

# VulnLtd

22 February 2024 23:02

1 - Got a Home-Page with a contact Page

2 - When submitting a request , got an error saying --> `Your Slack Token has been Expired`

3 - After Fuzzing, Found out robots.txt, with a flag and secret login path.

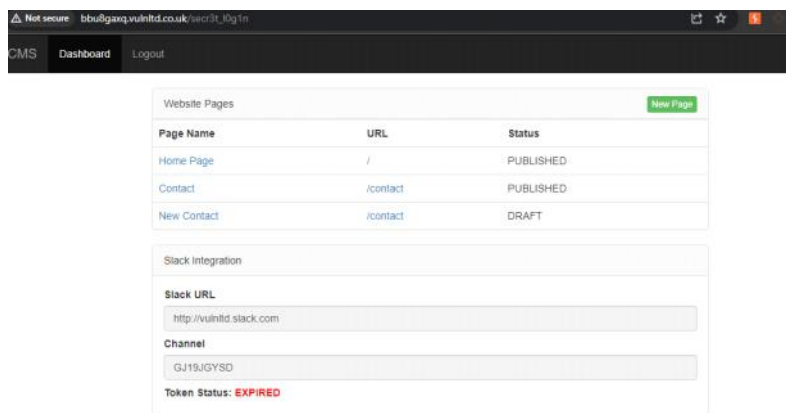
`/secr3t_l0g1n/`

4 -Found a documentation, exposing guest login

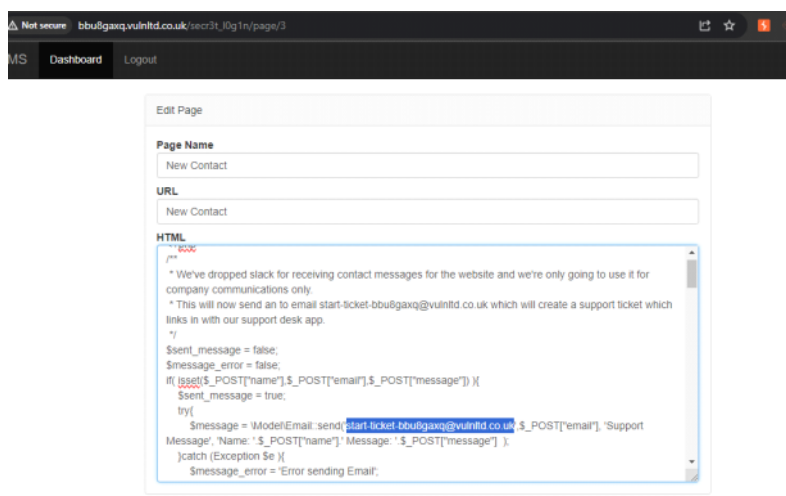
Login as Guest user --> `username : guest , password : Tuesday`

5 - Intercept the login request and change the cookie parameter, `isadmin=False --> isadmin=True`

6 - and now I can see other pages inside it.



7 - After reviewing the mentioned website pages, found out this email address, in `New Contact Page`



8 - In this page, the comments mentioned convey that we can may send email to this given email address and then gotcha some kinda ticket generation from there.

And I send a email to that email address, and got reply from them

## Ticket Created Inbox x



start-ticket-bbu8gaxq@vulnltld.co.uk via sendgrid.net  
to me ▾

Your support ticket has been created, you can view it at <http://support.bbu8gaxq.vulnltld.co.uk/6JnS1wIMjM>

Many Thanks

VulnLtd - Online Support

[^FLAG^510C25C1CBAF74B40F1F392965F0C0BA^FLAG^]

9 - Here we got another subdomain of the target i.e [support.target.com](http://support.target.com) with our ticket reference.

10 - Well, At this point I get stuck so took bit hint from other walkthroughs, and found that we can signup in slack using the company email address that we got when generating support ticket.

Update Method	Update From	Created At	Action
email	no-reply-TQ3WP3IKzHorsepamEy1cFUq@slack.com	22/02/2024 03:33	<a href="#">view</a>
email	no-reply@slack.com	22/02/2024 03:30	<a href="#">view</a>
email	prakharpowal2004@gmail.com	22/02/2024 03:26	<a href="#">view</a>
portal		22/02/2024 03:17	<a href="#">view</a>
portal		22/02/2024 03:17	<a href="#">view</a>
portal		22/02/2024 03:16	<a href="#">view</a>
email	prakharpowal2004@gmail.com	22/02/2024 03:15	<a href="#">view</a>

11-And after signup through company email address(mentioned in above screenshot), I got the confirmation link.

support.bbu8gaxq.vulnltld.co.uk/6JnS1wIMjM/7

slack

## Confirm your email to join Vuln Ltd

Hello! Once you've confirmed your email address, you'll be the newest member of the Slack workspace **Vuln Ltd**. 🌟

