CYBERSECURITY GLOSSARY

Presented by the **CyberCoast**, an initiative of FloridaWest Economic Development Alliance.

CYBERCOAST

PENSACOLA, FL

Developed by the cybersecurity and penetration testing professionals at **Raxis**.

Raxis is an elite team of professionals who attack and assess cybersecurity systems. The company's ethical hackers have successfully breached some of the most sophisticated corporate networks in the US.

Account Enumeration

The process of identifying valid usernames, allowing a malicious actor to build a list of valid users for brute-force attacks. This can be done in many ways, including eliciting success and error messages on login and “forgot password” web pages.

Administrative Interface

Also “admin interface.” An interface, often a webpage, that allows users of an application to change administrative settings, such as user access, passwords, and other sensitive settings. Administrative users may be able to view sensitive information as well, possibly including logs, camera footage, and other sensitive data. Many vendor products are delivered with admin interfaces that use default credentials or that require no credentials at all. If these configurations are not hardened before the systems are deployed, they become a critical security risk, as a hacker could be able to, not only access the system, but also set a password and lock-out valid users of the system.

Administrator (Admin) Access

Users with administrative access have a higher level of access than normal user and often have the rights to view an edit key information, such as passwords, and system users.

API

An “Application Programming Interface” (API) allows separate programs to communicate with each other. An API may be a set of functions developed and used internally within a company so that various web and mobile applications can access the same features, or an API may be provided by a vendor to its customers so that their developers can interface with the vendor systems in their code, for example, to view payment data or to edit values within the vendor tool.

Authentication Bypass

This is a condition where the verification process systems use to manage access to privileged functions is bypassed to access the privileged logic or data that it was intended to protect. This condition can occur for a number of reasons, including but not limited to, exploitation of a vulnerability, access to privileged processes through exposed services, and back doors or other side input channels left over from the development process.

Barriers to Entry

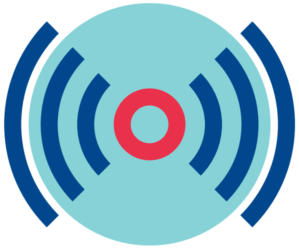
Physical barriers to entry, such as locked doors that require keys or badges to open or receptionists or security guards, are meant to stop people who are not meant to have access to a building or area.

Basic Authentication

An insecure authentication built into the HTTP protocol in which the client sends HTTP requests with the Authorization header that contains the word “Basic” word followed by a space and a base64-encoded string username:password.

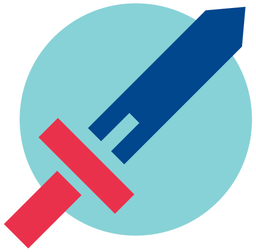
Broadcast Name Resolution

Poisoning These attacks listen for NetBIOS, LLMNR, or MDNS broadcast requests, which are generated when a host is attempting to resolve a hostname not within DNS. A hacker may then respond to the host and request that the host authenticate back to the hacker’s host, allowing the hacker to capture Windows authentication traffic and perform offline dictionary-based password cracking attempts or conduct SMB Relay attacks.



Broken Access Control

Broken access control is item #5 on the 2017 OWASP Top Ten list and refers to any way in which a user can access portions of a web application that should not be available to them. One example occurs when a hacker who knows the URL for an admin function can enter the URL in a browser directly and access the page without logging in. Another example is when user input is not sanitized, allowing a hacker to perform a SQL injection attack to view, edit, or delete data.



Broken Authentication

Broken authentication is item #2 on the 2017 OWASP Top Ten list, and it refers to any application flaw that allows unintended access to the application. Examples include default and weak passwords that are easy to guess or could be victims of automated or manual brute-force and dictionary attacks. Session attacks, such as session hijacking are also included because a successful attack provides a hacker with access to the application as the owner of the stolen session.

Brute-Force Attack

An attack where many requests are sent to a server with the intent of guessing a value, often a password, by sending a large number of possible candidates. A common example is an attack on a login page where the list of requests contains every permutation of letters, numbers within a certain length string.

Caching

Storing data for faster retrieval, usually in memory or on a disk. This allows data to be retrieved quickly from the cache without accessing a database or other, more secure, storage. Sensitive data should never be cached as it is not a secure method of storing data.

CAPTCHA

"Completely Automated Public Turing test to tell Computers and Humans Apart." CAPTCHAs provide an automated way to differentiate between humans and computers and are used on login pages and other sensitive pages where hackers may be tempted to run scripts to guess values. Examples include selecting all of the photos that contain a certain item or typing in characters that are displayed as a graphic on the webpage.

Certificate Authority (CA)

An trusted entity that issues digital certificates. Because a valid CA has a verifiable identity, the digital certificates they issue can be used by viewers to verify the validity of the website they are accessing. An organization may host its own CA or rely on third party CA services, such as Verisign, Thawte, Comodo, or others, to validate certificates.

Ciphertext

The output of encrypting plaintext using an encryption algorithm. It cannot be read until it is decrypted using a key.

Cisco Smart Install

A plug-and-play configuration and image-management tool provided on Cisco switches that automates configuration tasks that would otherwise require manual effort. Although this offers ease of use, this default feature could also be used by hackers to gain access to systems using default, well-documented rules available freely on the internet.

Cleartext

Unencrypted text, often derived by decrypting ciphertext.

CLI

A "Command Line Interface" (CLI) accepts text input and returns text output.

Clickjacking

An browser-based attack vector that leverages multiple transparent layers to trick a user into clicking on a button or link on another page when they were intending to click on the top-level page. This technique can be used be a malicious actor to bypass cross-site request forgery tokens and execute actions in the context of the authenticated user, as if the user was executing the actions themselves.

Client-Side

An action that takes place on the user's computer, such as JavaScript running in a user's browser. See server-side.

Content Security Policy Header (CSP)

This is an HTTP Response header that specifies which dynamic resources, such as JavaScript and CSS, are allowed to load from the website. It protects against cross-site scripting (XSS) attacks, and later version also protect against clickjacking and other attacks. Common ways that this header is include restricting inline scripts (such as malicious injected scripts), restricting remote scripts with "src" pointing to an external site, and restricting insecure JavaScript methods such as "eval." The "frame-ancestors" CSP directive blocks clickjacking attacks.

