Open Redirect

One of the most common and largely overlooked vulnerabilities by web developers is Open Redirect (also known as "Unvalidated Redirects and Forwards"). A website is vulnerable to Open Redirect when parameter values (the portion of URL after "?") in an HTTP GET request allow for information that will redirect a user to a new website without any validation of the target of redirect. Depending on the architecture of a vulnerable website, redirection could happen after certain action, such as login, and sometimes it could happen instantaneously upon loading of a page.

An example of a vulnerable website link could look something like this: https://www.example.com/login.html?RelayState=http%3A%2F%2Fexample.com%2Fnext

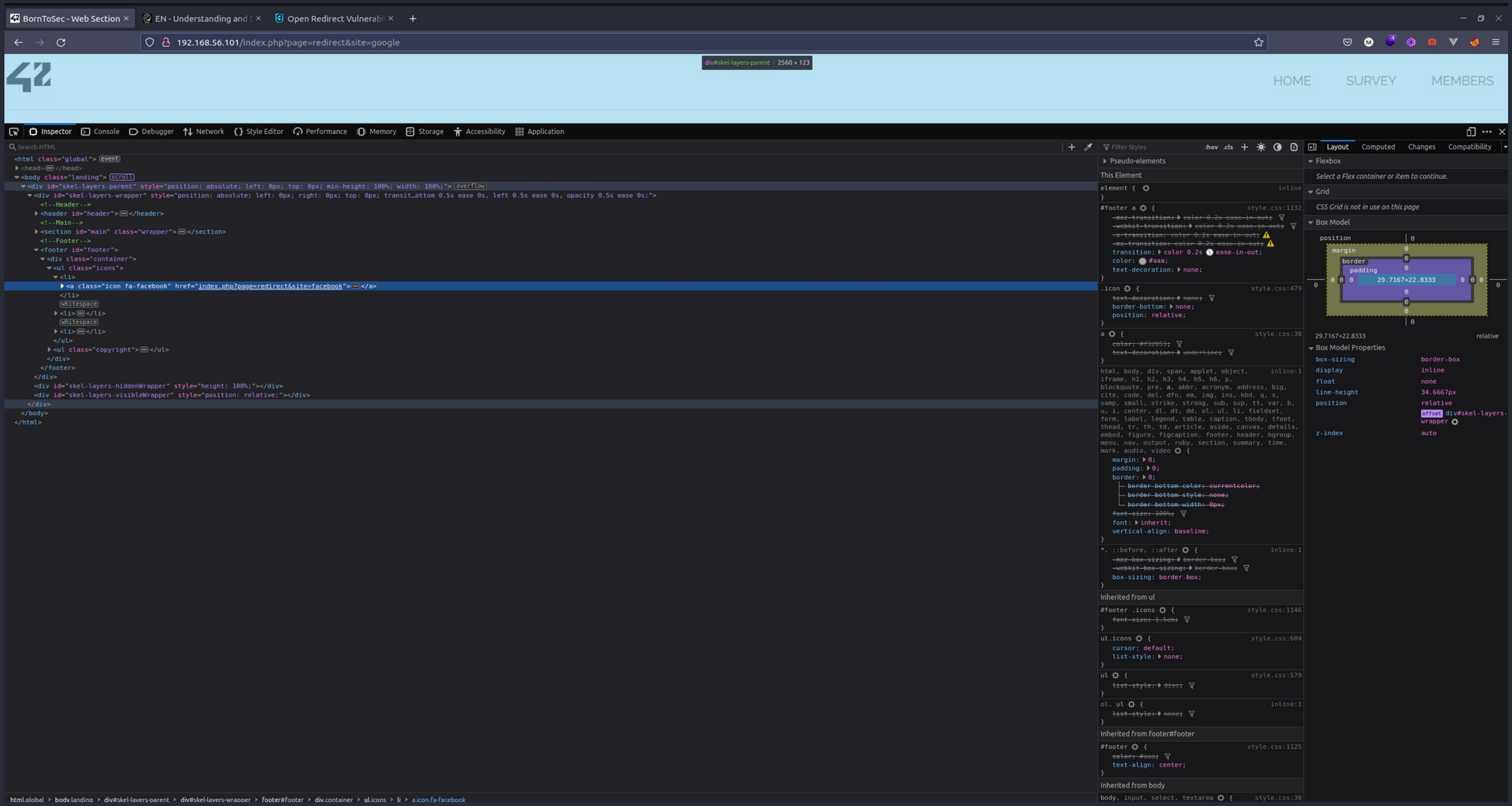
In this example, "RelayState" parameter indicates where to send user upon successful login (In our example it is "http://example.com/next"). If website doesn't validate the

