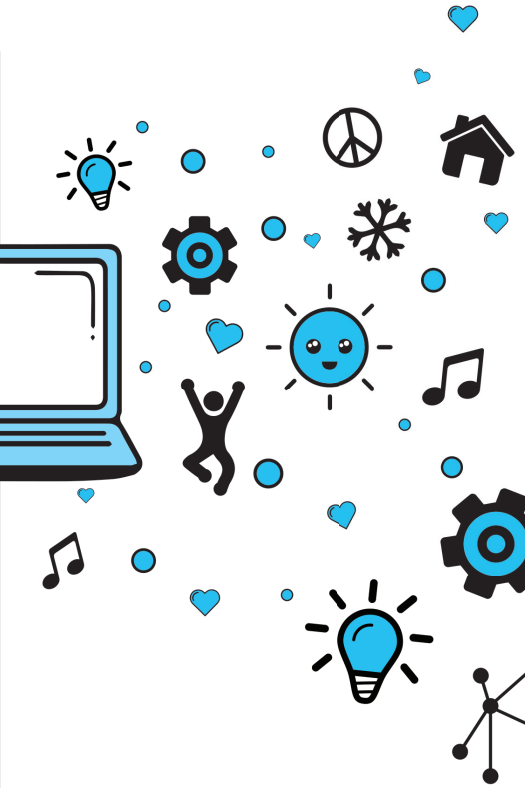
etik web geliştirme



ETİK WEB SİTE GELİŞTİRME VE BAKIM KILAVUZU

EDRi
EUROPEAN DIGITAL RIGHTS

Türkçesi : alternatif bilişim

Güvenlik aslında oldukça basittir. Karmaşık olan şey bir ihlalden sonraki temizliktir.

Sitenizi ziyaret edenler saygıyı hak ediyor. Bu da onların bilgilerinin üçüncü şahıslara sızdırılmasına sebep olan özensizlikleri yapmamak ve yeterli güvenliği sağlamak anlamına geliyor.

Sitenizi ziyaret edenlere saygı göstermek aynı zamanda veri koruma mevzuatlarına uymaya yönelik büyük bir adım atma anlamına da geliyor.

Bu yayın, EDRi ağı uzmanlarının (Anders Jensen-Urstad, Walter van Holst, Maddalena Falzoni, Hanno "Rince" Wagner, Piksel), dış destekçilerin (Gordon Lennox, Achim Klabunde, Laura Kalbag, Aral Balkan) ve Public Interest Technology ve EDRi'de eski Ford-Mozilla üyesi Sid Rao'nun çok önemli katkılarıyla birlikte kapsamlı kolektif bir çalışmanın sonucudur. Bu kılavuz fikrinin sahibi ve süreci başarılı bir şekilde yöneten Joe McNamee'ye de özel teşekkürler..

Proje Koordinasyonu: Guillermo Peris, Topluluk Koordinatörü, EDRi

Tasarım: Heini Järvinen, Kıdemli İletişim Müdürü, EDRi

Türkçe broşürün çevirisi Gülüm Şener ve Sinan Aşçı, grafik işleri Himmet Doğan tarafından yapılmıştır.

European Cultural Foundation (Avrupa Kültür Derneği) desteğiyle basılmıştır.

European Cultural Foundation

İçindekiler

0. Sunuş

Bir web sitesi neredeyse bir canlı gibidir. Çoğunlukla, sitenin kendisi statik değildir ve dinamik özelliklerine ek olarak, sitenin çevresi de sürekli değişime uğrar. Bu durum da daha fazla değişikliğe yol açar.

Bir web sitesini ziyaret edenler de çok çeşitli olabilir. Kullandıkları teknolojiler ve uzmanlıkları oldukça çeşitlidir.

Birçok web sitesi de çeşitli harici hizmetlere ve kaynaklara bağlıdır. Onlar da gelişmeye devam eder.

Web geliştiricileri, kullanıcıların artan beklentileri ve birçok organizasyonun web site geliştirmeye ayırdığı sınırlı kaynak sorunuyla uğraşırken, dış kaynak ve servisler kullanma eğilimi artmaktadır.

Örneğin, site geliştiricilerinin, "bedava" olan yazı tipi ve betik gibi kaynakları almaları ve onları tasarladıkları web sitelerinde kullanmaları giderek daha da yaygınlaşmaktadır. Bunlar site geliştiriciler için "bedava" olsa da, kullanıcılar ve sitenin sahibi kuruluş için istenilmeyen yan etkileri olabilir. Örneğin, bazı kaynaklar ve servisler, özellikle de bilgi oburu internet şirketleri tarafından sağlananlar, kişisel veri gizliliğinin altını oyabilirler. Başka servisler ise güvenlik üzerine olumsuz etkilere sahip olabilir. Her iki durumda da site sahiplerinin itibarı zarar görebilir, hatta yasal zorluklarla bile karşılaşılabilir.

İşte buna dikkat etmek gerekir. Fakat bu sorunla ilgili farkındalık genel olarak azdır ve bu tür uygulamalar çoktan yaygınlaşmıştır bile. Bu metnin amacı, sorunları açıklamak ve mümkün olduğu kadar kullanışlı çözümler ortaya koymaktır.

Bu rehber, teknik konseptlere güçlü şekilde hâkim olan web geliştiricileri ve bakımcılarını hedeflemektedir. Dokümanı kısa ve öz tutup kullanılabilirliğini arttırmak adına, gerekli yerlerde arkaplan bilgileri için linkler yer almaktadır.