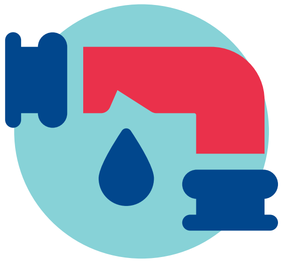
Crack a Hash

To "crack a hash" is the process of changing the hashed value to a cleartext value. Passwords are often stored securely as a one-way hash. Tools, such a hashcat, Crackstation, John the Ripper,and Cain, allow hackers to automate the process of reversing on-way hashes. Passwords that are very secure may take so long to crack that it would be unfeasible to crack them, but weaker passwords may crack in less than a second with a powerful took like hashcat and a strong dictionary list and rules. Password crackers work by guessing large numbers of passwords (based on a provided dictionary list and rules, such as password length and included characters); if the guessed hash matches the hash that the hacker is attempting to crack, then the password cracker has discovered the cleartext password.

CrackMapExec (CME)

A post-exploitation tool used by pen testers (or hackers) after they have gained access to an Active Directory environment. CME uses native Active Directory (AD) calls to automate attacks that gain access to more machines and data, often without alerting IDS/IPS systems and other tools meant to watch for an attack.

Cross-Domain Referer Leakage



When a user follows a link from one page to another, it typically adds an HTTP "Referer" header, which includes the full URL of the site from which the link was clicked. When this URL contains sensitive information, such as a session token, it leaks the sensitive URL through this request header. The server that processes the request then has access to the sensitive information sent by the application, which can in turn be saved in a database or access log.

Cross-Domain Script

A script used on a webpage that is invoked from a different domain than the webpage itself. This external script is executed by the browser within the security context of the invoking application. It can therefore do anything that the application's own scripts can do, such as accessing application data and performing actions within the context of the current user.

Cross-Origin Resource Sharing (CORS)

Origin restrictions define the scope by which a client-side web application running from one origin is permitted to obtain data from another origin. By doing so, it limits unsafe HTTP requests that can be automatically launched toward destinations that differ from the running application's origin. Cross-origin resource sharing (CORS) can allow for modification of these same-origin restrictions.

Cross-Site Request Forgery (CSRF)

This occurs when an attacker submits forms to the web application in the context of another authenticated user. For example, a hacker may direct a user to a malicious URL that automatically submits a form to the web application from the user's browser. If the affected user is currently logged in to the application, the hacker can execute any action on their behalf.

Cross-Site Scripting (XSS)

#7 on the 2017 OWASP Top Ten list. A reflected attack that injects malicious client-side executable code into web application parameters to be returned by the application output and ultimately executed by the browser. Because it appears that the script is from a trusted source, the end-user's browser accepts it and runs the script, permitting the attacker to take actions on the application's behalf, such as accessing cookies, and session tokens as well as other sensitive data. This attack can also be used to rewrite the webpage in order to trick the user, embarrass the company or cause other issues. XSS attacks are usually ephemeral, but If the injected code is populated into a database for later use by the application, it is referred to as Persistent XSS.

Dark Web

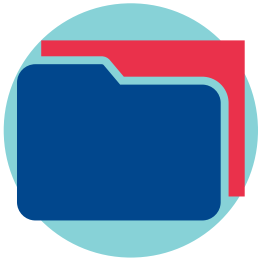
The part of the internet that is not available to search engines or direct browsing. Access requires an anonymous browser, such as Tor. The dark web is known for illegal and even dangerous activities, including the sale of sensitive information, such as PII including Social Security numbers, credentials, and other information that could harm users or companies. The term, Dark Web often carries a negative connotation, but it also facilitates free speech and provides necessary anonymity to journalists, activists, political dissidents, and whistle blowers among others.

Distributed Denial of Service (DDoS)

A "Distributed Denial of Service Attack" DDoS attack, like a DoS, attack attempts to make systems and services inaccessible by overwhelming them with so many requests for data that they can no longer respond to any requests. While a DoS attack is run from one attacking system, a DDoS attack is run from multiple systems at the same time, making it even more difficult to thwart. DDoS attacks typically originate from bot nets.

Default Documents

Default documents are any documents that are automatically available with a new system or software. Usually these documents are meant to guide users through setup or to provide system or debugging information. When these documents are available externally, they may provide hackers with key information about system versions or code in use.



Denial of Service (DoS)

An attack that floods a server or system with traffic in an attempt to overload the system so that it shuts down.

Directory Browsing

When a web browser allows the client to see file directories in the browser. It is best practice to block directory browsing.

DNS

A "Domain Name Server" (DNS) translates domain names, such as raxis.com, to the IP addresses where the systems actually run. Browsers use these directories to load internet resources. The internet uses openly accessible DNS servers, but companies also often create their own DNS servers for internal resources, and the information stored in them can be very useful for hackers. For example, a hacker who has gained access to an internal network could use a DNS server to discover the subnet(s) where servers are located in order to attempt server attacks on them or in order to discover what types of devices are running on the subnet where they have gained access.

DNS Amplification Attack

A distributed denial-of-service (DDoS) attack where an attacker uses responses from open DNS resolvers to overwhelm a server or network with an amplified amount of traffic in order to crash the targeted systems or make them inaccessible.

DNS Zone Transfer (AXFR)

A DNS server can send a part of its database (a zone) to another DNS server. Such a zone transfer is used to populate the zone data of a secondary DNS server. Because DNS zone transfers don't have a process for authentication, hackers can use them to transfer key information to their servers, allowing them to locate and enumerate internal hosts and to plan attacks against them. To prevent this, DNS servers should be configured to only allow zone transfers from trusted IPs.

Domain Administrator (DA)

This is a Windows account with administrative privileges in a Windows Active Directory (AD) domain. A hacker who gains access to a DA account may be able to create new or re-active former user accounts and to build a persistent presence in the entire network.

DRDOS (DrDos, DR-DOS, DR DOS)

A "Distributed Reflection Denial of Service" attack as denial of service attacks performed using vulnerable victim machines discovered by a hacker to perform a DDOS attack on a target. Systems vulnerable to NTP-based amplification attacks, for example, could unknowingly be used in such an attack, and, as a result, could placed on an internet blacklist.

EAP

The "Extensible Authentication Protocol" (EAP) passes authentication information between WiFi workstations and authentication servers. Many variations of EAP exist to accommodate specific authentication standards.

Egress Filtering

Egress filtering is used to restrict and monitor outbound traffic from one network to another. A hacker, or even a disgruntled employee, can leverage a lack of egress filtering to exfiltrate sensitive data from an organization's network. Organizations should set up an egress policy that denies all traffic by default and only allows approved traffic to trusted destinations. Only traffic necessary for business reasons should be allowed out while all other traffic is denied.

