

# BP复习与Nmap学习

## 一、BP的复习

### 1.Burp Proxy

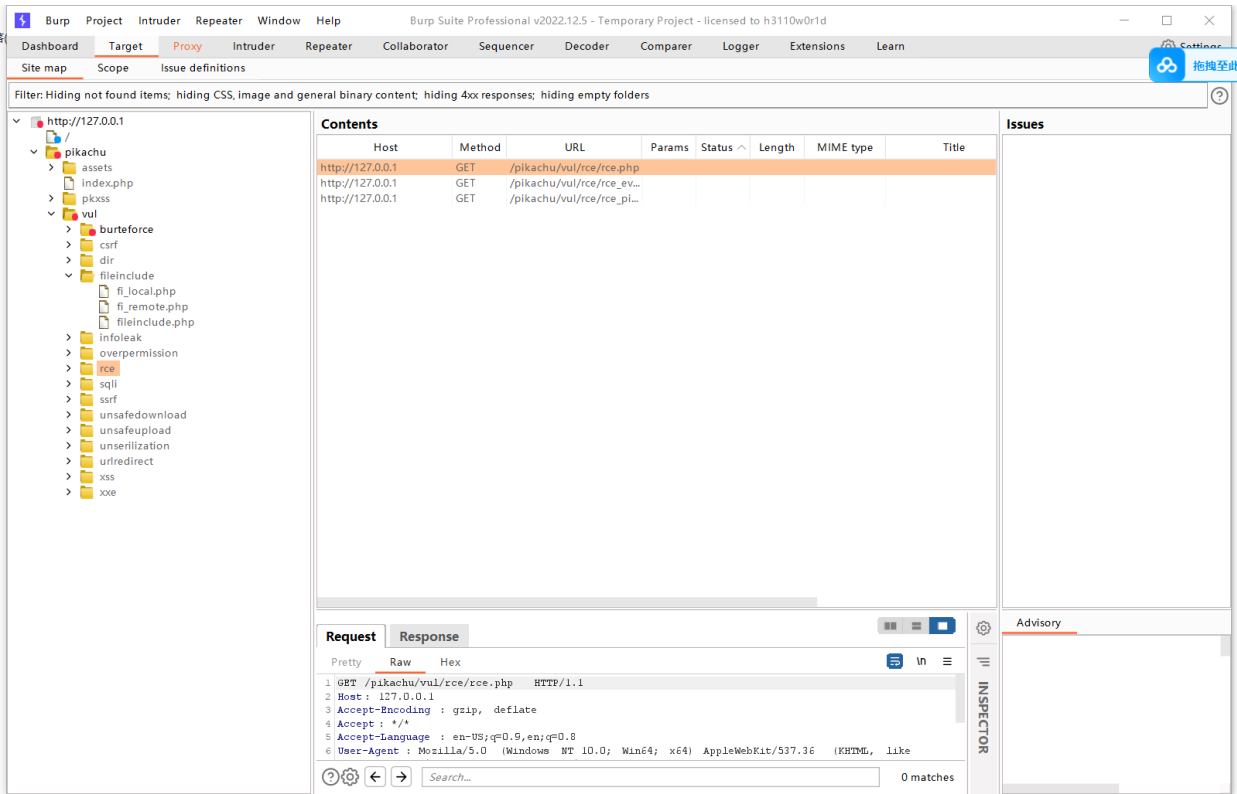
截获的报文中存在的一些参数，Raw指web请求的院士格式，纯文本。而hex更多用于00截断

PrettyRawHex

```
1 GET /pikachu/vul/burteforce/bf_form.php HTTP/1.1
2 Host : 127.0.0.1
3 sec-ch-ua : "Not?A_Brand";v="8", "Chromium";v="108"
4 sec-ch-ua-mobile : ?0
5 sec-ch-ua-platform : "Windows"
6 Upgrade-Insecure-Requests : 1
7 User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
8 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
9 Sec-Fetch-Site : none
10 Sec-Fetch-Mode : navigate
11 Sec-Fetch-User : ?1
12 Sec-Fetch-Dest : document
13 Accept-Encoding : gzip, deflate
14 Accept-Language : zh-CN,zh;q=0.9
15 Connection : close
16
17
```

