

Laporan pentest aktif terbatas — techindo.com

Tanggal penilaian: 10 Oktober 2026 (WITA)
Aset tepat: <https://techindo.com>
Putusan eksekutif: Input q **terbukti membentuk atribut HTML baru** pada og:title, tetapi handler sentinel tidak berjalan saat pemuatan alami Chromium offline dan tidak ada dampak keamanan yang terbukti. Kontrol publik terbaru menolak dua POST API tanpa kredensial dan dua upaya login sintetis; tiga pencarian tidak membuktikan SQL injection. Untuk kegagalan keamanan berdampak pada sampel, validated_control_failures = 0, validated_exploit_chains = 0, dan reportable_findings = 0. Tidak ada P1/P2/P3 atau PoC eksploitasi berdampak yang tervalidasi. F3 memutuskan **NO-GO**, F4 APPROVED = 0, dan tidak ada hop F5. Ini adalah **cakupan origin eksternal yang dibatasi**, bukan pernyataan bahwa situs aman atau audit seluruh aplikasi selesai. Source backend, akun uji pembandingan, dan observasi DB/queue/mail milik pemilik tidak tersedia. [Putusan F3 terbaru](#), [anti-halu independen](#), dan [addendum kontrol publik](#) menjadi dasar pembaruan ini.

Otorisasi, waktu, dan metode

Batas	Rekaman yang diperiksa
Engagement awal	engagement.json , ID tac-1096947517a8, hanya origin di atas, berakhir 2026-10-10T15:59:00Z (23:59 WITA). Tidak mengizinkan POST yang mengubah data produksi.
Engagement lanjutan	engagement-followup-20261010.json , ID tac-da2843605f64, origin dan batas waktu sama; mengizinkan POST sintetis terbatas dengan kewajiban cleanup. Izin ini tidak berlaku surut untuk engagement awal.
HTTP first-party tersimpan	78 request ke origin tepat: 52 di engagement awal (39 GET, 10 HEAD, 3 OPTIONS) dan 26 di engagement lanjutan (14 GET, 12 POST), sehingga total metode 53 GET, 10 HEAD, 12 POST, 3 OPTIONS . Delapan request terbaru menguji API artikel, pencarian, dan login dengan input sintetis. Semua URL request dan URL efektif yang diperiksa tetap pada origin. Angka ini ukuran arsip, bukan bukti tidak ada trafik lain. Anti-halu terbaru .
Pemeriksaan terpisah	Tiga GET HTTP pasif ke penyedia data dns.google (dua) dan crt.sh (satu), terpisah dari 78 HTTP first-party: 81 HTTP lintas semua host pada arsip. Satu handshake TLS dengan SNI dan verifikasi hostname untuk host tepat adalah artefak non-HTTP tersendiri. Lookup pasif tidak memberi izin menguji subdomain/IP yang muncul. Bukti TLS/DNS .
Integritas	427/427 digest cocok pada 13 daftar SHA-256 lokal, 427 path unik. Ini membuktikan konsistensi berkas terhadap daftar lokal, bukan provenance server atau kelengkapan semua aktivitas. Raw preflight TAC untuk 30 request perluasan lama tidak tersimpan terpisah; kronologi preflight bagian itu tidak dapat direproduksi penuh secara independen. Audit anti-halu terbaru .

Fase REDCELL	Status pada bukti ini
F0 otorisasi	Dua engagement membatasi origin, waktu, dan teknik; preflight lanjutan tercatat pada lane terkait.
F1 recon/kontrol	78 HTTP first-party, tiga GET pasif ke penyedia data, dan satu TLS terpisah; POST sintetis hanya pada engagement lanjutan.
F2 intel	NO-MATCH: produk, versi, modul, dan konfigurasi prasyarat CVE belum teridentifikasi. Recheck .
F3 chain	NO-GO , chain siap review 0, hop siap eksekusi 0, termasuk setelah kontrol publik terbaru. Evaluasi ulang .
F4-F5	APPROVED = 0; tidak ada eksekusi hop chain. POST F1 adalah kontrol eksploratif, bukan eksploitasi F5.
F6-F7	Gate menjalankan replay Chromium offline pada lane atribut dan parsing independen pada kontrol publik; anti-halu memeriksa artefak. Gate publik , gate atribut .