Encryption

Converting cleartext data to letters and numbers (ciphertext) that appear random using cryptographic keys. As long as the technology used to perform the encryption is current and secure, only a user with access to the key associated with the encryption should be able to decrypt the value.

End of Life (EOL)

Software and hardware reach end of life when vendors discontinue supporting the products and releasing patches. End of Life software presents an ever increasing risk because it is no longer patched against emerging threats.

Enterprise Administrator (EA)

This is a Windows account with administrative privileges across Active Directories (AD) for all domains with a forest. A hacker who gains access to an EA account can make forest-wide changes, such as changing domain site replication and modifying domain trusts, as well as establishing a persistent presence across all domains within an organization.

ESSID

"Extended Service Set Identification" (ESSID) refers to the identifying name of a WiFi network. This name will be the same as the SSID that WiFi users use to join the wireless network, though the ESSID also encompasses all of the access points within the WiFi network as well as their clients.

Ethical Hacking

See "Pen Test." Ethical hacking is any authorized attempt to hack an agreed upon scope. Ethical hacking encompasses pen tests to red team tests and anything in between with a goal of discovering security vulnerabilities so that they can be corrected.

Expired Certificate

SSL Certificates, used create an encrypted link between a browser and a web server, are issued by a Certificate Authority (CA) and are signed by the CA. These certificates expire (usually in 1-3 years of issue), and website administrators are required to purchase a new SSL certificate from a CA and implement it on their site (hopefully) before the old one expires. Browsers confirm that a certificate has not expired, and mark the site as insecure if it has. The danger of expired certificates is that a hacker could create a certificate that appears to be issued by a your company and apply it to their server. If users of your site get used to ignoring the browser's warning, they may use the hacker's site without realizing that the warning is different, and the hacker could perform a man-in-the-middle (MiTM) attack and view the user's (possibly sensitive) data.

FTP

The "File Transfer Protocol" (FTP) allows users to transfer files from computer to computer over the internet. It's an insecure service that sends data in cleartext without encryption. SFTP or FTPS are secure alternative to FTP.

GET Request

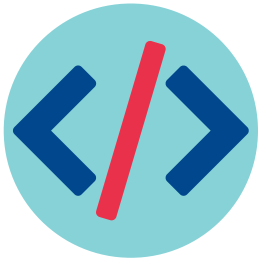
The GET HTTP request method can be used to request data from a resource. Parameters are often sent as part of the URL querystring. GET requests are saved in a browser's history and can be cached and bookmarked, as well as logged on intermediate systems, such as proxy servers. GET requests should never be used when sending sensitive data such as passwords or session tokens.

Guest Wireless Network

A wireless network that is intended for guest users. These networks often only allow internet access or restricted access to public areas required by guests at an organization. Because guest networks don't restrict user access as much as internal networks at an organization do, access to resources should be severely limited and based on business need.

Hardcoding

Entering data directly into code instead of reading the value from a separate location (configuration file, database, etc). Hardcoding sensitive data is less secure because code often must be stored in a location that can be available externally or where there can be fewer controls around who sees the code. However, If sensitive data, such as passwords, are stored in a configuration file or database, the data can be better protected, and a hacker who gains access to the code itself, would not automatically gain access to the sensitive data.



Heartbleed

Heartbleed is a buffer over read bug in the OpenSSL cryptography library. It affects the Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) implementations of OpenSSL in a feature called the heartbeat, which occurs when a computer accesses a website and the website responds to let the computer know that it is active and listening for requests. This call and response is done by exchanging data back and forth from the client to the server. Normally, when a computer makes a request, the heartbeat only sends back the amount of data the computer sent. However, for servers affected by the heartbleed bug, a hacker could make a request to the server and request data from the server's memory beyond the total data of the initial request, up to 65,536 bytes. This effectively allows the hacker to remotely dump whatever is in the running memory of the affected systems at the time of attack, including passwords and other sensitive data.

HIPAA

The "Health Insurance Portability and Accountability Act" (HIPAA) is a US federal law enacted in 1996 to safeguard Protected Health Information (PHI) from being disclosed without the patient's consent and knowledge. The HIPAA Privacy Rule was created by the US Department of Health and Human Services to implement the requirements of HIPAA. Healthcare providers, plans, and clearinghouses, as well as people and organizations with access to the data for other reasons, such as billing, processing claims, or data analysis, are subject to the HIPAA privacy rule. The HIPAA Security Rule protects a subset of PHI, "Electronic Protected Health Information" (e-PHI), and it includes discovering and protecting against threats to the data, whether external or through impermissible use of the data, as well as ensuring the confidentiality, integrity, and availability of all e-PHI and certifying the compliance of the workforce.

Host Header Poisoning

The HTTP Host header has been a mandatory request header since HTTP/1.1. It's used to identify the back-end component with which the client wants to communicate and is most important when several applications (possibly hosted on cloud-based or vendor platforms) are accessed through on IP address. Web servers trust this value by design and do not sanitize it by default. However, when additional processing is performed on the value, such as browser redirect or logging , it may expose the server to injection attacks such as SQL injection, web cache poisoning, business logic flaws, and other attacks.

HTTP

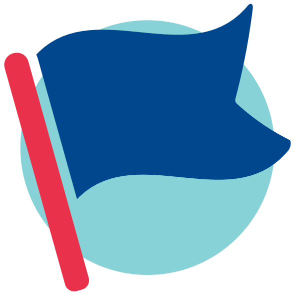
The Hypertext Transfer Protocol is an application layer protocol that transfers data between networked devices. It runs on top of other layers of the network protocol stack. Use HTTPS to add security features.

HTTP Request Methods

Most commonly, users can request that the server perform actions using the GET, HEAD, POST, PUT, DELETE, CONNECT, OPTIONS, TRACE and PATCH methods. While the GET and POST methods are used to display and update data during normal website use, the other methods should usually be restricted on external sites to prevent hackers from gaining unintended access. The TRACE method can sometimes be used in reflected cross-site scripting attacks as well.