### 2.Spider

蜘蛛爬取功能有助于我们了解整个网站的结构，在文件越权访问有一定的用途。



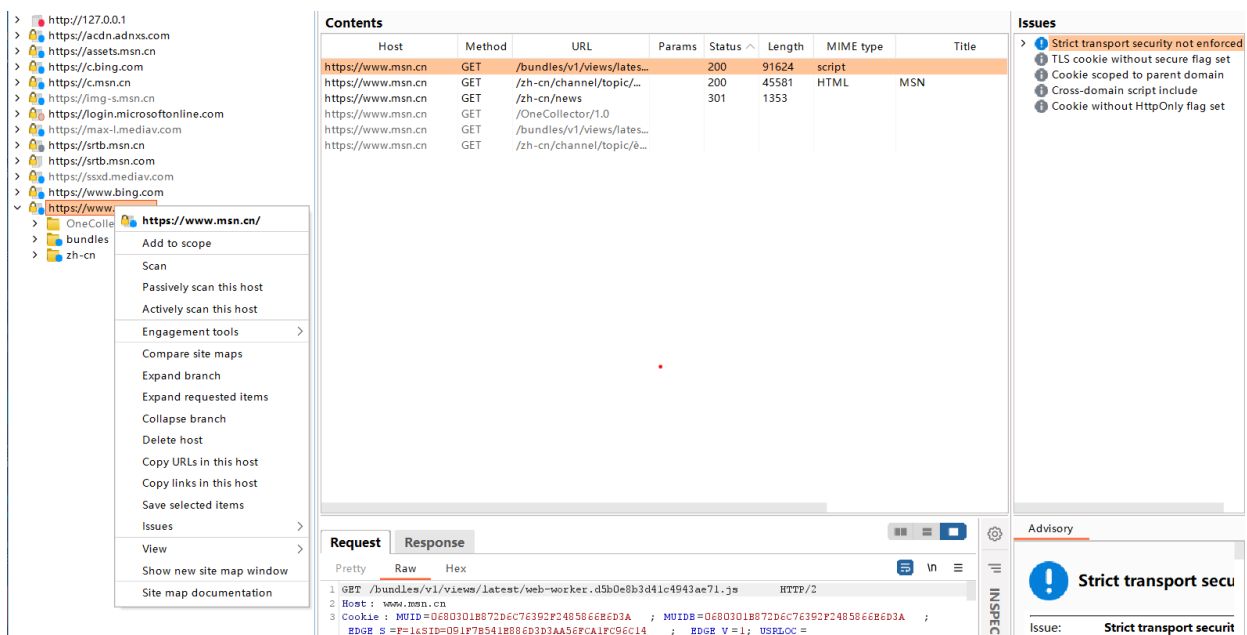
### 3.Decoder

其实这个工具网上有很多在线的，进行编码和解码














## 4. Burp Scanner

可以自动检查url的漏洞，如下图中选择<https://www.msn.cn/zh-cn/news>进行测试，选择Actively ...进行漏洞扫描



结果如下，也可以在Issues里生成html文件的漏洞报告：

## Issues

- >  Cleartext submission of password [3]
-  Cross-site scripting (DOM-based)
- >  Password submitted using GET method [5]
- >  Password field with autocomplete enabled [3]
-  Unencrypted communications
- >  Cookie without HttpOnly flag set [2]
- >  Vulnerable JavaScript dependency [6]
- >  File upload functionality [3]
-  HTTP TRACE method is enabled
- >  Email addresses disclosed [4]
- >  **Frameable response (potential Clickjacking) [3]**

## Burp Scanner Report

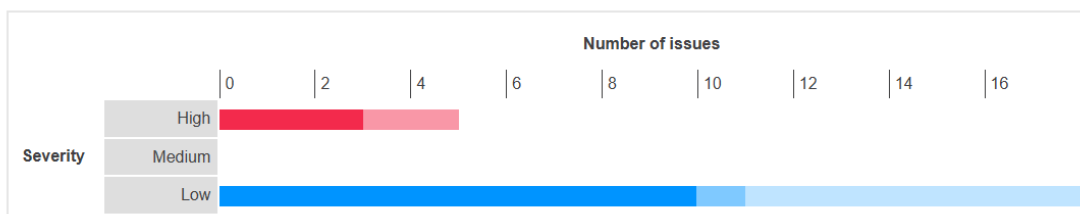


### Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			Total
		Certain	Firm	Tentative	
Severity	High	3	2	0	5
	Medium	0	0	0	0
	Low	10	1	7	18
	Information	9	3	0	12

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



查阅资料发现，BP中的扫描模式分为主动(Active Scanning)与被动(Passive Scanning)。

Passively scan this host

Actively scan this host

主动扫描模式下，占用太多的服务器性能，主要由于其生成过多的GET与POST请求，因此更多在非生产环境下进行。适用于如下漏洞：XSS、HTTP头注入、操作重定向、SQL注入、文件遍历等

被动扫描中BP不会发送新的数据请求，可以适用于生产环境的检测，适用于一些加密漏洞、cookie泄露漏洞、信息泄露等。

## 5.Burp Intruder

本功能共有四种模式，因为网上讲解比较混乱，现在记录如下。具体操作流程在暴力破解漏洞展示

- Sniper：使用单一的Payload组。它会针对每个位置设置Payload。这种攻击类型适用于对常见漏洞中的请求参数单独进行Fuzzing测试的情况。攻击请求的总数应该是Position数量和Payload数量的乘积。
- Battering ram：使用单一的Payload组。它会重复Payload并一次性把所有相同的Payload放入指定的位置。这种攻击适用于需要在请求中把相同的输入放到多个位置的情况。攻击请求的总数是Payload组中Payload的总数。
- Pitch fork：使用多个Payload组。攻击会同步迭代所有的Payload组，把Payload放入每个定义的位置中。这种攻击类型非常适合需要在不同位置中插入不同但相似输入的情况。攻击请求的总数应该是最小的Payload组中的Payload数量。
- Cluster bomb：使用多个Payload组。每个定义的位置中有不同的Payload组。攻击会迭代每个Payload组，每种Payload组合都会被测试一遍这种攻击适用于每个Payload组中的Payload都组合一次的情况。攻击请求的总数是各Payload组中Payload数量的乘积。

