Appendix F. Leveraging Dev Tools (Ek F. Geliştirme Araçlarından Yararlanma)

Leveraging Dev Tools(Dev Aletleri Kullanmak)

Bu ek, güvenlik test faaliyetlerine yardımcı olmak için tarayıcı Geliştirici Aracı işlevselliğinin kullanımı için çeşitli ayrıntıları özetler.

Açıkçası tarayıcıda işlevsellik bir alternatif değildir: DAS (Dinamik Uygulama Güvenliği Testi) araçları, SAST (Statik Uygulama Güvenliği Testi) araçları veya bir test cihazı deneyimi, ancak bazı test faaliyetleri için kullanılabilir ve üretimle ilgili görevleri rapor edebilir.

Accessing Dev Tools (Dev Araçlara Erişim)

Dev Aletleri açmak çeşitli şekillerde gerçekleştirilebilir.

1. Klavye kısayolu üzerinden `F12`. .
2. Klavye kısayolu üzerinden `ctrl` + `shift` + `i` Windows'ta.
3. Klavye kısa kesimi aracılığıyla `cmd` + `option` + `i` Mac'te.
4. Web sayfası sağ tıklama bağlamı menüsü aracılığıyla ve ardından seçimi `Inspect` Google Chrome'da.
5. Web sayfası sağ tıklama bağlamı menüsü aracılığıyla ve ardından seçimi `Inspect Element` Mozilla Firefox'ta.
6. Google Chrome'daki üçlü nokta 'kabob' menüsü aracılığıyla ve ardından seçimi `More Tools` Ve sonra `Developer Tools`. .
7. Mozilla Firefox'taki üçlü satır 'hamburger' (veya 'pancake') menüsü aracılığıyla daha sonra seçin `Web Developer` Ve sonra `Toggle Tools`. .
8. Edge / I'deki dişli simge ayarları menüsü aracılığıyla daha sonra seçin `Developer Tools`. .

> NOT: Aşağıdaki talimatların çoğu Dev Tools'un zaten açık veya aktif olduğunu varsayıyor.

Capabilities (Yetenekler)

Fonksiyonellik	Chrome*	Firefox	Kenar / IE	Safari
Kullanıcı-Ajan Anahtarlama	Y	Y	Y	Y
Düzenleme/Ressen Talepleri	N	Y	N	N
Kurabiye Düzenleme	Y	Y	Y	N
Yerel Depolama Düzenleme	Y	Y	Y	N
Engelli CSS	Y	Y	Y	Y
JavaScript'i devre dışı bırakın	Y	Y	N	Y
HTTP Başlıklarını Görüntüleyin	Y	Y	Y	Y
Ekran Görüntüleri	Y	Y	Y	N
Çevrimdışı Mod	Y	Y	N	N
Kodlama ve Kod Çözme	Y	Y	Y	Y
Duyarlı Tasarım Modu	Y	Y	Y	Y

* Google Chrome için geçerli olan her şey tüm Chromium tabanlı uygulamalar için geçerli olmalıdır. (Bu, 2019/2020 civarında Microsoft yeniden commbaring Edge'i içerir.)

