New issue

Jump to bottom

IonizeCMS-V1.0.8.1-Unverified post request parameters lead to sql injection #404

Open **EricFrank900528** opened this issue on Apr 11 · 1 comment

EricFrank900528 commented on Apr 11 • edited

1.Information

Exploit Title: IonizeCMS-V1.0.8.1-Unverified post request parameters lead to sql injection
Exploit date: 11.04.2022
Exploit Author: ericfrank900528@gmail.com
Vendor Homepage: https://github.com/ionize/ionize
Affect Version: V1.0.8.1
Description: SQL injection in Ionize CMS 1.0.8.1 allows attackers to execute commands remotely via a sql injection request from client.

2.Vulnerability Description

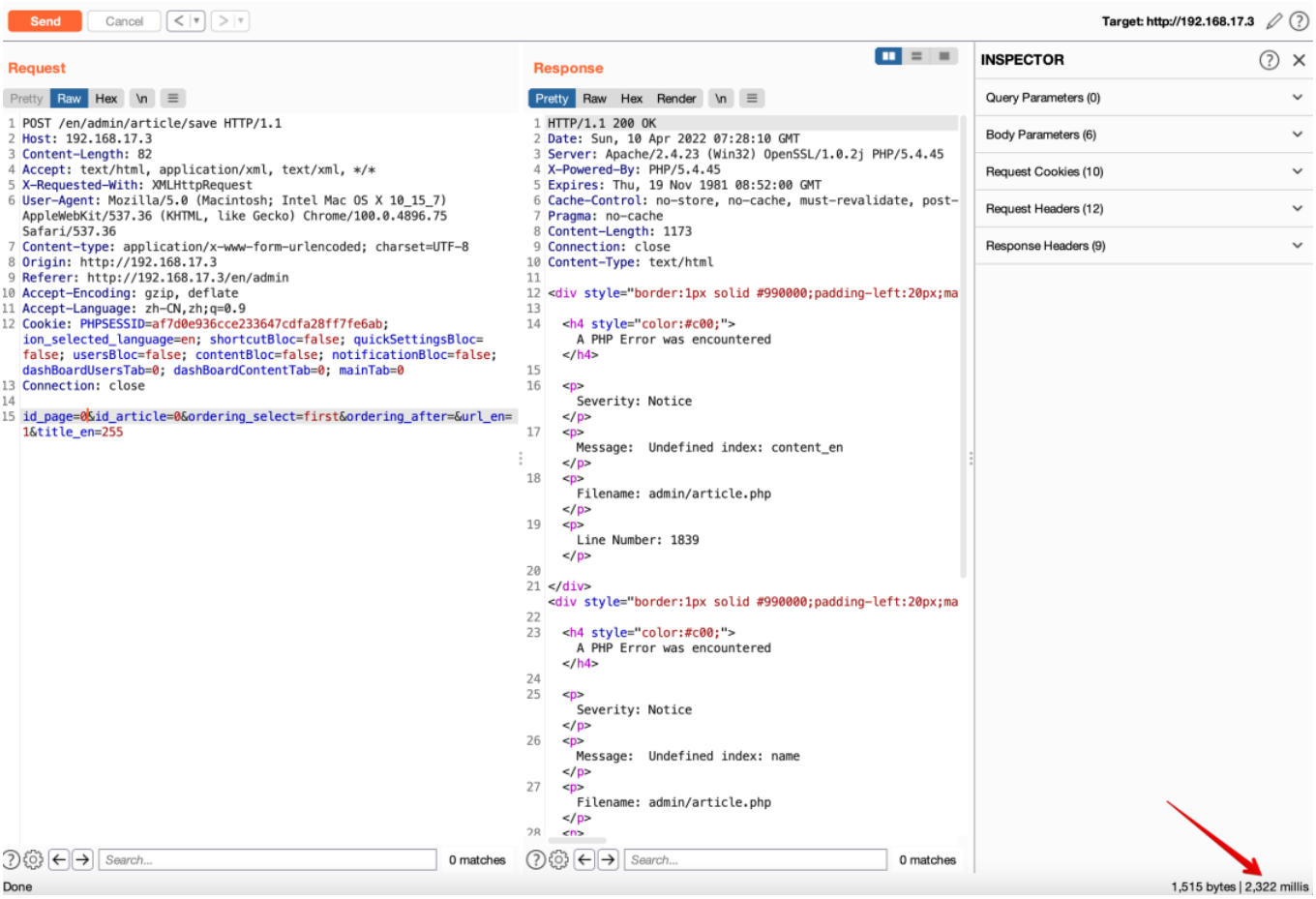
The exploit code is located in the project's application/models/article_model.php file
In the shift_article_ordering method, the code is as follows.
The POST parameter id_page is spliced into the sql statement without any processing or inspection, resulting in a SQL injection vulnerability.