HttpOnly Flag

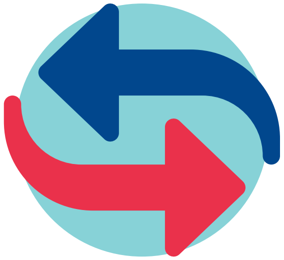
HttpOnly is a supplementary flag included in a Set-Cookie HTTP response header. Using the HttpOnly flag when generating a cookie helps mitigate the risk of client-side script accessing the protected cookie. It can help prevent certain client-side attacks, such as Cross-Site Scripting (XSS), from trivially capturing the cookie's value via an injected script attack.



HTTPS

Hypertext Transfer Protocol Secure. Usually serves web pages on port 443. It uses TLS (or the insecure SSL protocol) to serve pages. Non-web applications, such as VPNs, may also encapsulate data in HTTPS.

ICMP



The “Internet Control Message Protocol” (ICMP) is used by network devices to debug issues, such as whether data is reaching its destination quickly enough. If an error occurs on a receiving device, it can use ICMP to send information back to the sending device. Terminal utilities such as ping and traceroute use ICMP to perform network diagnostics. ICMP can be exploited as part of a DDoS attack.

IKE Aggressive Mode

An IKE authentication configuration designed to increase speed but that may also leak a hashed version of the PSK, allowing malicious actors to perform an offline dictionary attack against the IKE VPN encryption keys. It uses a pre-shared key (PSK) to communicate. The configuration could allow an attacker to capture and crack the PSK of a VPN gateway and gain unauthorized access to private networks.

IKE Main Mode

A method of IKE authentication that uses a six-way handshake where parameters are exchanged in multiple rounds with encrypted authentication information. Main mode does not leak a hashed version of the PSK.

IKE VPN

The IKE protocol ensures security for SA communication without the pre-configuration that would otherwise be required and is used by a majority of VPNs. IKEv1 was introduced in 1998, and IKEv2 was introduced in 2005. The IKE negotiation usually runs on UDP port 500.

Implied Trust Relationship Exploitation

This involves abuse of relationships, often created unintentionally, between security domains.

Hackers can abuse local system or Active Directory (AD) domain trust relationships to expand access across an organization’s environment. This is often a significant component of “moving laterally” and “escalating privileges.” A trust allows for the possibility of access between domains, domain accounts, local accounts, or even a method for a malicious actor to jump from one network to another. An example is a trust that’s created between accounts that share the same password. A hacker could gain access to the password through a brute-force password-guessing attack, a phish, by compromising a host and extracting hashes, by acquiring cached credentials,or by token impersonation. Once a password is known, the hacker can test other accounts and systems within a given environment to determine if they can locate any trust relationships that would aid them in expanding access.

Incident Response (IR)

The way an organization responds to a cyberattack or data breach. This includes thwarting the attack by shutting down systems, examining logs to discover when the attack took place and which systems are involved, informing affected users, customers, or employees if they were affected by the breach, as well as any other research and decisions that must be made before systems can safely be placed online.

Information Leakage

Also called Information Disclosure. This occurs anytime information that could aid a hacker is exposed, specifically externally. Examples are websites with HTTP headers that reveal software and server version, systems that reveal information about code or databases in error messages, or even systems that display cleartext passwords.

Injection

Injection attacks against applications occur when a hacker enters malicious data as input into the application. Examples include SQL injection (SQLi) in which the malicious data would include escape characters leading into SQL commands to view, add, change or delete database values or even to change the database itself using Database Manipulation Language (DML) commands. Other injections, such as cross-site scripting (XSS) inject scripting language commands to manipulate the page. Injection attacks should be prevented by verifying all user input and stripping out characters that are not a part of a whitelist of allowed values before it’s used within application, server or database code. Injection is item #1 on the 2017 OWASP Top Ten list.

Input Sanitization

The process of filtering input data, such as from a user, before it’s processed by an application, in order to protect systems from malicious input such as SQL injection, cross-site scripting or directory path traversal.

Insecure Deserialization

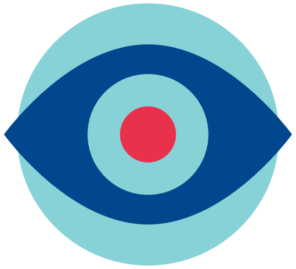
Insecure deserialization is item #8 on the 2017 OWASP Top Ten list, though it is primarily difficult to exploit and usually requires manual effort instead of being discovered by a scanner. A successful attack, though, can be a critical vulnerability, as it may allow remote code execution attacks. Serialized objects have been converted into a format (files, datastores, XLM, JSON, etc) that can be saved to a disk or sent over a network. An insecure deserialization attack occurs when an application attempts to deserialize a malicious object provided by a hacker.

Insecure Direct Object Reference (IDOR)

This is an access control vulnerability that occurs when a website uses user-supplied input to access objects directly. When database objects are referenced, this could allow a hacker to gain access to unintended This is an access control vulnerability that occurs when a website uses user-supplied input to access objects directly. When database objects are referenced, this could allow a hacker to gain access to unintended records through horizontal or vertical privilege escalation. When static files are referenced, a hacker may be able to change the filename to view other, possibly sensitive, files stored in the system. This vulnerability was #4 on the 2007 OWASP Top Ten.

Insufficient Logging & Monitoring

Insufficient Logging & Monitoring is item #10 on the 2017 OWASP Top Ten list and refers to a lack of logging, a lack of timely alerts about possible security issues, or even logs that are only stored locally. This vulnerability is often a key part of a major attack, including attacks where hackers gain persistent access to a network because catching an attack early (possibly during initial scans by a hacker) and discontinuing access is a key part of preventing such an attack. Logging is also key in incident response (IR) follow-ups so that companies can discover what occurred, what needs to be fixed, and if the hacker is still present in the systems. Leaving logging and alerting active during a penetration test or a red team test is a great way to test its effectiveness.



Internal IP Address

Also "Local IP Address." The IP address assigned by the local network router through DHCP. Only other devices on the same network can access the device unless it has a separate external IP address. The following ranges are reserved for internal IP addresses:
10.0.0.0/8 IP addresses: 10.0.0.0 – 10.255.255.255
172.16.0.0/12 IP addresses: 172.16.0.0 – 172.31.255.255
192.168.0.0/16 IP addresses: 192.168.0.0 – 192.168.255.255

IoT

The "Internet of Things" (IoT) refers to the billions of devices around the world that are connected to the internet. This includes smart devices, such as refrigerators, ovens, coffee makers, thermostats, garage door openers, security cameras, lighting, toys and more. There devices often may not include security measures or may not make it clear to consumers how to setup and maintain security features.

