

# cPanel Security Tokens

Prepared for: cPanel, Inc. Partners & Customers

May 25, 2011

# Table of Contents

<b>Executive Summary</b>	<b>1</b>
<b>What are security tokens?</b>	<b>1</b>
Examples	1
<b>Benefits of security tokens</b>	<b>1</b>
<b>Potential drawbacks of security tokens</b>	<b>1</b>
<b>When are security tokens available?</b>	<b>2</b>
<b>How to use this feature</b>	<b>3</b>
<b>How do security tokens help prevent XSRF attacks?</b>	<b>3</b>
<b>Who's affected by security tokens?</b>	<b>3</b>
<b>How do I enable or disable security tokens?</b>	<b>4</b>
<b>Possible error pages</b>	<b>5</b>
<b>Glossary</b>	<b>8</b>
<b>Terms</b>	<b>8</b>

# Executive Summary

## What are security tokens?

Security tokens help combat a common form of web application vulnerability called XSRF (Cross-Site Request Forgery) . This vulnerability utilizes weaknesses in the design of web authentication mechanisms to allow an attacker perform actions as another user.

## Examples

The red portions of the following URLs represent security tokens.

### WHM URL with a security token:

<https://example.com:2087/cpsess6347821693/scripts4/listaccts>

### cPanel URL with a security token:

<https://example.com:2083/cpsess5890916836/frontend/x3/index.html>

## Benefits of security tokens

The cPanel Security Tokens feature is a powerful method for stopping XSRF attacks before they start.

## Potential drawbacks of security tokens

The drawbacks of the cPanel Security Tokens feature fall into two categories:

- Existing methods of employing this measure require that the target site be designed with security tokens in mind from the outset. All pages must be capable of handling a security token, while links and page functionality must be capable of passing and accepting the unique piece of data. As a result, using security tokens may require redesigning legacy cPanel applications. In many cases, this redesign can introduce significant obstacles and challenges, as well as long-term maintenance issues. Please note that security tokens are only available for applications served by *cpsrvd*.
- When this feature is enabled, URLs become dynamic, resulting in broken bookmarks.

## **When are security tokens available?**

Security tokens became available to customers as part of cPanel & WHM version 11.25.0. For new installations and upgrades, the feature was available by opt-in only. In version 11.28, new installations include security tokens by default. Servers upgraded from prior versions still require opting in.

# How to use this feature

## How do security tokens help prevent XSRF attacks?

Typically, a web browser authenticates to a secured web destination once per browsing session. A XSRF attack utilizes that persistent authentication to deceptively initiate requests to an authenticated web destination without the knowledge of the browser's user. This attack commonly takes the form of hidden requests to another secured site within a malicious page. If the viewer of a page with hidden requests has previously visited and authenticated against the target site, then he or she will not see the requests initiated by the malicious page. A XSRF attack can use this routine process to exploit any exposed functionality of the target site and gather privileged information.

The use of security tokens has proven to be an effective technique in warding off XSRF attacks. Security tokens are unique pieces of data passed between the browser and the target site during requests. This technique blocks malicious sites from attacking other web destinations because they lack the required unique data.

The cPanel Security Tokens feature implements protection by including a security token within the URL of all requests rather than including it in request parameters or inside of the authentication mechanism. This feature inserts the security token into the URL, where it is parsed out of requests by the cPanel & WHM application server (*cpsrvd*) and handed off to the authentication layer. All parts of cPanel web applications can use security tokens by using relative URLs instead of absolute URLs, a very simple design pattern.

