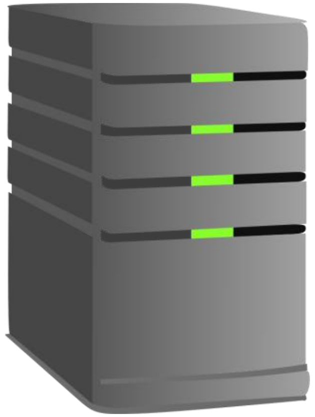
Data exposure

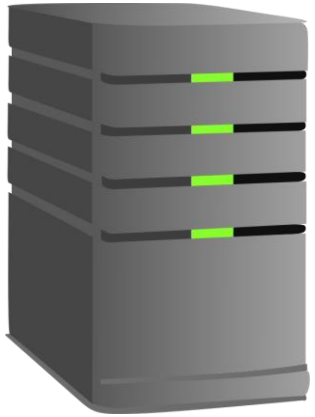
Fredrik Hesse

#6

Accidentally publishing data

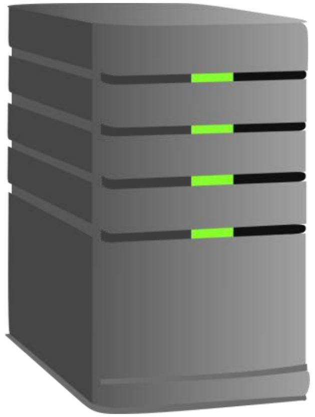
Thinking data wont be published



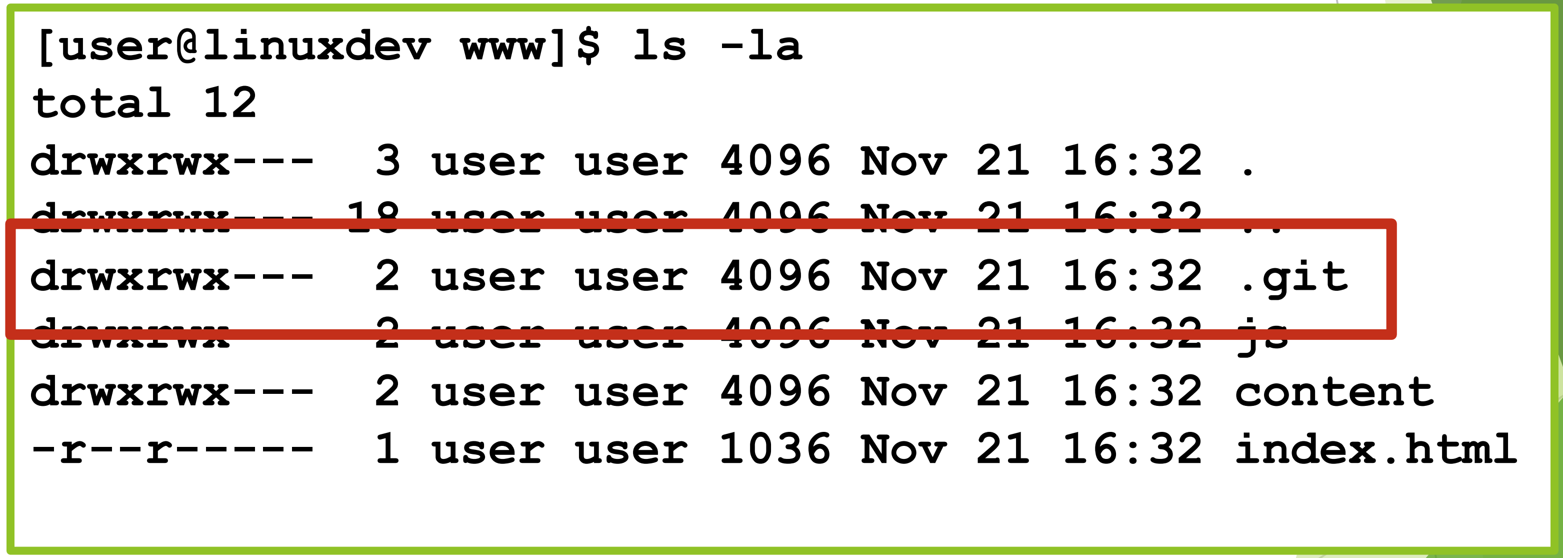


Files on the server

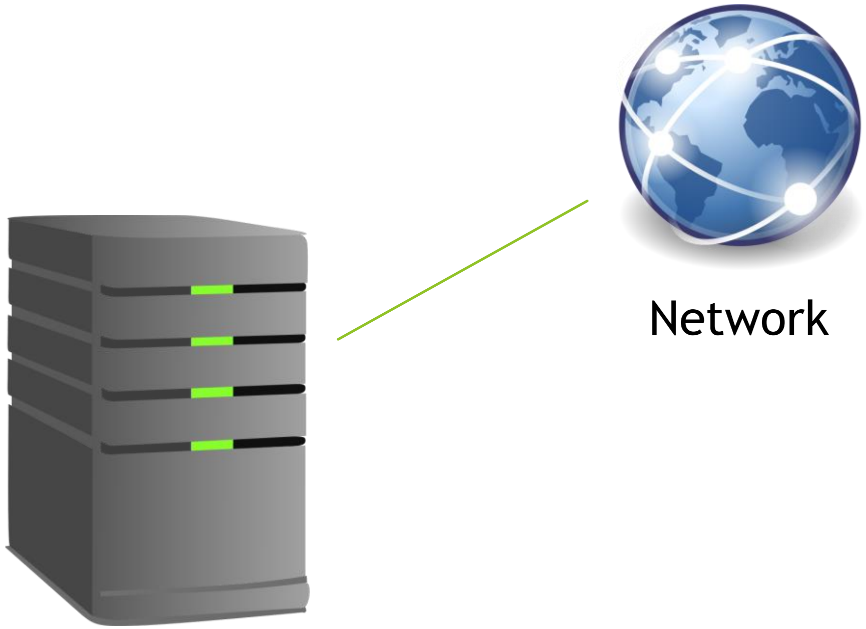
```
[user@linuxdev www]$ ls -la
total 12
drwxrwx---  3 user user 4096 Nov 21 16:32 .
drwxrwx--- 18 user user 4096 Nov 21 16:32 ..
drwxrwx---  2 user user 4096 Nov 21 16:32 .git
drwxrwx---  2 user user 4096 Nov 21 16:32 js
drwxrwx---  2 user user 4096 Nov 21 16:32 content
-r--r-----  1 user user 1036 Nov 21 16:32 index.html
```



Files on the server

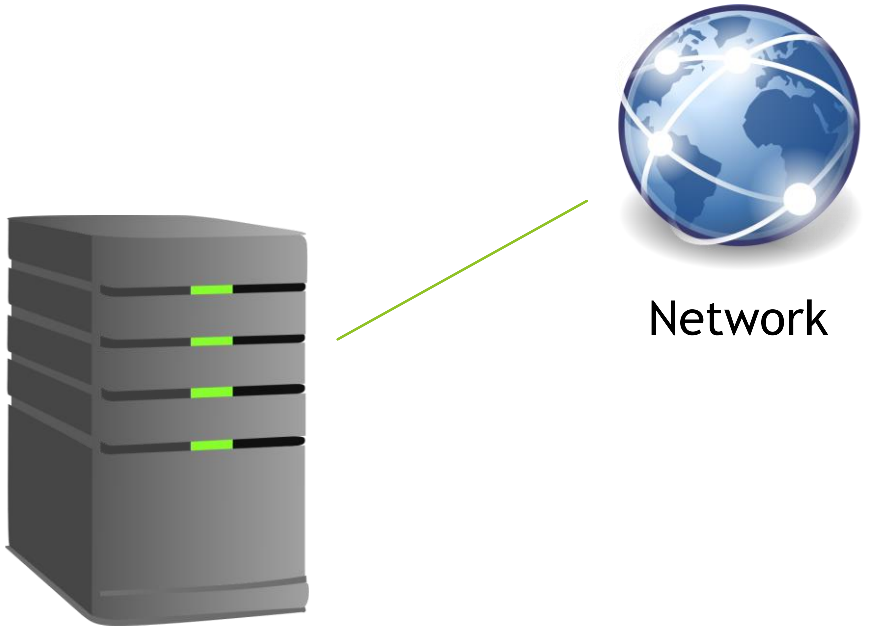


```
[user@linuxdev www]$ ls -la
total 12
drwxrwx---  3 user user 4096 Nov 21 16:32 .
drwxrwx--- 18 user user 4096 Nov 21 16:32 ..
drwxrwx---  2 user user 4096 Nov 21 16:32 .git
drwxrwx---  2 user user 4096 Nov 21 16:32 js
drwxrwx---  2 user user 4096 Nov 21 16:32 content
-r--r-----  1 user user 1036 Nov 21 16:32 index.html
```



