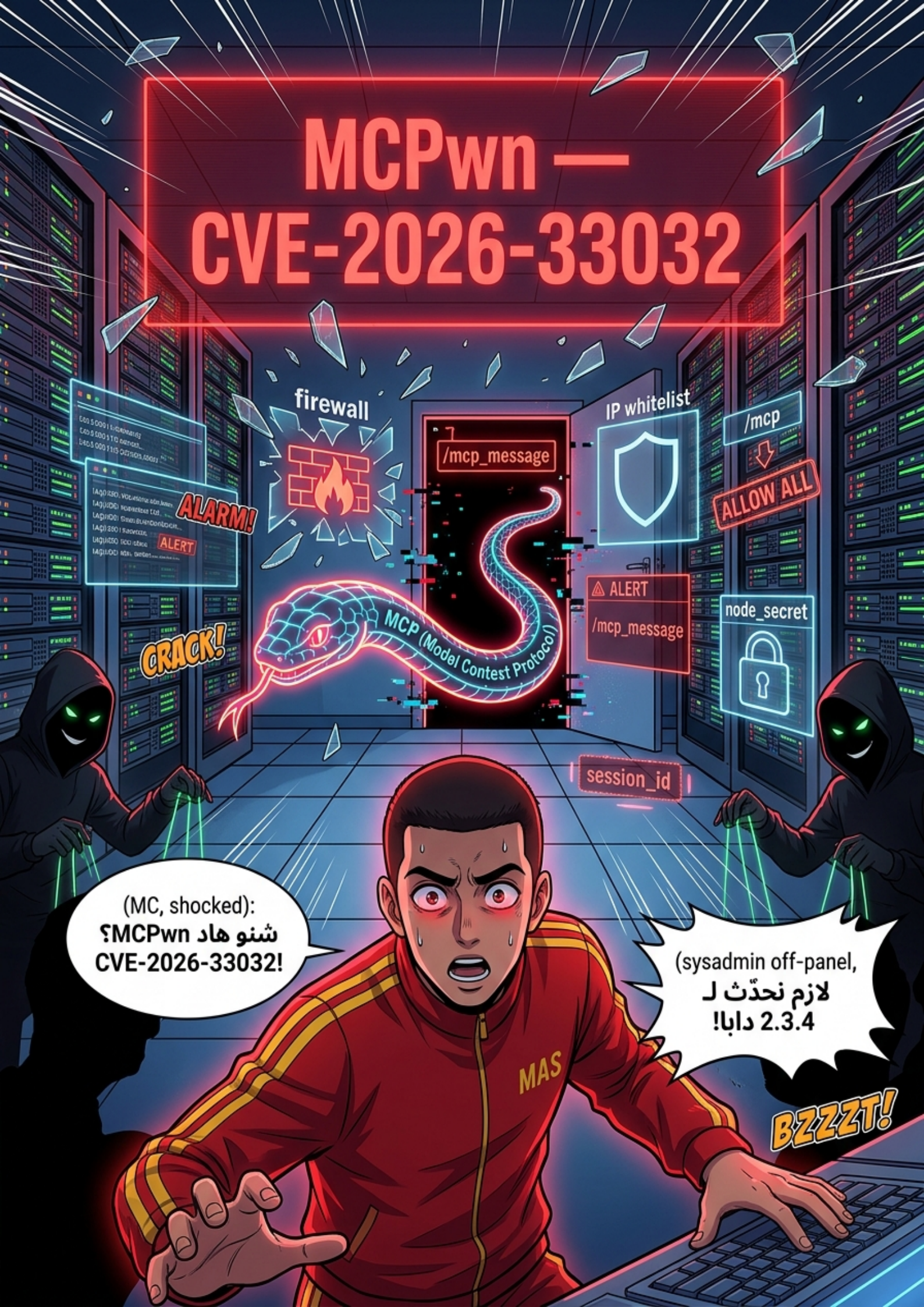
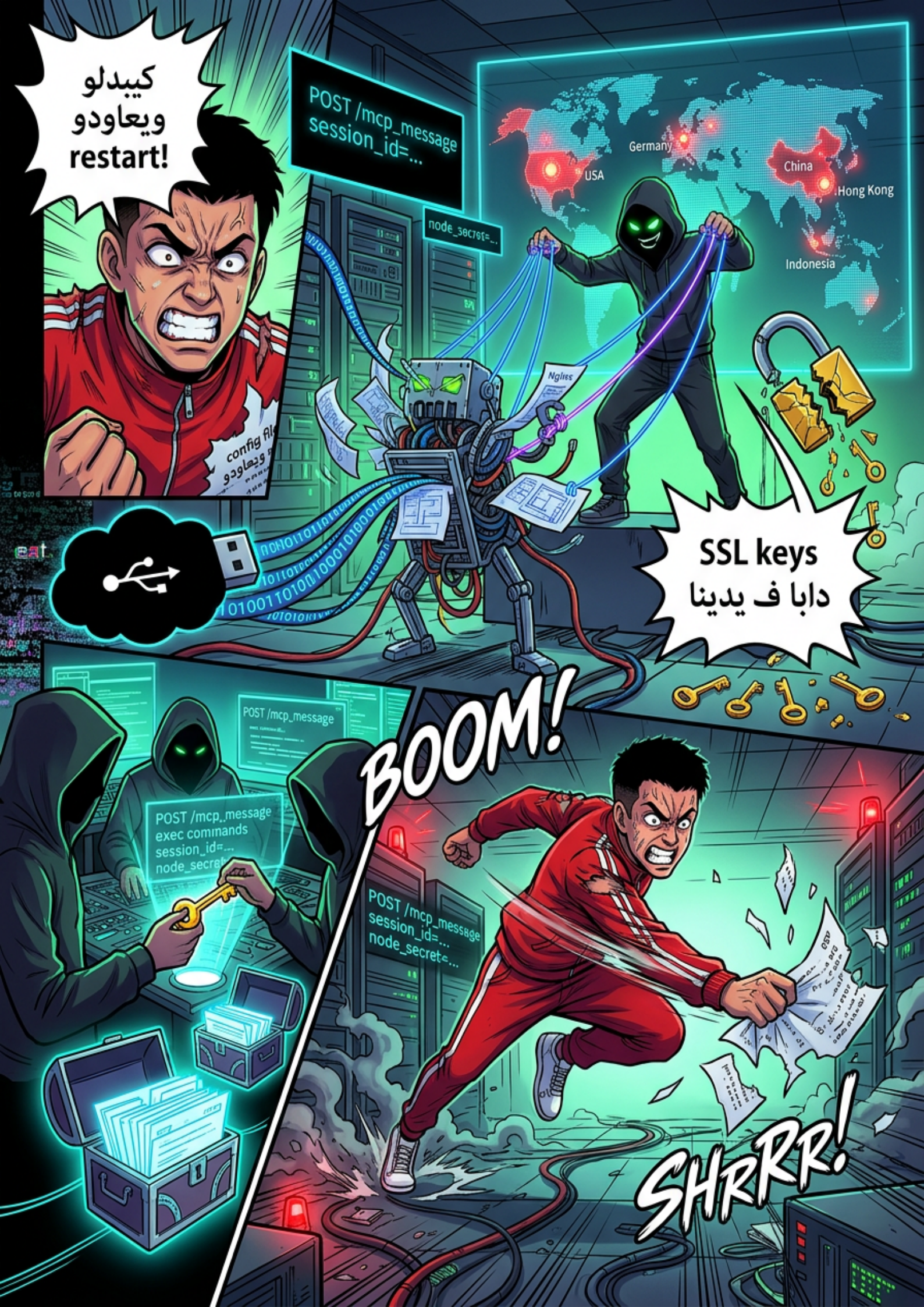
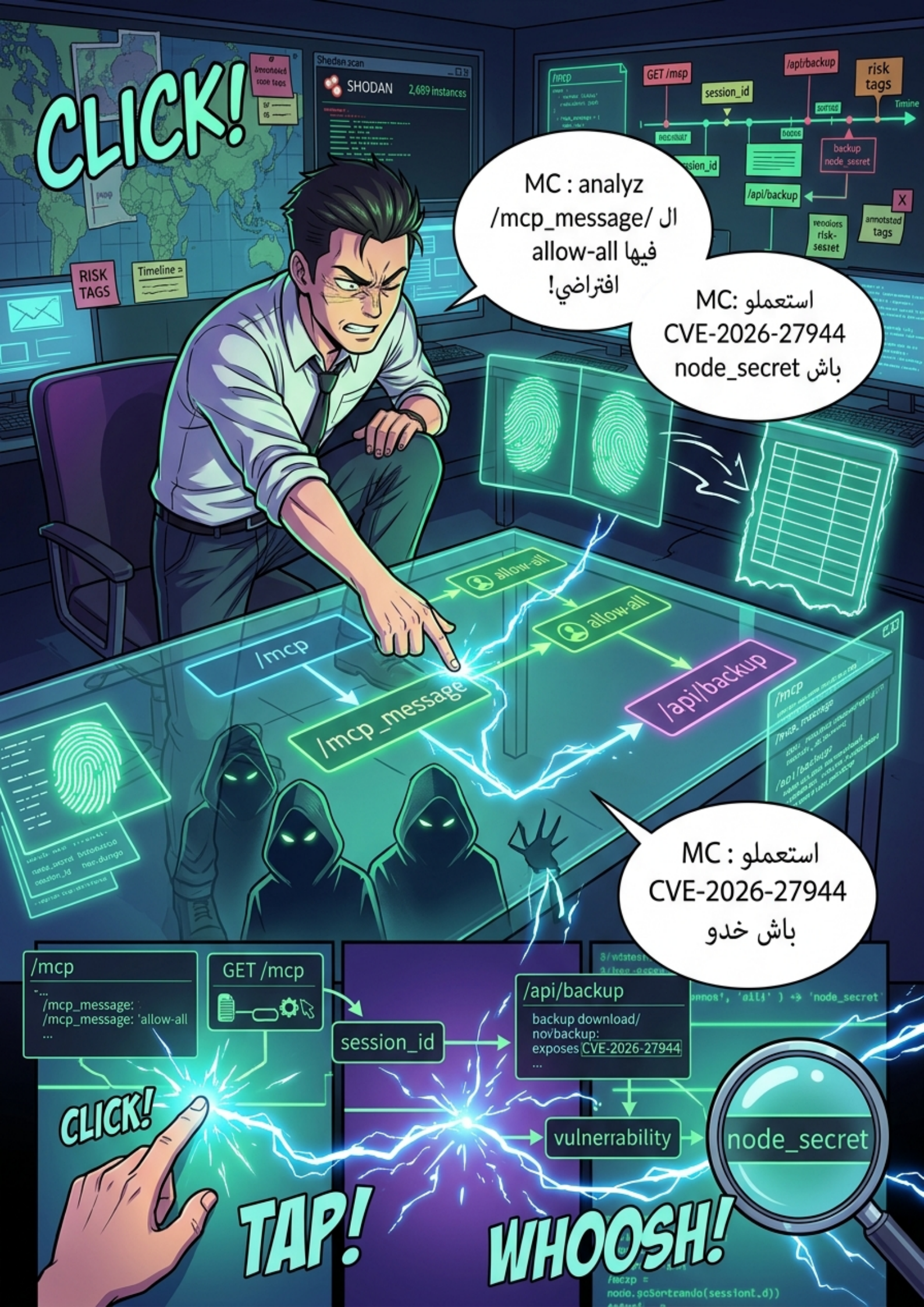
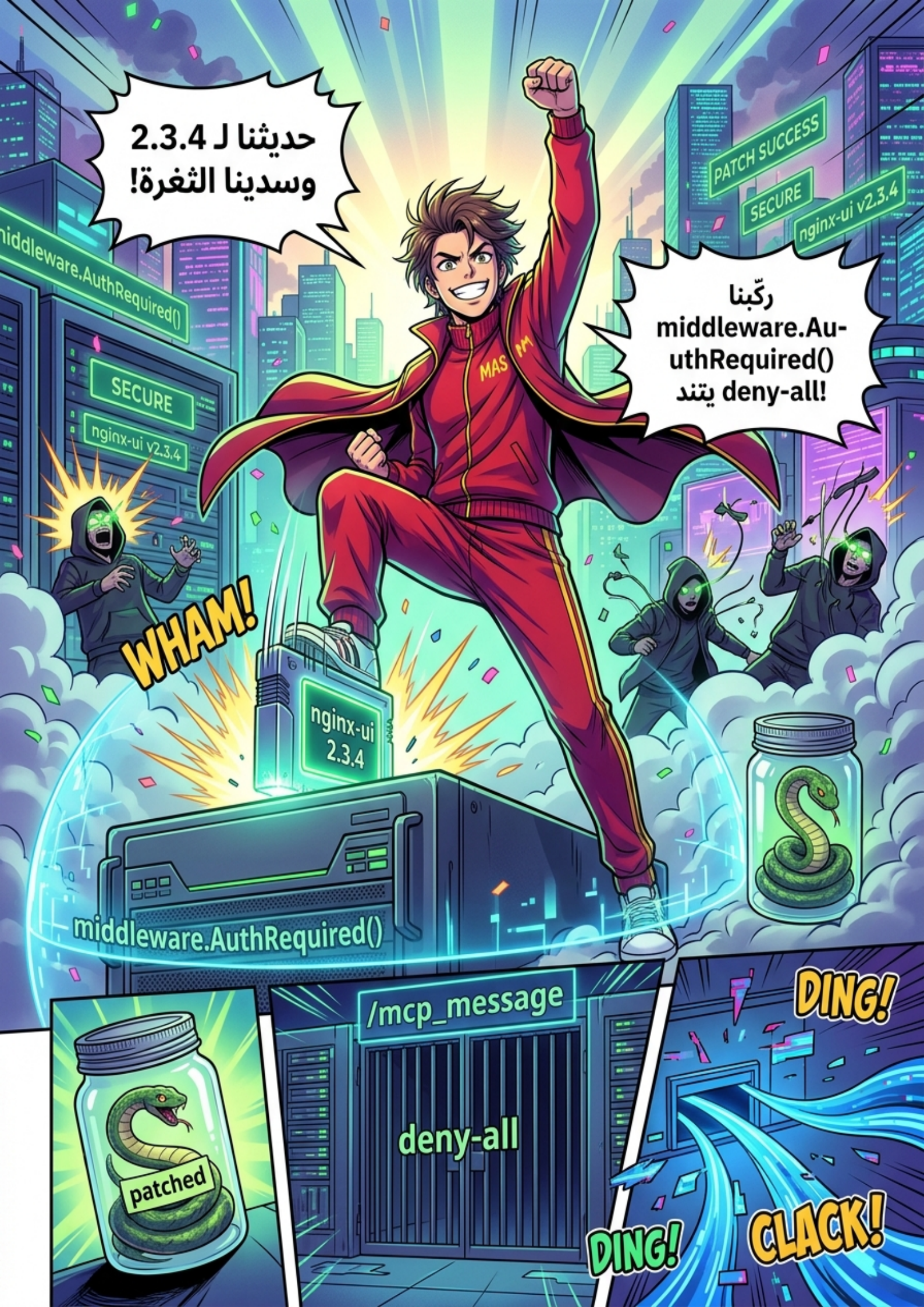

MCPwn — CVE-2026-33032
firewall
/mcp_message
IP whitelist
/mcp
ALLOW ALL
ALARM!
ALERT
CRACK!
MCP (Model Contest Protocol)
⚠ ALERT
/mcp_message
node_secret
session_id
(MC, shocked):