## Who's affected by security tokens?

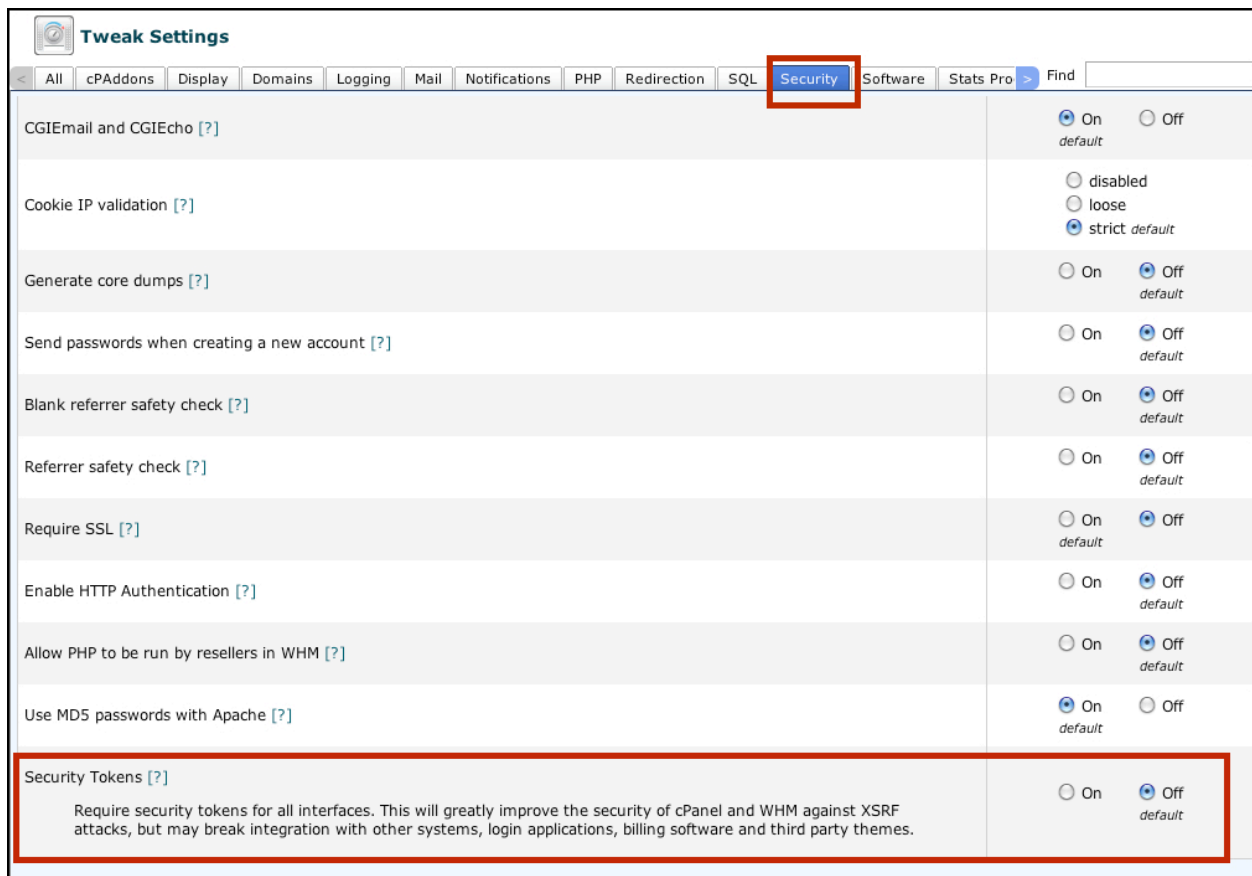
Third party developers need to update applications to allow security tokens. Since this is an opt-in feature, applications must have the capacity to handle servers with security tokens enabled, as well as servers with security tokens disabled.

Security tokens also affect cPanel & WHM users. When this feature is enabled, URLs become dynamic, resulting in broken bookmarks.

## How do I enable or disable security tokens?

To enable the cPanel Security Tokens feature, click *Tweak Settings* from the WHM interface. Next, click the *Security* tab. Beside the *Security Tokens* setting, select *On*. To disable the feature, select *Off*. The default for this setting is *Off*.