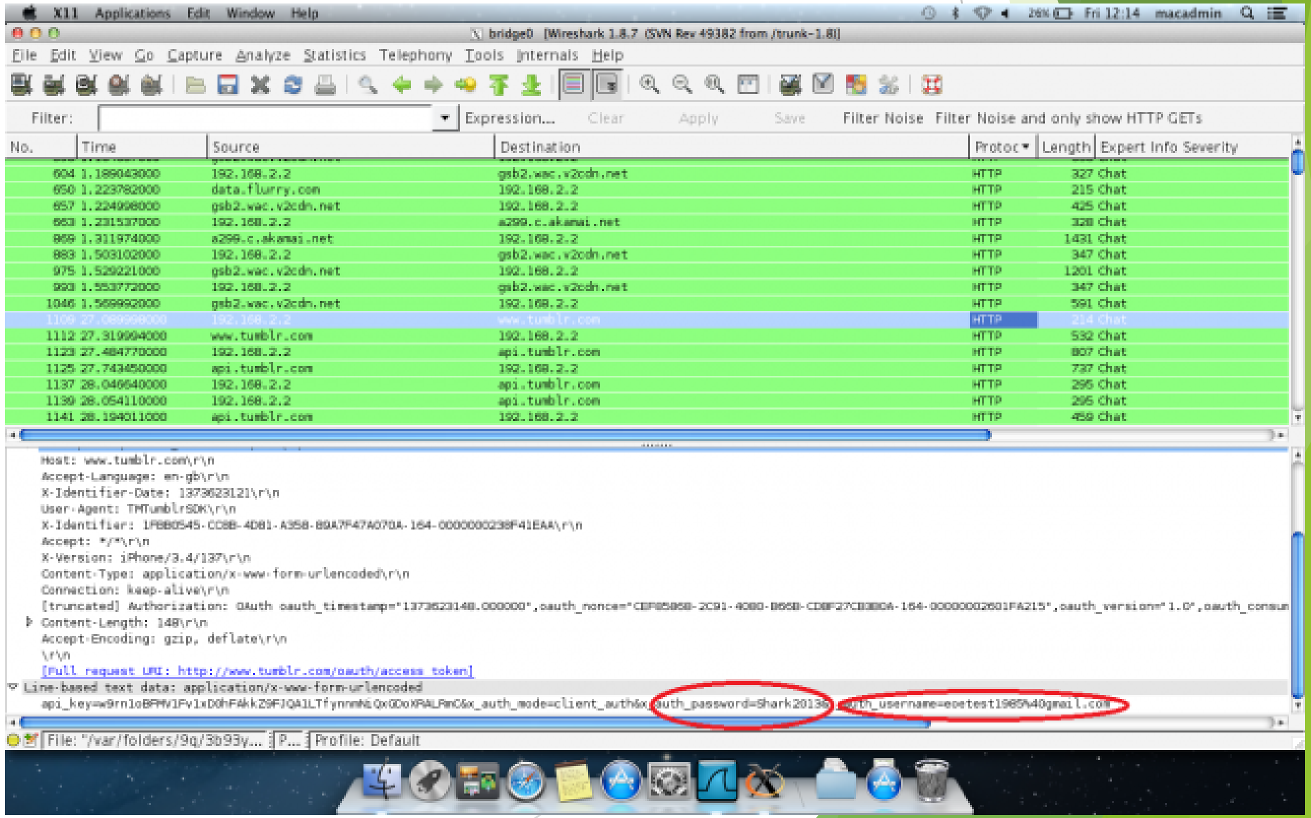
Network

Files on the server



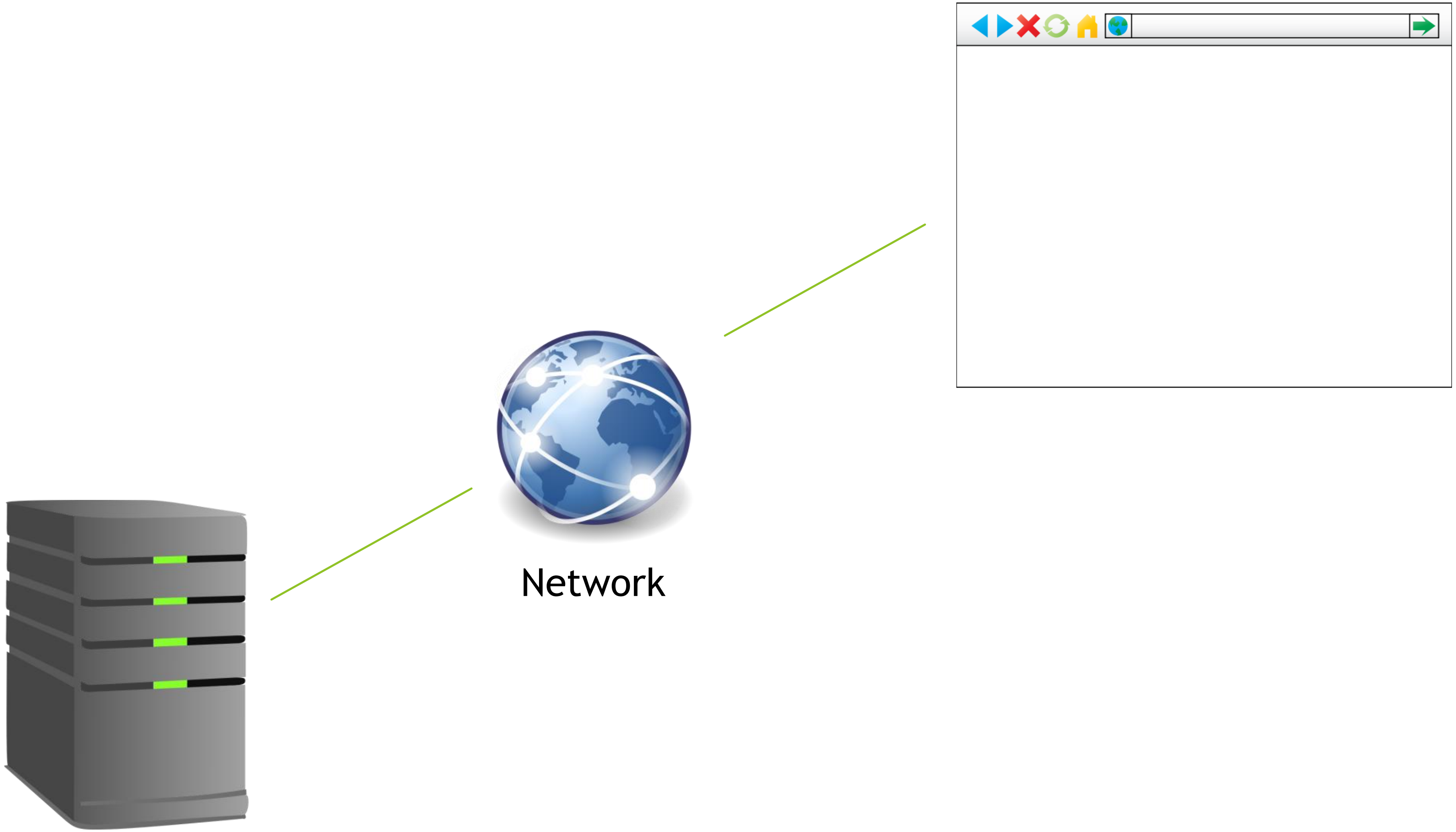
Network

Files on the server


X11 Applications Edit Window Help
Fri 12:14 macadmin
bridge0 [Wireshark 1.8.7 (SVN Rev 49382 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save Filter Noise Filter Noise and only show HTTP GETs

