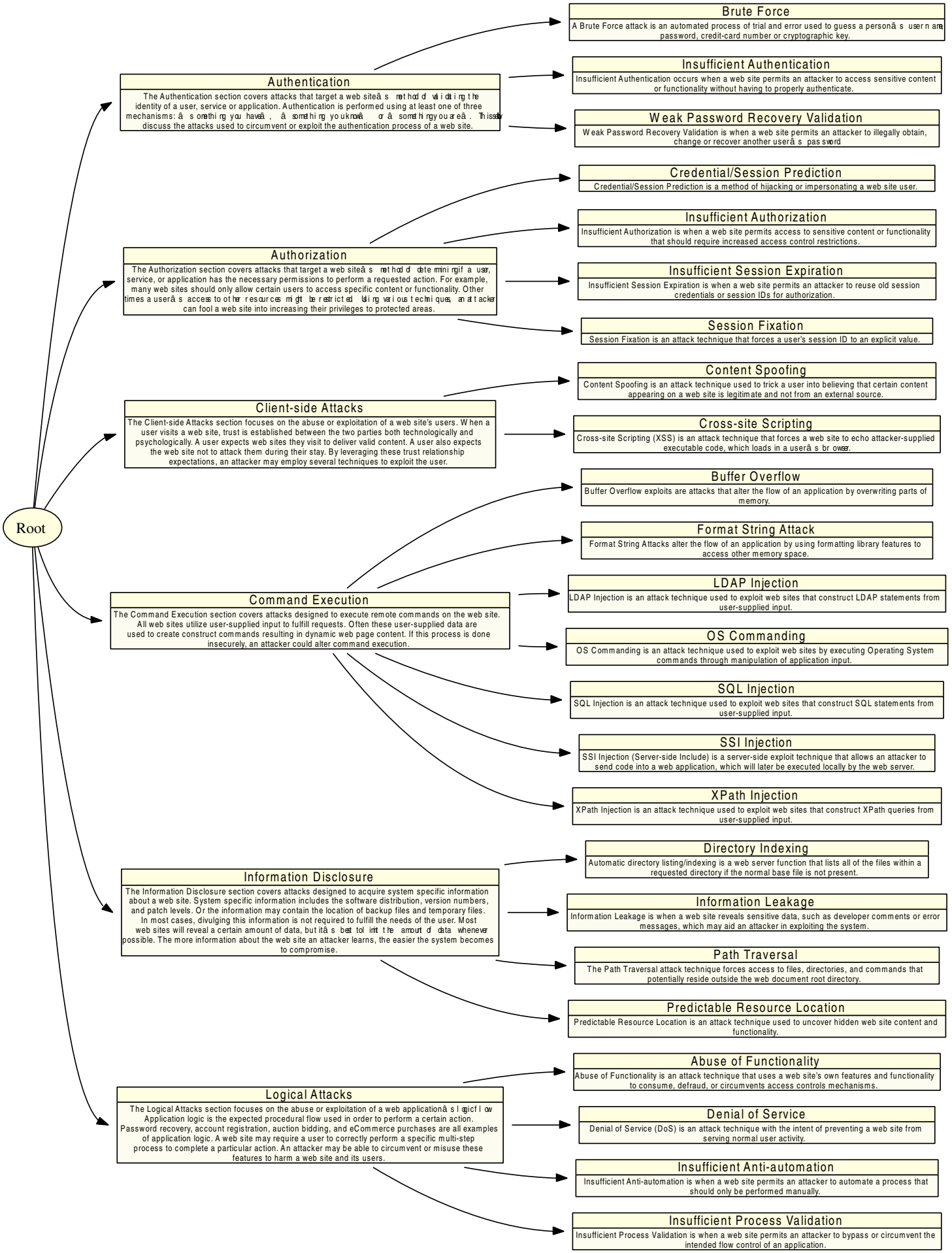
Root
Authentication
The Authentication section covers attacks that target a web siteâ s method of validating the identity of a user, service or application. Authentication is performed using at least one of three mechanisms: â s omething you haveâ , â s omething you knowâ or â s omething you areâ . Thissdiscuss the attacks used to circumvent or exploit the authentication process of a web site.
Brute Force
A Brute Force attack is an automated process of trial and error used to guess a personâ s user n ame password, credit-card number or cryptographic key.
Insufficient Authentication
Insufficient Authentication occurs when a web site permits an attacker to access sensitive content or functionality without having to properly authenticate.
