Web Application Pentesting

Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

HTTP Digest Authentication RFC 2069

HTTP Digest Authentication

- Basic Authentication sends User:Pass in plaintext
- Digest Authentication sends a Hash of the password
- RFC 2069, 2617

http://en.wikipedia.org/wiki/Digest_access_authentication

Initial Version – RFC 2069

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Digest     realm="testrealm@host.com",
                             nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
                             opaque="5ccc069c403ebaf9f0171e9517f40e41"

   The client may prompt the user for the username and password, after
   which it will respond with a new request, including the following
   Authorization header:

Authorization: Digest        username="Mufasa",
                             realm="testrealm@host.com",
                             nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
                             uri="/dir/index.html",
                             response="e966c932a9242554e42c8ee200cec7f6",
                             opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

Source: http://tools.ietf.org/html/rfc2069

Response Calculation

Hash1 = MD5(Username:Realm:Password)

Hash1 = MD5(admin:Pentester Academy:asdss)

Hash2 = MD5(method:URI)

Hash2 = MD5(GET:/lab/webapp/digest2/1)

Response Calculation

Hash1 = MD5(Username:Realm:Password)

Hash2 = MD5(method:URI)

Response = MD5(Hash1:Nonce:Hash2)

Wireshark