Hasil kontrol dan dampaknya

Permukaan	Observasi tervalidasi pada sampel	Status keamanan dan batas dampak
/api/subscribe JSON	Satu POST email sintetis dengan sintaks valid mendapat 201 /success:true; satu sintaks tanpa @ dan satu field email absen masing-masing 422 /success:false. Gate JSON .	Penolakan dua varian invalid Observed . Penyimpanan, email keluar, dan perbaikan menyeluruh atas kandidat F11 Not proven . Arsip ^{manual} terpisah merekam respons berbeda tetapi tidak memuat request POST mentah lengkap; rekonsiliasi .
/api/subscribe form encoded	Satu POST sintetis mendapat 429 /success:false; tidak ada retry/evasion pada lane ini. Gate form encoded .	STOP hanya untuk lane newsletter form encoded . Penyebab 429 dan keputusan validator Unknown . Kontrol GET/CTA dan /panduan yang tidak terkait berjalan kemudian sesuai arsip; 429 tidak menghentikan seluruh audit.
/api/cta-event	Dua POST JSON dengan cta_id bertipe string dan array masing-masing 204 dengan body kosong. Kontrol F1 .	Penerimaan HTTP Observed ; record analytics, pembaca record, atau kerusakan keputusan bisnis Not proven .
/panduan	GET form dan dua POST sintetis masing-masing 200 . form_ts ada pada respons skor 25/100 , dan dihilangkan pada respons skor 0/100 ; marker nama/email juga berbeda di antara dua POST. Gate form .	Perbedaan respons Observed . Sebab skor tidak terisolasi; status 200/skor 0 tidak membuktikan bypass CSRF, penolakan aman, penyimpanan kontak, atau pengiriman notifikasi.

Permukaan	Observasi tervalidasi pada sampel	Status keamanan dan batas dampak
/cari?q=	Dua GET lama menunjukkan og:title malformed. Dua GET baru dengan atribut inert versus handler sentinel masing-masing 200, tanpa 406/429/redirect. Parser HTML5 dan DOM Chromium offline menunjukkan q membentuk atribut onload pada <meta property="og:title"> hanya pada varian event: HTML attribute injection valid . Sentinel tetap false setelah load alami pada rekaman F1 dan replay gate. Addendum , gate .	Cacat encoding atribut Observed , tetapi eksekusi JavaScript, XSS, open redirect, dan efek keamanan Not proven . file:// tidak menerapkan header CSP live; pengujian ini tidak membuktikan CSP memblokir atau membolehkan eksekusi di situs live. Source template dan versi runtime belum tersedia.
/api/artikel	Dua POST JSON tanpa kredensial memakai body sintetis tidak valid yang identik; perubahan hanya header X-Forwarded-For loopback. Keduanya 401 dengan body respons identik, tanpa ID objek atau redirect. Gate publik .	Tidak ada bypass autentikasi atau bukti penulisan objek pada sampel. Log atau efek samping internal tetap Unknown tanpa pemeriksaan pemilik.
/cari kontrol boolean	GET baseline ai menampilkan 33 artikel ; dua varian AND dan OR masing-masing 0 hasil , semuanya 200 tanpa error SQL yang tampak. Gate publik .	Perbedaan hasil Observed ; tidak ada diferensial boolean yang membuktikan eksekusi SQL. SQLi Not proven , dan tiga sampel tidak membuktikan seluruh query aman.
/admin/login	GET form, lalu dua POST memakai kredensial sintetis dan cookie yang sama, masing-masing dengan token _csrf yang cocok atau tanpa field token. Keduanya 200 dan tetap menampilkan form; pesan menunjukkan penolakan kredensial versus penolakan request. Tidak ada redirect atau cookie sesi baru pada respons POST. Gate publik .	Tidak ada login admin atau bypass CSRF pada sampel. Status 200 bukan sesi berhasil; kontrol CSRF pada aksi lain Not verified .
/token-ai/hitung	Tiga GET kontrol 200 menghasilkan nilai render/fallback berbeda untuk parameter jobs yang berbeda. Kontrol F1 .	Output kalkulator publik bukan bukti harga tagihan, transaksi, atau perubahan state finansial.
Auth lintas akun, BOLA/IDOR, injection lain, SSRF	Kontrol login sintetis di atas ditolak; tidak ada dua sesi pembandingan, source sink backend, atau endpoint baca data privat yang tervalidasi. Matriks cakupan , gate publik .	Dampak akses lintas akun, query/command sink, fetch server-side, dan alur privilege lain belum dapat dinilai . Tidak ada finding untuk kelas tersebut dari sampel ini.
WordPress, file/config, CORS/cache, TLS/subdomain	Path WordPress standar yang diuji memberi 404; beberapa path file memberi 403/404/406 tanpa file rahasia terunduh; root publik tidak membuka ACAO/ACAC pada satu kontrol; satu handshake TLS exact-host lulus. Matriks cakupan .	Tidak membuktikan WordPress absen, file lain aman, kebijakan endpoint privat, atau konfigurasi TLS menyeluruh. Tidak ada match CVE tervalidasi karena versi deployment tidak diketahui; freshness advisory untuk server ini Not verified .