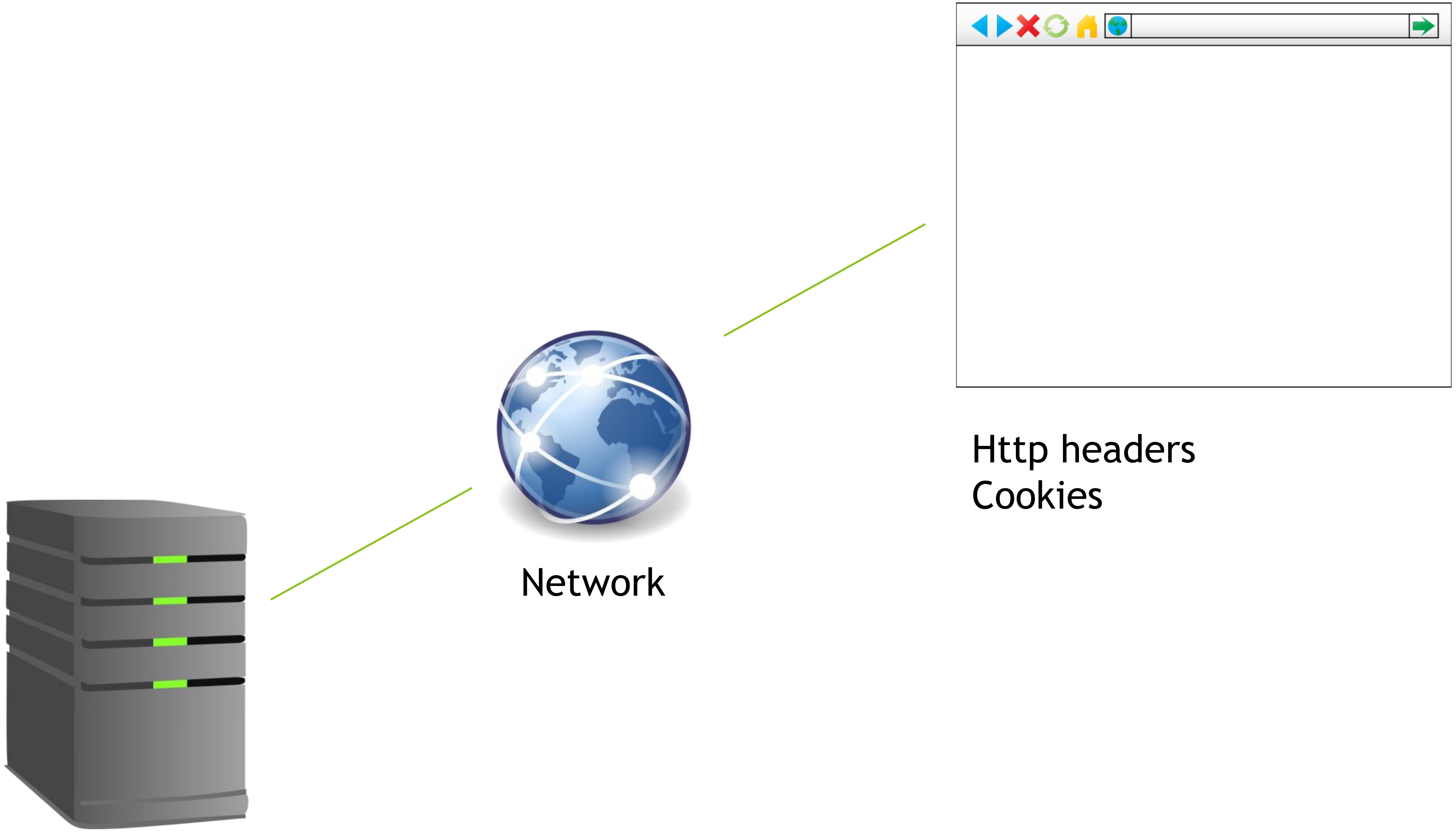
```
No.    Time            Source               Destination          Protoc  Length Expert Info Severity
  604 1.189043000     192.168.2.2          gsb2.wac.v2cdn.net   HTTP     327 Chat
  650 1.223782000     data.flurry.com      192.168.2.2          HTTP     215 Chat
  657 1.224998000     gsb2.wac.v2cdn.net   192.168.2.2          HTTP     425 Chat
  663 1.231537000     192.168.2.2          a299.c.akamai.net    HTTP     328 Chat
  869 1.311974000     a299.c.akamai.net    192.168.2.2          HTTP    1431 Chat
  883 1.503102000     192.168.2.2          gsb2.wac.v2cdn.net   HTTP     347 Chat
  975 1.529221000     gsb2.wac.v2cdn.net   192.168.2.2          HTTP    1201 Chat
  993 1.553772000     192.168.2.2          gsb2.wac.v2cdn.net   HTTP     347 Chat
 1046 1.569992000     gsb2.wac.v2cdn.net   192.168.2.2          HTTP     591 Chat
 1109 27.089998000    192.168.2.2          www.tumblr.com       HTTP     214 Chat
 1112 27.319994000    www.tumblr.com       192.168.2.2          HTTP     532 Chat
 1123 27.484770000    192.168.2.2          api.tumblr.com       HTTP     807 Chat
 1125 27.743450000    api.tumblr.com       192.168.2.2          HTTP     737 Chat
 1137 28.046640000    192.168.2.2          api.tumblr.com       HTTP     295 Chat
 1139 28.054110000    192.168.2.2          api.tumblr.com       HTTP     295 Chat
 1141 28.194011000    api.tumblr.com       192.168.2.2          HTTP     459 Chat
```

```
    Host: www.tumblr.com\r\n
    Accept-Language: en-gb\r\n
    X-Identifier-Date: 1373623121\r\n
    User-Agent: TMTumblrSDK\r\n
    X-Identifier: 1FBB0545-CC8B-4D81-A358-89A7F47A070A-164-0000000238F41EAA\r\n
    Accept: */*\r\n
    X-Version: iPhone/3.4/137\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    Connection: keep-alive\r\n
    [truncated] Authorization: OAuth oauth_timestamp="1373623148.000000",oauth_nonce="CEF85868-2C91-4080-B65B-CD8F27CB3BDA-164-00000002601FA215",oauth_version="1.0",oauth_consun
  ▷ Content-Length: 148\r\n
    Accept-Encoding: gzip, deflate\r\n
    \r\n
    [Full request URI: http://www.tumblr.com/oauth/access_token]
▽ Line-based text data: application/x-www-form-urlencoded
    api_key=w9rn1oBFMV1Fv1xD0hFAkkZ9FJQA1LTfynnmNiQxGDoXRALRmC&x_auth_mode=client_auth&x_auth_password=Shark2013&x_auth_username=eoetest1985%40gmail.com
```



