Basic Security Concepts

Overview

This document describes some basic security concepts that you can use to protect your system from cross-site request forgeries (XSRF) attacks.

XSRF attacks occur when a malicious user exploits the trust between a website and a user's browser. When a malicious user exploit that trust, they can run unauthorized commands on a website.

XSRF attacks rely on two items:

- Access to authentication credentials.
- Surreptitious execution of a command via a URL.

For more information about XSRF attacks, visit Wikipedia's XSRF article.

Authentication methods

We recommend that you use cookies as an authentication method for cPanel & WHM logins. An HTTP-authenticated session does **not** terminate unless you terminate the web browser application session. If you use HTTP authentication, the browser caches the login credentials until the system terminates the application.

Some browsers allow you to flush login credentials. However, do **not** rely on this method, and it does not exist in all browsers. When a web browser caches login credentials, the credentials become susceptible to XSRF attacks.

For more information, read our Authentication documentation.

Validated cookies

Malicious users can steal cookies and use them in XSRF attacks. Most browsers do **not** provide any protection to mitigate this attack. We provide an option that allows you to validate the incoming IP address as part of the cookie during the authentication process.

On subsequent authentication requests, the server compares the IP addresses to the original values in the cookies. A mismatched value causes an error that results in a re-authentication request.

> **Important:**
> When you use validated cookies, we recommend that you disable service subdomain access. If you do **not** disable service subdomain access, any attempt to access interfaces via a service domain will cause the system to record the local host's IP address (usually `127.0.0.1`), which renders IP address validation useless.

To disable service subdomains, disable the following settings in the *Domains* section of WHM's *Tweak Settings* interface (*WHM >> Home >> Server Configuration >> Tweak Settings)*:

- *Service subdomains*
- *Service subdomain creation*

Require SSL

You can also require your users to log in via SSL or TLS to improve your system's security. If users log in to their accounts over ports `2082`, `2086`, or `2095`, the system sends authentication credentials in plain text. The authentication credentials become easy to steal, read, and use again later.

For more information about how to access cPanel & WHM services securely, read our How to Log in to Your Server or Account documentation.

Security tokens

cPanel & WHM includes security tokens to help combat XSRF attacks. The system inserts unique security tokens into the URL for a single login session. Any requests that a user makes without the appropriate token produce an error and result in a request for re-authentication. This action effectively stops XSRF attacks because the malicious URL will **not** contain the appropriate token.

> **Warning:**
> Security tokens may cause problems with custom scripts and some third-party applications that integrate with cPanel & WHM. We **strongly** recommend that you verify that third-party applications are compatible with security tokens before you enable them. If you **must** use applications that are not compatible with security tokens, we recommend that you use URL referrer checks instead.

URL referrer checks

The HTTP referrer identifies the URL of the page from which a user originated. Referrer checks only function correctly when you enable the blank referrer check, and typically result in a large number of false positive alerts. However, if you **must** use third-party applications that are not compatible with security tokens, you can use referrer checks in place of security tokens

> **Important:**
> If you cannot use security tokens on your server, we **strongly** recommend that you enable the following options in the *Security* section of WHM's *Tweak Settings* interface (*WHM >> Home >> Server Configuration >> Tweak Settings)*:
>
> - *Blank referrer safety check*
> - *Referrer safety check*

Password strength

Weak passwords provide insignificant protection against brute force attacks. Brute force attacks occur when a malicious user guesses the password for a specific account via the trial-and-error message. This process is most often an automated process that uses dictionary terms. Use WHM's *Password Strength Configuration* interface *(WHM >> Home >> Security Center >> Password Strength Configuration)* to set your user's minimum password strength.

> **Notes:**
> - We **strongly** recommend that you set a value of `50` or higher.
> - The minimum password strength requirement **only** applies to passwords that cPanel & WHM creates and modifies. A user with shell access may use the `passwd` command to set a weak password.

Additional documentation

Suggested documentationFor cPanel usersFor WHM usersFor developers

- Basic Security Concepts
- How to Determine Password Strength
- cPanelID
- Problems When You Log Out Of An Account
- How to Purchase a KernelCare License

Error rendering macro 'contentbylabel' : parameters should not be empty

- Basic Security Concepts
- How to Determine Password Strength
- cPanelID
- Problems When You Log Out Of An Account
- How to Purchase a KernelCare License

- Guide to API Authentication - API Tokens in WHM
- Guide to API Authentication - Username and Password Authentication
- Guide to API Authentication - Secure Remote Logins
- Guide to API Authentication
- Guide to API Authentication - Two-Factor Authentication