شنو هاد MCPwn؟
CVE-2026-33032!
(sysadmin off-panel,
لازم نحدّث لـ
2.3.4 دابا!
MAS
BZZZT!


كيبدلو
ويعاودو
restart!
POST /mcp_message
session_id=...
node_secret=...
Germany
USA
China
Hong Kong
Indonesia
config file
SSL keys
دابا ف يدينا
POST /mcp_message
POST /mcp_message
exec commands
session_id=...
node_secret=...
BOOM!
POST /mcp_message
session_id=...
node_secret=...
SHRRR!


CLICK!
SHODAN 2,689 instances
RISK TAGS
Timeline
MC : analyz /mcp_message/ ال فيها allow-all افتراضي!
MC: استعملو CVE-2026-27944 باش node_secret
/mcp
/mcp_message
allow-all
allow-all
/api/backup
MC : استعملو CVE-2026-27944 باش خدو
/mcp
/mcp_message: 'allow-all
GET /mcp
session_id
/api/backup
backup download/ nov/backup:
exposes CVE-2026-27944
vulnerrability
node_secret
CLICK!
TAP!
WHOOSH!


حديثنا لـ 2.3.4
وسدينا الثغرة!
middleware.AuthRequired()
SECURE
nginx-ui v2.3.4
PATCH SUCCESS
SECURE
nginx-ui v2.3.4
ركّبنا
middleware.Au-
uthRequired()
يتند deny-all!
WHAM!
nginx-ui
2.3.4
middleware.AuthRequired()
patched
/mcp_message
deny-all
DING!
DING!
CLACK!