Umuyoruz ki, bu rehber geliştiricileri ve bakımcıları Web'i özüne; yani temel hakları, demokrasiyi ve ifade özgürlüğünü arttıran, merkezi olmayan bir araca, geri döndürmelerine yardımcı olacaktır.

Bu bizim de İnternetimiz. Hepimiz sorumluluk almalıyız.

1. Giriş

BEKLENTİLER

Bir web sitesinin ziyaretçileri, bir dizi haklı beklentilere sahiptir.

Güvende olmak isterler. Cihazlarına ya da cihazları üzerindeki bilgilere bir zarar gelmesini istemezler. Gizliliklerine saygı duyulmasını isterler. Bu gerekliliklerden bazıları AB'nin Genel Veri Koruma Tüzüğü (GDPR) gibi yasal düzenlemelerde ele alınmıştır.

Daha önceleri, bu mesele teknik olarak yalın ve güvenilir bir hizmet olmaktan ibaretti. Ama bir miktar bozuk, kullanışsız ve öngörülemeyen bir hizmet, kullanıcıların, bu hizmetin temel beklentileri karşılamayacağını kabul etmek zorunda oldukları anlamına gelir. Siteyi kullanmaya devam etmeyebilirler. Ama bu durumda daha da önemlisi, eğer hizmeti kullanmaya devam etmeye karar verirlerse, hoş görmemeleri gereken önemli problemleri idare etmek zorunda kalacaklardır.

GÜVENİRLİK VE GÜVENLİK

Mevcut sosyal ve siyasal iklimde, çoğu insan doğruluk ve güvenirlik hakkında endişeli. Bir kullanıcı siteden indirilen bir yazılıma ne kadar güvenmelidir? Site üzerinde sağlanan linklere ne kadar güvenmelidir?

Ve her daim genelgeçerimiz: güvenlik. Eğer "emniyet", bir sistemin zarar vermeyeceğinden emin olmaksa, "güvenlik" de sistemi kaza veya saldırı sonucu zarara uğramaktan korumaktır. Yani elimizdeki üçlü takım şunlardan oluşur: erişilebilirlik, bütünlük ve gizlilik. Sistem bileşenlerinin hatalarına, dağıtık hizmet engelleme (DDoS) veya başkaca saldırılara rağmen sistemler, servisler ve veriler erişilebilir olmalıdırlar. Hizmet ve veri bütünlüğünü korumak için önlemler alınmalıdır. Hasar görmüş bir veritabanı, bir veritabanı olarak hala kullanışlı mıdır? Veriler tabii ki sadece gerekli hakları olan kişilere görünür olmalıdır.

KİŞİSEL VERİLER VE GENEL VERİ KORUMA TÜZÜĞÜ'NE UYUMLULUK

Avrupa Birliği'ndeki kuruluşlar (ya da hedef kitlesi AB vatandaşları olan kuruluşlar) Avrupa Birliği'nin Genel Veri Koruma Yönetmeliği'ne (GDPR) uymak zorundadır. AB içerisindeki bütün bireylerin (veya AB şirketlerinin) verilerinin

korunması ve kişisel gizlilikleri üzerine olan bu yönetmelik, bireylere kendi verilerinin üzerinde kontrol hakkı vermeyi ve bu kontrolün yapılacağı ortamı basitleştirmeyi amaçlar. Ayrıca kişisel verilerin AB dışına aktarılmasıyla da ilgilenir.

Fakat GDPR karmaşık bir yönetmeliktir. Bu konuda danışmanlık, eğitim, yorumlama rehberleri ve kontrol listesi hizmetleri sunan birçok şirket vardır. Buna ek olarak, AB üyesi her ülke kendisine ait, yorumlama ve yaptırım konularında sorumluluk sahibi veri koruma kurullarına sahiptir.

Kişisel Veriler (ayrıca ABD'de, biraz farklı anlam taşıyan, PII olarak anılan Kişisel Olarak Tanımlanabilir Bilgiler) kimliği belirlenmiş veya belirlenebilecek gerçek kişi ('veri öznesi') hakkında herhangi bir bilgi demektir. Kimliği belirlenebilir gerçek kişi, dolaylı veya dolaysız olarak, bir isim, kimlik numarası, konum verisi, çevrimiçi bir belirteç veyahut daha çok fiziksel, psikolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğine ait bir veya daha çok faktörle kimliği belirlenebilen kişidir.

GDPR'ye göre IP adresi kişisel bir veridir. Bunun sebebi, IP adresinin başka bilgilerle bağlantılı olduğunda bir insanla eşleştirilebilmesidir. Bazı işlevler için kullanılan üçüncü parti çözümler veyahut üçüncü taraflarca kullanılan Javascript veya görsel içerikler, web site ziyaretçesinin IP adresini o üçüncü parti sağlayıcılara açık hale getirebilir. Bu sebeple, GDPR nazarında, üçüncü parti sağlayıcılarının her biriyle veri işleme anlaşması yapmak gerekebilir. Varsayılan gizlilik, çeşitli düzeylerde veri işlediğiniz bir hizmet sağlıyorsanız, o hizmetin varsayılan ayarlarının gizliliğe en çok önem veren ayar olması anlamına gelir. Kullanıcıya bu ayarı istedikleri takdirde değiştirme seçeneği sunulabilir. Bunun olabilecek en kullanıcı dostu biçimde yapılması gerekir.