Weak Password Recovery Validation
Weak Password Recovery Validation is when a web site permits an attacker to illegally obtain, change or recover another userâ s pas sword
Authorization
The Authorization section covers attacks that target a web siteâ s method of determinig if a user, service, or application has the necessary permissions to perform a requested action. For example, many web sites should only allow certain users to access specific content or functionality. Other times a userâ s access to other resources might be restricted using various techniques, an attacker can fool a web site into increasing their privileges to protected areas.
Credential/Session Prediction
Credential/Session Prediction is a method of hijacking or impersonating a web site user.
Insufficient Authorization
Insufficient Authorization is when a web site permits access to sensitive content or functionality that should require increased access control restrictions.
Insufficient Session Expiration
Insufficient Session Expiration is when a web site permits an attacker to reuse old session credentials or session IDs for authorization.
Session Fixation
Session Fixation is an attack technique that forces a user's session ID to an explicit value.
Client-side Attacks
The Client-side Attacks section focuses on the abuse or exploitation of a web site's users. When a user visits a web site, trust is established between the two parties both technologically and psychologically. A user expects web sites they visit to deliver valid content. A user also expects the web site not to attack them during their stay. By leveraging these trust relationship expectations, an attacker may employ several techniques to exploit the user.
Content Spoofing
Content Spoofing is an attack technique used to trick a user into believing that certain content appearing on a web site is legitimate and not from an external source.
Cross-site Scripting
Cross-site Scripting (XSS) is an attack technique that forces a web site to echo attacker-supplied executable code, which loads in a userâ s br owser.
Command Execution
The Command Execution section covers attacks designed to execute remote commands on the web site. All web sites utilize user-supplied input to fulfill requests. Often these user-supplied data are used to create construct commands resulting in dynamic web page content. If this process is done insecurely, an attacker could alter command execution.
Buffer Overflow
Buffer Overflow exploits are attacks that alter the flow of an application by overwriting parts of memory.
Format String Attack
Format String Attacks alter the flow of an application by using formatting library features to access other memory space.
LDAP Injection
LDAP Injection is an attack technique used to exploit web sites that construct LDAP statements from user-supplied input.
OS Commanding
OS Commanding is an attack technique used to exploit web sites by executing Operating System commands through manipulation of application input.
SQL Injection
SQL Injection is an attack technique used to exploit web sites that construct SQL statements from user-supplied input.
SSI Injection
SSI Injection (Server-side Include) is a server-side exploit technique that allows an attacker to send code into a web application, which will later be executed locally by the web server.
XPath Injection
XPath Injection is an attack technique used to exploit web sites that construct XPath queries from user-supplied input.
Information Disclosure
The Information Disclosure section covers attacks designed to acquire system specific information about a web site. System specific information includes the software distribution, version numbers, and patch levels. Or the information may contain the location of backup files and temporary files. In most cases, divulging this information is not required to fulfill the needs of the user. Most web sites will reveal a certain amount of data, but itâ s best tol imit the amount of data whenever possible. The more information about the web site an attacker learns, the easier the system becomes to compromise.
Directory Indexing
Automatic directory listing/indexing is a web server function that lists all of the files within a requested directory if the normal base file is not present.
Information Leakage
Information Leakage is when a web site reveals sensitive data, such as developer comments or error messages, which may aid an attacker in exploiting the system.
Path Traversal
The Path Traversal attack technique forces access to files, directories, and commands that potentially reside outside the web document root directory.
Predictable Resource Location
Predictable Resource Location is an attack technique used to uncover hidden web site content and functionality.
Logical Attacks
The Logical Attacks section focuses on the abuse or exploitation of a web applicationâ s l ogicf l ow Application logic is the expected procedural flow used in order to perform a certain action. Password recovery, account registration, auction bidding, and eCommerce purchases are all examples of application logic. A web site may require a user to correctly perform a specific multi-step process to complete a particular action. An attacker may be able to circumvent or misuse these features to harm a web site and its users.
Abuse of Functionality
Abuse of Functionality is an attack technique that uses a web site's own features and functionality to consume, defraud, or circumvents access controls mechanisms.
Denial of Service
Denial of Service (DoS) is an attack technique with the intent of preventing a web site from serving normal user activity.
Insufficient Anti-automation
Insufficient Anti-automation is when a web site permits an attacker to automate a process that should only be performed manually.
Insufficient Process Validation
Insufficient Process Validation is when a web site permits an attacker to bypass or circumvent the intended flow control of an application.