Caido: koneksi MCP lokal/proyek berstatus siap dan HTTPQL menunjukkan 0 request tersimpan karena capture audit sebelumnya memakai curl; tidak ada Caido Replay atau scan yang dijalankan ([catatan koneksi](#)).

Keputusan triage dan tindakan pemilik

Respons HTTP 200/201/204/401, skor berbeda, 429, dan atribut HTML baru tidak mengisi rangkaian **PRODUCT-CONTROL → STATE-CHANGE → POST-CHANGE-CALL → EFFECT**. Tidak ada eksekusi alami pada kontrol atribut atau postcondition owner-side yang menunjukkan record tercipta/dikonsumsi, akses data tanpa izin, atau efek keamanan. Dua penolakan API dan dua penolakan login juga tidak mengesahkan kontrol di luar input ini. Karena itu injeksi atribut adalah **cacat markup valid yang perlu diperbaiki**, sedangkan XSS/chain dan kandidat lain **belum menjadi temuan kerentanan siap lapor**; tidak ada CVSS, root cause kode, jumlah korban, atau patch yang dapat dinyatakan tanpa source dan efek. [Gate chain terbaru](#).

Cleanup masih pending pada lima lane POST sintetis: newsletter JSON, newsletter form encoded, CTA, /panduan, dan kontrol publik terbaru. Marker lengkap dibatasi dalam ../evidence/subscribe-followup-20261010/owner-cleanup.json, ../evidence/subscribe-urlencoded-20261010/owner-cleanup.json, ../evidence/active-get-controls-20261010/owner-cleanup.json, ../evidence/panduan-active-controls-20261010/owner-cleanup.json, serta ../evidence/public-controls-20261010/owner-cleanup.json; nilainya sengaja tidak disalin ke laporan. Pemilik perlu mencari **hanya marker tepat** secara privat pada DB subscriber/assessment/analytics/artikel, mailing list, antrean email, dan log API/login yang relevan; catat hasil sebelum/sesudah, hapus **hanya** record sintetis yang ditemukan, lalu verifikasi cleanup. Keberadaan record atau efek samping internal masih **Unknown** dari respons HTTP, termasuk pada POST API 401 dan login yang ditolak.

Sesudah itu, pemilik dapat menyerahkan source/konfigurasi **sesuai deployment**, handler dan sink untuk newsletter, CTA, /panduan, pencarian, kalkulator, /api/artikel, serta login admin, berikut inventaris versi/modul. Audit input → validasi/encoding/otorisasi → sink; periksa urutan auth sebelum penulisan API dan pemeriksaan token pada login. Cocokkan advisory primer dengan rentang versi terdampak sebelum menilai CVE. Untuk auth/IDOR/CSRF atau perubahan state, gunakan dua akun uji dan fixture sintetis di lab dengan kontrol yang berbeda **hanya pada satu variabel**, pembacaan state sebelum/sesudah, post-change call, serta rollback. **Perbaiki pembentukan seluruh nilai atribut** og:title agar input tidak dapat membentuk atribut baru; contoh bersyarat dan uji regresi ada pada [addendum atribut](#). Ini rekomendasi untuk cacat markup, bukan patch yang telah diterapkan atau remediation finding XSS. Tidak ada kode yang dipatch pada audit ini.