IP Address

An "Internet Protocol" (IP) address is a numeric address assigned to each device on a network so that other devices know how to contact the device. External IP addresses are unique across the internet and are usually used to host websites or other external services. Internal IP addresses are used within a local network and are not available externally without a separate external IP address.

IPMI

The "Intelligent Platform Management Interface" (IPMI) is an open interface meant to allow the management and monitoring of server systems over a network. iDRAC (Integrated Dell Remote Access), iLO (HP's Integrated Lights Out), ILOM (Oracle's Integrated Lights Out Manager), and IMM (IBM's Integrated Management Module) are vendor-specific offerings that are compliant with the IPMI standard. The IPMI network protocol runs on port 623 (UDP and sometimes TCP).

The authentication process for IPMI version 2.0 mandates that the server send a salted SHA1 or MD5 hash of the requested user's password to the client prior to the client authenticating. This password hash can be cracked using an offline brute-force or dictionary attack. Since this issue is a key part of the IPMI specification, there is no easy path to fix the problem, short of isolating all affected systems into a separate network or removing the services. Disabling IPMI, or at least restricting access, can help re mediate the vulnerability.

IPv4

This version of the Internet Protocol was implemented in 1983 and addresses devices using a 32-bit format of four sets of one to three digit numbers divided by dots (ex: 192.168.0.1).

IPv6

This version of the Internet Protocol was implemented because IPv4 did not allow enough unique addresses for the entire internet. IPv6 addresses use a 128-bit format that contains both letters and numbers that are separated by single or double colons (ex: 2148:e734:3105:4e0::2301).

LDA

"Lightweight Directory Access Protocol" (LDAP) is a protocol used to access or authenticate data on a server for directory services authentication and to store data pertaining to users, groups, and applications. LDAP sends data in cleartext and can be exploited by LDAP passback attacks under certain circumstances. Access to sensitive data should be limited to authenticated users with the proper roles.

LLMNR

The "Link-Local Multicast Name Resolution" (LLMNR) protocol allows name resolution without a DNS server. On modern systems, LLMNR should be disabled in favor of DNS services. Broadcast name resolution poisoning attacks can be performed against systems that have LLMNR enabled.

Local Administrator

A local user account on a device that has administrative privileges on that device but no access to other devices. A common vulnerability within organizations is using the same password for multiple local admin accounts, which allows a hacker discovers or cracks one of the passwords to access several devices with admin rights.

Man in the Middle Attack (MiTM)

An attack where a hacker is able to intercept and/or alter network traffic. A common example is a hacker using a "sniffer" program that allows the hacker to view user credentials when they are submitted to a login page. Hackers can gain this access in a number of ways, including unpatched software or phishing attacks.

Metasploit

The Metasploit Framework (MSF) and Metasploit Pro (MSP) are free and paid tools available from Rapid7 in collaboration with the open source community. It provides command line (CLI) and, in the case of Metasploit Pro also GUI, tools to exploit known vulnerabilities. This well-known and highly respected tool is used by ethical penetration testers and by companies that are working to stay secure in order to test for vulnerabilities and to verify that they have been corrected.

Mimikatz

A free open-source post-exploitation tool that allows pen testers (and hackers), who have gained access to a Microsoft Windows machine, to dump sensitive data such as passwords, hashes, PINS, and Kerberos tickets from the machine's memory. The data gained from Mimikatz often is a key part of a chained attack that leads to greater access to more machines as well as accounts with greater access.

Mousejacking

The MouseJack vulnerability affects some wireless, non-Bluetooth, input devices. These peripherals connect to the host machine using a small USB radio transceiver that can be compromised by transmitting specially-crafted radio signals from an inexpensive device, up to 100 meters away. A hacker can leverage this vulnerability to transmit arbitrary mouse movements and keystrokes to execute commands on the victim's machine.

NAC

A "Network Access Control" (NAC) allows access management across devices on a network. A NAC can deny network access to compliant devices and restrict access at varying levels, for example, allowing only internet access to devices that are not configured as a part of the network or quarantining devices that appear to have malware installed.

NetBIOS

The "Network Basic Input/Output System" (NetBIOS), a broadcast name resolution protocol that is used by NBNS, allows applications on different computers to communicate within the same local area netwrk (LAN). On modern systems, NetBIOS should be disabled in favor of DNS services. Broadcast name resolution poisoning attacks can be performed against systems that have NetBIOS enabled.

Network Segmentation

Segmenting a network breaks it into smaller parts, or subnets, and it is used to improve security as well as performance. Segmenting a company's phone network for example, keeps the network more secure because a hacker that discovers a vulnerability in the phone software could be limited to attacking the phone systems and unable to access other company systems.

NTLM & NetNTLMv2

A Microsoft Windows authentication protocol. NTLM has many known vulnerabilities, and NTLM hashes that are discovered during pen tests are very often cracked during the test. NetNTLMv2, while still vulnerable in some ways, corrects many of the issues with NTLM, usually making NetNTLMv2 passwords more difficult to crack.

NTP

The "Network Time Protocol" (NTP) is a networking service which allows various devices to synchronize their time over a network. In some cases, hackers can use compromised or untrusted NTP servers to maliciously modify the time on a client device. This could be used to bypass or manipulate certain security restrictions or functions, especially those related to certificates or signatures with a "not before" or expiration date. Also, NTP server that are not configured properly could be used as part of a Distributed Denial of Service (DDoS) attack against other systems on the Internet.

Open Mail Relay

An SMTP server that is configured to allow unauthenticated relay of emails allows open relay. This is dangerous because a hacker who gains access to the mail server can send email messages, such as spam or phishing emails, from the domain to external email addresses.

Open Redirection

Open redirection vulnerabilities occur when an application allows parameter values within a URL GET request to include values that will redirect a user to a different site without validating the redirection target. Redirection functions should be removed from applications if possible, or a server-side list of allowed redirect URLs should be used so that the redirection target is set using an index to an item in the list instead of a URL. While this attack doesn't affect the site itself, the negative impact on users could affect user's trust.

Open Source Intelligence (OSINT)

Gathering information from publicly available resources. An example is gathering employee names, emails and phone numbers through search engines or social media sites, such as LinkedIn, before beginning a phishing attack on the discovered employees. Another example is discovering news articles about a company using a specific vendor, which allows a hacker to plan a more specific attack on company systems.

OWA

"Outlook Web Access" (OWA) is a browser-based email program provided by Microsoft. It has the same feel as Microsoft Outlook. OWA can be vulnerable to timing attacks that allow user enumeration as well as internal IP disclosure vulnerabilities.