application > models > article_model.php > Article_model > shift_article_ordering

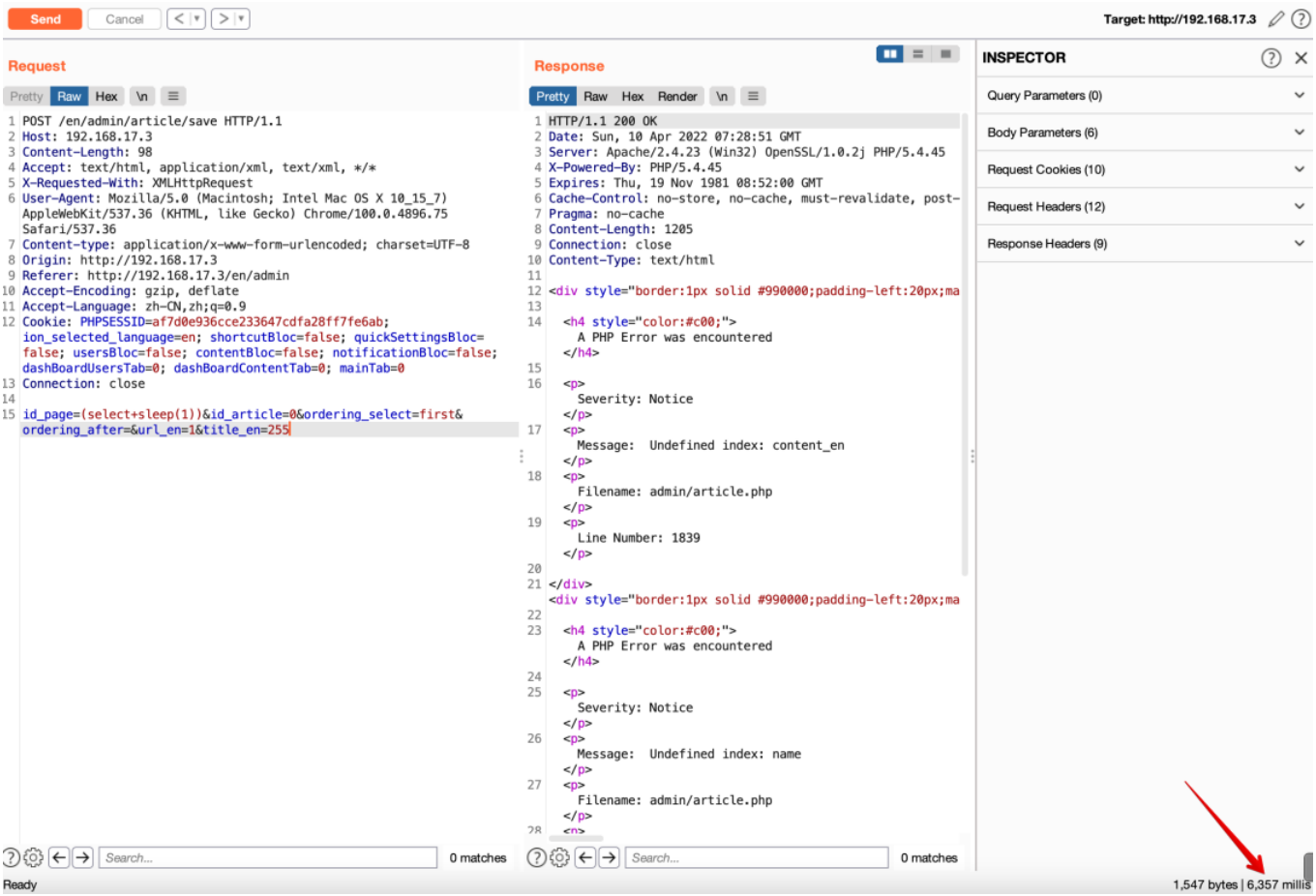
```
1452
1453
1454    /**
1455     * Updates articles ordering for the given page ID
1456     *
1457     * @param   Integer     $id_page    ID of the parent page
1458     * @param   Integer     $from       Ordering value from which start the reordering
1459     * @return  void
1460     */
1461    public function shift_article_ordering($id_page, $from = NULL)
1462    {
1463        $sql = 'UPDATE ' . $this->parent_table . ' SET ordering = ordering + 1 WHERE id_page=' .$id_page;
1464
1465        if ( ! is_null($from))
1466        {
1467            $sql .= ' AND ordering >= ' . $from;
1468        }
1469
1470        $this->{$this->db_group}->query($sql);
1471    }
1472
```