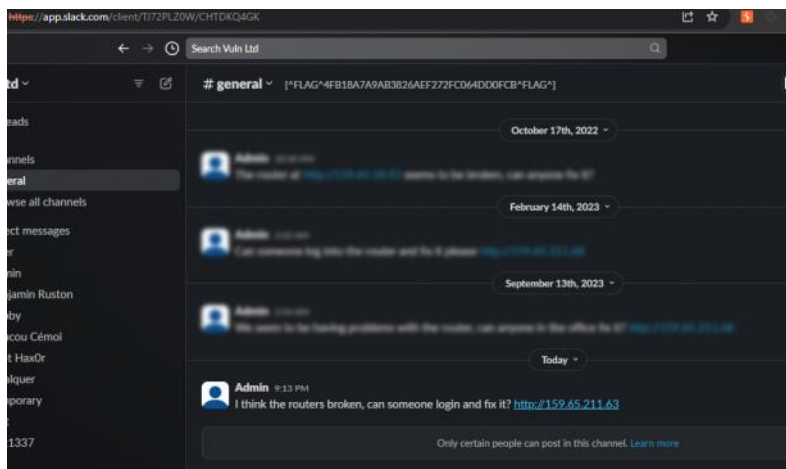
[CONFIRM EMAIL](#)

If you have any questions, simply reply to this email. We'd love to help.

If you didn't request this email, there's nothing to worry about — you can safely ignore it.

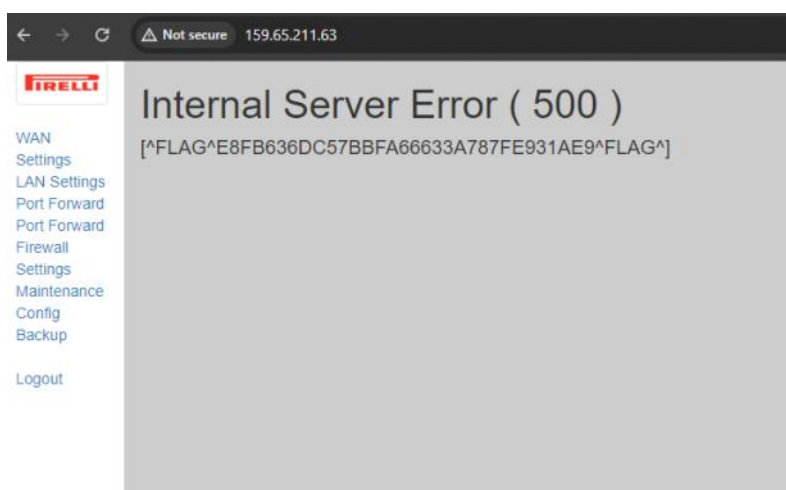
Vuln Ltd  
Workspace URL: vulnltld.slack.com

12 - By successful signup process, now I can join the slack group of the company,



13 - Now, the admin user asking to fix some router problem at the given IP Address. Well firstly there is a login Page.

Tries defaults credentials,  
And successfully logged-in as **username : admin , password : microbusiness**



14 - Through, Config Backup, found out a base64 encoded **.bak** file, exposing credentials.

```

"wan": {
  "type": "adsl",
  "isp": {
    "ip": "dhcp",
    "username": "09732837999@dslnet",
    "password": "d3FpPo5ew"
  }
},
"lan": {
  "ip": "192.168.1.1",
  "subnet": "255.255.255.0"
},
"firewall": {
  "active": true
},
"maintenance": {
  "admin_user": "admin",
  "admin_pass": "microbusiness",
  "enable_on_wan": true,
  "http_port": 80
},
"websites": [
  {
    "active": true,
    "name": "/intranet",
    "protected": {
      "type": "basic_auth",
      "username": "internet",
      "password": "4gH2k09e1cE53Mk"
    }
  }
],
"flag": "[^FLAG^F4AC9478B71EA056A1B2DE0DF824AC61^FLAG^]"

```

15 - Go to the `/intranet/` directory, through the given credentials, login

16 - Now, Again stuck at this point, I observed that there is some kind of filtering going on in the ``page`` parameter but then I take help from walkthrough and found out that, this can be bypassed as `adminadmin.php.php&something.html`

17 - Here, the middle ``admin.php`` get filtered in the backend, and then server will pass on the rest of the expression i.e `admin & .php --> admin.php`

← → ↻ Not secure 159.65.211.63/intranet/index.php?page=adminadmin.php.php&home.html

## VulnLtd Intranet - File Downloads

[Home](#)

### Download Files

[^FLAG^AD07238C44C1E92FA90B7363027F91D6^FLAG^]

No Files to download

Please supply a password to get the file list