Network

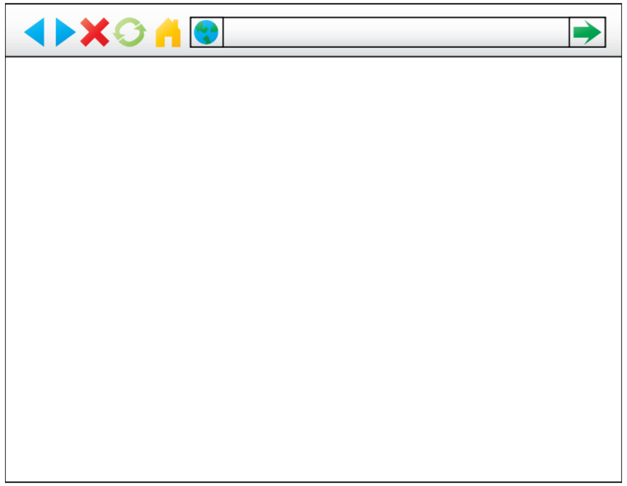
Files on the server



Http headers
Cookies

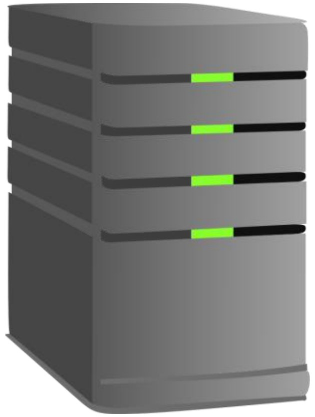
Network

Files on the server



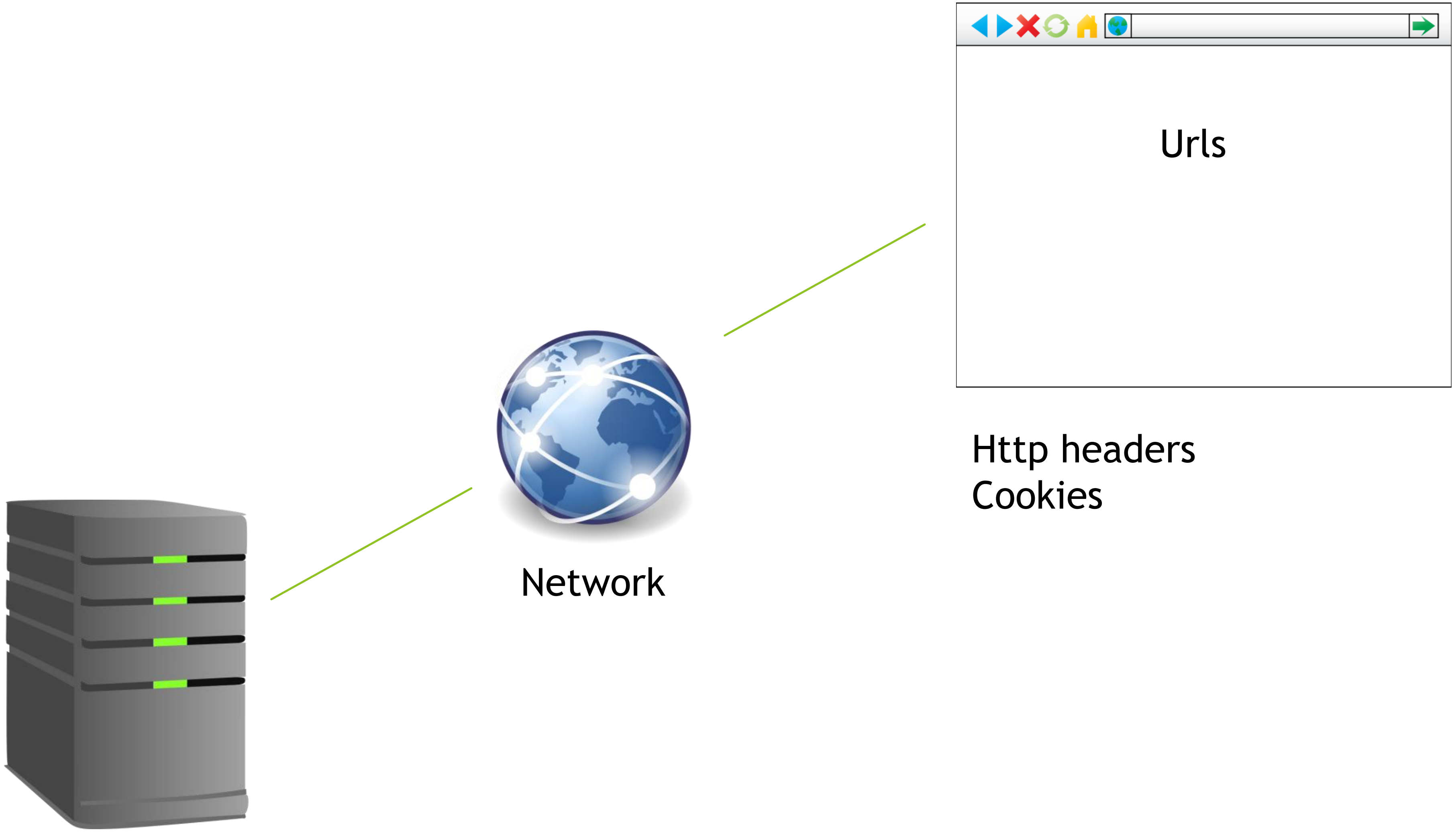
Http headers
Cookies

Network



Files on the server

```
Response Headers
        X-Usergroup: Admins
        X-Session: 14758f1afd44c09b7992073ccf00b43d
Cookies
        UserRole: Admin
```