Patching

Vendors release patches to correct security and functionality problems in software and firmware between version releases.

Path Traversal / Directory Traversal

Also known as a dot-dot-slash attack, directory climbing, and backtracking. This attack attempts to access directories and files that are stored outside of the web root folder that are not meant to be available to website users. Variables that reference files and directories using absolute file paths or using "dot-dot-slash" (../) sequences may be susceptible to this attack. A hacker would inject the dot-dot-slash values, which backtrack one directory each, at the start of the input string and reference common sensitive directories and filenames at the end of the string in an effort to make the code backtrack out of the web root and to follow a different path.
Ex: ../../../../../etc/shadow

PCI

The "Payment Card Industry Data Security Standard" (PCI DSS) is developed and managed by the PCI Security Standards Council, which was created in 2006 by five leading credit card issuers. They aim to help merchants keep payments secure by helping them implement policies, technologies and processes that protect them from breach and protect customers from theft of cardholder data. PCI compliance is required annually for companies that process, transmit, or store cardholder data, but there are varying levels of effort to become and remain compliant depending on the PCI compliance merchant level.

Pen Test

A "Penetration Test" or "Pen Test" (not "Pin Test") for short, is a test performed by an ethical hacker using a scope and guidelines set by a company. These tests are meant to show weaknesses that a hacker could exploit so that a company understands the risks and can begin correcting the findings in order of risk. These tests can focus on one area of the network (external, internal, web app, API, mobile app, wireless, etc) or combine several of the areas into a red team test.

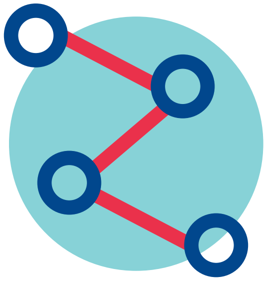
Phishing

Attempts to manipulate a person into taking an action through direct email correspondence. This may be anything from opening an email with an embedded object to navigating to a website to downloading and running a malicious file.

PII

"Personal Identifiable Information" (PII) applies to any data that could be used to identify a person either directly or indirectly. This includes Social Security number, name, address, phone number and email, as well as data that could be grouped together to identify a person, for example, birthdate, gender, race, and geographic indicators. PII should be considered sensitive data and carefully safeguarded.

Ping



Ping (originally "Packet Internet Groper" or "Inter-Network Groper") is a network application that can test if a system is operating and whether communications with the system or working correctly. Ping uses ICMP to send a small packet to the device and then listens for a response, which can be a success or an error (or no response).

Plaintext

Plaintext data refers to cleartext data before it is entered in an encryption program.

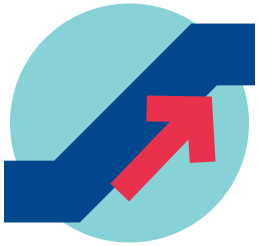
POST Request

The POST HTTP request can be used to send data to a server in order to create or update a resource. Parameters are sent through the request body. POST requests do not remain in browser history and cannot be cached or bookmarked. Requests that include sensitive data, such as passwords or session tokens should use the POST method.

Private Key

Private keys can be used to both encrypt and decrypt data as well as to authenticate computers and users and to digitally sign documents. These secret keys should be carefully safeguarded so that only the appropriate people can decrypt the encrypted data.

Privilege Escalation



An attack that attempts to obtain unauthorized access to systems within an organization through using access that has already been acquired to gain further access, such as higher permissions or access as new users. There are two types of privilege escalation. Horizontal privilege escalation occurs when a hacker is able to use access they've already acquired to gain access to other users accounts. Vertical privilege escalation occurs when a hacker is able to gain access to higher permissions whether through elevating the permissions of a user they already have access to or through gaining access to a new user with higher permissions. Misconfigurations, such as granting privileges to users that don't require them, as well as weak passwords, lack of patching, and social engineering are all methods hackers could use to enable this type of attack.

Privileged Account

An account that has more access, such as administrative rights to read or edit, than regular users do. These accounts should only be used when necessary and should require stronger passwords than regular user accounts. If a hacker gains access to such an account, they may be able to create a persistent presence on the network or gain other information or access than they would with a regular account.

PSE

A "physical security engagement" (PSE) is an test of physical security controls. This includes barriers to entry, such as locked doors, badge readers, security guards or receptionists who are able to stop hackers from entering buildings, as well as keeping sensitive documents in locked cabinets and computer desktops locked when employees are away. A lack of network security, such as not using a NAC to limit devices that can connect to the network, and unencrypted laptops or backup devices are also included.

Public Key

Public keys are used to encrypt data and are used in the processes of authenticating computers and users and confirming digitally signing documents. They can be shared with anyone who wishes to send encrypted data to the person who has the private key.

Ransomware

Ransomware is a type of malware that attempts to infect target systems (desktops, servers, etc) or networks by blocking access to the system and its data through encrypting the data on the system or setting system or file passwords that block access. A message demanding a fee to remove the blockers would be displayed.

RDP

The "Remote Desktop Protocol" (RDP) is a GUI remote control protocol developed by Microsoft for use with their operating systems. In many cases it may be insecure to allow RDP access exrernally unless a VPN is required for access.

Re-authentication

The process of reconfirming a user's active presence and intent to remain authenticated during an extended session. Websites can protect users who are no longer using the website by automatically logging them out of the system if they do not respond to a request to re-authenticate.

Red Team Test

This test involves a team of pen testers using various hacking and social engineering methods to attack a company's systems with the goal of gaining access to the network, confidential data, and anything else that a hacker would target. Companies can use internal red teams and/or hire external penetration testing experts like Raxis.

Rooted Device

A device where a user has obtained persistent root access. Rooted Apple devices are referred to as "jailbroken," while Android devices are simple referred to as "rooted." Users root devices in order to bypass vendor controls and to access unapproved programs, such as those found at underground app stores like Cydia, as well as to access the operating system of the device directly.

Salt

Random data that is used as input to a function that hashes data (such as passwords), usually by adding the salt to the start or end of the phrase to be hashed. Programs that store hashes store the salt as well so that the hash can be calculated by the program as needed. As each hash is stored with a different sale, and therefore becomes a different hash, a hacker who gains access to one cleartext password does not automatically have access to discover other accounts that have the same password.