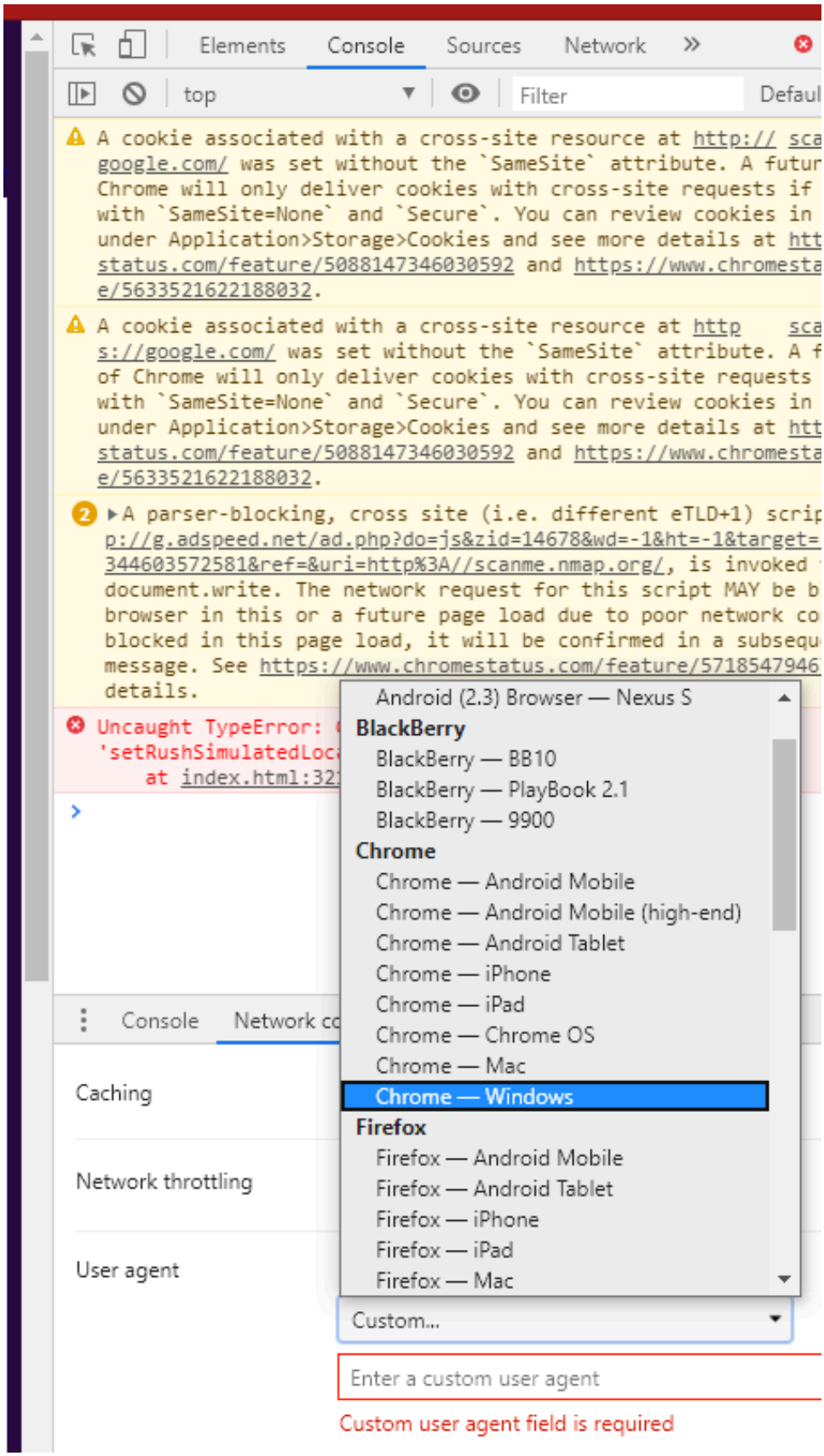
User-Agent Switching (Kullanıcı-Ajan Anahtarlama)

Related Testing (İlgili Testler)

- Tarayıcı Önbellek Zayıflıkları için Test

Google Chrome

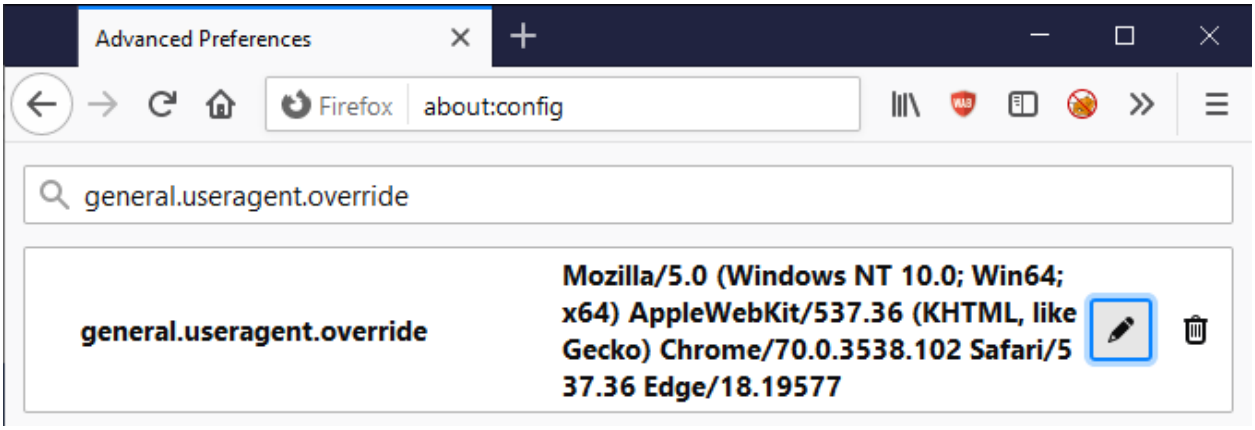
1. Geliştirici Araçları bölmenin sağ tarafındaki üçlü nokta 'kabob' menüsüne tıklayın, seçin `More tools` Ardından seçin `Network conditions` . .
2. “Otomatik olarak seçin” onay kutusunu kontrol edin.
3. Açma menüsünden kullanıcı temsilcisini seçin veya özel bir kullanıcı temsilcisi girin