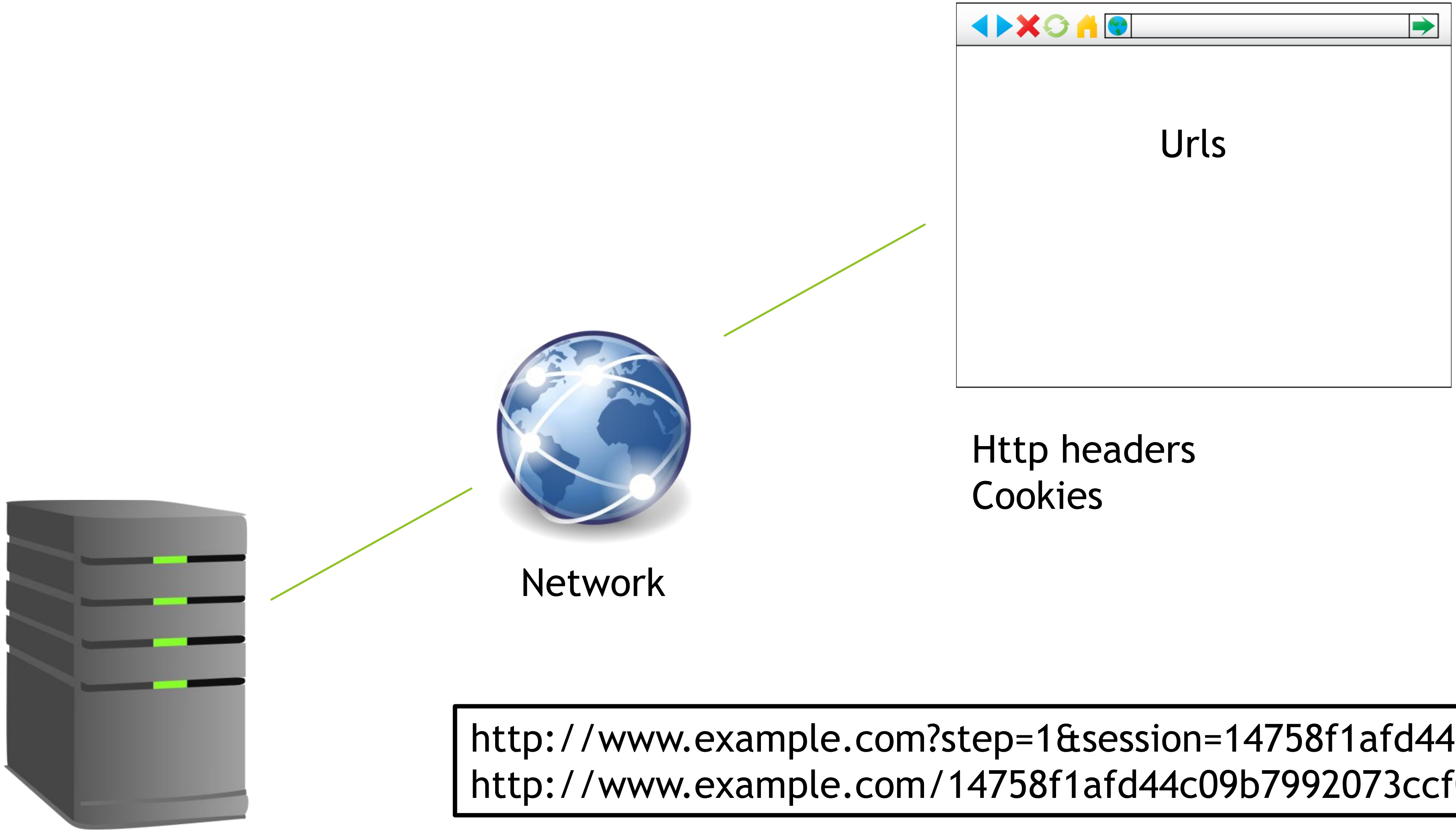


Files on the server

Network

Urls

Http headers
Cookies



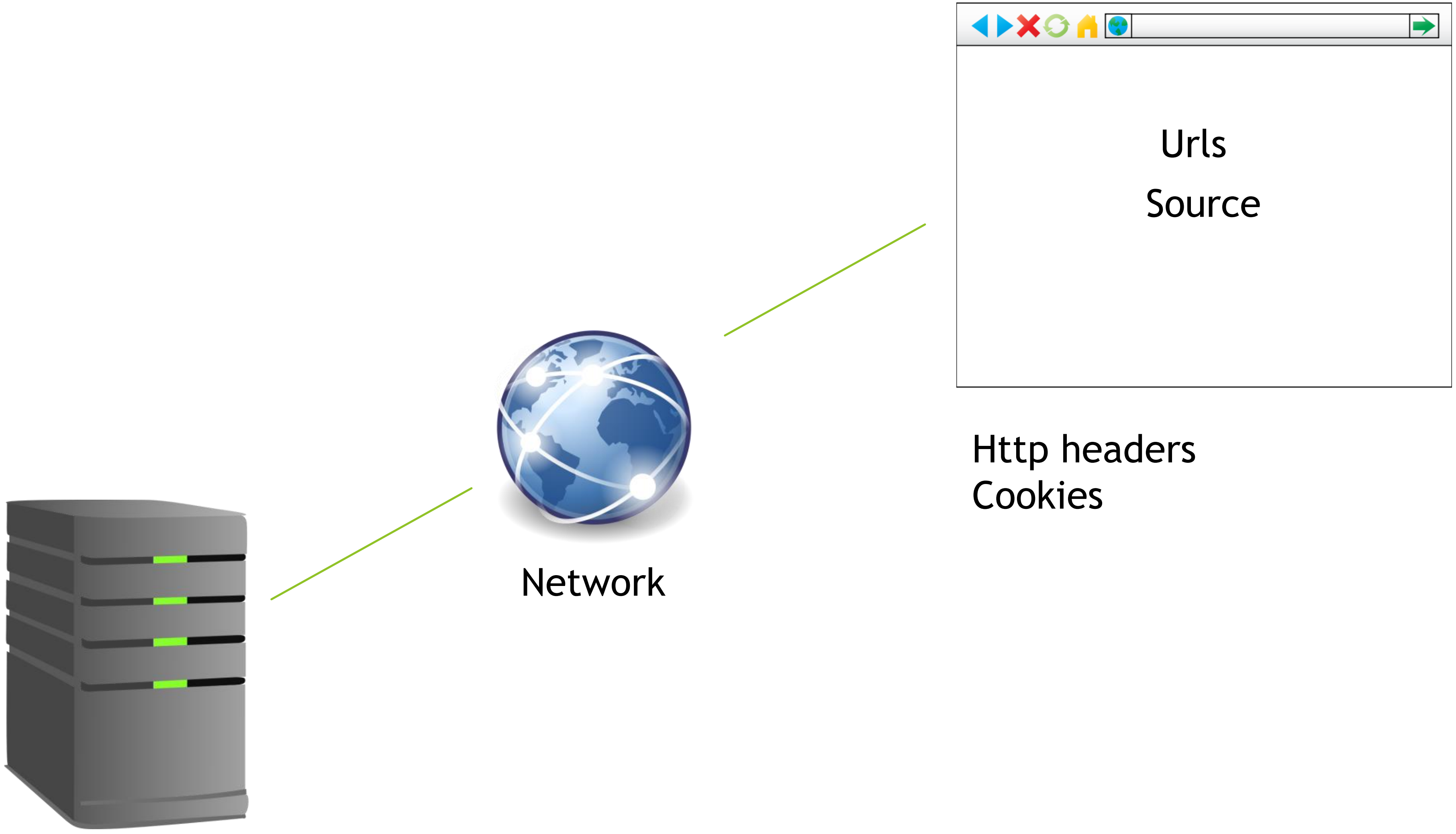
Urls

Http headers
Cookies

Network

Files on the server

```
http://www.example.com?step=1&session=14758f1afd44c09b7992073ccf00b43d
http://www.example.com/14758f1afd44c09b7992073ccf00b43d/index.html
```