Secure Flag

When the secure flag is set on a cookie, browsers will not submit the cookie in any requests that use an unencrypted HTTP connection. It is best practice to always include the secure flag when setting cookies used over SSL connections.

Security Misconfiguration

Security misconfigurations are item #6 on the 2017 OWASP Top Ten list and refer to any insecure configuration that could allow exploitation of a website or any of its back-end systems, such as servers and databases. Examples include unpatched systems, leaving default accounts available, and files that are not protected by authentication.

Self-Signed Certificate

SSL Certificates, used create an encrypted link between a browser and a web server, are issued and signed by a Certificate Authority (CA). Browsers confirm that certificates are signed by a trusted CA and implemented using a valid certificate path, which traces the certificate back to the trusted CA, and marks them as insecure if the CA is not trusted or if the path is invalid. Users can safely create and implement self-signed certificates to use internally for test systems or services that only run on the local network, but, because the browser has no way to prove that the certificate was created by the user, it will mark the certificate as insecure. The danger of self-signed certificates used externally is that a hacker could create a self-signed certificate, which appears to be issued by a trusted entity, and apply it to their server. If a user ignores the browser's warning and continues to use the hacker's site, the hacker could perform a man-in-the-middle (MiTM) attack and view the user's (possibly sensitive) data.

Sensitive Data Exposure

Sensitive data exposure is item #3 on the 2017 OWASP Top Ten list and refers to Man in the Middle (MitM) attacks in which hackers steal data in transit as well as stealing keys or cleartext sensitive data where they are exposed. Unencrypted sensitive data and weak encryption methods as well as server-side vulnerabilities that could make MitM attacks possible, are the main culprits in these attacks.

Server-Side

An action that takes place on a remote host, usually a web server. See client-side.

Session Expiration / Session Timeout

Web applications should be set to invalidate a user session after a period of inactivity. This session expiration or timeout protects users who did not logout from having someone else discover their logged-in session and take it over.

Session Fixation

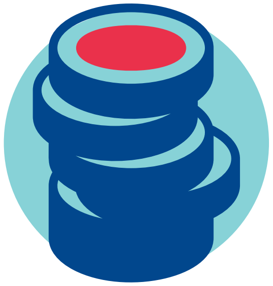
Websites that require authentication often create a session ID to identify a user and the access they should have as they move throughout the site after logging in. If a web application reuses session IDs for more than one login or does not invalidate them after a user logs off (or after a period of inactivity), a hacker who gained access to the session ID could access web pages within the authenticated part of the application using the session ID.

Session Hijacking

A session hijacking attack steals an established session between a client and web server after the user logs in or predicts what a session token will be based on easily guessed rules used in creating the token. A hacker could steal the session token using session sniffing, a cross-site scripting attack (XSS), or a man-in-the-middle (MiTM) attack. Using this session token, the hacker could access pages within the authenticated portion of the web application and view the same information as the user whose session token is being used.

Session Token

An encrypted, unique string that identifies an authorized and authenticated session. Once a user has successfully logged in, the session token, also known as a session ID, is the temporary, secret code that tells the application what the user is allowed to view and edit within the app.



SMB

"Server Message Block" (SMB) is a file protocol created for the Microsoft Windows operating system that allows files to be stored and shared easily across devices.

SMB Signing

SMB signing allows users to make the Microsoft SMB protocol more secure by allowing the recipients of the SMB packets to confirm their authenticity by digitally signing the communications between the hosts. It first became available in Microsoft Windows NT 4.0 Service Pack 3 (SP3) and Microsoft Windows 98. The options are "Required" (most secure), "Enabled" and "Not Enabled" (least secure), and different versions of Windows operating systems have different defaults. When SMB signing is disabled, Man in the Middle (MiTM) attacks, such as those used in conjunction with broadcast poisoning attacks, are much easier for a hacker to perform.

Smishing

A phsihing attack using text messages.

SMTP

"Simple Mail Transfer Protocol" (SMTP) is used by mail servers to send outgoing email.

SNMP

The “Simple Network Management Protocol” (SNMP) is an application layer protocol that is used for network monitoring. Many network devices come with SNMP capabilities and can be configured to communicate with network monitoring tools. SNMP uses community names to access the devices on the network either in read-only or read/write mode. Many devices come with the default, insecure community names “public” (read-only) and “private” (read/write). Because community names may allow access to read or edit sensitive information, they should be treated like passwords, and defaults should be replaced with strong values.

Spoof

Masquerading as a legitimate entity in order to trick people into taking an action based on their trust of that entity. Examples are phishing attacks from a false email address or phone number.

SQL Injection (SQLi)

In this attack, a SQL query is injected into the application via input parameters. A successful attack could read sensitive data from the database, modify data in the database, execute operations on the database (including administrative operations), recover files on the DBMS file system, or issue commands to the operating system.

SSH

“Secure Shell” or “Secure Socket Shell” (SSH) is a network protocol that encrypts data between a client an server in order to provide a way for users to securely access systems remotely. It is used by many system administrators to manage systems and applications remotely. SSH is a secure alternative to insecure terminal programs such as Telnet and rlogin and insecure file transfer programs such as FTP. There are several implementations of SSH, including OpenSSH, PuTTY, CyberDuck, and WinSCP.

SSL

“Secure Sockets Layer” (SSL) is a protocol for establishing authenticated, encrypted links between systems on a network, such as the internet. SSL was the predecessor to TLS. It was meant to keep sensitive data secure by preventing hackers from viewing the data while in transit. When a website is secured by SSL/TLS, the URL will include HTTPS instead of HTTP. The last version of SSL, SSL 3.0, was last updated in 1996. In 2014, SSL 3.0 was found vulnerable to the POODLE attack. All versions of SSL are considered deprecated, and modern browsers will not accept them.

SSL Certificate Pinning

This is a technique in which a mobile application is configured to trust only a small set of certificate authorities known to be used by the application’s servers. Mobile applications that do not enforce certificate pinning may be vulnerable to Man-in-the-Middle (MitM) attacks in which a hacker can route network traffic generated by the application to a proxy server they control.

SSO

“Single-Sign On” (SSO) is a proxied authentication method that allows users to authenticate to several disparate systems using the same credentials. An identity provider handles the credentials and informs the user’s applications whether the user is currently validly logged in or not.

Strict Transport Security Header (HSTS)

This is an HTTP Response header that can tell browsers that a website should only be accessed using HTTPS (not HTTP). The header includes options to use this rule for all subdomains (includeSubDomains) and to set an expire time (max-age=<expire-time>). If the user accesses the site using HTTPS once, the browser will enforce this header, but if the user only accesses the site via HTTP directly, the browser will ignore the header.