Verifikasi artefak lokal tanpa trafik target (membaca hash saja; tidak mencetak isi bukti):

```
Artefak evidence diperiksa menggunakan SHA-256 terhadap daftar hash arsip.
Verifikasi menghitung ulang hash setiap berkas dan membandingkannya dengan nilai yang dicatat.
Hasil historis akhir: 427/427 hash cocok pada 13 daftar lokal.
Pemeriksaan ini hanya membaca artefak; tidak mengirim trafik ke target.
Hash membuktikan konsistensi berkas, bukan provenance server atau seluruh aktivitas.
Path workstation dan tautan berkas privat tidak disertakan dalam salinan publik.
```

Catatan kronologi: angka 70 request dan 370 hash pada lampiran atribut adalah snapshot sebelum kontrol publik terakhir. Total akhir yang berlaku ada pada laporan utama: 78 request first-party dan 427/427 hash.

Addendum pentest aktif — injeksi atribut pada /cari?q=

Tanggal: 10 Oktober 2026 (WITA)
Aset dan izin: <https://techindo.com> saja; [engagement lanjutan](#) ID tac-da2843605f64 berlaku hingga 2026-10-10T15:59:00Z (23:59 WITA). Addendum ini menilai lane F1/F6 yang telah selesai, tanpa trafik target baru. [Laporan utama](#) memuat cakupan lainnya.

Putusan

HTML attribute injection pada `<meta property="og:title">` **tervalidasi pada dua respons tersimpan:** input pencarian q dapat membentuk atribut onload dalam DOM. Namun handler sentinel **tidak berjalan** saat load alami Chromium offline pada rekaman F1 maupun replay gate independen. Tidak ada akses data, perubahan state, atau efek keamanan yang terbukti. Karena itu **XSS dan severity keamanan belum terbukti**, `validated_control_failures=0`, `validated_exploit_chains=0`, dan `reportable_findings=0` untuk kegagalan keamanan berdampak dalam sampel. F3 **NO-GO**, chain/hop siap review 0, F4 `APPROVED=0`, F5 tidak dijalankan. [Gate F6](#), [anti-halu](#), [re-evaluasi F3](#).

Bukti dan batas metode

Pemeriksaan	Hasil yang didukung
Asal lane	Form first-party menunjuk GET /cari?q=; respons sebelumnya menempatkan bagian q di metadata <code>og:title</code> yang terpotong. Ini memberi hipotesis atribut yang diuji dengan kontrol inert dan handler sentinel tanpa eksfiltrasi. Prioritas intel , recon .
Preflight dan request	TAC raw <code>allowed:true</code> dan preflight tercatat sebelum dua GET baru ke origin tepat; keduanya 200, <code>curl_exit=0</code> , URL efektif sama, tidak mengikuti redirect, tanpa 406/429/Location. Jeda awal sekitar 1,623 detik; semua sebelum expiry. Gate , preflight.json , manifest.json . Ini dua sampel, bukan cakupan seluruh variasi q; 406 Mod_Security pada arsip lain bukan bukti bypass WAF di lane ini.
Source HTML dan DOM	Parser HTML5 membaca satu meta[property="og:title"] per respons, dengan nilai content terpotong pada prefiks tetap. Kontrol inert membentuk atribut tambahan biasa; varian event membentuk onload berisi assignment sentinel lokal. Tidak ada URL sink, node script, atau meta refresh yang memuat marker pada dua body. Analisis DOM , gate . Mekanisme source/template server belum diketahui.

Pemeriksaan	Hasil yang didukung
Eksekusi browser	Chromium headless 150 memuat salinan byte-identik melalui file:// dengan jaringan eksternal diblokir; tanpa dispatch event manual. Sentinel tetap false pada kontrol inert dan event, termasuk replay independen F6. Rekaman browser , gate . Hasil negatif berlaku untuk handler/elemen/sampel ini; tidak menguji semua event atau browser live.
CSP	Salinan file:// tidak menerapkan header CSP respons live . Karena situs tidak dibuka live dalam browser pada lane ini, bukti tersebut tidak menetapkan apakah CSP live memblokir atau mengizinkan eksekusi.
Integritas dan total	Lane baru 25/25 hash cocok; 12 daftar akhir seluruh arsip 370/370 path unik cocok. Total HTTP first-party menjadi 70 (49 GET, 10 HEAD, 8 POST, 3 OPTIONS): 52 pada engagement lama, 18 pada engagement lanjutan. Tiga GET HTTP DNS/CT pasif ke penyedia data terpisah, sehingga 73 HTTP lintas semua host ; satu handshake TLS exact-host adalah non-HTTP tersendiri. Hash lokal tidak membuktikan provenance server atau kelengkapan trafik. Anti-halu .