Elements
Console
Sources
Network
top
Filter
Android (2.3) Browser — Nexus S
BlackBerry
BlackBerry — BB10
BlackBerry — PlayBook 2.1
BlackBerry — 9900
Chrome
Chrome — Android Mobile
Chrome — Android Mobile (high-end)
Chrome — Android Tablet
Chrome — iPhone
Chrome — iPad
Chrome — Chrome OS
Chrome — Mac
Chrome — Windows
Firefox
Firefox — Android Mobile
Firefox — Android Tablet
Firefox — iPhone
Firefox — iPad
Firefox — Mac
Console
Caching
Network throttling
User agent
Custom...
Enter a custom user agent
Custom user agent field is required

Şekil 6. F-1: Google Chrome Dev Araçları Kullanıcı-Ajan Anahtarlama İşlevselliği

Mozilla Firefox'un

1. Firefox'un teslimatı `about:config` sayfa ve tıklayın `I accept the risk!` . .
2. Girin `general.useragent.override` Arama alanına doğru.
3. Araya bak `general.useragent.override` , eğer bu tercihi göremiyorsanız, bir dizi radyo düğmesi gösteren birini arayın `Boolean, Number, String` Seçin `String` Ardından artı işaretini tıklayın `Add` düğmesi `about:config` Sayfa.
4. Değerini belirleyin `general.useragent.override` User-Agentİhtiyacınız olan herhangi bir Kullanıcı-Ajanı için.



Şekil 6. F-2: Mozilla Firefox Kullanıcı-Ajan Anahtarlama İşlevselliği

Daha sonra çöp kutusuna tıklayın `Delete` Sağdaki düğmeye `general.useragent.override` Geçitliyi kaldırmayı ve varsayılan kullanıcı temsilcisine geri dönmeyi tercih edin.

Edit/Resend Requests (Düzenleme/Ressen Talepleri)

Related Testing (İlgili Testler)

- Kimlik Doğrulama Testi
- Yetkilendirme Testi
- Oturum Yönetimi Testi
- Giriş Doğrulama Testi
- İş Mantık Testi

Mozilla Firefox'un

1. Seçin `Network` Taba.
2. Web uygulamasında herhangi bir işlem yapın.
3. Listeden HTTP isteğine sağ tıklayın ve seçin `Edit and Resend` . .
4. İstenilen değişiklikleri yapın ve üzerine tıklayın `Send` Düğme.
5. Değiştirilmiş istek üzerine sağ tıklayın ve seçin `Open in New Tab` . .

Cookie Editing (Kurabiye Düzenleme)

Related Testing (İlgili Testler)

- Kimlik Doğrulama Testi
- Yetkilendirme Testi
- Oturum Yönetimi Testi
- Çerez özellikleri için test

