

A6 – Sensitive Data Exposure

Nedir?(Top 10 2013-A6-Sensitive Data Exposure. Owasp.

https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure .)

Hassas verilerinize (çalışmayan veya taşınan hatta müşterilerin tarayıcılarında tutulan veriler gibi) erişebilecek kişiler verilerin güvenliği için doğrudan veya dolaylı olarak tehdit oluşturabilir. Bu verilerin açık/okunabilir olarak depolanması saldırıların kolayca erişip kullanabilmesine olanak sağlar.

Saldırıları genellikle direkt olarak kriptolu veriyi kırmaya çalışmazlar. Sunuculardan, müşterilerin tarayıcılarından veya taşınan verileri çalmak, aradaki adam saldırısı (man-in-the-middle attack) yapmak veya anahtarları çalmak gibi yollar kullanırlar.

Uygulama

Owasp 2013 -> A6 – Sensitive Data Exposure -> Information Disclosure -> Robots.txt sayfasındaki açıklamalardan yola çıkarak Mutillidae uygulamasının robots.txt dosyasına erişim ve içeriği adım adım anlatılmaktadır.

Robots.txt nedir?(<https://support.google.com/webmasters/answer/6062608?hl=tr>)

robots.txt dosyası, arama motoru tarayıcılarının sitenizde erişmesini istemediğiniz yerleri gösteren ve sitenizin kök dizininde bulunan bir dosyadır.

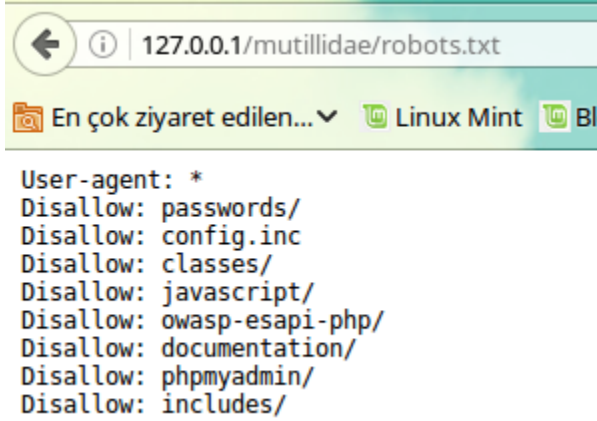
(<https://adrvs.wordpress.com/2017/02/14/robot-txt-dosyasi/>)

Robots.txt dosyası sitenizin kök dizininde bulunur. Yani bir arama motoru sitenizi indexlemeye çalıştığında ilk yaptığı şey sitenizin kök dizininde bu dosyayı aramak olacaktır. Bu dosya mevcut ise sitenizde izin verdiğiniz kısımları gezmeye başlarlar. Eğer bu dosya mevcut değilse sitenizin tamamını taraması gerektiğini düşüneceğinden her yerini indexlerler.

Robots.txt dosyası bazı kaynaklara göre bir güvenlik zafiyeti olarak değerlendirilmektedir. Bunun nedeni ise sitenizin güvenlik açısından sorun oluşturabilecek dizinlerini burada kaydetmiş oluyorsunuz. Yani bir arama motoru sitenizin gezmeyeceği yerleri bu dosyayı okuyarak görebilir. Bunu kötü niyetli bir kişi okursa admin paneline otomatik olarak ulaşabilir. Sitenizin sorun oluşturabilecek her dizini burada olduğu için direkt olarak Robots.txt dosyasını okuyup sitenizde zafiyet armaya çalışabilecek kişiler olabilir.

URL	http://127.0.0.1/mutillidae/robots.txt
HTTP Talep Türü	GET

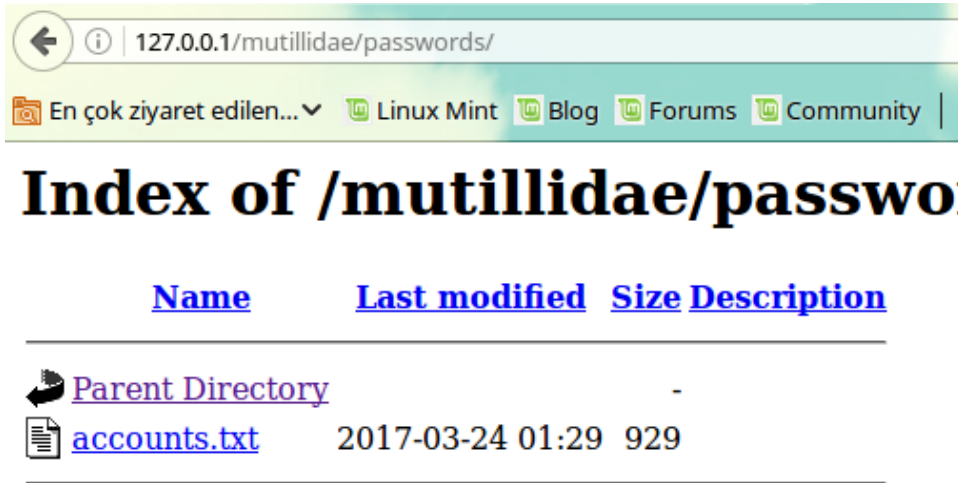
1. URL'e "http://127.0.0.1/mutillidae/robots.txt" yazılarak içeriği kontrol edilir. Aşağıda robots.txt içerisinde indekslenmesi istenmeyen dizinler görülmektedir.