Her halükârda, veri özneleri kendi verileri üzerinde hak sahibidir. Ve hizmet veren kuruluşların, güvenlik kazaları veya veri sızıntısı olduğunda belirli sorumlulukları vardır.

Bu sebeple GDPR'a uyumluluk uzmanlık gerektiren bir alandır. Yine de, bu metindeki prensiplere sadık kalmak yasal uyumluluğa doğru bir adım atmak anlamına geldiği gibi etik olarak da uygun bir yaklaşım olacaktır. Buna ek olarak, birçok ücretsiz kaynak, sizin için ve web sitenizin ziyaretçileri için iyi bir şey olan uyumluluğu güvene almak için erişime hazırdır. Örneğin Avrupa Veri Koruma Denetmeninin web hizmetleri rehberine bakabilirsiniz:

https://edps.europa.eu/data-protection/our-work/publications/guidelines/web-services_en

2. Genel Öneriler

- Veri işlemeyi, mümkün olduğu kadar bireylerin kendi cihazları üzerinde yapmasını sağlayın.
- Kullanıcı verisiyle iş yapacağınız zaman şifreleme kullanın. İlgili tüm iletişimler için uçtan uca (end-to-end) şifreleme sağlayın. Bunun amacı kişisel verilerin kolayca görünmemesidir.
- Mümkün olduğunda veri azaltma yöntemleri kullanın. Sadece işlem görmesi gereken veriyi işleyin.
- En iyi çözümler sık sık birinci parti kaynak kullanmak (yani sizin yönettiğiniz kaynaklar) ve olabildiği kadar üçüncü parti çözümlerden kaçınmaktır. Bir başka deyişle, her şeyi kendi sunucunuzda yönetmeye çalışın. Buna üçüncü parti kod ve içerikler de dahildir. Örneğin:
  - Çerezler (Cookies)
  - CSS dosyaları
  - Görseller
  - Görüntü ve ses dosyaları gibi medyalar
  - JavaScript (kullanmayı tercih ediyorsanız)
  - Üçüncü parti içeriğe sahip çerçeve (frame / iframe)
  - Yazı tipi dosyaları (İhtiyaç duyarsanız)
- Eğer JavaScript veya yazı tipi dosyası gibi bir kaynağın indirilmesi sağlayıcısı tarafından engelleniyor, üçüncü parti şeklinde kullanılmaya zorlanıyorsa, o sağlayıcılar gizlilik dostu değildir ve onlardan kaçınılmalıdır. Eğer üçüncü parti kaynakları yüklemeniz gerekirse, Alt-Kaynak Bütünlüğü (Kıs.: SRI; İng.: Subresource Integrity) kullanımı iyi bir fikir olabilir.

Detaylar için: https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

3. Güvenlik Önerileri

Güvenlik bir süreçtir ve her şeyi kapsamak zorundadır. Güvenlik kararları alınırken, değişen ve potansiyel olarak çelişebilen hedefler dikkate alınmalı, bütüncül bir yaklaşım sergilenmelidir. Güvenliğe dair kararlar, bir servisin hızı ve kullanıcı dostu olması gibi özelliklerini etkileyebilir ve ihtiyaç duyulan kaynaklar –yani harcanan para ve emek zamanı– konusunda büyük etkileri olabilir.

Genel olarak, şunları başarabilmelisiniz:

- Siteniz internetin geri kalanı için zarar kaynağı olmamalı,
- Sitenizin bütünlüğü korunabilmeli,
- Tüm iletişim güvenli olmalı,
- Ziyaretçilerin güvenliği ve gizliliği korunmalı,

Bu hedeflere ulaşmak genellikle şu iki ayak üzerine kuruludur: Paylaşım ve standartlar. Tehditler ve önlemler değiştikçe konuyla ilgili e-posta listeleri gibi kanallarda bilgi paylaşımı önem kazanır. En azından kullanıcının, yerel Bilgisayar Acil Müdahale Ekibini (CERT) / Bilgisayar Acil Hazırlık Ekibini ve Bilgisayar Güvenlik Arıza Müdahale Ekibini (CSIRT) tanıması gerekir. Ayrıca uygun ve güncel ölçütleri sağlayarak zincirin en zayıf halkası olmaktan kaçınır.

ISO

ISO, ilginizi çekebilecek çeşitli ölçütler yayınlamış durumda. Bu ölçütlere kalite ve güvenlik alanındaki şunlar da dahildir:

- ISO / IEC / IEEE 90003:2018 Yazılım mühendisliği
- ISO / IEC 27000 bilgi güvenliği ölçütleri

Bu ölçütler başka bir çok şeyin yanında çok kullanışlı olabilen ortak bir kelime dağarcığı da paylaşır. Kullanışlı olabilecekleri bir yer de GDPR uyumluluğudur.

DNSSEC

Alanadınız için yapılan DNS sorgularına verilecek yanıtları doğrulamak iyi bir şeydir.

TOR

İnsanlar, gizliliklerini ve güvenliklerini korumak için Tor Browser kullanmayı tercih edebilir. Uygulamanıza barındırma hizmeti seçerken, Tor bağlantılarına izin verildiğinden emin olun. Örneğin, Onionshare aracı kullanılarak, var olan bir web sitesinin anonim ve sansürlenemeyen versiyonu sadece birkaç tık ile kolayca yayınlanabilir.

https://onionshare.org/

HTTPS

Aradaki adam (man in the middle) saldırılarından ve gizli dinlemelerden kaçınmak için web sitenizde şifrelenmemiş bağlantılara izin vermeyin ve her zaman HTTPS yoluyla bağlantı kurmayı destekleyin. HTTPS kullanmanın en temel motivasyonu ulaşılan web sitesinin kimliğinin doğrulanması, gizliliğin korunması ve alışverişi yapılan verinin bütünlüğüdür. Daha zorlayıcı olmak için, **HSTS (HTTP Katı Aktarım Güvenliği)** kullanmayı düşünebilirsiniz.

