**中国电子科技集团公司第二十二研究所**

**检测扫描报告**

2021年10月

**网站安全检测—漏洞检测**（www.chinagpr.com）

发现页面：455个

发现高危：00个

检测时间：2021/9/7 8:08

检测用时：0天16小时25分51秒

链接深度：3

目录深度：7

检测广度：5000

 **1 指纹信息**

**目录**

 **2 风险级别**

 **3 风险汇总**

 **4 漏洞汇总**

 · 漏洞类型列表

 · 漏洞类型排名

 **5 漏洞详情**

 · 高风险

 · 中风险

 · 低风险

 **6 网站总体情况评价**

 **7 网站总体安全建议**

 **8 联系我们**

**指纹信息** ——————————————————————————————————

1

|  |  |  |  |
| --- | --- | --- | --- |
| 应用模板 | — | 操作系统版本 | — |
| 应用程序版本 | Apache | 应用程序语言 | PHP |
| 开发端口  |  |

**风险级别** ——————————————————————————————————

2

|  |
| --- |
| **middle** |
| **中风险 利用此类漏洞需要一定条件，攻击者无法直接实施攻击，对于这类漏洞可以延后处理。** |

**风险汇总** ——————————————————————————————————

33

|  |  |
| --- | --- |
| **vul_num_chart_184784d6-05d6-4fcd-8271-21dcd3551ecd** | **vul_per_chart_184784d6-05d6-4fcd-8271-21dcd3551ecd** |

**漏洞汇总** ——————————————————————————————————

43

* **漏洞类型列表**

| 风险名称 | 风险级别 | 影响页面数量 |
| --- | --- | --- |
| 没有CSRF保护的HTML表单 | 中 | 14 |
| 易受攻击的Javascript库（JQ升级） | 中 | 3 |
| 慢速的HTTP拒绝服务攻击（服务器） | 中 | 1 |
| 源代码泄露 | 中 | 1 |
| 可能的敏感目录 | 低 | 8 |
| 可能的相对路径覆盖 | 低 | 3 |
| 没有设置HttpOnly标志的Cookie | 低 | 1 |
| 点击劫持:缺少X-Frame-Options标头 | 低 | 1 |
| 登录页面密码猜测攻击 | 低 | 1 |
| 没有安全标志的Cookie设置 | 低 | 1 |
| 发现电子邮件地址 | 信息 | 4 |
| 鍐呭瀹夊叏鏀跨瓥锛圕SP锛夋湭瀹炴柦 | 信息 | 1 |
| 启用自动完成的密码类型输入 | 信息 | 1 |

* **漏洞类型排名**

 

**漏洞详情** ——————————————————————————————————

53

**中风险**

14 没有CSRF保护的HTML表单

[HTML form without CSRF protection]

**漏洞编号：**CWE-352

**漏洞说明：**

此警报可能是误报，需要手动确认。 跨站点请求伪造，也称为一键式攻击或会话骑行，缩写为CSRF或XSRF，是一种恶意利用网站，从而从网站信任的用户传输未经授权的命令。 ? ?? WVS发现了一个HTML表单，没有实现明显的CSRF保护。有关受影响的HTML表单的详细信息，请参阅详细信息。"

**修补建议：**

检查此表单是否需要CSRF保护，并在必要时实施CSRF对策。

**影响页面：**

        **http://www.chinagpr.com/gb2312/**

**技术细节：**

请求信息

GET /gb2312/ HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 19:23:34 GMT

Server: Apache

Last-Modified: Fri, 16 Jul 2021 05:55:36 GMT

ETag: "5c0222-869a-5c7373c8984ce"

Accept-Ranges: bytes

Vary: Accept-Encoding,User-Agent

Content-Length: 34458

Keep-Alive: timeout=15, max=250

Connection: Keep-Alive

Content-Type: text/html

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/gb2312/news/changjianwenti/**

**技术细节：**

请求信息

GET /gb2312/news/changjianwenti/ HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 22:10:28 GMT

Server: Apache

Last-Modified: Fri, 16 Jul 2021 05:55:48 GMT

ETag: "5c0398-2fce-5c7373d496268"

Accept-Ranges: bytes

Vary: Accept-Encoding,User-Agent

Content-Length: 12238

Keep-Alive: timeout=15, max=142

Connection: Keep-Alive

Content-Type: text/html

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/gb2312/service/certificate/list\_29\_3.html**

**技术细节：**

请求信息

GET /gb2312/service/certificate/list\_29\_3.html HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 22:29:45 GMT

Server: Apache

Last-Modified: Fri, 16 Jul 2021 05:55:55 GMT

ETag: "5c02e2-2493-5c7373db27ce2"

