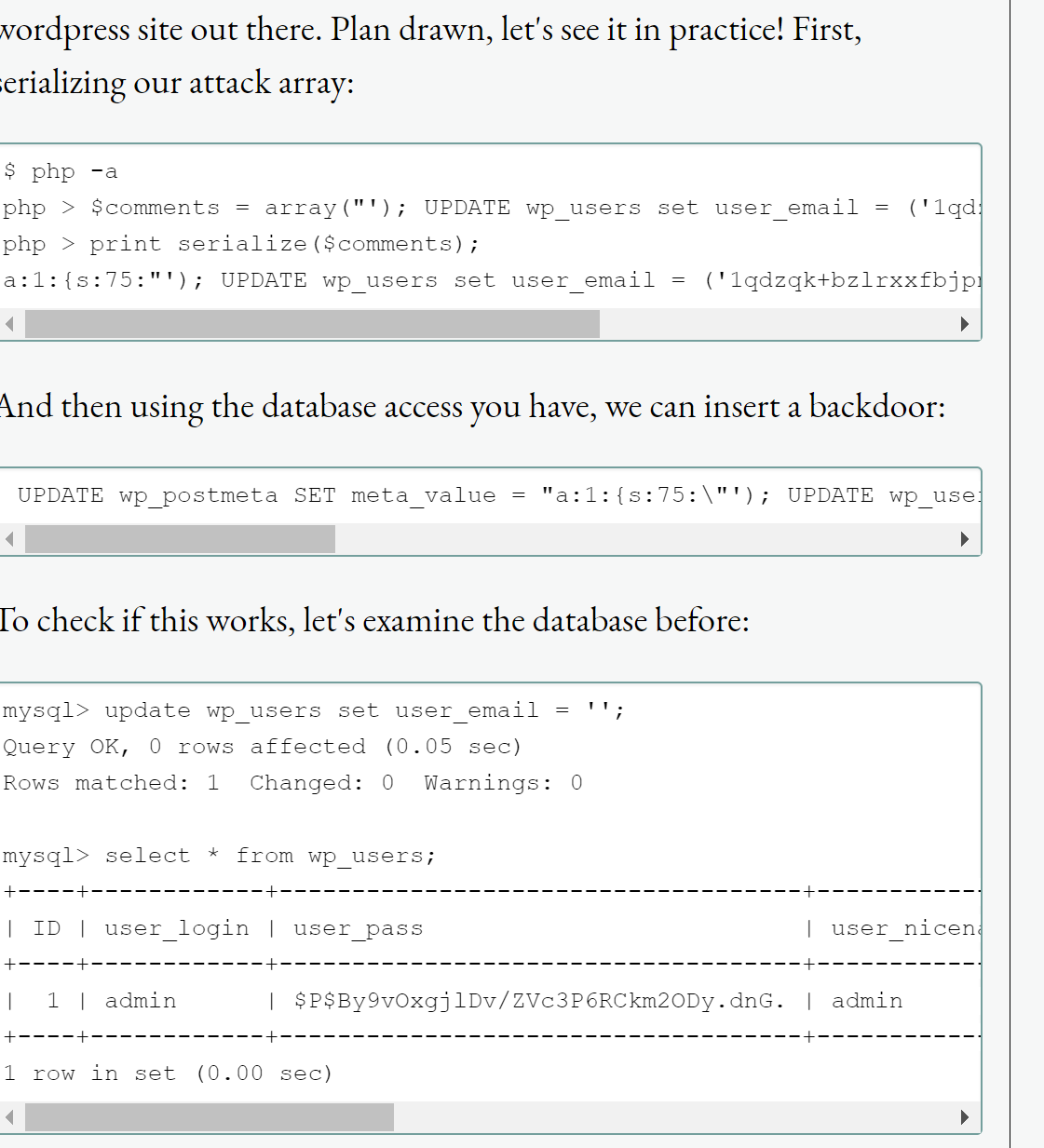
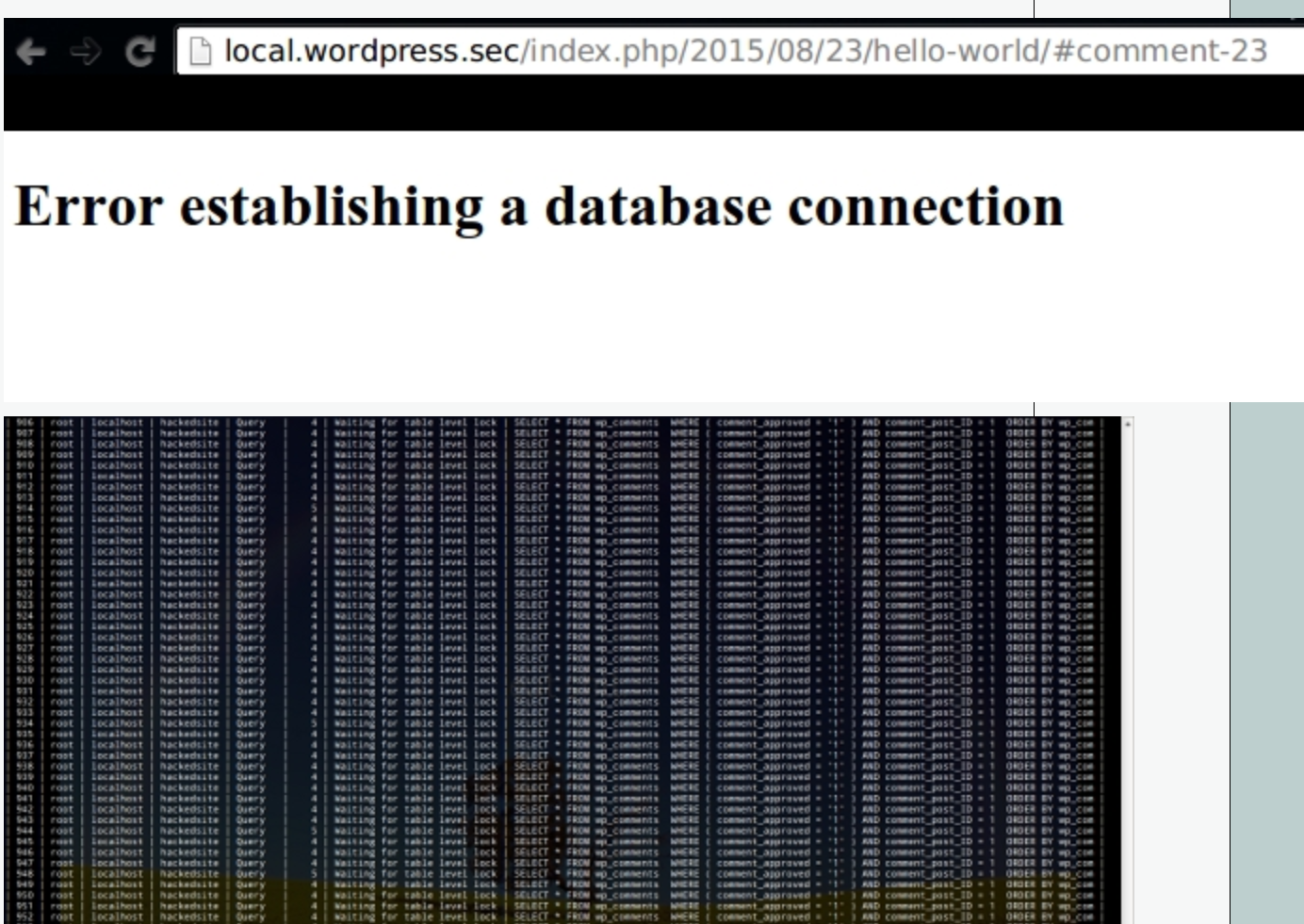
5 Vulnerabilities in Wordpress Version 4.2