Google Chrome

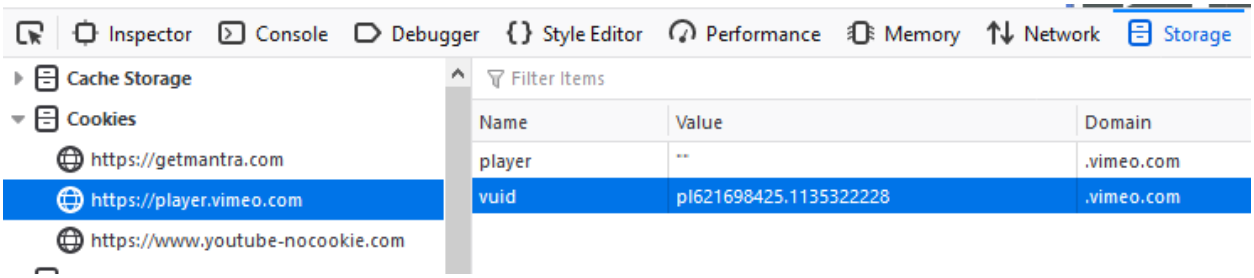
1. Tıklayını tıklayın `Application` Taba.
2. Genişletin `Cookies` Alt kısımlarda `Storage` Başa doğru.
3. İlgili alan adı seçin.
4. İçine çift tıklayın `Value` Herhangi bir çerez değerini düzenlemek için sütun.

> Not: Çerezler, basarak seçildikten sonra silinebilir deletetuşu veya sağ tıklama bağlamı menüsünden.

Mozilla Firefox'un

1. Tıklayını tıklayın `Storage` Taba.
2. Genişle `Cookies` Bölüm.
3. İlgili alan adı seçin.
4. İçine çift tıklayın `Value` Herhangi bir çerez değerini düzenlemek için sütun.

> Not: Çerezler, basarak seçildikten sonra silinebilir deletetuşu veya sağ tıklama bağlamı menüsünden çeşitli seçeneklerle.



Şekil 6. F-3: Mozilla Firefox Çerez Düzenleme İşlevselliği

Local Storage Editing (Yerel Depolama Düzenleme)

Related Testing (İlgili Testler)

- Tarayıcı Depolama Test Edin

Google Chrome

1. Tıklayını tıklayın `Application` Taba.
2. Genişletin `Local Storage` Alt kısımlarda `Storage` Başa doğru.
3. İlgili alan adı seçin.
4. İçine çift tıklayın `Value` Herhangi bir çerez değerini düzenlemek için sütun.
5. Uygulanabilir Hücrede çift tıklayın düzenlemesi için `Key` ya da `Value` . .

> Not: Düzenleme Session Storageya da Index DBEsasen aynı adımları takip eder.
>
> Not: Öğeler sağ tıklama bağlamı menüsü üzerinden eklenebilir veya silinebilir.

Mozilla Firefox'un

1. Tıklayını tıklayın `Storage` Taba.
2. Genişle `Local Storage` Bölüm.

3. İlgili alan adı seçin.
4. Uygulanabilir Hücrede çift tıklayın düzenlemesi için `Key` ya da `Value`. .

> Not: Düzenleme Session Storageya da Index DBEsasen aynı adımları takip eder.
>
> Not: Öğeler sağ tıklama bağlamı menüsü üzerinden eklenebilir veya silinebilir.

Disable CSS (Engelli CSS)

Related Testing (İlgili Testler)

- Müşteri tarafı Kaynak Manipülasyonu için Test

(Genel)

Tüm büyük tarayıcılar, Dev Araçlar Konsolu ve JavaScript işlevselliğinden yararlanan CSS'yi manipüle etmeyi destekler:

- Tüm dış stil sayfalarını kaldırmak için: `$('style,link[rel="stylesheet"]').remove();`
- Tüm iç stil sayfalarını kaldırmak için: `$('style').remove();`
- Tüm satır içi stilleri kaldırmak için: `Array.prototype.forEach.call(document.querySelectorAll('*'),function(el){el.removeAttribute('style');});`
- Baş etiketinden her şeyi kaldırmak için: `$('head').remove();`

Disable JavaScript (JavaScript'i devre dışı bırakın)

Google Chrome

1. Web geliştirici araç çubuğunun sağ tarafındaki üçlü nokta 'kabob' menüsüne tıklayın ve tıklayın `Settings`. .
2. On The On The Altyazıları `Preferences` sekmesi, altında `Debugger` bölüm, kontrol edin `Disable JavaScript` Kontrol kutusu.