**Warning:** Please be aware that enabling this setting will require security tokens for all interfaces and may break integration with other systems, login applications, billing software, and third-party themes. We recommend that you verify that third-party applications are compatible with security tokens before enabling them. If you must use applications that are not compatible with security tokens, we strongly recommend using URL referrer checks instead.



The screenshot shows the WHM Tweak Settings interface. The 'Security' tab is selected and highlighted with a red box. The 'Security Tokens' setting is also highlighted with a red box. The setting is currently set to 'Off' (default), with 'On' also available. The description for the 'Security Tokens' setting reads: 'Require security tokens for all interfaces. This will greatly improve the security of cPanel and WHM against XSRF attacks, but may break integration with other systems, login applications, billing software and third party themes.'

Setting Name	Options
CGIEmail and CGIEcho [?]	<input checked="" type="radio"/> On <input type="radio"/> Off default
Cookie IP validation [?]	<input type="radio"/> disabled <input type="radio"/> loose <input checked="" type="radio"/> strict default
Generate core dumps [?]	<input type="radio"/> On <input checked="" type="radio"/> Off default
Send passwords when creating a new account [?]	<input type="radio"/> On <input checked="" type="radio"/> Off default
Blank referrer safety check [?]	<input type="radio"/> On <input checked="" type="radio"/> Off default
Referrer safety check [?]	<input type="radio"/> On <input checked="" type="radio"/> Off default
Require SSL [?]	<input type="radio"/> On <input checked="" type="radio"/> Off default
Enable HTTP Authentication [?]	<input type="radio"/> On <input checked="" type="radio"/> Off default
Allow PHP to be run by resellers in WHM [?]	<input type="radio"/> On <input checked="" type="radio"/> Off default
Use MD5 passwords with Apache [?]	<input checked="" type="radio"/> On <input type="radio"/> Off default
Security Tokens [?] Require security tokens for all interfaces. This will greatly improve the security of cPanel and WHM against XSRF attacks, but may break integration with other systems, login applications, billing software and third party themes.	<input type="radio"/> On <input checked="" type="radio"/> Off default

**Screenshot 1:** Security tokens setting in the WHM *Tweak Settings* interface.

## Possible error pages

These are examples of possible error pages that users may encounter when security tokens are enabled.

- If a security token for the requested page is missing, users will see this message.

### Access Denied: Security Token Failure

Functions in cPanel / WHM are available only directly through the cPanel and WHM interfaces or through our [XML API](#). The administrator of the system has enabled additional security token checks which have flagged this request as possibly malicious. This may be due to an expired session cookie or the use of an older theme which has not been updated to work with the security token system.

---

**Request Info:**

**Requested page:** /scripts/command  
**Error message:** security token missing

**Form Data:**

<u>Key</u>	<u>Value</u>
PFILE	main

---

To proceed with this request you must supply a valid login password. If you did not initiate this request, please logout and login again. **Continue at Your Own Risk!**

Username:

Password:

[Click here to proceed with the current request](#)

[Click here to logout](#)

- If a security token for the requested page has the wrong value, users will see this message.

## Access Denied: Security Token Failure

Functions in cPanel / WHM are available only directly through the cPanel and WHM interfaces or through our [XML API](#). The administrator of the system has enabled additional security token checks which have flagged this request as possibly malicious. This may be due to an expired session cookie or the use of an older theme which has not been updated to work with the security token system.