Subnet

A subnet (also subnetwork) is a logical subset of a network based on IP address. Subnets make networks more efficient by allowing network traffic to travel shorter distances without being sent through routers to reach their destination. Subnets blocks can include varying numbers of IP addresses depending on the design of the network.

TCP

The “Transmission Control Protocol” (TCP) defines how to establish and maintain network conversation between applications. It works with the Internet Protocol (IP) as TCP/IP.

TCP Timestamp

TCP Timestamps are an important component of reliable high speed communications because they keep TCP packets in the correct sequence. They may also provide hackers with information about system uptime, which may allow them to calculate whether recent security patches that require a reboot have been installed.

Telnet

A remote login protocol that was introduced in 1969. Telnet is an insecure service that sends usernames, passwords, and data over cleartext without encryption. SSH is a secure alternative to telnet.

TLS

“Transport Layer Security” (TLS) is a protocol for establishing authenticated, encrypted links between systems on a network, such as the internet. TLS is the successor to SSL, which has been deprecated. It was meant to keep sensitive data secure by preventing hackers from viewing the data while in transit. When a website is secured by SSL/TLS, the URL will include HTTPS instead of HTTP. The most recent version of TLS, published in 2018 is TLS 1.3.

Transporter

A secure device created by Raxis to perform remote tests. Companies that purchase a Raxis pen test that would usually require Raxis to be onsite (such as internal network, wireless network, or internally-facing web applications) could use a Raxis Transporter device to allow Raxis to perform the testing remotely.

Unrestricted File Upload

Applications that allow file uploads should restrict the uploaded files in several ways to protect against malicious input. If the application uses a file name input by users, a hacker could inject characters within the file name or path in an attempt to view or edit files within the file structure. Applications should ignore filenames sent by the user and replace them with internally created filenames. The files that are uploaded could also be malicious, and applications should verify that the files are limited to necessary file types. As hackers could use a false file extension in naming a file, it is important to check the file itself to discover the true file type. Files should also be checked for malicious content before uploading it to a server.

Updating

Minor changes between software upgrades. Also known as patching.

Upgrading

Moving to a newer version of the software. This usually includes improvements and noticeable changes.

Using Components with Known Vulnerabilities

Using Components with Known Vulnerabilities is item #9 on the 2017 OWASP Top Ten list and refers to web applications using an out of date software or systems. This includes client-side or server-side code, web or application servers, operating systems (OS), databases (DBMS), applications, APIs, libraries, and run-time environments that have known vulnerabilities. Because the vulnerabilities are already known, it is likely easier for a hacker to discover that they exist and to find examples of how to exploit them.

Verbose Application Error

An application error that reveals information about the code, database or other systems in use. Hackers can use this information to build a plan of attack by mapping out internal systems. Several web application servers and languages default to showing detailed stack trace errors to aid in debugging. These should be limited to internal test applications, and, in all other cases, the errors should be recorded to internally logs that can only be viewed by the developers and administrators who require the information.

Vishing

A phishing attack using phone calls.

VLAN

A “Virtual Local Area Network” (VLAN) is comprised of devices on several physical LANs that are configured to act as if they were on one LAN. A VLANs is a logical, not a physical network, which allows more flexibility. A VLAN may also describe the implementation of network boundaries aka segmentation.

VNC

“Virtual Network Computing” (VNC) is a remote control protocol that allows GUI access and control of a remote system and the resources, such as printers and network drives, that it has access to. VNC has several vulnerabilities and is an insecure way to implement remote access.

VPN

A “Virtual Private Network” (VPN) establishes encrypted communications (a tunnel) between the computer that runs the VPN client and the devices it communicates with. VPNs keep data in transit secure when a device is connected to public, unsecured WiFi, such as at hotels and coffee shops. VPNs are keep data secure for remote employees connecting to in-office systems.

WEP

“Wired Equivalent Privacy” (WEP) was the one of the earlier wireless network security protocols. It’s obsolete and extremely vulnerable to attack, and newer devices likely don’t offer it as an option.

WPA

“Wi-Fi Protected Access” (WPA) is a wireless security protocol that was adopted in 2003 to replace WEP. It uses a pre-shared key (PSK) which all users enter to gain access to the access point. Because the PSK is transmitted during the negotiation between a client and the access point, an attacker can observe, capture, and decrypt the PSK, then using it to gain access to the wireless network.

WPA2

“Wi-Fi Protected Access 2” (WPA2) is a wireless security protocol that was adopted in 2004. It uses AES encryption, which is an improvement, but it still has vulnerabilities that can be exploited. It comes in two varieties: WPA2 Personal (WPA2 PSK), which uses a shared passphrase, and WPA2 Enterprise, which uses the users’ network credentials to determine whether the user is permitted to connect to the wireless network. When WPA2-Enterprise is used with client-side certificates, the endpoint must present the certificate to the wireless network before authentication takes place, adding a strong layer of security.

WPA3

“Wi-Fi Protected Access 3” (WPA3) is a wireless security protocol that became available in 2020 as is available on newer routers. It has a number of new security features, including longer key sizes and forward secrecy, which prevents hackers who discover the Wi-Fi password in the future from reading a user’s past internet activity.

WPAD

The “Web Proxy Automatic Discovery” (WPAD) protocol was designed to automate the discovery of web Proxy servers. These can allow a malicious actor to conduct a Man in the Middle (MiTM) attack against a user’s Windows web browser, also known as a WPAD attack. When a browser first attempts to load a page, it checks for the existence of a server called WPAD, and, if this server is found, it deploys a Proxy configuration setting to the browser. If a hacker responds to the WPAD request with their host system as the proxy, all of the user’s web browser traffic is forwarded to the hacker, and, from that point forth, the malicious actor will have access to the browser traffic, allowing further attacks against the user and their system.

XML External Entities (XXE)

These attacks affect applications that process XML input using an XML parser that is not configured securely (often a default), allowing a hacker to possibly view files within the app server filesystem or to interact with back-end and other systems that the application can access internally. XXE attacks can sometimes be escalated to denial of service (DoS) attacks as well as other attacks on the back-end infrastructure. XXE is item #4 on the 2017 OWASP Top Ten list.

CYBERCOAST
PENSACOLA, FL

CyberCoastFlorida.com