

# 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](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

```
▼ Hypertext Transfer Protocol
▼ HTTP/1.1 401 Unauthorized\r\n
  ▶ [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
    Request Version: HTTP/1.1
    Status Code: 401
    Response Phrase: Unauthorized
    Content-Type: text/html; charset=utf-8\r\n
    Cache-Control: no-cache\r\n
    WWW-Authenticate: Digest realm="Pentester Academy" nonce="c671e71e6105016b797f16b809a0ac69" opaque=""\r\n
    Content-Encoding: gzip\r\n
    Vary: Accept-Encoding\r\n
    Date: Thu, 19 Sep 2013 15:29:57 GMT\r\n
    Server: Google Frontend\r\n
  ▶ Content-Length: 1100\r\n
    Alternate-Protocol: 80:quic\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.412894000 seconds]
    \[Request in frame: 75\]
    \[Next request in frame: 144\]
    \[Next response in frame: 150\]
    Content-encoded entity body (gzip): 1100 bytes -> 2780 bytes
  ▶ Line-based text data: text/html
```