Vulnerability Scan

Summary: 38 vulnerabilities found

HIGH 0 MED 12 LOW 26 INFO 82

	Name	Vulnerability
	Login Form Is Not Submitted Via HTTPS	
	Slow HTTP POST vulnerability	
	Cookie Does Not Contain The "HTTPOnly" Attribute	
	Path-Based Vulnerability	
	Sensitive form field has not disabled autocomplete	
	Path-Based Vulnerability	
	Cookie Does Not Contain The "secure" Attribute	
	Cookie Does Not Contain The "secure" Attribute	
	Path-Based Vulnerability	
	Cookie Does Not Contain The "HTTPOnly" Attribute	
	Cookie Does Not Contain The "HTTPOnly" Attribute	
	Path-Based Vulnerability	
	Cookie Does Not Contain The "secure" Attribute	
	SSL Server Allows Anonymous Authentication Vulnerability	
	PHP Session Fixation Vulnerability	
	Mail Server Accepts Plaintext Credentials	
	Mail Server Accepts Plaintext Credentials	
	POP3 Server Allows Plain Text Authentication Vulnerability	
	OpenSSH Commands Information Disclosure Vulnerability	

Add the following attribute to the form or input element: autocomplete="off" This attribute prevents the browser from prompting the user to save the populated form values for later reuse.

Results:
```
http://www.fredsmithplumbing.com/wp-login.php -- Form field does not
set autocomplete="off".
```

Path-Based Vulnerability

QID: 150004 **CVSS Base: 2.1**
Category: Web Application **Port: -**
CVEID: -

Threat:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

Impact:
The contents of this file or directory may disclose sensitive information.

Solution:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Results:
```
http://www.fredsmithplumbing.com/search/common/ -- HTTP/1.1 200 OK
```

Cookie Does Not Contain The "secure" Attribute

QID: 150122 **CVSS Base: 6.4**
Category: Web Application **Port: -**
CVEID: -

Threat:
The cookie does not contain the "secure" attribute.
Based on the latest release of the PCI-DSS, this vulnerability is a PCI Fail.
PCI-DSSv3.1 requirement 6.5.10 is focused on secure session management, and refers to session cookies needing to have the "secure" attribute set within the Cardholder Data Environment.
Refer to PCI-DSSv3.1 for details.

Impact:
Cookies with the "secure" attribute are only permitted to be sent via HTTPS. Session cookies sent via HTTP expose an unsuspecting user to sniffing attacks that could lead to user impersonation or compromise of the application account.

Solution:
If the associated risk of a compromised account is high, apply the "secure" attribute to cookies and force all sensitive requests to be sent via HTTPS.

Results:
```
http://www.fredsmithplumbing.com/wp-login.php --
wordpress_test_cookie=WP+Cookie+check; path=/;
domain=www.fredsmithplumbing.com
```

Cookie Does Not Contain The "secure" Attribute

QID: 150122 **CVSS Base: 6.4**
Category: Web Application **Port: -**