Temuan ini adalah **cacat encoding output yang dapat diperbaiki**, bukan XSS yang telah dieksekusi. Tuple PRODUCT-CONTROL → STATE-CHANGE → POST-CHANGE-CALL → EFFECT berhenti pada kontrol q dan atribut DOM. Raw TAC preflight untuk 30 request perluasan lama masih tidak tersimpan terpisah; arsip baru tidak menutup gap historis tersebut. Cleanup owner pada **empat lane POST sintetis sebelumnya** tetap pending dan dibatasi ke ../evidence/{subscribe-followup-20261010,subscribe-urlencoded-20261010,active-get-controls-20261010,panduan-active-controls-20261010}/owner-cleanup.json; lane dua GET ini tidak membuat record sintetis. Pemilik harus mencari marker tepat secara privat, menghapus hanya record uji yang ditemukan, dan mencatat bukti sebelum/sesudah, tanpa menyalin nilainya ke laporan.

Perbaikan dan verifikasi pemilik

Telusuri pembentukan og:title pada source **yang benar-benar terpasang**. Bentuk judul lengkap sebagai satu string, lalu encode **sekali** ketika ditempatkan ke nilai atribut content; pertahankan encoding dokumen yang sesuai. **Contoh bersyarat bila template deployment adalah PHP dengan UTF-8** (bukan klaim bahasa/server, lokasi root cause, atau patch produksi):

```
$title = 'Hasil pencarian "' . $query . '"' | Techindo';
echo '<meta property="og:title" content="'
    . htmlspecialchars($title, ENT_QUOTES | ENT_SUBSTITUTE, 'UTF-8')
    . '">';
```

htmlspecialchars dengan ENT_QUOTES mengubah kedua jenis tanda kutip, sedangkan ENT_SUBSTITUTE menangani urutan UTF-8 tidak valid; lihat [manual resmi PHP](#), diperiksa 10 Oktober 2026. Manual mencantumkan API untuk PHP 4–8 tetapi tidak memberi tanggal pembaruan spesifik pada halaman yang diperiksa; **versi PHP deployment Not verified**. Contoh ini berlaku hanya jika template itu memang PHP dan nilai judul memakai UTF-8. Uji regresi di lab pemilik dengan parser/browser: meta[property="og:title"].getAttribute('content') harus berisi **seluruh judul yang diharapkan** dan elemen itu tidak boleh memperoleh atribut tambahan dari q. Jika evaluasi XSS dilanjutkan, gunakan lingkungan lab yang meniru header CSP live, natural event, kontrol negatif, dan efek yang dapat diamati sebelum membuat klaim keamanan.

Addendum pentest aktif — kontrol API, pencarian, dan login

Tanggal penilaian: 10 Oktober 2026 (WITA)
Origin dan izin: <https://techindo.com> saja; [engagement lanjutan](#) ID tac-da2843605f64, berlaku hingga 2026-10-10T15:59:00Z (23:59 WITA). Ini laporan lane **delapan request** TASK 084, bukan pengujian seluruh aplikasi. [Laporan utama terbaru](#) memuat angka kumulatif; [addendum atribut](#) adalah snapshot lane sebelumnya.

Hasil dan putusan

Kontrol dan bukti	Observasi terverifikasi	Batas keamanan
Dua POST JSON /api/artikel tanpa kredensial, body sintetis sengaja tidak valid, baseline versus satu header X-Forwarded-For loopback	Kedua request body identik dan kedua respons 401 identik, tanpa ID objek atau redirect. Gate F6 , recon F1 .	Bypass autentikasi tidak terjadi pada sampel. Tidak ada pembuktian penulisan artikel; log atau efek samping backend masih Unknown tanpa akses pemilik.
Tiga GET /cari: query dasar versus varian AND dan OR	Baseline menampilkan 33 artikel ; masing-masing varian 0 hasil , semuanya 200 tanpa error SQL yang tampak. Gate F6 .	Pencarian literal masuk akal; tidak ada diferensial boolean yang membuktikan SQL injection. Source query/sink belum tersedia, sehingga SQLi Not proven dan keamanan seluruh query tidak disimpulkan.
GET /admin/login, lalu dua POST dengan kredensial sintetis dan cookie GET yang sama, token _csrf ada versus dihilangkan	Kedua POST 200 tetapi form login tetap tampil. Respons pertama menolak kredensial; respons tanpa token menolak request. Tidak ada redirect atau cookie sesi baru pada respons POST. Gate F6 .	Tidak ada login admin atau bypass CSRF pada sampel. Status 200 bukan keberhasilan. Efektivitas CSRF pada kasus/aksi lain Not verified .