Eğer sunucuya yönetici erişimine sahipseniz, eğer sizin sunucunuzsa, **Let's Encrypt** kullanabilir ve ihtiyacınız olan tüm alan adları için sertifika edinebilirsiniz. Paylaşımlı barındırmanız varsa, Let's Encrypt sertifikalarını destekleyen sağlayıcıyı seçin.

https://letsencrypt.org/

HTTPS kullandığınız zaman sadece güvenli şifreleme yöntemlerine izin verdiğinizden emin olun. Bazı eski HTTPS versiyonları zamanı geçmiş şifrelemeleri sebebiyle artık güvenli değillerdir. İnternette web sunucunuzu test edebilmeniz için ücretsiz kaynaklar var. Örneğin:

https://www.ssllabs.com/ssltest/

CSP

İçerik Güvenliği Politikası (CSP) uygulayın. Bu, Dünya Çapında Ağ Konsorsiyumu'nun (W3C) bir güvenlik katmanıdır ve bunu betikler (scripts), biçem sayfaları (style sheets) ve görseller gibi dış kaynakların web sitenizden yüklenmesini engellemek için web sunucunuzda aktif hale getirebilirsiniz. CSP size, Siteler Arası Betik Çalıştırma (XSS) ve veri enjeksiyonu dahil, belirli saldırı çeşitlerini tespit etmeniz ve verilen zararı hafifletmeniz için yardım sağlar. Bu saldırılar veri erişiminden site içeriğini bozmaya ve kötü amaçlı yazılım dağıtımına kadar her şey için yapılır. Politika kurallarını istediğiniz URL'leri izinliler listesine alarak özelleştirebilirsiniz.

Eğer web sunucusu yapılandırmasına erişiminiz yoksa bile **.htaccess** dosyasıyla veya direkt web sitenizin başlıkları (header) ile CSP'yi etkinleştirebilirsiniz.

Mozilla tarafından ücretsiz sağlanan bir hizmetle CSP yapılandırmanızı test edebilirsiniz:

https://observatory.mozilla.org/

JAVASCRIPT

JavaScript'ten kaçınılması gerektiği, çünkü bazı kullanıcılar için dışlayıcı olduğu veya bazı kullanıcıların erişim seviyesini düşürdüğü yönünde bir görüş var. Fakat başlı başına Javascript kullanmak, içeriklerin erişilmez hale geleceği anlamına gelmez. Yine de kullanmanın bazı gereklilikleri vardır.

https://webaim.org/techniques/javascript/

JavaScript uygulamak genellikle yanında JavaScript'siz bir versiyon yaratma gerekliliğini beraberinde getirir. En iyisi JavaScript zorunluluğu olmayan bir web sitesi tasarlamak ve JavaScript temelli özellikleri bunun üzerine kurmaktır. Böylelikle her kullanıcı için erişilebilir bir gezinti (browsing) deneyimi sağlanabilir. Bir <noscript> etiketi kullanarak, JavaScript'i tarayıcısında etkinleştirmemeyi tercih eden kullanıcılar ve JavaScript desteklemeyen tarayıcı kullananlar için alternatif içerik tanımlayın.

HASSAS VERİLERİ GÜVENCE ALTINA ALMAK

Kullanıcılarının kişisel verilerini depolayan bir web siteniz varsa, örneğin kişisel hesaplarıyla oturum açıyorlarsa:

- Güçlü parola kullanımını zorunlu kılın;
- Parola ve diğer hassas bilgileri asla düz metin saklamayın. Saklanan hassas verileri her zaman şifreleyin ya da hashing kullanın;
- İki faktörlü kimlik doğrulamasını (2FA) destekleyin;
- Eğer web sitesinin yönetici kapasitesi sınırlıysa yukarıdaki görevlerin yükünü bir kimlik sağlayıcısına (identity provider) verin ve tek girişle oturum açmayı etkinleştirin. Lütfen kimlik sağlayıcısı seçerken bunun gizlilikten ödün anlamına gelebileceğini unutmayın.

Eğer sitenizde kişisel hesaplar gerekli değilse, ve sadece blog gönderilerine yorum yapabilme özelliğini arzu ediyorsanız **Discourse** veya **Coral Project** gibi üçüncü parti açık kaynak eklentileri kullanabilirsiniz:

https://www.discourse.org/

https://coralproject.net/

Daha fazla bilgi için: https://darekkay.com/blog/static-site-comments/

DDOS SALDIRILARINA KARŞI KORUMA

Dağıtık Hizmet Engelleme (DDoS) saldırıları, genellikle hedef makineyi yoğunluktan çalışamaz hale getirmek niyetiyle birçok kaynaktan aşırı sayıda yapılan istekler ile gerçekleştirilir. Eğer bir STK için (aktivist girişim veya sivil toplum grubu) uygulama yazıyorsanız DDoS saldırılarına karşı korumayı göz önünde bulundurun. Bazı DDoS mücadele teknikleri, web sitesinin ziyaretçisi ve barındırma sağlayıcısı arasında, ters vekil (reverse proxy) görevinde üçüncü parti bir servis kullanır. Fakat bazı DDoS ile mücadele teknikleri üçüncü parti kullanımını gerektirmeyerek ağ düzeyinde saldırıyı karşılayabilir.