"RelayState" parameter value to make sure that target web page is legitimate and intended, attacker could manipulate that parameter to send a victim to a fake page crafted by

attacker: https://www.example.com/login.html?RelayState=http%3A%2F%2FEvilWebsite.com

Walk through

Step 1 : Open the code inspector in your browser



```
<html class="global"> event
  <head>…</head>
  <body class="landing"> scroll
    <div id="skel-layers-parent" style="position: absolute; left: 0px; top: 0px; min-height: 100%; width: 100%;"> overflow
      <div id="skel-layers-wrapper" style="position: absolute; left: 0px; right: 0px; top: 0px; transit…ottom 0.5s ease 0s, left 0.5s ease 0s, opacity 0.5s ease 0s;">
        <!--Header-->
        <header id="header">…</header>
        <!--Main-->
        <section id="main" class="wrapper">…</section>
        <!--Footer-->
        <footer id="footer">
          <div class="container">
            <ul class="icons">
              <li>
                <a class="icon fa-facebook" href="index.php?page=redirect&site=facebook">…</a>
              </li>
              whitespace
              <li>…</li>
              whitespace
              <li>…</li>
            </ul>
            <ul class="copyright">…</ul>
          </div>
        </footer>
      </div>
      <div id="skel-layers-hiddenWrapper" style="height: 100%;"></div>
      <div id="skel-layers-visibleWrapper" style="position: relative;"></div>
    </div>
  </body>
</html>
```

html.global > body.landing > div#skel-layers-parent > div#skel-layers-wrapper > footer#footer > div.container > ul.icons > li > a.icon.fa-facebook

Pseudo-elements

This Element

```
element {                                              inline
}
#footer a {                                  style.css:1132
    ~~-moz-transition: color 0.2s ease-in-out;~~
    ~~-webkit-transition: color 0.2s ease-in-out;~~
    ~~-o-transition: color 0.2s ease-in-out;~~
    ~~-ms-transition: color 0.2s ease-in-out;~~
    transition: color 0.2s ease-in-out;
    color: #aaa;
    text-decoration: none;
}
.icon {                                       style.css:479
    ~~text-decoration: none;~~
    border-bottom: none;
    position: relative;
}
a {                                            style.css:38
    ~~color: #f32853;~~
    ~~text-decoration: underline;~~
}
html, body, div, span, applet, object,         inline:1
iframe, h1, h2, h3, h4, h5, h6, p,
blockquote, pre, a, abbr, acronym, address, big,
cite, code, del, dfn, em, img, ins, kbd, q, s,
samp, small, strike, strong, sub, sup, tt, var, b,
u, i, center, dl, dt, dd, ol, ul, li, fieldset,
form, label, legend, table, caption, tbody, tfoot,
thead, tr, th, td, article, aside, canvas, details,
embed, figure, figcaption, footer, header, hgroup,
menu, nav, output, ruby, section, summary, time,
mark, audio, video {
    margin: 0;
    padding: 0;
    border: 0;
      ~~border-bottom-color: currentcolor;~~
      ~~border-bottom-style: none;~~
      ~~border-bottom-width: 0px;~~
    ~~font-size: 100%;~~
    font: inherit;
    vertical-align: baseline;
}
*, ::before, ::after {                         inline:1
    ~~-moz-box-sizing: border-box;~~
    ~~-webkit-box-sizing: border-box;~~
    box-sizing: border-box;
}
```

Inherited from ul

```
#footer .icons {                             style.css:1146
    ~~font-size: 1.5em;~~
}
ul.icons {                                    style.css:604
    cursor: default;
    list-style: none;
}
ul {                                          style.css:579
    ~~list-style: disc;~~
}
ol, ul {                                       inline:1
    ~~list-style: none;~~
}
```

Inherited from footer#footer

```
#footer {                                    style.css:1125
    ~~color: #aaa;~~
    text-align: center;
}
```

Inherited from body

```
body, input, select, textarea {                style.css:30
```

Flexbox

Select a Flex container or item to continue.

