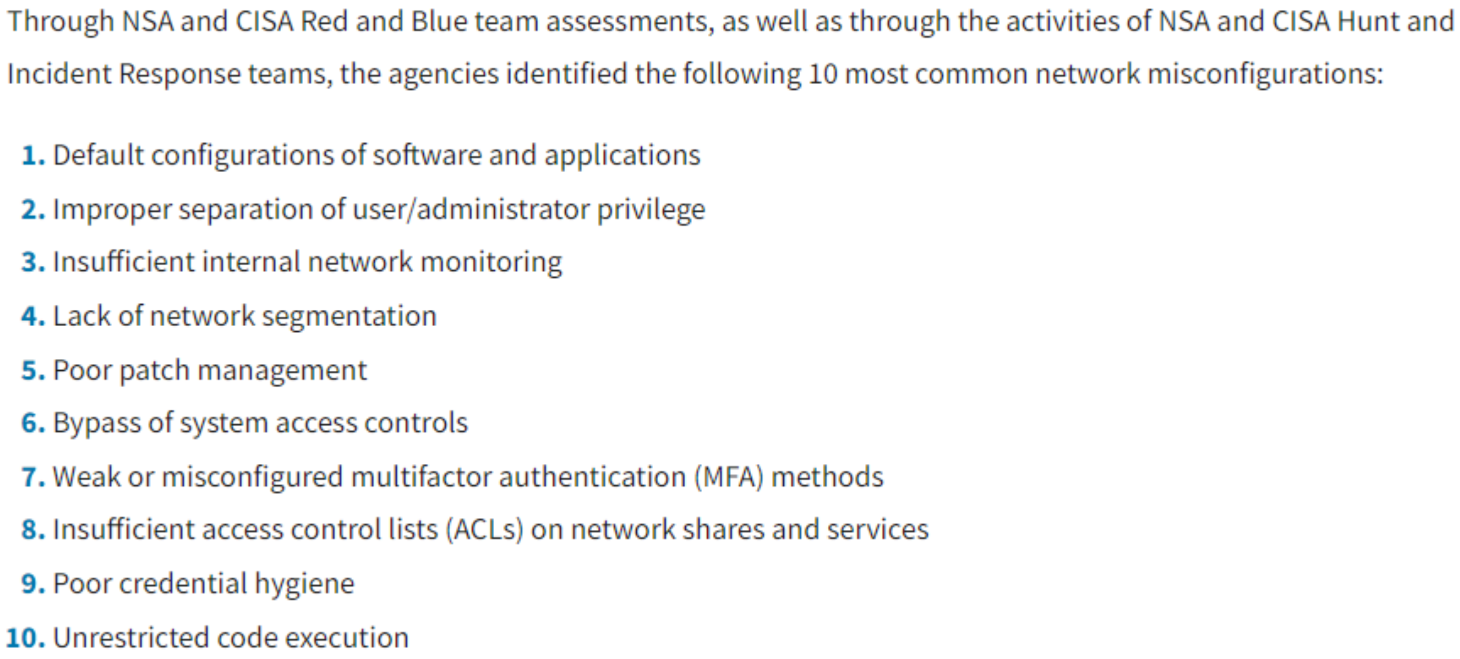
There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.

2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey

https://owasp.org/www-project-top-ten/

https://owasp.org/www-project-web-security-testing-guide/stable/

### TOP 10 Most Cybersecurity Misconfiguration



Through NSA and CISA Red and Blue team assessments, as well as through the activities of NSA and CISA Hunt and Incident Response teams, the agencies identified the following 10 most common network misconfigurations:

1. Default configurations of software and applications
2. Improper separation of user/administrator privilege
3. Insufficient internal network monitoring
4. Lack of network segmentation
5. Poor patch management
6. Bypass of system access controls
7. Weak or misconfigured multifactor authentication (MFA) methods
8. Insufficient access control lists (ACLs) on network shares and services
9. Poor credential hygiene
10. Unrestricted code execution

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a

### Gather Basic Information Local Host

```
$ ip address
$ ip route
$ cat /etc/resolv.conf
$ sudo netstat -tunap
```

### Steps Typical Vulnerability Scan

1° Discovery phase to perform host and port enumeration.
2° Records what services, system and version are running into database for further analysis.
3° Tries to determine services is listening and version, operational system version, find any known vulnerabilities.
4° Produces a report on what it suspects could be vulnerable.