The screenshot shows a web browser window with the address bar displaying "127.0.0.1/mutillidae/robots.txt". Below the address bar, there is a navigation bar with a search icon, a dropdown menu labeled "En çok ziyaret edilen...", and several social media icons including Linux Mint, Blog, Forums, and Community. The main content area displays the robots.txt file content, which lists disallowed paths: passwords/, config.inc, classes/, javascript/, owasp-esapi-php/, documentation/, phpmyadmin/, and includes/.

```
User-agent: *  
Disallow: passwords/  
Disallow: config.inc  
Disallow: classes/  
Disallow: javascript/  
Disallow: owasp-esapi-php/  
Disallow: documentation/  
Disallow: phpmyadmin/  
Disallow: includes/
```

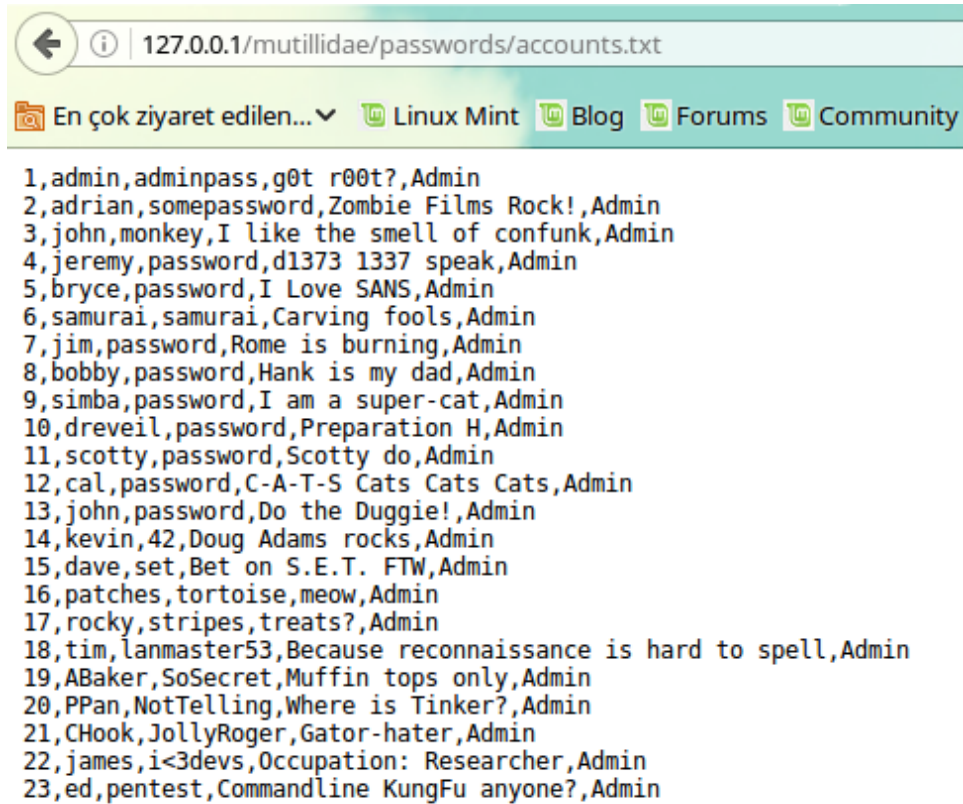
2. URL'in devamına /passwords/ yazılarak kök dizin içerisindeki bu dosyanın içeriğine bakılır. "accounts.txt" isminde bir dosya görülmektedir. Kullanıcı hesapları ile ilgili bilgiler içerdiği tahmin edilen bu dosya kontrol edilir.



The screenshot shows a web browser window with the address bar displaying "127.0.0.1/mutillidae/passwords/". Below the address bar, there is a navigation bar with a search icon, a dropdown menu labeled "En çok ziyaret edilen...", and several social media icons including Linux Mint, Blog, Forums, and Community. The main content area displays the "Index of /mutillidae/passwords/" directory listing. The table has columns for Name, Last modified, Size, and Description. It lists two items: "Parent Directory" and "accounts.txt".

Name	Last modified	Size	Description
Parent Directory		-	
accounts.txt	2017-03-24 01:29	929	

3. URL'in devamına accounts.txt yazılarak kullanıcı isimleri, şifreleri vb. bilgilerin bulunduğu içerik görüntülenebilmektedir.



The screenshot shows a web browser window with the address bar displaying `127.0.0.1/mutillidae/passwords/accounts.txt`. Below the address bar, there is a navigation bar with links for "En çok ziyaret edilen...", "Linux Mint", "Blog", "Forums", and "Community". The main content area displays a list of 23 entries, each consisting of a username, a password, and a role (all are "Admin").

```
1,admin,adminpass,g0t r00t?,Admin
2,adrian,somepassword,Zombie Films Rock!,Admin
3,john,monkey,I like the smell of confunk,Admin
4,jeremy,password,d1373 1337 speak,Admin
5,bryce,password,I Love SANS,Admin
6,samurai,samurai,Carving fools,Admin
7,jim,password,Rome is burning,Admin
8,bobby,password,Hank is my dad,Admin
9,simba,password,I am a super-cat,Admin
10,dreveil,password,Preparation H,Admin
11,scotty,password,Scotty do,Admin
12,cal,password,C-A-T-S Cats Cats Cats,Admin
13,john,password,Do the Duggie!,Admin
14,kevin,42,Doug Adams rocks,Admin
15,dave,set,Bet on S.E.T. FTW,Admin
16,patches,tortoise,meow,Admin
17,rocky,stripes,treats?,Admin
18,tim,lanmaster53,Because reconnaissance is hard to spell,Admin
19,ABaker,SoSecret,Muffin tops only,Admin
20,PPan,NotTelling,Where is Tinker?,Admin
21,CHook,JollyRoger,Gator-hater,Admin
22,james,i<3devs,Occupation: Researcher,Admin
23,ed,pentest,Commandline KungFu anyone?,Admin
```