Mozilla Firefox'un

1. Dev aletler üzerinde `Debugger` sekmesi, geliştirici araç çubuğunun sağ üst köşesindeki ayarlar dişli düğmesine tıklayın.

2. Seçin `Disable JavaScript` Bırakmadan (bu, JavaScript devre dışı bırakıldığında, esnek öğenin bir onay
işareti vardır) bir etkinleştirilen / devre dışı bırakılabilir bir menü
öğesidir).

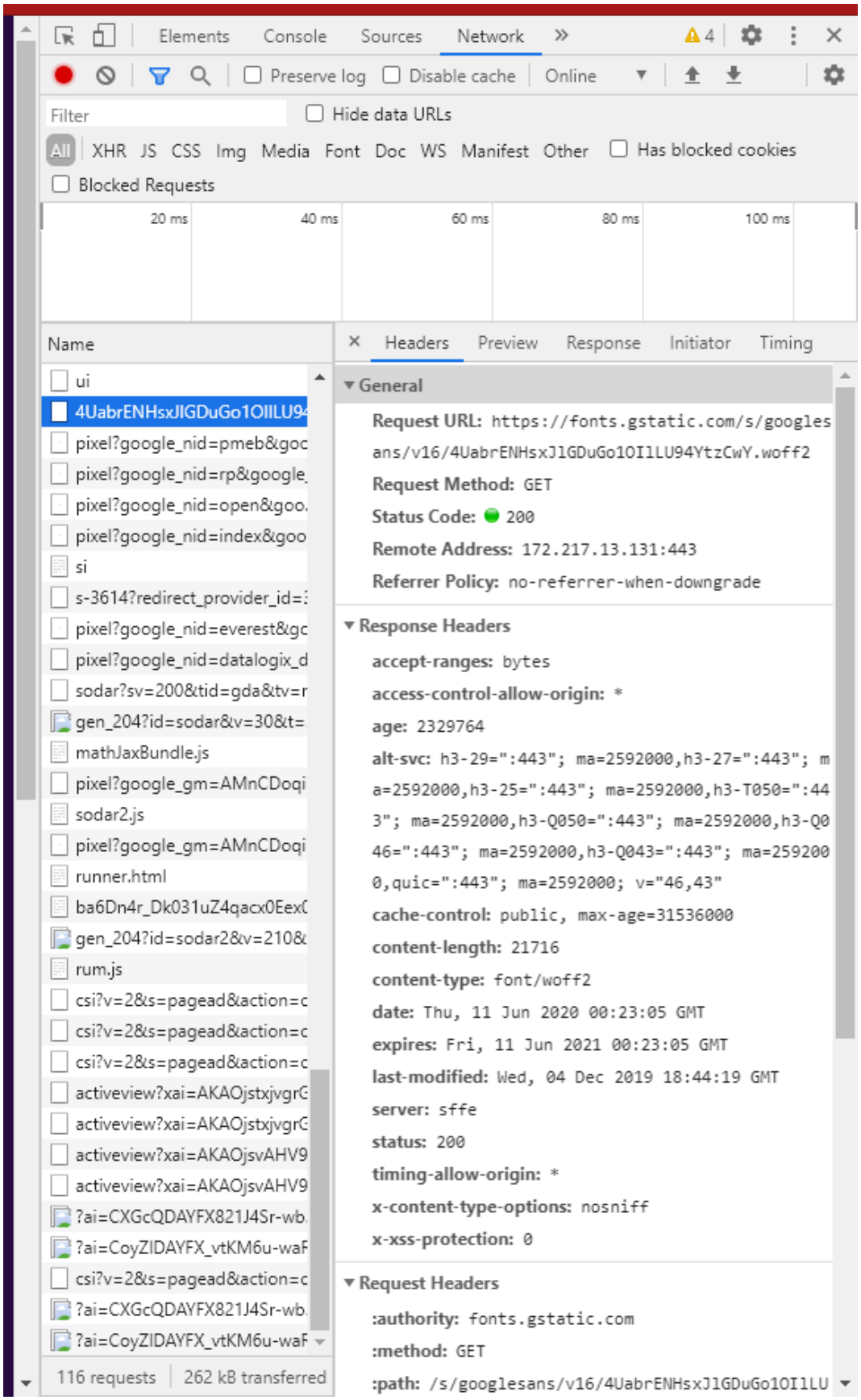
View HTTP Headers (HTTP Başlıklarını Görüntüleyin)