### Test Local Vulnerability Nmap (Obs: For Online Scans Use Proxychains/TOR)

```
$ sudo nmap -sV --script vulners --script-args mincvss=4 <IP Address Target>
```

```
$ cd /usr/share/nmap/scripts
git clone https://github.com/vulnersCom/nmap-vulners.git
git clone https://github.com/scipag/vulscan.git
```

```
$ sudo nmap -sV --script nmap-vulners/vulners.nse <IP Address Target>
$ sudo nmap -sV -p 22 --script vulscan/vulscan.nse --script-args vulscandb-exploitdb.csv <IP Address Target>
$ sudo nmap -sV --script=vuln <IP Address Target> [Run All Vuln Scripts]
```

### Nikto

Nikto is a popular web vulnerability scanner that can find SQL injection, XSS, and other common vulnerabilities in websites. It can identify installed software using page headers and files. Nikto supports both HTTP and HTTPS protocols.

```
$ nikto --help
$ nikto -dbcheck
$ nikto -h http://scanme.nmap.org
$ nikto -h https://nmap.org -ssl
$ nikto -h <IP Address Target> -o website-scan.htm -Format html
```

### Nessus
https://www.tenable.com/products/nessus/nessus-essentials

### OpenVAS Greenbone
https://openvas.org/
https://greenbone.github.io/docs/latest/index.html

### GVM-Kali (Greenbone Vulnerability Management)
https://www.kali.org/tools/gvm/

```
$ sudo apt install gvm
$ sudo gvm-check-setup -h
$ sudo greenbone-feed-sync --type nvt
$ sudo gvm-setup -h
$ sudo gvm-start
$ sudo gvm-stop
```

A browser window will open with a security warning that can be ignored. If the browser does not automatically open, start your browser manually and navigate to **https://127.0.0.1:9392**. Click the Advanced button and scroll down and accept the risk on the warning screen to proceed.