## 6.Burp Repeater

用来手动修改、补发个别HTTP请求的工具。在渗透测试中修改请求参数、重放攻击等等。可以在左边修改各种参数，在右边看见回显。

Request	Response
<div><div>PrettyRawHex</div><div><div>1 GET /pikachu/ HTTP/1.1</div><div>2 Host: 127.0.0.1</div><div>3 sec-ch-ua: "Not?A_Brand";v="8", "Chromium";v="108"</div><div>4 sec-ch-ua-mobile: ?0</div><div>5 sec-ch-ua-platform: "Windows"</div><div>6 Upgrade-Insecure-Requests: 1</div><div>7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36</div><div>8 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</div><div>9 Sec-Fetch-Site: none</div><div>10 Sec-Fetch-Mode: navigate</div><div>11 Sec-Fetch-User: ?1</div><div>12 Sec-Fetch-Dest: document</div><div>13 Accept-Encoding: gzip, deflate</div><div>14 Accept-Language: zh-CN,zh;q=0.9</div><div>15 Cookie: PHPSESSID=boqoc04u3bdrav14meknsluf3h</div><div>16 Connection: close</div><div>17</div><div>18</div></div></div>	<div><div>PrettyRawHexRender</div><div><div>1 HTTP/1.1 200 OK</div><div>2 Date: Fri, 14 Jun 2024 13:07:51 GMT</div><div>3 Server: Apache/2.4.39 (Min64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02</div><div>4 X-Powered-By: PHP/7.3.4</div><div>5 Expires: Thu, 15 Nov 1981 08:52:00 GMT</div><div>6 Cache-Control: no-store, no-cache, must-revalidate</div><div>7 Pragma: no-cache</div><div>8 Connection: close</div><div>9 Content-Type: text/html; charset=utf-8</div><div>10 Content-Length: 35389</div><div>11</div><div>12 &lt;!DOCTYPE html&gt;</div><div>13 &lt;html lang="en"&gt;</div><div>14 &lt;head&gt;</div><div>15 &lt;meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /&gt;</div><div>16 &lt;meta charset="utf-8" /&gt;</div><div>17 &lt;title&gt;Get the pikachu &lt;/title&gt;</div><div>18</div><div>19 &lt;meta name="description" content="overview &amp; stats" /&gt;</div><div>20 &lt;meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /&gt;</div><div>21</div><div>22 &lt;!-- bootstrap &amp; fontawesome --&gt;</div><div>23 &lt;link rel="stylesheet" href="assets/css/bootstrap.min.css" /&gt;</div><div>24 &lt;link rel="stylesheet" href="assets/font-awesome/4.5.0/css/font-awesome.min.css" /&gt;</div><div>25</div><div>26 &lt;!-- page specific plugin styles --&gt;</div><div>27</div><div>28 &lt;!-- text fonts --&gt;</div><div>29 &lt;link rel="stylesheet" href="assets/css/fonts.googleapis.com.css" /&gt;</div><div>30</div><div>31 &lt;!-- ace styles --&gt;</div><div>32 &lt;link rel="stylesheet" href="assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /&gt;</div><div>33</div><div>34 &lt;!--[if lte IE 9]&gt;</div><div>35 &lt;link rel="stylesheet" href="assets/css/ace-part2.min.css" class="ace-main-stylesheet" /&gt;</div><div>36 &lt;![endif]&gt;</div><div>37 &lt;link rel="stylesheet" href="assets/css/ace-skins.min.css" /&gt;</div></div></div>

## 二、Nmap的使用

## 1.扫描单个地址

```
nmap 192.168.1.138
```

## 2.扫描多个目标地址

```
nmap 192.168.1.138 192.168.1.139
```

## 3.扫描一批目标地址

```
nmap 192.168.1.138-140
```

## 4.扫描某个网段

```
nmap 192.168.1.138/24
```

## 5.扫描某个文件中所有的目标地址

```
nmap -iL 1.txt
```

## 6.扫描除某一个地址之外的所有地址

```
nmap 192.168.1.138/24 -exclude 192.168.1.138
```

## 7.路由跟踪

```
nmap -traceroute 192.168.1.138
```

## 8.探测操作系统

```
nmap -O 192.168.1.138
```

## 9.检查防火墙状态

```
nmap -sF -T4 192.168.1.138
```

## 10.鉴权扫描，弱口令检查

```
nmap --script=auth 192.168.1.138
```

## 11.暴力破解

```
nmap --script=brute 192.168.1.138
```

## 12.渗透漏洞检测

```
nmap --script=vuln 192.168.1.138
```

## 13.模糊测试

```
nmap --script=fuzzer 192.168.1.138
```