Deflect'i incelemek işinize yarayabilir. Deflect ücretsiz bir açık kaynak kodlu çözümdür. Kâr amacı gütmeyen bir dijital güvenlik kuruluşu tarafından geliştirilmiştir.

https://docs.deflect.ca/en/latest/about_deflect.html

Fakat bütün DDoS ile mücadele hizmetleri, trafiğinizin kontrolünü bir üçüncü partiye devretmeniz anlamına gelir; bunun farkedilemeyecek kadar hızlı olup olmaması veya hizmetin sürekli kontrolde olup olmaması fark etmez. Bu sebeple, itibar veya başka türlü riskler dikkatlice değerlendirilmelidir.

STATİK WEBSİTELERİ GERİ DÖNDÜ

Gerçekten dinamik web sitesine ihtiyacınız var mı? Eğer veri tabanı ihtiyacınız yoksa, HTML5 gibi modern web standartlar, size sadece statik kaynaklar (HTML, CSS ve belki sadece JavaScript ve font dosyaları) kullanarak son moda web sitesi yaratma imkanı sağlar.

Bu, dolaşım menüleri ve benzeri yapıları kendi elinizle yapmanız anlamına gelmez. Jekyll (GitHub Pages popülerleşti), Hugo veya Pelican gibi statik site üreticileri size Markdown veya basit HTML kullanarak web siteleri yaratma olanağı verir ve onları sizin için tümüyle birbirleri ile bağlantılandırılmış HTML'e dönüştürür. Eğer GitLab Pages kullanıyorsanız dönüştürme ve dağıtım kolayca otomatikleştirilebilir.

Statik web siteleri, veri tabanlarına bağlanmaları gerekmediği için eşsiz erişilebilirlik zamanlarına ulaşabilir. Tek ihtiyaçları olan şey, statik dosyaları sunmaları gereken basit bir web sunucusudur. Sonuç olarak, güvenlik sorunlarından daha az etkilenirler.

4. Maliyetli “ücretsiz” üçüncü parti hizmetlerin alternatifleri

Google, Facebook, Amazon ve diğer veri devlerine ait araçları kullanmanın, çevrimiçi hizmetlerin ziyaretçilerinin gizliliğinin korunmasıyla genellikle bağdaşmadığı düşünülür.

Kullanıcılarının gizliliğini önemseyen etik geliştiriciler, bu şirketlerin veya yan şirketlerinin hizmetlerini, doğrudan veya dolaylı olarak kullanmama eğilimindedirler. Etik, kullanımı kolay ve gizlilik bilincine sahip çok sayıda alternatif mevcuttur ve bunların çoğu Prism Break’te bulunabilir.

https://prism-break.org/

Maalesef, üçüncü parti hizmetlerin bazen çok işlevli olduklarını da biliyoruz, bu nedenle, aşağıdaki listede, bazı veri azaltma yöntemleri ve yaygın hizmetlerin alternatiflerini bir araya getirdik.

ANALİZLER (ANALYTICS)

Analizlerin genellikle kusurlu olduğunu ve birçok takip engelleyici tarafından engellendiğini belirtmek önemlidir, dolayısıyla bunları kullanmak doğru bilgi sağlamaz. Ancak ille de kullanmanız gerekiyorsa, Google Analytics veya başka bir üçüncü parti analiz hizmetini kullanmak yerine, **Matomo** (eski adıyla **Piwik**) ile web sitenizdeki trafiği izleyebilirsiniz. Gizlilikle uyumlu ve kurulumu çok kolay bir analiz platformudur, verileri otomatik olarak anonimleştirmek için yapılandırılabilir, böylece minimum miktarda kişisel veri işlemiş olursunuz. Bu şekilde, GDPR ile uyumlu hale gelirsiniz. Eğer kişisel verileri işlemeye karar verirseniz, Matomo size GDPR yükümlülüklerine daha kolay uyum sağlamanız için çeşitli özellikler sunar.

https://matomo.org/

VİDEOLAR

YouTube, Google’ın ve diğer eski Google yan kuruluşlarının çok uluslu holding kuruluşu olan Alphabet Inc.’e aittir. Sitenizde YouTube’dan bir video barındırırken gizliliği artırılmış modu etkinleştirme seçeneği vardır. Bu, YouTube’un, videoyu oynatmadıkları sürece web sitenizin ziyaretçilerinin cihazlarına izleme çerezleri yerleştiremeyeceği anlamına gelir. “Video bittiğinde önerilen videoları göster” de devre dışı bırakılmalıdır. İçerik yönetim sisteminiz için bir eklenti kullanmayı tercih ediyorsanız, bu seçenekleri dikkate alan bir eklenti arayın.

