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 Hashing Time! (RFC 2069)

Response Calculation (RFC 2069)

Hash1 = MD5(Username:Realm:Password)

Hash2 = MD5(method:URI)

Response = MD5(Hash1:Nonce:Hash2)

Hash1 Calculation

Hash1 = MD5(Username:Realm:Password)

```
PentesterAcademy# python
Python 2.7.1 (r271:86832, Jul 31 2011, 19:30:53)
[GCC 4.2.1 (Based on Apple Inc. build 5658) (LLVM build 2335.15.00)] on darwin
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>> import hashlib
>>>
>>> hash1 = hashlib.md5('admin:Pentester Academy:asdss').hexdigest()
>>>
>>> hash1
'a524e9245a8bf88560d2bb74a02a8779'
>>>
>>>
```

Hash2 Calculation

Hash2 = MD5(method:URI)

```
PentesterAcademy#
PentesterAcademy# python
Python 2.7.1 (r271:86832, Jul 31 2011, 19:30:53)
[GCC 4.2.1 (Based on Apple Inc. build 5658) (LLVM build 2335.15.00)] on darwin
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>> import hashlib
>>>
>>> hash2 = hashlib.md5('GET:/lab/webapp/digest2/1').hexdigest()
>>>
>>> hash2
'210e62c14f54e4a5f76da73fc1cfa73b'
>>>
>>>
```

Response Calculation

Response = MD5(Hash1:Nonce:Hash2)

```
>>>
>>> import hashlib
>>>
>>> nonce = "c671e71e6105016b797f16b809a0ac69"
>>>
>>> hash1 = hashlib.md5('admin:Pentester Academy:asdss').hexdigest()
>>>
>>> hash2 = hashlib.md5('GET:/lab/webapp/digest2/1').hexdigest()
>>>
>>> response = hashlib.md5("%s:%s:%s" % (hash1, nonce, hash2)).hexdigest()
>>>
>>> hash1
'a524e9245a8bf88560d2bb74a02a8779'
>>> hash2
'210e62c14f54e4a5f76da73fc1cfa73b'
>>> response
'8b8e22a52910eaeab8c9eff78beed84c'
>>>
```