detectify

Back to finding list

Mark as

Inspect exploit

Login Cross Site Request Forgery (CSRF/XSRF)

NAME	VALUE
Found at	https://box.kiwiz.co.uk/admin
Tags	HIGH NEW

CVSS Score

More info

What does this mean?

The web site seems to be lacking CSRF token on a login form.

Read more at our knowledge base.

What can happen?

An attacker can force an unsuspecting user to sign in to the attacker's account. What can be done from there depends on the application. Example: An attacker can force an unsuspecting user to login to the attacker's account and when the user buys something, the credit card is added to the attacker's account.

Module Version
1.1.2

Released
2017-03-02

Request & Response

Below you can see the request header sent by Detectify and the response header that Detectify received from your domain.

General

Request URL	https://box.kiwiz.co.uk/admin

Method	GET

Request

Request-Line	GET /admin HTTP/1.1
Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/f6fafb3037bbcf445adeca266f0de678f7ba83d1
Accept-Encoding	gzip, deflate
Accept-Language	en-US

Response

Status-Line	HTTP/1.1 200 OK
Transfer-Encoding	chunked
X-Frame-Options	DENY
Strict-Transport-Security	max-age=31536000
Server	nginx
X-Content-Type-Options	nosniff
Content-Security-Policy	frame-ancestors 'none';
Connection	keep-alive
Content-Encoding	gzip
Date	Thu, 04 Jan 2018 16:20:43 GMT
Content-Type	text/html; charset=utf-8

Details

Below you can find more detailed information about the finding. Depending on the finding type, you might see a code snippet, screenshots, or other information.

```
<form class="form-horizontal" role="form" onsubmit="do_login(); return false;">
    <div class="form-group">
      <label for="inputEmail3" class="col-sm-3 control-label">Email</label>
      <div class="col-sm-9">
        <input name="email" type="email" class="form-control" id="loginEmail" placeholder="Email">
      </div>
    </div>
    <div class="form-group">
      <label for="inputPassword3" class="col-sm-3 control-label">Password</label>
      <div class="col-sm-9">
        <input name="password" type="password" class="form-control" id="loginPassword" placeholder="Passwo
rd">
      </div>
    </div>
    <div class="form-group">
      <div class="col-sm-offset-3 col-sm-9">
        <div class="checkbox">
          <label>
            <input name='remember' type="checkbox" id="loginRemember"> Remember me
          </label>
        </div>
      </div>
    </div>
    <div class="form-group">
      <div class="col-sm-offset-3 col-sm-9">
        <button type="submit" class="btn btn-default">Sign in</button>
      </div>
    </div>
  </form>
```

Resources

If you'd like to read up on this finding, here are some handy resources you can check out.

- REMEDIATION - Detectify Support Center - Login CSRF
- REMEDIATION - Detectify Support Center - CSRF
- STACK OVERFLOW - How to protect against login CSRF?
- VIDEO - What is a CSRF?

Tell us what you think

This improvement would be the best thing since sliced bread...

Send feedback