Accept-Ranges: bytes

Vary: Accept-Encoding,User-Agent

Content-Length: 9363

Keep-Alive: timeout=15, max=242

Connection: Keep-Alive

Content-Type: text/html

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/template/default/**

**技术细节：**

请求信息

GET /template/default/ HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 20:19:48 GMT

Server: Apache

Last-Modified: Fri, 02 Jul 2021 08:04:57 GMT

ETag: "600665-6fde-5c61f6959eae0"

Accept-Ranges: bytes

Vary: Accept-Encoding,User-Agent

Content-Length: 28638

Keep-Alive: timeout=15, max=266

Connection: Keep-Alive

Content-Type: text/html

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/phone/member/template/**

**技术细节：**

请求信息

GET /phone/member/template/ HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 23:36:30 GMT

Server: Apache

Last-Modified: Mon, 13 Jun 2016 01:41:48 GMT

ETag: "5c06db-2236-5351efddd8f00"

Accept-Ranges: bytes

Vary: Accept-Encoding,User-Agent

Content-Length: 8758

Keep-Alive: timeout=15, max=50

Connection: Keep-Alive

Content-Type: text/html

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/index.html**

**技术细节：**

请求信息

GET /index.html HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 17:13:51 GMT

Server: Apache

Last-Modified: Tue, 20 Jul 2021 08:49:51 GMT

ETag: "5c0cd2-8670-5c78a231baa84"

Accept-Ranges: bytes

Vary: Accept-Encoding,User-Agent

Content-Length: 34416

Keep-Alive: timeout=15, max=25

Connection: Keep-Alive

Content-Type: text/html

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/phone/member/**

**技术细节：**

请求信息

GET /phone/member/ HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 19:39:27 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Set-Cookie: DedeUserID=deleted; expires=Mon, 07-Sep-2020 19:39:26 GMT; path=/

Set-Cookie: DedeUserID\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 19:39:26 GMT; path=/

Set-Cookie: DedeLoginTime=deleted; expires=Mon, 07-Sep-2020 19:39:26 GMT; path=/

Set-Cookie: DedeLoginTime\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 19:39:26 GMT; path=/

Vary: User-Agent,Accept-Encoding

Content-Length: 4770

Keep-Alive: timeout=15, max=114

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/phone/member/reg\_new.php**

**技术细节：**

请求信息

GET /phone/member/reg\_new.php HTTP/1.1

Referer: http://www.chinagpr.com/

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd;DedeUserID=deleted;DedeUserID\_\_ckMd5=deleted;DedeLoginTime=deleted;DedeLoginTime\_\_ckMd5=deleted

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 22:58:26 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Set-Cookie: DedeUserID=deleted; expires=Mon, 07-Sep-2020 22:58:26 GMT; path=/

Set-Cookie: DedeUserID\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 22:58:26 GMT; path=/

Set-Cookie: DedeLoginTime=deleted; expires=Mon, 07-Sep-2020 22:58:26 GMT; path=/

Set-Cookie: DedeLoginTime\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 22:58:26 GMT; path=/

Vary: User-Agent,Accept-Encoding

Content-Length: 8541

Keep-Alive: timeout=15, max=99

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/phone/member/login.php**

**技术细节：**

请求信息

GET /phone/member/login.php HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 23:15:34 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Set-Cookie: DedeUserID=deleted; expires=Mon, 07-Sep-2020 23:15:33 GMT; path=/

Set-Cookie: DedeUserID\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 23:15:33 GMT; path=/

Set-Cookie: DedeLoginTime=deleted; expires=Mon, 07-Sep-2020 23:15:33 GMT; path=/

Set-Cookie: DedeLoginTime\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 23:15:33 GMT; path=/

Vary: User-Agent,Accept-Encoding

Content-Length: 4792

Keep-Alive: timeout=15, max=282

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/gb2312/service/certificate/**

**技术细节：**

请求信息

GET /gb2312/service/certificate/ HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 20:52:13 GMT

Server: Apache

Last-Modified: Fri, 16 Jul 2021 05:55:55 GMT

ETag: "5c02df-2b9f-5c7373db27ce2"

Accept-Ranges: bytes

Vary: Accept-Encoding,User-Agent

Content-Length: 11167

Keep-Alive: timeout=15, max=250

Connection: Keep-Alive

Content-Type: text/html

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/phone/member/index\_do.php**

**技术细节：**

请求信息

GET /phone/member/index\_do.php?dopost=regnew&fmdo=user HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 21:00:22 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Set-Cookie: DedeUserID=deleted; expires=Mon, 07-Sep-2020 21:00:21 GMT; path=/

Set-Cookie: DedeUserID\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 21:00:21 GMT; path=/