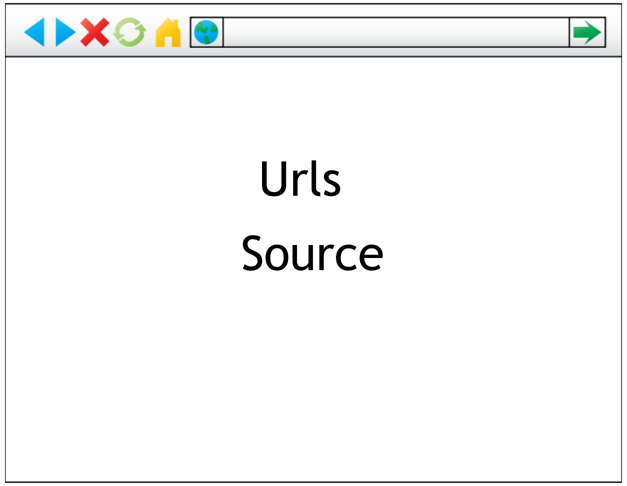
Urls

Source

Http headers
Cookies

Network

Files on the server

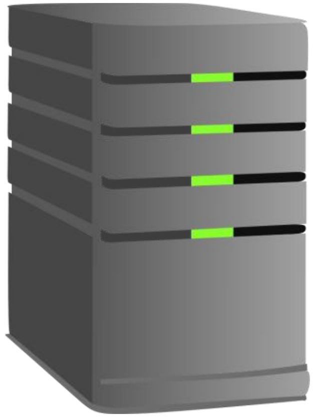


Urls

Source

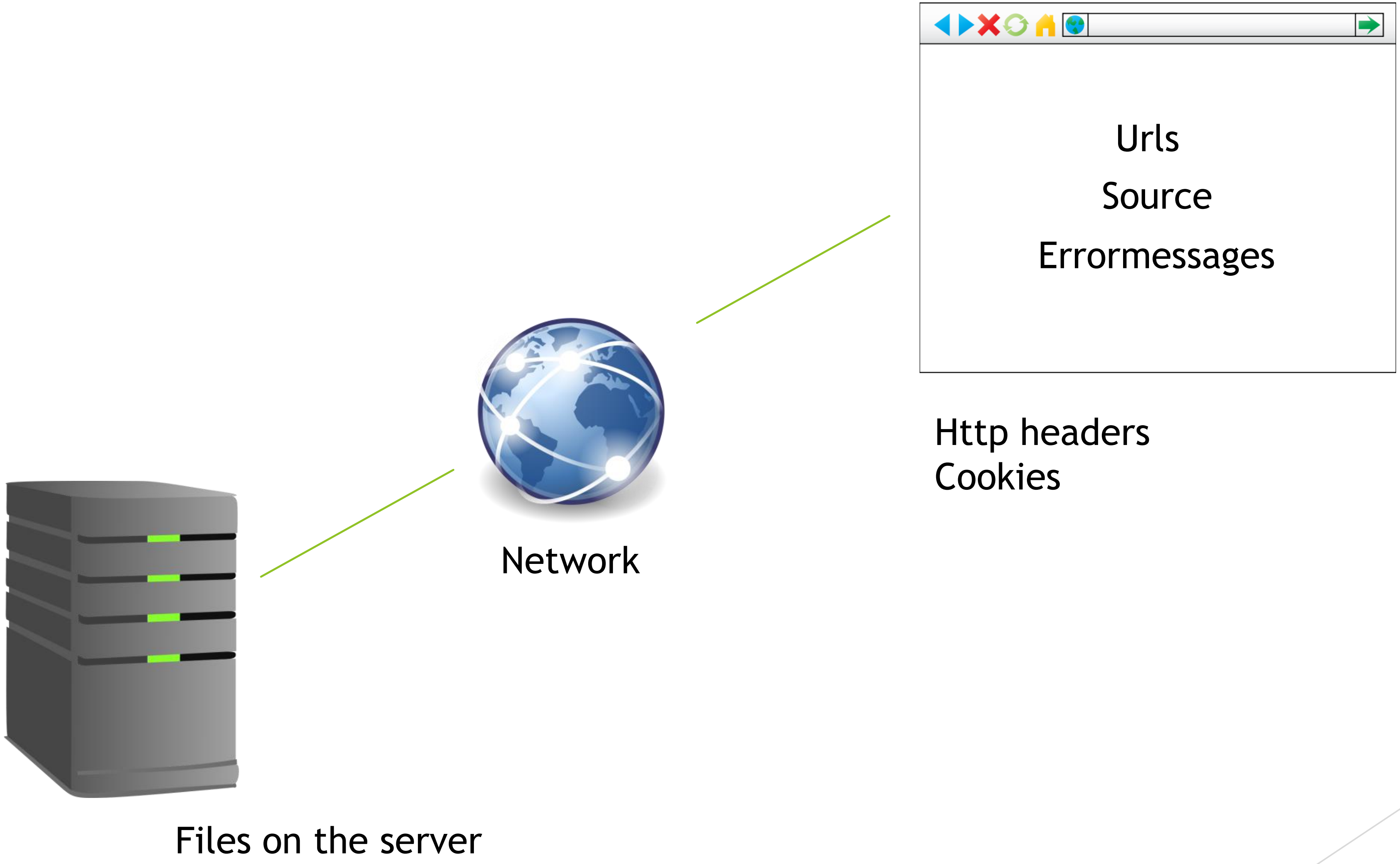
Http headers
Cookies

Network



Files on the server

```
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwULLTEyMzE0Mjg3NjgPZB
YEZg9kFgwCBA8PFgIeB1Zpc2libGVoZGQCBQ8PFgIfAGhkZAIGDw8WAh8AaGQWAgIBDw8WAh4EVGV4dAU
PMDc3MSAtIDE0IDE1IDE2ZGQCBw8PFgIfAGhkZAIIDw8WAh8AaGRkAgoPDxYCHwBoZBYEAgEPDxYCHwBoZ
BYCAgEPDxYCHwEFBDEwMDBkZAIDDw8WAh8AaGQWAgIBDw8WAh8BBQIzMGRkAgEPDxYCHwEFFzwhLS0g
U2lzc2lzIHZlcnNpb24gLS0+ZGRkj6kdnfLuJSOWJIP6KsrotyG0+85G0/SQFeKZF0W2Uz4=" />
```