**NATIONAL VULNERABILITY DATABASE (NVD)**
https://nvd.nist.gov/

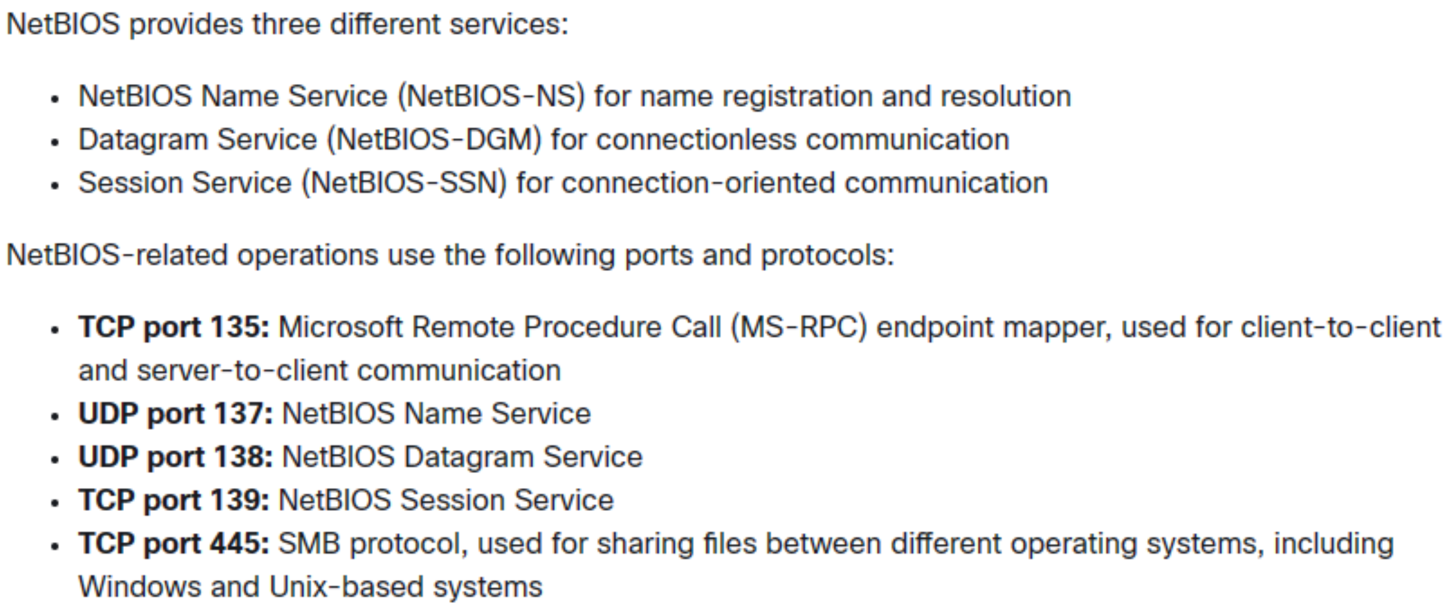
https://nvd.nist.gov/vuln/search

**Common Vulnerabilities Exposures (CVE)**
https://cve.mitre.org/

**Common Weakness Enumeraton (CWE)**
https://cwe.mitre.org/

**Common Vulnerability Scoring System (CVSS)**
https://www.first.org/cvss/

**Protocols Local Network**



NetBIOS provides three different services:

- NetBIOS Name Service (NetBIOS-NS) for name registration and resolution
- Datagram Service (NetBIOS-DGM) for connectionless communication
- Session Service (NetBIOS-SSN) for connection-oriented communication

NetBIOS-related operations use the following ports and protocols:

- **TCP port 135:** Microsoft Remote Procedure Call (MS-RPC) endpoint mapper, used for client-to-client and server-to-client communication
- **UDP port 137:** NetBIOS Name Service
- **UDP port 138:** NetBIOS Datagram Service
- **TCP port 139:** NetBIOS Session Service
- **TCP port 445:** SMB protocol, used for sharing files between different operating systems, including Windows and Unix-based systems

**Scanning for SMB Vulnerabilities with Nmap/enum4linux**

```
$ sudo su
# nmap -sN <IP Address Targets>
# nmap -Pn -p 445 --script=smb-vuln-ms17-010 192.168.10.0/24 -oN targets-smb-vulns.txt
# enum4linux --help
# enum4linux -a <IP Address Target>
# enum4linux -U <IP Address Target>
# enum4linux -Sv <IP Address Target>
# enum4linux -P <IP Address Target>
```

**SMB Enumeration Internal Network**

```
$ ls -l /usr/share/nmap/scripts | grep smb-enum
$ sudo nmap -A -p139,445 <IP Address>
$ sudo nmap -p139,445 --script=smb-enum-users <IP Address>
$ sudo nmap -p139,445 --script=smb-enum-groups <IP Address>
$ sudo nmap -p139,445 --script=smb-enum-shares <IP Address>
$ sudo nmap -sn --script=smb-check-vulns --script-args=unsafe=1 <IP Address Target>
```