Grid

CSS Grid is not in use on this page

Box Model

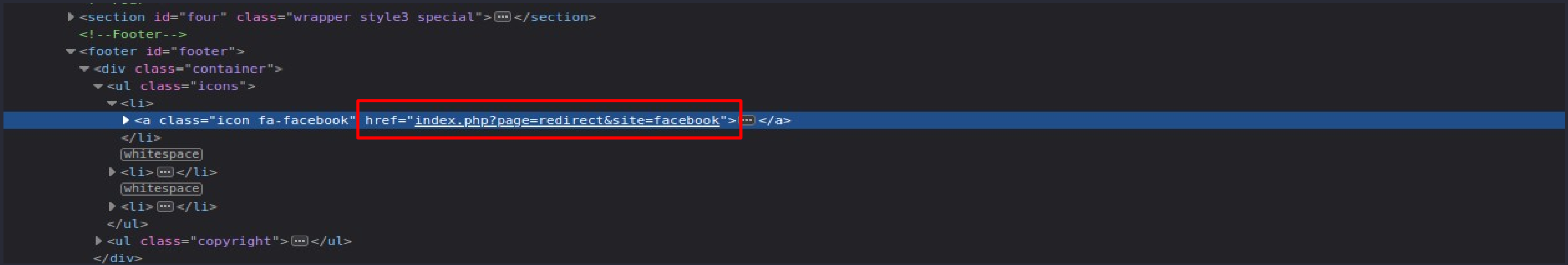
```
position        0
  margin        0
    border      0
      padding   0
0 0 0   29.7167×22.8333   0 0 0
                0
                0
                0
                0
```

29.7167×22.8333 relative

Box Model Properties

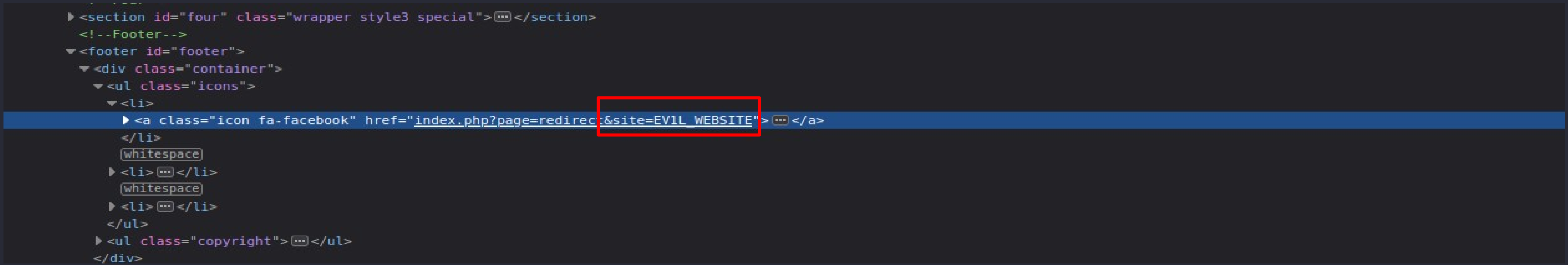
```
box-sizing      border-box
display         inline
float           none
line-height     34.6667px
position        relative
                offset div#skel-layers-wrapper
z-index         auto
```