Related Testing (İlgili Testler)

- Bilgi Toplaması

Google Chrome

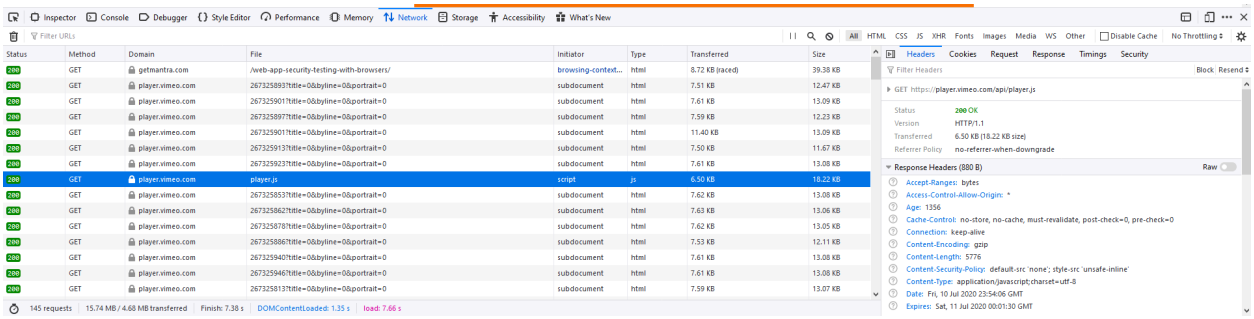
1. On The On The Altyazıları `Networking` Dev Araçlar'daki sekme herhangi bir URL veya istek seçin.
2. Alt sağ el tavasında seçin `Headers` Taba.


Elements
Console
Sources
Network
Preserve log
Disable cache
Online
Filter
Hide data URLs
All
XHR
JS
CSS
Img
Media
Font
Doc
WS
Manifest
Other
Has blocked cookies
Blocked Requests
20 ms
40 ms
60 ms
80 ms
100 ms
Name
ui
4UabrENHsxJlGDuGo1OIlLU94
pixel?google_nid=pmeb&goc
pixel?google_nid=rp&google_
pixel?google_nid=open&goo.
pixel?google_nid=index&goo
si
s-3614?redirect_provider_id=
pixel?google_nid=everest&gc
pixel?google_nid=datalogix_d
sodar?sv=200&tid=gda&tv=r
gen_204?id=sodar&v=30&t=
mathJaxBundle.js
pixel?google_gm=AMnCDoqi
sodar2.js
pixel?google_gm=AMnCDoqi
runner.html
ba6Dn4r_Dk031uZ4qacx0EexC
gen_204?id=sodar2&v=210&
rum.js
csi?v=2&s=pagead&action=c
csi?v=2&s=pagead&action=c
csi?v=2&s=pagead&action=c
activeview?xai=AKAOjstxjvgrG
activeview?xai=AKAOjstxjvgrG
activeview?xai=AKAOjsvAHV9
activeview?xai=AKAOjsvAHV9
?ai=CXGcQDAYFX821J4Sr-wb.
?ai=CoyZIDAYFX_vtKM6u-waF
csi?v=2&s=pagead&action=c
?ai=CXGcQDAYFX821J4Sr-wb.
?ai=CoyZIDAYFX_vtKM6u-waF
116 requests
262 kB transferred
Headers
Preview
Response
Initiator
Timing
General
Request URL: https://fonts.gstatic.com/s/googles
ans/v16/4UabrENHsxJlGDuGo1OIlLU94YtzCwY.woff2
Request Method: GET
Status Code: 200
Remote Address: 172.217.13.131:443
Referrer Policy: no-referrer-when-downgrade
Response Headers
accept-ranges: bytes
access-control-allow-origin: *
age: 2329764
alt-svc: h3-29=":443"; ma=2592000,h3-27=":443"; m
a=2592000,h3-25=":443"; ma=2592000,h3-T050=":44
3"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q0
46=":443"; ma=2592000,h3-Q043=":443"; ma=259200
0,quic=":443"; ma=2592000; v="46,43"
cache-control: public, max-age=31536000
content-length: 21716
content-type: font/woff2
date: Thu, 11 Jun 2020 00:23:05 GMT
expires: Fri, 11 Jun 2021 00:23:05 GMT
last-modified: Wed, 04 Dec 2019 18:44:19 GMT
server: sffe
status: 200
timing-allow-origin: *
x-content-type-options: nosniff
x-xss-protection: 0
Request Headers
:authority: fonts.gstatic.com
:method: GET
:path: /s/googlesans/v16/4UabrENHsxJlGDuGo1OIlLU