Delapan request: **2 POST API + 3 GET pencarian + 1 GET/2 POST login** pada origin tepat. Raw TAC preflight menyatakan allowed:true; preflight 2026-10-09 21:01:11 UTC mendahului request pertama. Semuanya sebelum expiry, curl_exit=0, URL efektif sama, tanpa redirect follow. Urutan status **401, 401, lalu enam 200; tidak ada 406, 429, 5xx, 3xx, atau** Location pada lane ini. Bukti: [preflight.json](#), [manifest.json](#), [gate](#). Ini hanya membuktikan delapan artefak yang diberikan, bukan ketiadaan trafik lain.

Tidak ada path file/config yang terbukti dapat dibaca: arsip lama hanya memiliki status 403/404/406 tanpa isi rahasia. Lane ini juga tidak menemukan parameter redirect atau sink fetch server-side untuk SSRF. Karena itu tidak dibuat klaim eksposur file, open redirect, atau SSRF dari status/field permukaan. [Gate F6](#).

Verdict: validated_control_failures=0, validated_exploit_chains=0, reportable_findings=0 untuk kegagalan keamanan berdampak pada sampel ini. [F3 terbaru NO-GO](#), chain/hop siap review 0, F4 APPROVED=0, F5 tidak dijalankan. Tidak ada root cause kode, affected population, atau severity yang dapat dipertanggungjawabkan. Penolakan tiga kontrol ini tidak menyatakan situs aman.

Total arsip, cleanup, dan tindak lanjut pemilik

Kumulatif kini **78 HTTP first-party** (52 engagement awal + 26 lanjutan; **53 GET, 10 HEAD, 12 POST, 3 OPTIONS**), ditambah **3 GET HTTP pasif** ke penyedia data DNS/CT yang terpisah (**81 HTTP lintas semua host**) dan **1 handshake TLS** non-HTTP. Daftar SHA-256 akhir **427/427** cocok pada 13 daftar lokal; lane ini **57/57**, preflight **5/5**. Hash lokal hanya membuktikan konsistensi berkas, bukan provenance server atau seluruh aktivitas. [Anti-halu independen](#). Gap raw preflight TAC untuk 30 request perluasan awal tetap ada.

Cleanup owner pending pada lima lane POST sintetis: newsletter JSON, newsletter form encoded, CTA, /panduan, dan lane kontrol publik ini. Penanda yang tepat berada dalam berkas terbatas `../evidence/{subscribe-followup-20261010,subscribe-urlencoded-20261010,active-get-controls-20261010,panduan-active-controls-20261010,public-controls-20261010}/owner-cleanup.json`; nilainya tidak disalin di sini. Pemilik perlu mencocokkan marker secara privat pada DB, queue, mailing list, dan log API/login yang relevan, lalu mencatat bukti sebelum/sesudah serta menghapus **hanya** record uji yang ditemukan. Jangan menganggap POST API 401 atau login yang ditolak pasti menciptakan maupun tidak menciptakan catatan internal.

Untuk penilaian lanjutan, pemilik perlu menyerahkan source/config deployment yang cocok untuk urutan autentikasi dan penulisan `/api/artikel`, query pencarian, serta validasi CSRF login. Sediakan akun uji dan fixture sintetis di lab untuk kontrol permission dan state sebelum/sesudah. Tidak ada patch kode atau pengujian target tambahan dari penyusunan addendum ini. Caido terhubung secara lokal, tetapi tidak ada Replay/scan yang dijalankan pada audit ini ([catatan koneksi](#)).

Verifikasi lokal tanpa trafik target:

```
cd ../evidence/public-controls-20261010
sha256sum -c PREFLIGHT_SHA256SUMS
sha256sum -c SHA256SUMS
```