Step 2 : Find an open redirect link, for example on the social media buttons



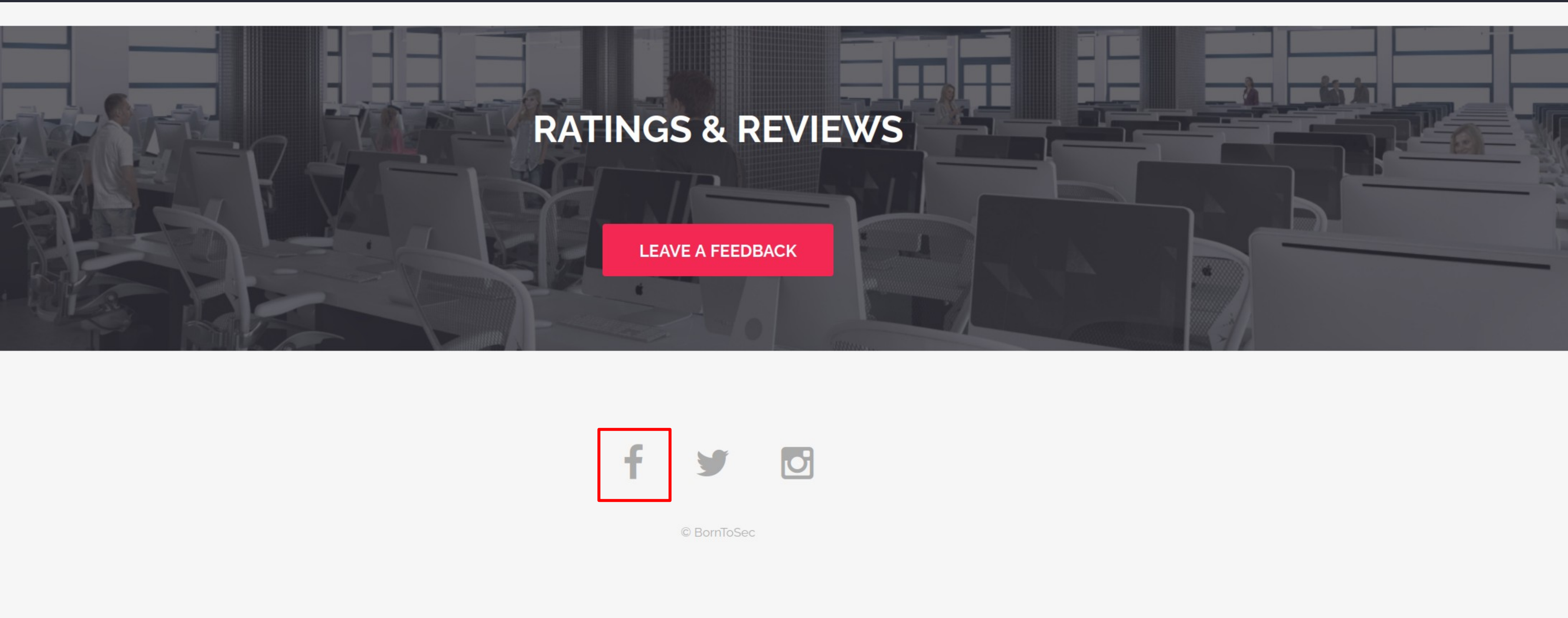
```
▸<section id="four" class="wrapper style3 special">⋯</section>
 <!--Footer-->
▾<footer id="footer">
  ▾<div class="container">
    ▾<ul class="icons">
      ▾<li>
        ▸<a class="icon fa-facebook" href="index.php?page=redirect&site=facebook">⋯</a>
        </li>
        whitespace
      ▸<li>⋯</li>
        whitespace
      ▸<li>⋯</li>
      </ul>
    ▸<ul class="copyright">⋯</ul>
    </div>
```

Step 3 : Change the site argument to your malicious website



```
▸<section id="four" class="wrapper style3 special">⋯</section>
 <!--Footer-->
▾<footer id="footer">
  ▾<div class="container">
    ▾<ul class="icons">
      ▾<li>
        ▸<a class="icon fa-facebook" href="index.php?page=redirect&site=EVIL_WEBSITE">⋯</a>
        </li>
        whitespace
      ▸<li>⋯</li>
        whitespace
      ▸<li>⋯</li>
      </ul>
    ▸<ul class="copyright">⋯</ul>
    </div>
```