Şekil 6. F-4: Google Chrome Başlıkları Görüntüleyin

Mozilla Firefox'un

1. On The On The Altyazıları `Networking` Dev Araçlar'daki sekme herhangi bir URL veya istek seçin.
2. Alt sağ el tavasında seçin `Headers` Taba.



Şekil 6. F-5: Mozilla Firefox Başlıkları Görüntüleyin

Screenshots (Ekran Görüntüleri)

Related Testing (İlgili Testler)

- Raporlama

Google Chrome

1. Basına basın `Toggle Device Toolbar` düğme veya tuşa basın `ctrl` + `shift` + `m` . .
2. Cihaz Aracı çubuğundaki üçlü nokta 'kabob' menüsünü tıklayın.
3. Seçin `Capture screenshot` ya da `Capture full size screenshot` . .

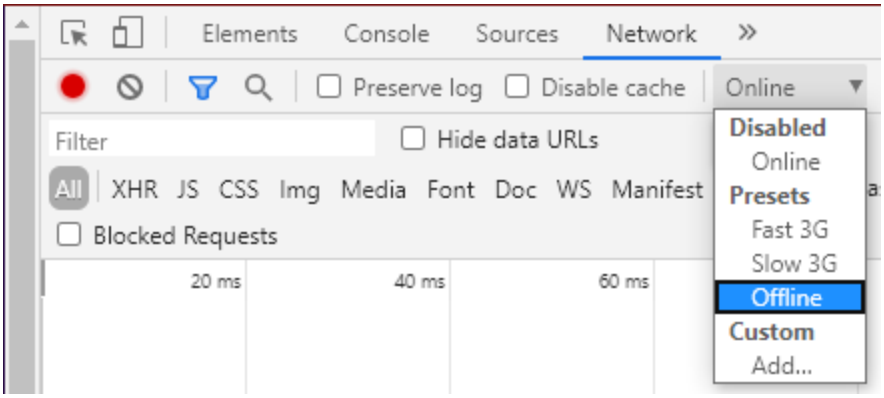
Mozilla Firefox'un

1. Üçlü noktaya basın `ellipsis` Adres çubuğunda düğme.
2. Seçin `Take a Screenshot` . .
3. Her ikisini de seçin `Save full page` ya da `Save visible` Seçenek.

Offline Mode (Çevrimdışı Mod)

Google Chrome

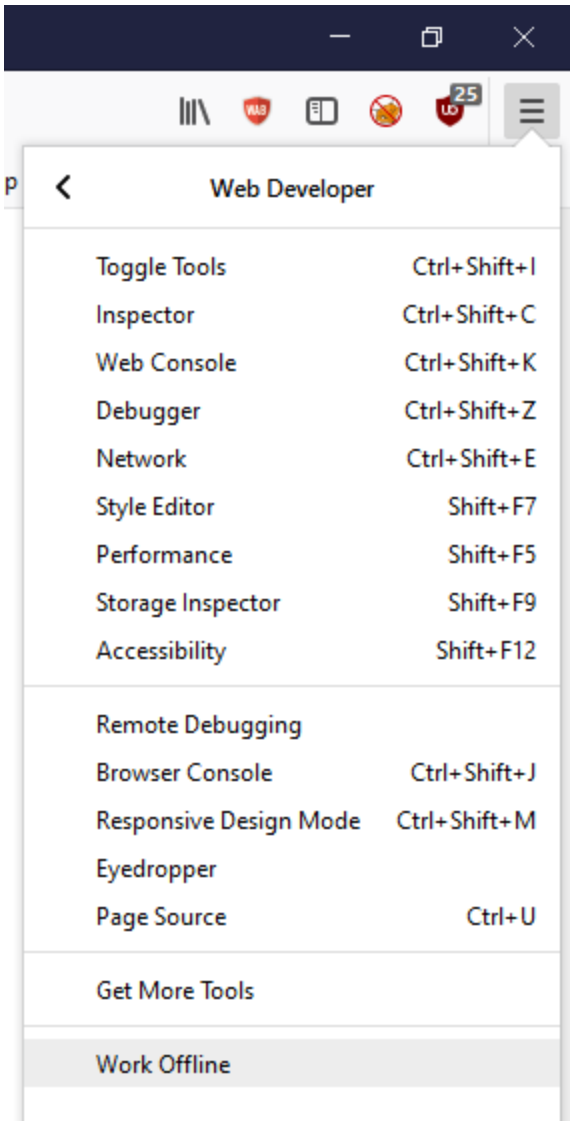
1. Gezinti yapmak için `Network` Taba.
2. İçinde `Throttle` Bırakma seçimi `Offline` . .