Daha da iyi bir çözüm, Peertube kullanmayı, hatta kendi Peertube'unuzu kurmayı düşünmektir. **Peertube** hakkında açıklama için bkz:

https://framatube.org/videos/watch/9db9f3f1-9b54-44ed-9e91-461d262d2205

Bunun ek faydası, kötü amaçlı yayından kaldırma isteklerine karşı Youtube'a göre daha korunaklı olmaktır. Ayrıca, içeriğinize hiçbir reklam malzemesi eklenmeyecektir. Eğer video barındıran sitenin (YouTube gibi) hem sizin hem de kendisi için para kazanması amacıyla kişisel verileri kullanmasını onaylıyorsanız, Peertube uygun bir seçenek değildir. Elbette bu yaklaşıma güveniyorsanız, ana şirket Google sizin reklamveren dostu olmadığınıza karar verdiğinde veya para kazanma kurallarını keyfi olarak bir günden diğerine değiştirdiğinde, Youtube'un bunu iptal edebileceğini de unutmayın.

Vimeo, Pro kullanıcılarının video dosyalarını, Google Analytics içeren oynatıcısı olmadan kullanmasına izin verir, dolayısıyla **Peertube**'i kullanamamanız durumunda, bu yararlı bir geçici çözüm olabilir.

HARİTALAR

Eğer web sitenize bir harita gömmek için Google Haritalar API'sını kullanırsanız, kullanıcıları Google gizlilik politikasını kabul etmeye zorlamış olursunuz. Bunun yerine alternatif olarak **OpenStreetMap.**'i kullanabilirsiniz.

https://www.openstreetmap.org/

YAZI TİPLERİ VE SİMGELER

Kullanıcıları Google gizlilik politikasını kabul etmeye zorlayan Google Yazı Tiplerini kullanmak yerine şunları kullanabilirsiniz:

- **Fork Awesome** geniş bir açık kaynak kodlu simgeler kütüphanesi.

  https://forkawesome.github.io/Fork-Awesome/

- Sadece bazılarını yüklemek istiyorsanız, kendi simge koleksiyonunuzu oluşturmanıza izin veren **Fontello.**

  http://fontello.com/
  https://github.com/fontello/fontello/

- **Fontspring,** yazı tiplerini kendinizin barındırdığı, "takip değil, güven" ilkesine dayanan bir yazı tipi kaynağıdır.

  https://www.fontspring.com/fair-fonts

- **FontSquirrel**, ticari kullanım için % 100 ücretsiz yazı tipleri ve kendi sunucularınızda barındırabilmeniz için yazı tipleri sunar.

  http://www.fontsquirrel.com/

Son olarak, aldığı bir Google Fonts URL'inden, tamamen yerel bir CSS ve yazı tipi dosyaları seti oluşturan Google Fonts indiricilerine başvurabilirsiniz. Bu, geliştiricilerin Google Fonts üzerindeki tüm yazı tiplerini çok az çaba göstererek veya hiç çaba harcamadan, ancak onları gerçekte Google'dan yüklemeden kullanmasına olanak tanır. İhtiyacınız olan yazı tipi dosyasını indirebilir ve kendi web sunucunuzda barındırabilirsiniz.

SOSYAL MEDYA İKONLARI

Sosyal medya platformlarının sunduğu "beğen" veya "paylaş" gibi sosyal medya düğmelerine ilişkin yerleştirme kodları, kullanıcı bu düğmelere tıklamasa bile, bu sosyal ağlara bilgiler gönderir. Bundan kaçınarak aynı işlevselliği sağlamanın birçok yolu vardır. Bunlardan biri Social Share Privacy kullanmaktır. JavaScript ve JavaScript olmayan seçenekleri mevcuttur.

https://panzi.github.io/SocialSharePrivacy/

Hem takipten hem de JavaScript'ten kaçınmak için başka bir alternatif, sosyal medya düğmeleri üreticisi **Sharingbuttons.io**'dur. JavaScript kullanmadıkları için çok hızlı yüklenirler ve web sitenizin yüklenmesini engellemezler.

https://sharingbuttons.io/

Başka bir çözüm elbette düğmeleri kendinizin oluşturması olacaktır.

CAPTCHAS

Kullanıcılar tarafından oluşturulan herhangi bir içerikte (örneğin yorumlar) spam oluşmasını önlemek için bir Captcha kullanmak isteyebilirsiniz. Ama bunu seçmemeniz için birçok neden vardır.

Captchalar engelli kullanıcılar için ciddi engeller oluşturabilirler. Gerçek kullanıcıları "botlardan" ayırmaya çalışırken, genellikle belirli şeyleri duyma veya görme - ve ardından yanıt verme- gibi başka beceriler istenir. Doğası gereği bu, görme veya işitme sorunları olan ziyaretçiler için hizmeti zor veya imkansız hale getirecektir. [*Aşağıdaki "Web sitesini herkes için erişilebilir yapma" konusuna bakın.*]

Şu anda, birçok Captcha'nın gizlilik sorunu var. Google Captcha yalnızca can sıkıcı olmakla kalmıyor, aynı zamanda kullanıcıları hakkında kişisel olarak tanımlanabilir ek veriler de topluyor.

https://www.businessinsider.com.au/google-no-captcha-adtruth-privacy-research-2015-2

Harici JavaScript kodu yüklemeyi gerektirmeyen basit Captcha yöntemleriyle web sitenizi korumak için daha iyi seçenekler de vardır. Bazı eklentilerin ayarlar için farklı seçenekleri vardır. Bunları yapılandırırken kullanıcı deneyimine ve gizliliğine dikkat edin.