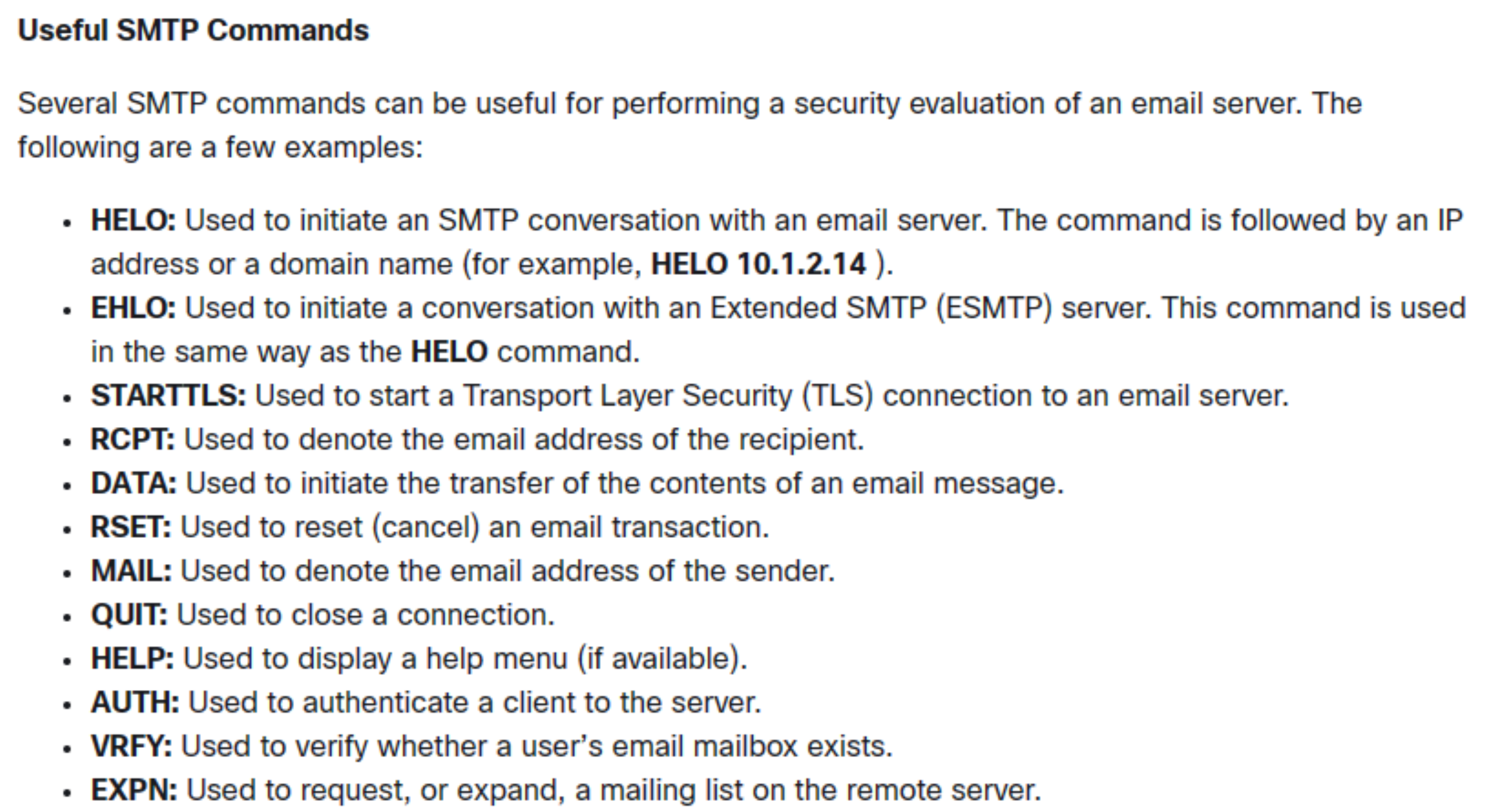
### Scanning for SNMP Vulnerabilities with Nmap

```
$ ls -l snmp* /usr/share/nmap/scripts
$ sudo nmap -p 161 --script=snmp-info <IP Address Target>
```

### Scanning for SMTP Vulnerabilities with Nmap

Ports = TCP 25, 465, 587

```
$ ls -l smtp* /usr/share/nmap/scripts
$ sudo nmap -p 25 --script=smtp-open-relay <IP Address Target>
$ telnet <IP Address Target> 25
$ searchsploit smtp
$ smtp-user-enum -M VRFY -U users-list.txt -t <IP Address Target>
```



**Useful SMTP Commands**

Several SMTP commands can be useful for performing a security evaluation of an email server. The following are a few examples:

- **HELO:** Used to initiate an SMTP conversation with an email server. The command is followed by an IP address or a domain name (for example, **HELO 10.1.2.14** ).
- **EHLO:** Used to initiate a conversation with an Extended SMTP (ESMTP) server. This command is used in the same way as the **HELO** command.
- **STARTTLS:** Used to start a Transport Layer Security (TLS) connection to an email server.
- **RCPT:** Used to denote the email address of the recipient.
- **DATA:** Used to initiate the transfer of the contents of an email message.
- **RSET:** Used to reset (cancel) an email transaction.
- **MAIL:** Used to denote the email address of the sender.
- **QUIT:** Used to close a connection.
- **HELP:** Used to display a help menu (if available).
- **AUTH:** Used to authenticate a client to the server.
- **VRFY:** Used to verify whether a user's email mailbox exists.
- **EXPN:** Used to request, or expand, a mailing list on the remote server.

### Owasp ZAP

```
$ sudo apt update
```

```
$ sudo apt install zaproxy -y
```

ZAP Quick Start > Manual Explore > URL to explore: http://10.0.0.123 > Launch Browser (auto proxy localhost)

ZAP Quick Start > Automated Scan > URL to attack: http://10.0.0.123 > Set spider If Modern HtmlUnit > Attack

ZAP Sites > vulnerabilities > GET:/login,password,username > Attack > Fuzz (highlight password field)

ZAP Add > File: > /usr/share/wordlists/fasttrack.txt > OK > Start Fuzzer

**WPScan**

```
$ wpscan --url website.com --api-token <83428234ybjhdfg6756542347723477893>
```