Şekil 6. F-6: Google Chrome Çevrimdışı Seçenek

Mozilla Firefox'un

1. Üçlü satır 'hamburger' (veya 'pancake') menüsünden seçim `Web Developer` Ve sonra `Work Offline` . .



Şekil 6. F-7: Mozilla Firefox Çevrimdışı Seçenek

Encoding and Decoding (Kodlama ve Kod Çözme)

Related Testing (İlgili Testler)

- Birçok (belki de çoğu) Web Uygulaması Güvenlik Testi türleri çeşitli kodlama türlerinden yararlanabilir.

General (Genel)

Tüm büyük tarayıcılar, ipleri Kodlamayı ve kod çözmeyi Dev Tools Konsolu ve JavaScript işlevselliğinden yararlanan çeşitli şekillerde destekler:

- Base64 kod: `btoa("string-to-encode")`
- Base64 decode: `atob("string-to-decode")`
- URL kod kodlayıcı: `encodeURIComponent("string-to-encode")`
- URL çözme: `decodeURIComponent("string-to-decode")`
- HTML kod kodu: `escape("string-to-encode")`
- HTML çözme: `unescape("string-to-decode")`

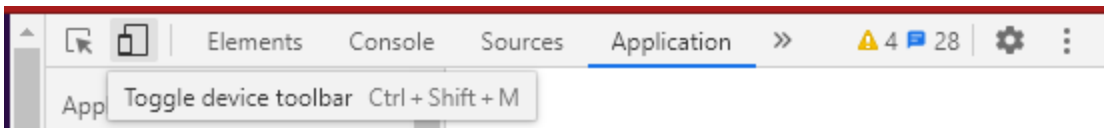
Responsive Design Mode (Duyarlı Tasarım Modu)

Related Testing (İlgili Testler)

- Tarayıcı Önbellek Zayıflıkları için Test
- Alternatif Kanalda Zayıf Kimlik Doğrulama Testi
- Clickjacking için Test

Google Chrome

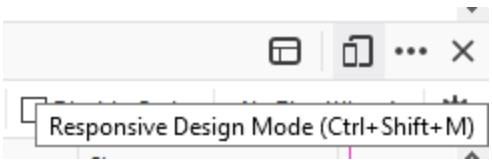
1. Tıklayını tıklayın `Toggle device toolbar` düğme veya tuşa basın `ctrl` + `shift` + `m` . .



Şekil 6. F-8: Google Chrome Duyarlı Tasarım Modu

Mozilla Firefox'un

1. Tıklayını tıklayın `Responsive Design Mode` düğme veya tuşa basın `ctrl` + `shift` + `m` . .



Şekil 6. F-9: Mozilla Firefox Duyarlı Tasarım Modu

Referances (Referanslar)

- Tarayıcılarla Web Uygulaması Güvenlik Testi

- Black Hills Bilgi Güvenliği - Webcast: Ücretsiz Araçlar! Webapp Pentests'te Geliştirici Araçları ve JavaScript Nasıl Kullanılır
- Greg Malcolm - Chrome Geliştirici Araçları: Armory'ye Baskın
- UserAgent Strings Listesi