Alternatif Captcha örnekleri:

- Drupal

  https://www.drupal.org/project/captcha
- Wordpress For Contact form 7 with honeypot :

  https://wordpress.org/plugins/contact-form-7-honeypot/
- Wordpress Secure Image Captcha:

  https://wordpress.org/plugins/securimage-wp/
- Securimage:

  https://www.phpcaptcha.org/
- IndyCaptcha:

  https://github.com/dyne/indycaptcha

VE DAHA FAZLASI

Etkinlik organizasyon araçları

Birçok aktivizm etkinliği fiziksel buluşmalara bağlıdır ve katılımcıların bilgilerinin üçüncü parti uygulamalarla paylaşılmaması açıkça önemlidir.

- **Odoo** (eski adıyla OpenERP), CRM, web sitesi /e-ticaret, faturalandırma, muhasebe, üretim ve etkinlik yönetimi gibi birçok uygulamayı içeren bir yönetim yazılımıdır. Topluluk sürümü açık kaynaktır.

  https://www.odoo.com
  https://www.odoo.com/page/events
- **Attendize** açık kaynaklı bir bilet satış ve etkinlik yönetimi platformudur..

  https://www.attendize.com/

Web sitelerini herkes için erişilebilir hale getirme

Erişilebilir web sitesi tasarımı, engelli kullanıcıların hizmetlere eşit erişime sahip olup olmadığını belirtir. Erişilebilirlik, yüksek kaliteli web siteleri ve web araçları oluşturmak ve insanları ürünlerini ve hizmetlerini kullanmaktan dışlamak

istemeyen geliştiriciler ve kuruluşlar için birinci derecede önemlidir. W3C gibi kuruluşlar bu konuda faydalı standartlar geliştirmiştir.

https://www.w3.org/WAI/

https://www.w3.org/standards/webdesign/accessibility

https://www.washington.edu/accesscomputing/sites/default/files/30-Web-Accessibility-Tips.pdf

Web'i "çözülmekten" koruyun

Kontrolünüz dışında bulunan harici bilgilere, genellikle bağlantılar yoluyla ulaşılır. Bu bağlantılar, farklı web sitelerine dağılmış bilgileri "web" ile ilişkilendirirken, kontrolünüz dışındaki bağlantılar en sonunda internetten kaybolabilir. Bağlantıların başarısız olması, sansürden DDoS saldırılarına veya bir web sitesi alan adının sürdürülememesine kadar bir dizi nedenden kaynaklanabilir. Ancak, web sitenizin kullanıcılarının bağlantılı içeriğe güvenilir bir şekilde erişebilmelerini sağlamak sizin sorumluluğunuzdadır.

Merkezi arşivleme hizmetlerini (örneğin İnternet Arşivi veya perma.cc) kullanabilir veya **Amber** aracını kullanarak kendi arşivinizi oluşturabilirsiniz. Bu hizmetler ve açık kaynak araçları, web sitesine bağlı her sayfanın anlık görüntüsünü oluşturur ve korur.

http://amberlink.org/

https://perma.cc/

Etik reklamcılık

Kullanıcıları izleyen ve verilerini satan reklam teknolojisi kullanmaktan kaçınmayı düşünebilirsiniz. Bu zararlı iş modelini atlatmanın alternatifleri vardır.

https://docs.readthedocs.io/en/latest/advertising/ethical-advertising.html

Web sitesi araması

Web sitenizde bir arama aracı kullanıyorsanız, kullanıcıları takip etmeyen **Startpage** gibi özel arama motorlarını dikkate alın.

https://startpage.com

https://choosetoencrypt.com/search-engines/private-search-engines-a-complete-guide/

5. Sözlük

BİRLİKTE İŞLERLİK: Arayüzleri, önemli kısıtlamalar olmaksızın diğer ürünler veya sistemlerle birlikte çalışmak üzere tasarlanan bir ürün veya sistemin özelliği.

CMS (İÇERİK YÖNETİMİ SİSTEMİ): Dijital içeriğin oluşturulmasını ve yönetilmesini sağlayan bir sistemdir.

CSP (İÇERİK GÜVENLİĞİ POLİTİKASI): Güvenilir web sayfalarında kötü amaçlı içeriğin yürütülmesi ile sonuçlanan, siteler arası betik çalıştırma (XSS), clickjacking (sahte butonlara tıklama) ve diğer kod enjeksiyon saldırılarını önlemek için tanıtılan bilgisayar güvenlik standardı.

CRONJOB: Unix benzeri işletim sistemlerinde bir görev zamanlayıcısı olan Cron yazılımı tarafından başlatılan bir görevdir. Yazılım ortamlarını kuran ve bakımını yapan kişiler, belirli zamanlarda, tarihlerde veya aralıklarla periyodik olarak çalışmak üzere işleri (komutlar veya kabuk betikleri) planlamak için Cron'u kullanır. Genellikle sistem bakımını veya yönetimini otomatikleştirir.

DDOS (DAĞITIK HİZMET ENGELLEME): Failin, bir veya daha fazla sunucuyu, geçici veya süresiz olarak bozarak ağ hizmetini hedeflenen kullanıcılar için kullanılamaz hale getirmeye çalıştığı bir saldırı. Bu tipik olarak, olağan iletişimin bir kısmının veya tamamının önlenmesi amacıyla, hedeflenen ortamın birçok kaynaktan gelen istekler veya özel tip trafik ile doldurup, sistemin yoğunluktan çalışamaz hale getirilmesiyle yapılır.