---

**Request Info:**

**Requested page:** /scripts4/listaccts  
**Error message:** security token has wrong value

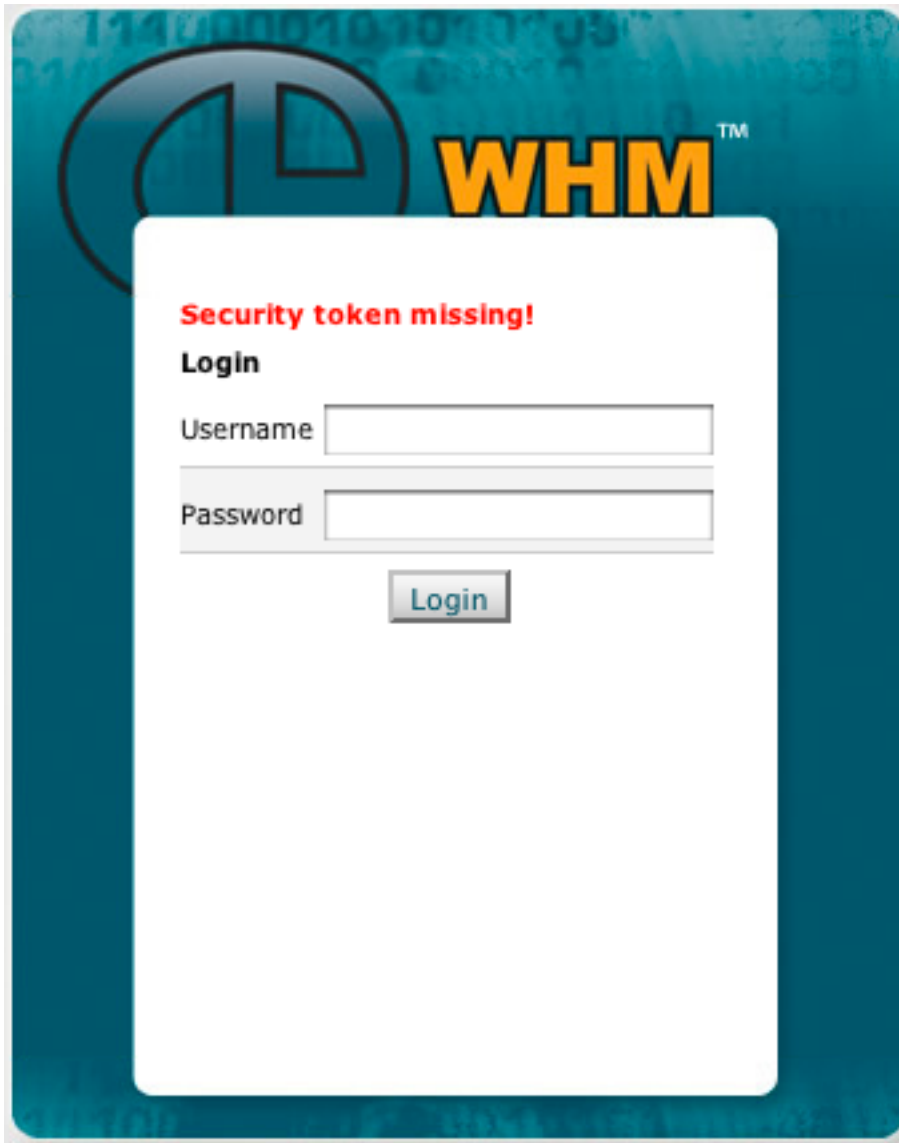
**Form Data:**

<u>Key</u>	<u>Value</u>
------------	--------------

To proceed with this request you must supply a valid login password. If you did not initiate this request, please logout and login again. **Continue at Your Own Risk!**

- **Users will see this login request if the following conditions are met:**

1. An active cPanel, WHM, or Webmail session is in progress.
2. The user refreshes the interface or requests a new interface.



# Glossary

## Terms

### **URL (Universal Resource Locator)**

On the web, a URL is a string of characters that identifies the location of a website. Since IP addresses are difficult to remember, URLs are used instead. For example, it is much easier to remember to go to [www.example.com](http://www.example.com) than <http://208.77.188.166>. “URL” is often used synonymously with the terms “URI” and “web address,” although there are technical differences among the three.

### **XSRF Attack (Also, CSRF)**

XSRF and CSRF stand for Cross-Site Request Forgery. This attack exploits a trusted website by forcing a user to execute unauthorized commands, usually through a hyperlink. To help prevent XSRF attacks, you can use *Tweak Settings* to limit the functions that cPanel and WHM perform by requiring that each request come from a domain or IP on your server.