

Open Redirect Report - 14.3 -14

Tester: Stanley Ford

Lab 14.3

- General information:
 - Testing period: 22.01.2023
 - Test object: <http://51.250.73.193:8081/>
- Description of actions:

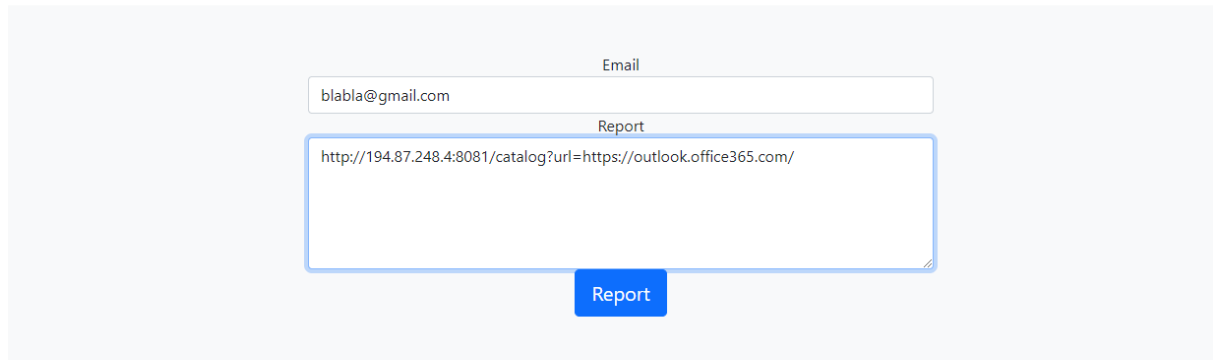
First of all, you always want to see what's going on in the code. That's why I inspected the code of the shopping page.

```
60
61
62
63
64
65 <div class="container">
66
67   <div class="row">
68
69     <div class="col">
70       <div class="card mb-3" style="max-width: 540px">
71         <div class="row g-0">
72           <div class="col-md-4">
73             
78           </div>
79           <div class="col-md-8">
80             <div class="card-body">
81               <h5 class="card-title"><Card title/></h5>
82               <p class="card-text">
83                 This is a wider card with supporting text below as a natural lead-in to
84                 additional content. This content is a little bit longer.
85               </p>
86               <p class="card-text">
87                 <small class="text-muted">last updated 3 mins ago</small>
88               </p>
89               <a class="btn btn-primary" href="http://194.87.248.4:8081/catalog?url=http://194.87.248.4:8081/pay/0" role="button">Buy</a>
90             </div>
91           </div>
92         </div>
93       </div>
94     </div>
95     <div class="col">
96       <div class="card mb-3" style="max-width: 540px">
97         <div class="row g-0">
98           <div class="col-md-4">
99             
104           </div>
105           <div class="col-md-8">
106             <div class="card-body">
107               <h5 class="card-title"><Card title/></h5>
108               <p class="card-text">
109                 This is a wider card with supporting text below as a natural lead-in to
110                 additional content. This content is a little bit longer.
111               </p>
112               <p class="card-text">
113                 <small class="text-muted">last updated 3 mins ago</small>
114               </p>
115               <a class="btn btn-primary" href="http://194.87.248.4:8081/catalog?url=http://194.87.248.4:8081/pay/1" role="button">Buy</a>
116             </div>
117           </div>
118         </div>
119       </div>
120     </div>
121   </div>
122 </div>
```

In the screenshot, I've highlighted an interesting line of code, from which you can see that the "Buy" button on the site redirects us [to http://194.87.248.4:8081/pay/0](http://194.87.248.4:8081/pay/0)

Apparently, the payment page. This is an obvious vulnerability of Open-Redirect, because we are redirected to a direct, undisguised link, without using an ID.

The site has a form for contacting the administrator, in which you can enter a link with a redirect to some other site. I took a random one, literally from the next tab of my browser:



The screenshot shows a web application interface for submitting a report. At the top, there is a navigation bar with links: Home, Features, Pricing, and Report Admin. Below this is a form with two input fields. The first field is labeled 'Email' and contains the text 'blabla@gmail.com'. The second field is labeled 'Report' and contains a long URL: 'http://194.87.248.4:8081/catalog?url=https://outlook.office365.com/'. Below the 'Report' field is a blue button labeled 'Report'.

After sending the report, I was redirected to a page with a flag
:flag{Subm1t_0p3n_r3d1r3ct}

What if I sent a request to the admin with a redirect to instead of a harmless site with mail to my phishing one?

Laboratory work was performed :)

Self-Assessment Questions:

- List the tools (programs and utilities) that you used to solve this lab: Web browser (Google Chrome)
- List the vulnerabilities you were able to find: Open redirect
- Give advice on how to improve protection: For redirection, it is recommended to use the links stored in the database table and address them by the number

Alternatively, you can disable any protocols except http and https, or use a whitelist of sites to which redirects are allowed.