FLOSS (FREE LIBRE OPEN SOFTWARE): Herhangi bir amaçla kullanılmak, kopyalanmak, çalışmak ve değiştirilmek üzere serbestçe lisanslanan ve insanların yazılım tasarımını geliştirmeleri için kodları açık şekilde paylaşılan yazılımdır. Bu, yazılımın kısıtlayıcı lisanslama altında olduğu ve kaynak kodun genellikle kullanıcılardan gizlendiği sahipli yazılımın tersidir. Açık kaynaklı yazılımlarla ilgili kısıtlamalar da vardır. Bunlar, temel doğasının özgür kalması için gereklidir. Ayrıca, açık kaynaklı yazılımlar onu geliştirmek ve sürdürmek isteyen aktif ve kendini bu işe adamış bir topluluğa dayanır.

GDPR (AVRUPA BİRLİĞİ GENEL VERİ KORUMA DÜZENLEMESİ): AB'deki tüm bireyleri kapsayan ve öncelikli olarak bireylere kişisel verileri üzerinde kontrol sağlamayı ve düzenleyici ortamı basitleştirmeyi amaçlayan bir AB veri koruma düzenlemesidir. Ayrıca, kişisel verilerin AB dışındaki yargı bölgelerine aktarılmasını da ele almaktadır.

GEÇİCİ ÖNLEM (STOPGAP): Daha iyi bir şey elde edilene kadar kullanılan geçici önlem veya kısa süreli düzeltme.

KİŞİSEL VERİ: Kimliği belirlenmiş veya belirlenebilir gerçek bir kişiyle ('veri öznesi') ilgili herhangi bir bilgi. Kimliği belirlenebilir gerçek kişi, doğrudan veya dolaylı olarak, özellikle bir ad, bir kimlik numarası, konum verisi, çevrimiçi bir tanımlayıcı veya fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğini belirten bir referansla tanımlanabilen gerçek kişidir. (GDPR tarafından tanımlandığı şekliyle)

PEER-TO-PEER (P2P): Görevleri, iş yüklerini veya gerçekten verileri eşler arasında bölen dağıtık bir uygulama mimarisi. Eşler uygulamada eşit derecede ayrıcalığa sahip katılımcılardır. Eşlerin düğümlerden (node) oluşan bir peer-to-peer ağ oluşturdukları söylenir.

STK: Sivil Toplum Kuruluşu.

TOR: Başlangıçta anonim iletişimi sağlamak üzere ABD ordusu tarafından geliştirilen özgür yazılım. Tor internet trafiğini, herhangi bir kullanıcının yerini ve kullanımını ağ gözetimi veya trafik analizi yapanlardan gizlemek için, yedi binden fazla röleden (relay) oluşan ücretsiz, dünya çapında ve gönüllü bir ağ katmanı içerisinden yönlendirir. Tor Tarayıcı, Tor arkaplan işlemlerini otomatik olarak başlatır ve Tor ağı üzerinden trafiği yönlendirir.

UÇTAN UCA ŞİFRELEME: Sadece iletişim kuran tarafların içeriğe ulaşabildiği iletişim sistemi. Prensip olarak, telekom sağlayıcıları, internet erişim sağlayıcıları, transit sağlayıcıları ve hatta iletişim hizmeti sağlayıcısı da dahil olmak üzere potansiyel gizli dinleme cihazlarının iletişimin şifresini çözmesini önler. Uçtan uca, kullanıcıdan hizmete veya kullanıcıdan kullanıcıya anlamına gelebilir.

ÜÇÜNCÜ PARTİ İÇERİĞİ: En basitçe, mülkiyet haklarının başka bir tarafça tutulduğu veya bu tarafların ekipmanlarından dinamik olarak alındığı çeşitli içeriklerdir.

VARSAYILAN GİZLİLİK: Veri sorumlusu bir kuruluşun, varsayılan olarak, her bir belirli amaç için, işlenmesi gerekli en az verinin işlendiğinden emin olmasını sağlayan ilkedir. Yani kullanıcı daha az koruyucu ayarları seçme seçeneğine sahip olsa bile en koruyucu güvenlik ayarı varsayılandır.

European Digital Rights

2002 yılında kurulan EDRi, çevrimiçi hakları ve özgürlükleri savunan en büyük Avrupa ağıdır.

Halen 42 sivil toplum kuruluşu EDRi üyesidir ve 30 gözlemci çalışmalarımıza yakından katkıda bulunmaktadır.

Misyonumuz, gizlilik, veri koruma ve ifade ve bilgi özgürlüğü dahil olmak üzere dijital ortamda insan haklarını ve hukukun üstünlüğünü teşvik etmek, korumak ve savunmaktır.

Vizyonumuz, devlet otoritelerinin ve özel şirketlerin çevrimiçi ortamda herkesin temel hak ve özgürlüklerine saygı duyduğu bir Avrupa içindir. Genel amacımız, sivil toplumun ve bireylerin haklarının kontrolü kendi ellerinde olacak şekilde teknolojik ilerlemeyi benimsemeleri için güçlendirildikleri yapıları inşa etmektir.

KİTLE GÖZETİMİ.
KEYFİ SANSÜR.
İÇERİK KISITLAMALARI.

Şirketler ve hükümetler özgürlüklerimizi giderek kısıtlamaktadır.

ŞİMDİ bağış yap:
https://edri.org/donate

GİZLİLİK!
İFADE ÖZGÜRLÜĞÜ!
BİLGİ VE KÜLTÜRE ERİŞİM!

Çevrimiçi hakları ve özgürlükleri savunuyoruz.

EDRi

EUROPEAN DIGITAL RIGHTS

https://edri.org

@edri

brussels@edri.org