[**CVE-2015-3440**](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3440) For this exploit, Wordpress 4.2 versions are vulnerable to stored XXS. An unauthenticated attacker can inject JavaScript in Wordpress comments. The script is triggered when the comment is viewed. If this vulnerability is triggered by a logged-in admin, the attacker can allow the vulnerability to execute arbitrary code on the server via the plugin and theme editors. The attacker could change the admin password, create new admin accounts, or any other action that the currently-logged in administrator has privileges to do on the target system. This vulnerability allows remote attackers to inject arbitrary web script or HTML via a long comment that is improperly stored because of limitations on the MySQL TEXT data type. This vulnerability was fixed in Wordpress 4.2.1 with a bug fix.



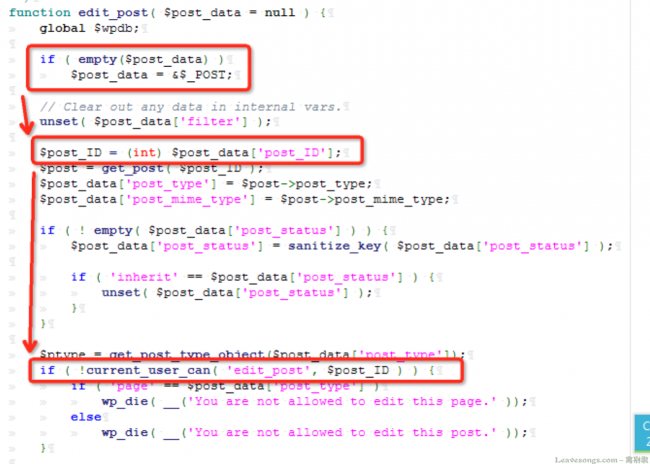
**CVE-2015-2213** This is an SQL injection vulnerability in the wp\_untrash\_post\_comments function in wp-including /post.php. It allows remote attackers to execute arbitrary SQL commands via a comment that is mishandled after retrieval from the trash. Under the vulnerability the attacker can access the database, inject a SQL statement, and then use the database access to insert a backdoor. There are SQL statements that if you enter enough could cause the website to shutdown from a DoD attack. This had a CVSS score of 7.5. It allowed for unauthorized disclosure of information, unauthorized modification, and disruption of service. This vulnerability was fixed in Wordpress 4.2.4.





[**CVE-2015-5731**](https://www.cvedetails.com/cve/CVE-2015-5731/)**-** This vulnerability is a cross-site request forgery in wp-admin/post.php in Wordpress before 4.2.4 allows remote attackers to hijack the authentication of administrators for requests that lock a post, and consequently cause a denial of service (editing blockage). It has a CVSS score of 6.8. For this vulnerability, the victim must voluntarily interact with the attack mechanism. This vulnerability allows unauthorized disclosure of information, unauthorized modification, and disruption of service. This vulnerability was patched in the 4.2.4 version.

# CVE-2015-5623- This vulnerability is found in versions before 4.2.3 and does not properly verify the edit\_posts\_capability, which allows remote authenticated users to bypass intended access restriction and create drafts by leveraging the Subscriber role, as demonstrated by a post-quickdraft-save action to wp-admin/post.php. The CVSS score is 4.0. The attack complexity for this is low. I think it was found by messing with the page source code.



**CVE-2017-6816**

This vulnerability existed in Wordpress versions through 4.7.2 before version 4.7.3 came out after and was no longer vulnerable to the attack. Unintended files could be deleted by administrators using the plugin deletion functionality. This has a CVSS score of 4.0. This was an input validation error and was a security bypass vulnerability. It has a low access complexity and requires that the attacker be logged into the system in order to perform the attack.