Urls

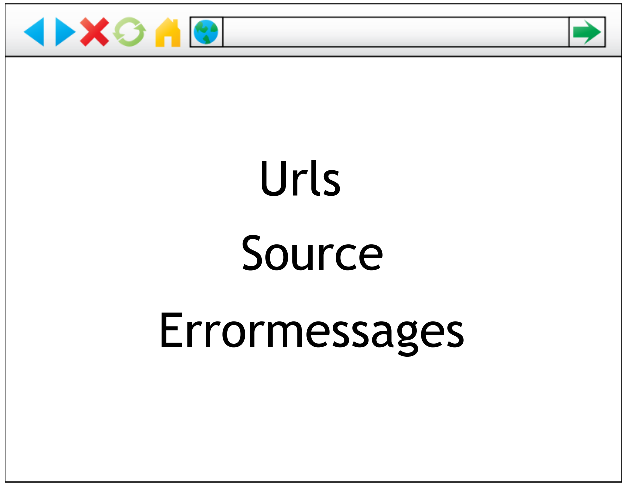
Source

Errormessages

Http headers
Cookies

Network

Files on the server



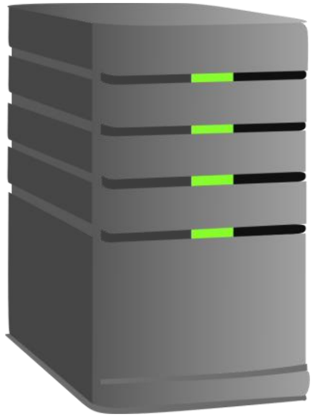
Urls

Source

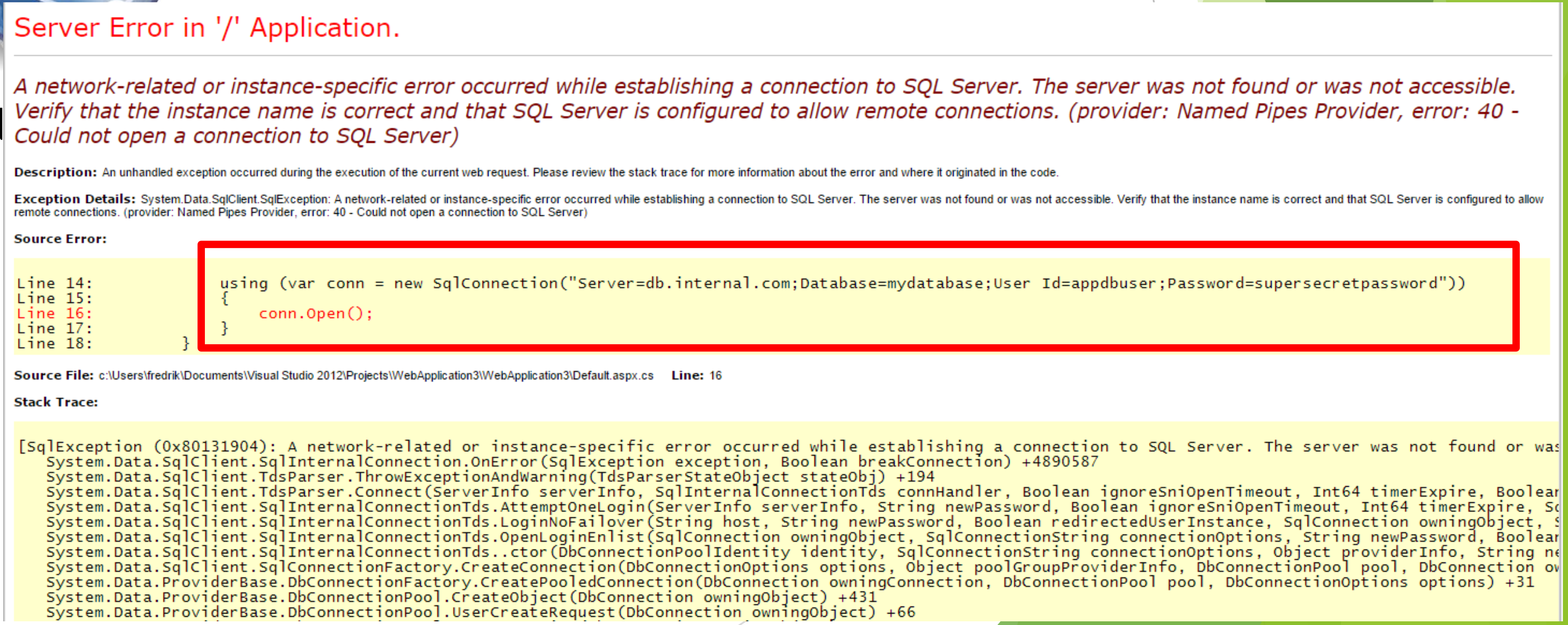
Errormessages

Http headers

N



Files on the server



Server Error in '/' Application.

A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)

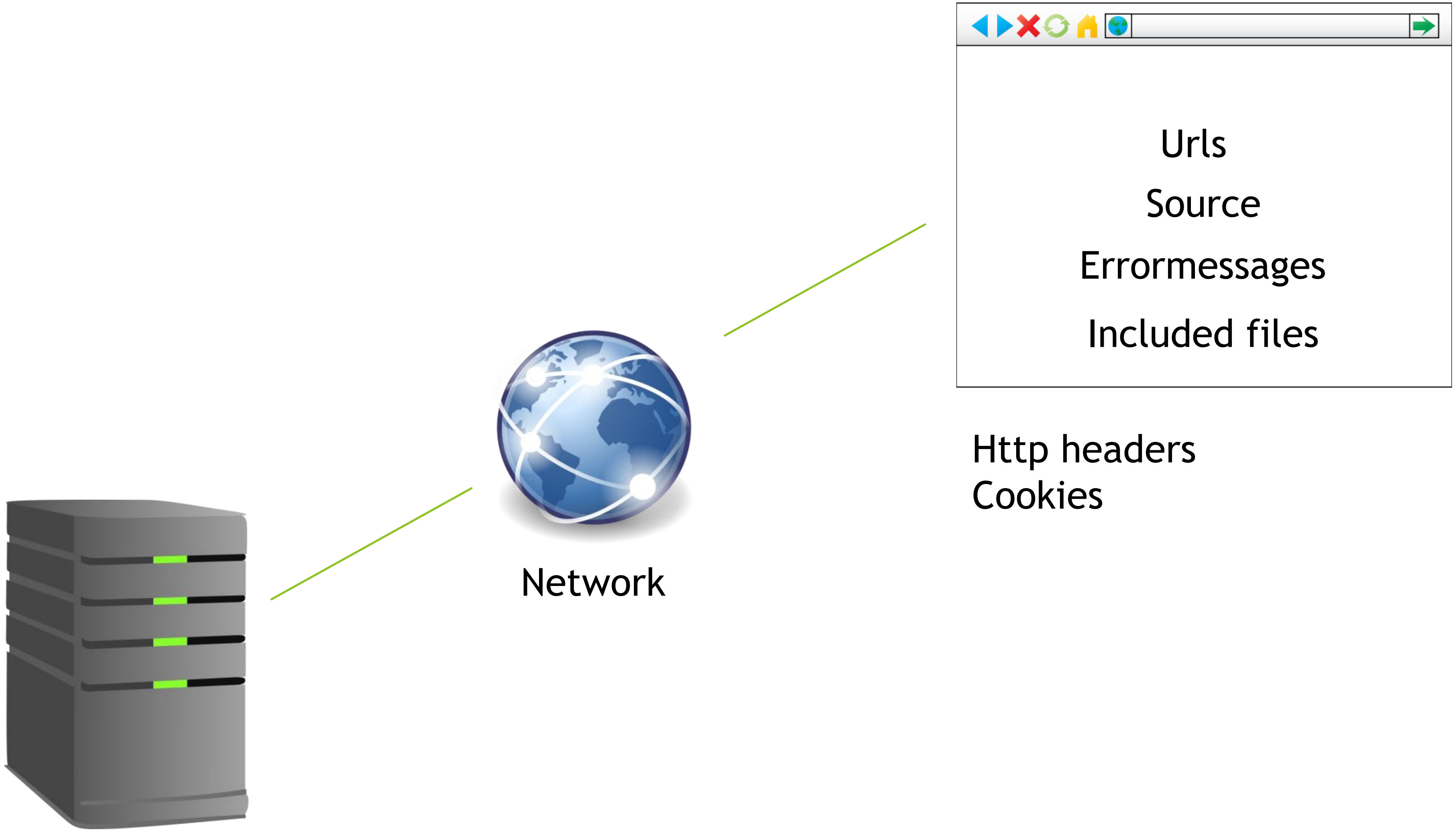
Source Error:

```
Line 14:            using (var conn = new SqlConnection("Server=db.internal.com;Database=mydatabase;User Id=appdbuser;Password=supersecretpassword"))
Line 15:            {
Line 16:                conn.Open();
Line 17:            }
Line 18:        }
```

Source File: c:\Users\fredrik\Documents\Visual Studio 2012\Projects\WebApplication3\WebApplication3\Default.aspx.cs   **Line:** 16

Stack Trace:

```
[SqlException (0x80131904): A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was
   System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection) +4890587
   System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +194
   System.Data.SqlClient.TdsParser.Connect(ServerInfo serverInfo, SqlInternalConnectionTds connHandler, Boolean ignoreSniOpenTimeout, Int64 timerExpire, Boolea
   System.Data.SqlClient.SqlInternalConnectionTds.AttemptOneLogin(ServerInfo serverInfo, String newPassword, Boolean ignoreSniOpenTimeout, Int64 timerExpire, Sc
   System.Data.SqlClient.SqlInternalConnectionTds.LoginNoFailover(String host, String newPassword, Boolean redirectedUserInstance, SqlConnection owningObject, S
   System.Data.SqlClient.SqlInternalConnectionTds.OpenLoginEnlist(SqlConnection owningObject, SqlConnectionString connectionOptions, String newPassword, Boolea
   System.Data.SqlClient.SqlInternalConnectionTds..ctor(DbConnectionPoolIdentity identity, SqlConnectionString connectionOptions, Object providerInfo, String ne
   System.Data.SqlClient.SqlConnectionFactory.CreateConnection(DbConnectionOptions options, Object poolGroupProviderInfo, DbConnectionPool pool, DbConnection ow
   System.Data.ProviderBase.DbConnectionFactory.CreatePooledConnection(DbConnection owningConnection, DbConnectionPool pool, DbConnectionOptions options) +31
   System.Data.ProviderBase.DbConnectionPool.CreateObject(DbConnection owningObject) +431
   System.Data.ProviderBase.DbConnectionPool.UserCreateRequest(DbConnection owningObject) +66
```



