

Are_We_Up

Description

None

Category

#web

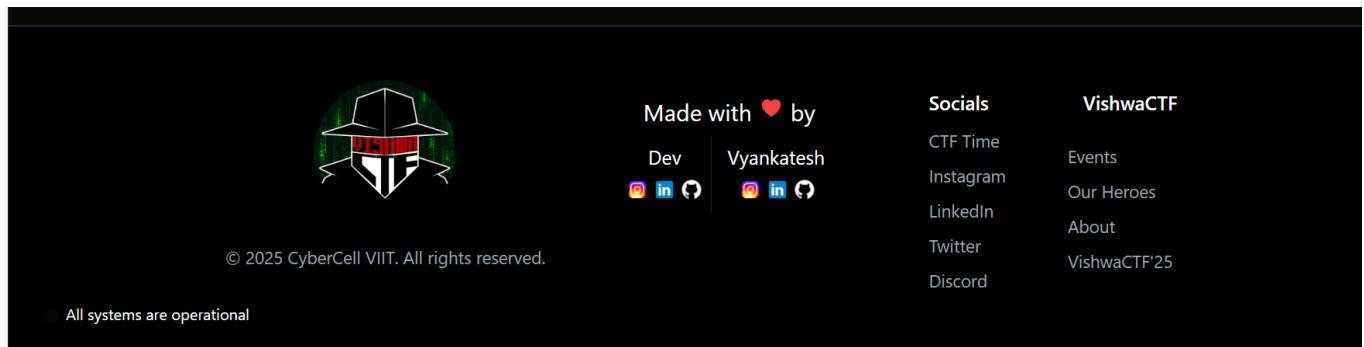
Hint

look at the status of our website (vishwactf.com/)...

Solution

Enumeration

Scrolling all the way down to the bottom of said website in the hint, we see a status check at bottom left.



This website reveals us 3 things:

1. A local:8080 is hosted but not reachable
2. A directory called /flag
3. Another website at the footer

Pune	Operational
Kolkata	Operational
1aq41l6hu5zm6lz30165y3la5t55fq49e	Operational
Delhi	Operational
Solapur	Operational
4cM5g7682WXNV09	Operational
Sigma-2	Operational
Tau-1	Operational
Tau-2	Operational
Tau-3	Operational
local:8080	Outage
/flag	Outage

Powered by Uptime

```
<title>server >status Page</title>
<style>
</style>
</head>
<body>
  <header class="siteHeader">
  </header>
  <div class="container">
  </div>
  <div class="siteFooter">
    <div class="container">
      <p class="siteFooter_poweredBy"> == $0
        "Powered by "
        <a href="/uptimer-a343s19" onclick="return false;" style="text-decoration: none; curs
          default;">Uptime</a>
      </p>
    </div>
  </div>
  <script>
  </script>
  <div class="glasp-extension-toaster" style="display: block; width: 320px; margin: unset; p
    g: unset; border: unset; border-radius: unset; outline: unset; background-color: unset; bo
    dow: unset; position: fixed; top: 40px; right: 24px; z-index: 9999;">
  </div>
  <div class="glasp-extension" style="display: block; width: unset; margin: unset; padding:
    t; border: unset; border-radius: unset; outline: unset; background-color: unset; box-shado
    set; position: fixed; bottom: 16px; right: 16px; z-index: 9999;">
  </div>
</body>
</html>
```

html body footer.siteFooter div.container p.siteFooter_poweredBy

At the time of writing, the said website is down. However:

1. The website has an URL input that is vulnerable to SSRF
2. Input MUST have http/https in the URL
3. the local/localhost doesn't work but 127.0.0.1:8000/flag works