3.How to Exploit

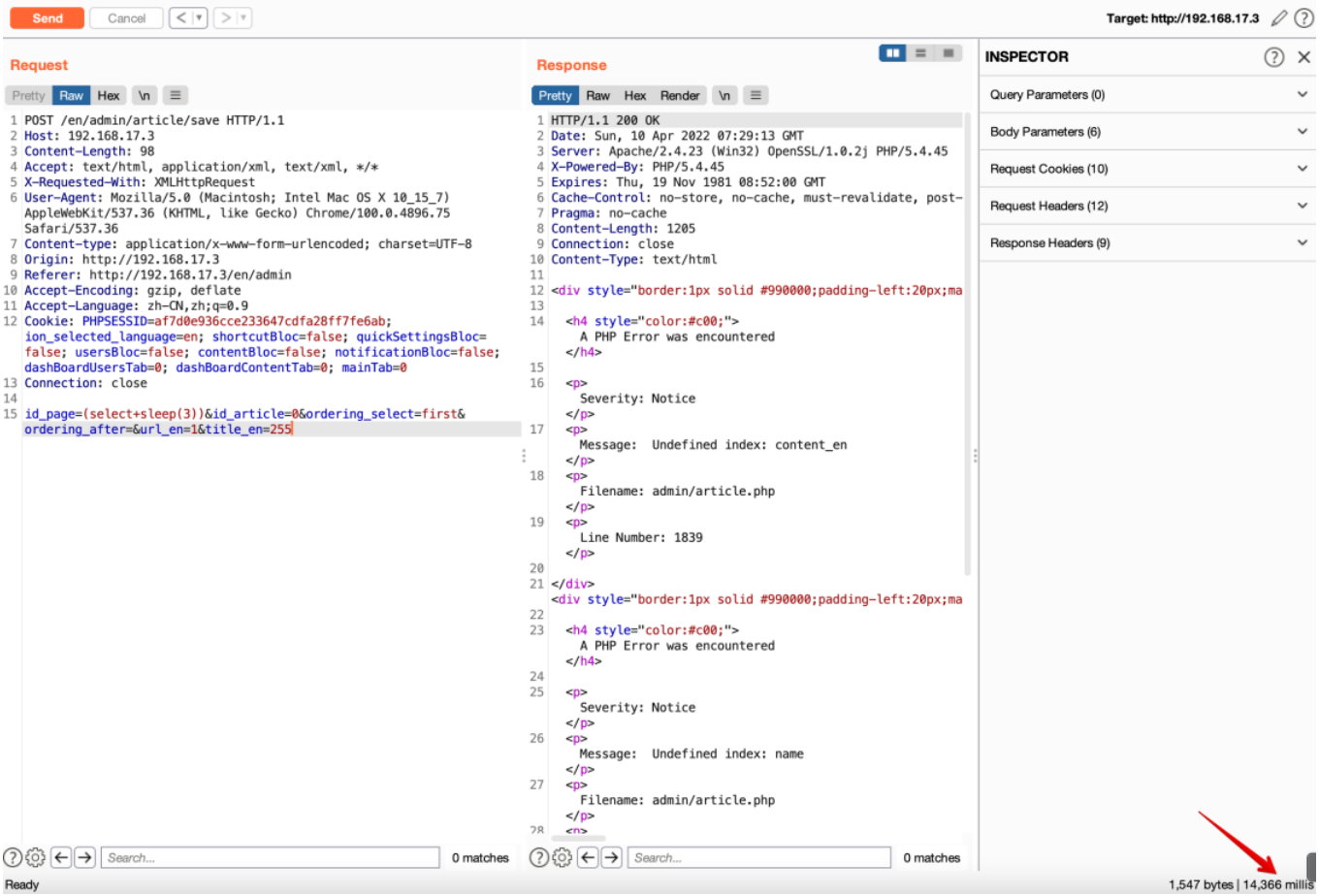
3.1Construct normal packet and send. In the image below, you can see that there is a 2 second network delay.



3.2Construct the injected data to execute `sleep(1)` . It can be found that the delay is more than 4 seconds. It is speculated that there are 4 records in total, so `sleep(1)` is executed 4 times.



3.3Construct the injection again to execute `sleep(3)` , this time with a delay of `2 + 4*3 = 14` seconds if the guess is correct.



4.Suggestion

Validate the parameters in the post request to avoid SQL injection

partikule commented on Apr 11 Member

Feel free to correct it : The project isn't maintained since 2017 !

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

2 participants