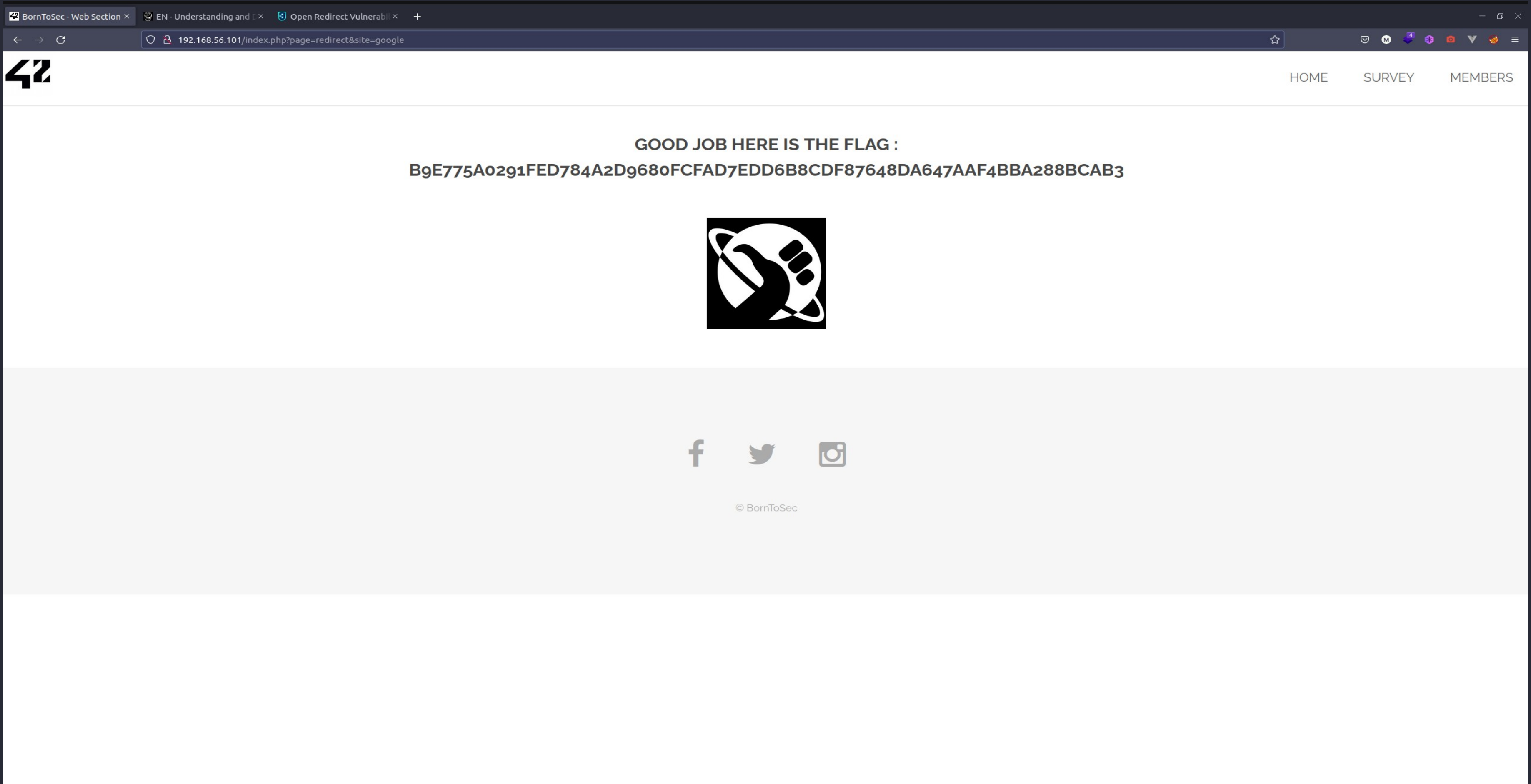
Step 4 : Click on the malicious link on the page



RATINGS & REVIEWS

© BornToSec

Step 5 : Get the flag !



GOOD JOB HERE IS THE FLAG :
B9E775A0291FED784A2D9680FCFAD7EDD6B8CDF87648DA647AAF4BBA288BCAB3

© BornToSec

How to fix

- Do not use forwards and redirects.

- Create a list of all trusted URLs, including hosts or a regex, in order to sanitize input. Prefer to use an allow-list approach when creating this list, instead of a block list.

- Force redirects to first go to a page that notify users they are redirected out of the website. The message should clearly display the destination and ask users to click on a link to confirm that they want to move to the new destination.