Urls

Source

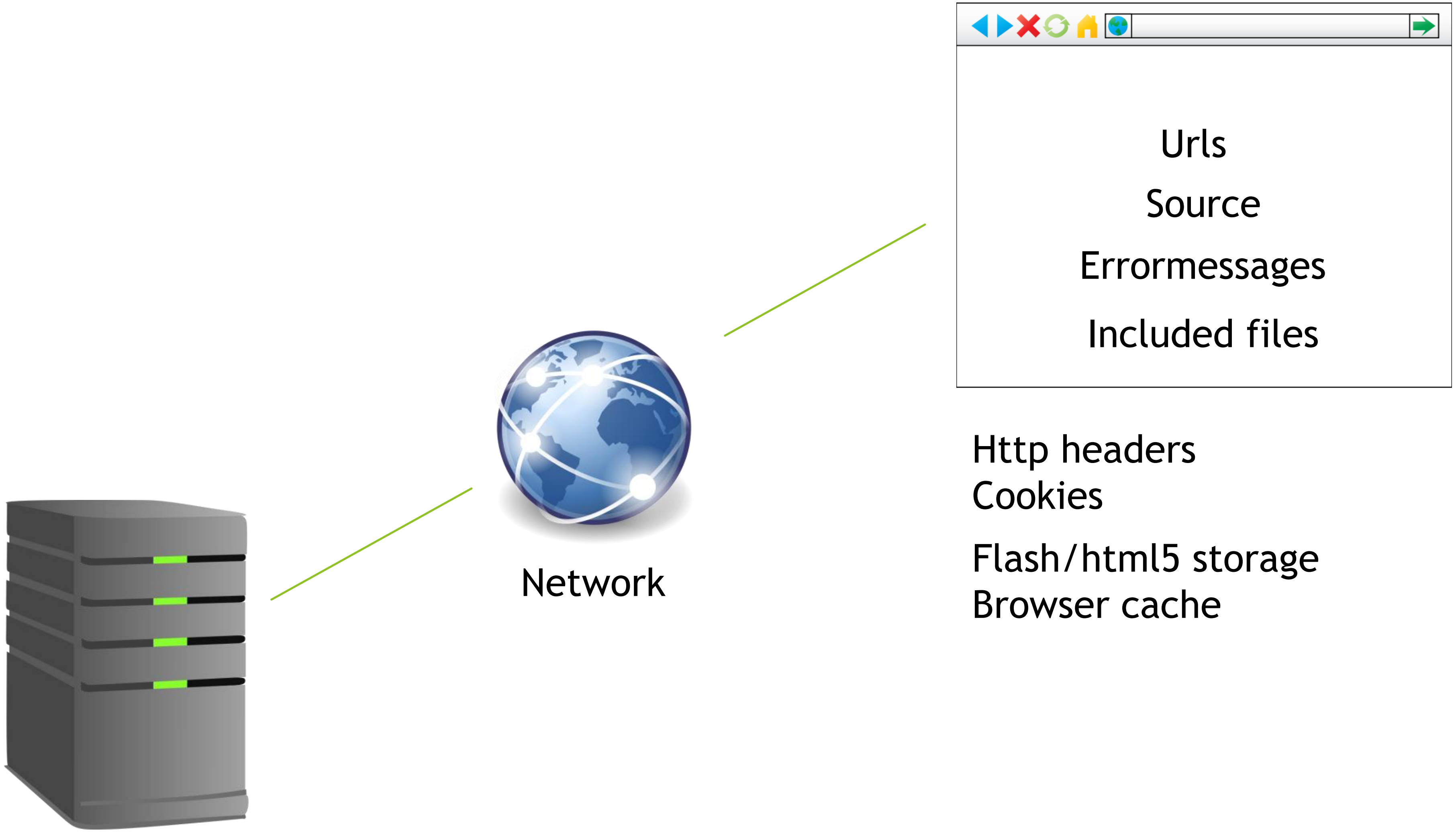
Errormessages

Included files

Http headers
Cookies

Network

Files on the server



Urls

Source

Errormessages

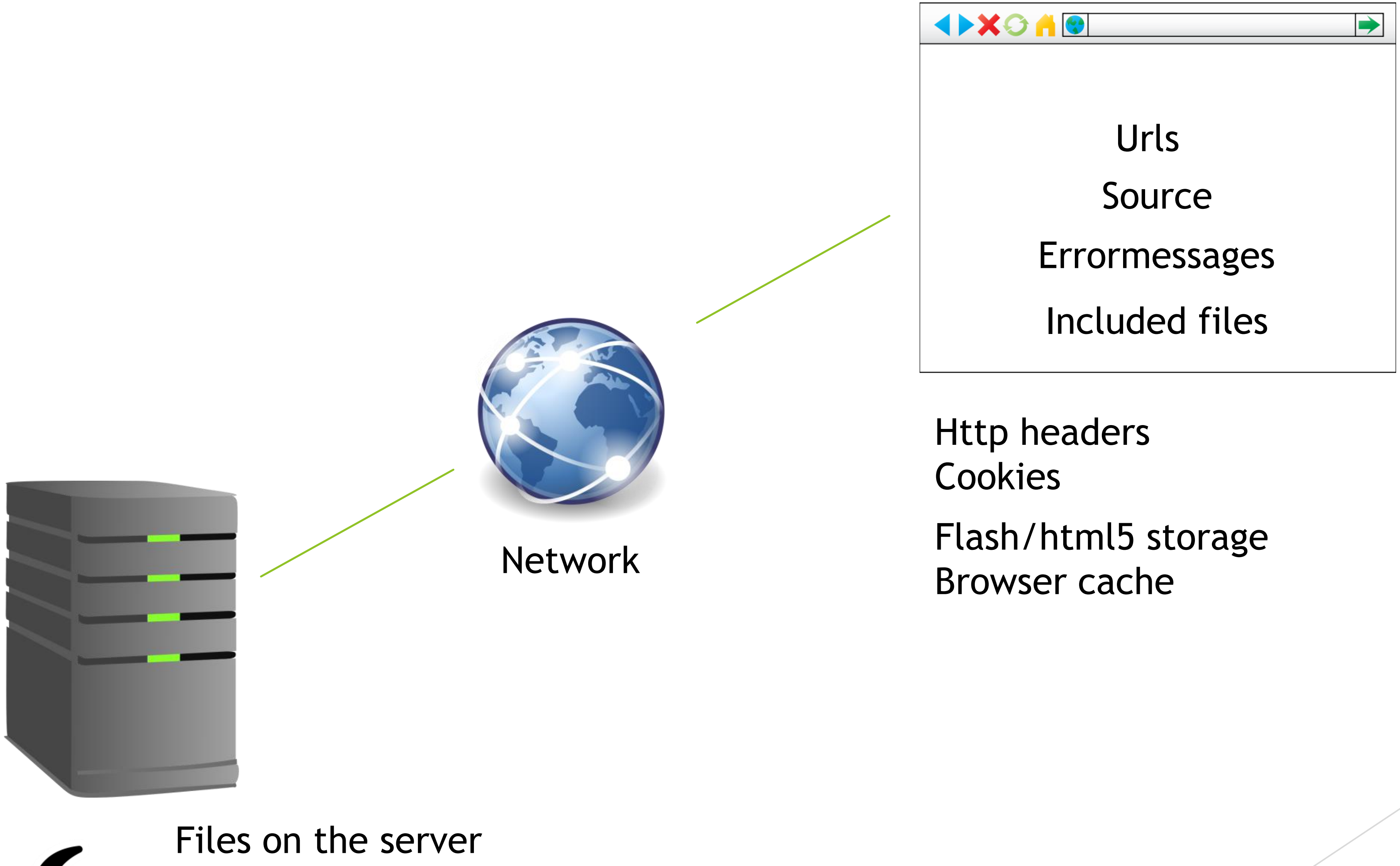
Included files

Http headers
Cookies

Flash/html5 storage
Browser cache

Network

Files on the server



Urls

Source

Errormessages

Included files

Http headers
Cookies

Flash/html5 storage
Browser cache

Network

Files on the server

- Know your application

- Know your application
- Check your server

- Know your application
- Check your server
- Consider everything published

www.owasp.org