Set-Cookie: DedeLoginTime=deleted; expires=Mon, 07-Sep-2020 21:00:21 GMT; path=/

Set-Cookie: DedeLoginTime\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 21:00:21 GMT; path=/

Vary: User-Agent,Accept-Encoding

Content-Length: 8541

Keep-Alive: timeout=15, max=118

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/gb2312/service/certificate/list\_29\_1.html**

**技术细节：**

请求信息

GET /gb2312/service/certificate/list\_29\_1.html HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 22:50:01 GMT

Server: Apache

Last-Modified: Fri, 16 Jul 2021 05:55:55 GMT

ETag: "5c02e1-2b9f-5c7373db2136a"

Accept-Ranges: bytes

Vary: Accept-Encoding,User-Agent

Content-Length: 11167

Keep-Alive: timeout=15, max=256

Connection: Keep-Alive

Content-Type: text/html

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/phone/member/resetpassword.php**

**技术细节：**

请求信息

GET /phone/member/resetpassword.php HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 23:16:19 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Set-Cookie: DedeUserID=deleted; expires=Mon, 07-Sep-2020 23:16:18 GMT; path=/

Set-Cookie: DedeUserID\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 23:16:18 GMT; path=/

Set-Cookie: DedeLoginTime=deleted; expires=Mon, 07-Sep-2020 23:16:18 GMT; path=/

Set-Cookie: DedeLoginTime\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 23:16:18 GMT; path=/

Vary: User-Agent,Accept-Encoding

Content-Length: 4919

Keep-Alive: timeout=15, max=280

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/gb2312/service/certificate/list\_29\_2.html**

**技术细节：**

请求信息

GET /gb2312/service/certificate/list\_29\_2.html HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 21:58:04 GMT

Server: Apache

Last-Modified: Fri, 16 Jul 2021 05:55:55 GMT

ETag: "5c02e0-2bea-5c7373db24a1a"

Accept-Ranges: bytes

Vary: Accept-Encoding,User-Agent

Content-Length: 11242

Keep-Alive: timeout=15, max=294

Connection: Keep-Alive

Content-Type: text/html

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/phone/member/template/**

**技术细节：**

请求信息

GET /phone/member/template/ HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 23:36:30 GMT

Server: Apache

Last-Modified: Mon, 13 Jun 2016 01:41:48 GMT

ETag: "5c06db-2236-5351efddd8f00"

Accept-Ranges: bytes

Vary: Accept-Encoding,User-Agent

Content-Length: 8758

Keep-Alive: timeout=15, max=50

Connection: Keep-Alive

Content-Type: text/html

Original-Content-Encoding: gzip

3 易受攻击的Javascript库

[Vulnerable Javascript library]

**漏洞编号：**CWE-16

**漏洞说明：**

您正在使用易受攻击的Javascript库。此版本的Javascript库报告了一个或多个漏洞。有关受影响的库和报告的漏洞的详细信息，请参阅攻击详细信息和Web引用。

**修补建议：**

升级到最新版本。

**影响页面：**

        **http://www.chinagpr.com/template/default/js/jquery-1.8.3.min.js**

**技术细节：**

请求信息

GET /template/default/js/jquery-1.8.3.min.js HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 19:10:37 GMT

Server: Apache

Last-Modified: Mon, 18 Nov 2013 02:11:58 GMT

ETag: "600664-16dc7-4eb6a129a3780"

Accept-Ranges: bytes

Vary: Accept-Encoding,User-Agent

Content-Length: 93639

Keep-Alive: timeout=15, max=148

Connection: Keep-Alive

Content-Type: application/javascript

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/phone/member/template/js/j.js**

**技术细节：**

请求信息

GET /phone/member/template/js/j.js HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Wed, 08 Sep 2021 00:28:34 GMT

Server: Apache

Last-Modified: Mon, 13 Jun 2016 01:41:48 GMT

ETag: "5c06d5-792a-5351efddd8f00"

Accept-Ranges: bytes

Vary: Accept-Encoding,User-Agent

Content-Length: 31018

Keep-Alive: timeout=15, max=230

Connection: Keep-Alive

Content-Type: application/javascript

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/phone/template/default/js/jquery-1.9.1.js**

**技术细节：**

请求信息

GET /phone/template/default/js/jquery-1.9.1.js HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 22:50:13 GMT

Server: Apache

Last-Modified: Sat, 09 Mar 2013 17:32:48 GMT

ETag: "5e066b-4185d-4d78154111000"

Accept-Ranges: bytes

Vary: Accept-Encoding,User-Agent

Keep-Alive: timeout=15, max=159

Connection: Keep-Alive

Content-Type: application/javascript

Original-Content-Encoding: gzip

Content-Length: 268381

1 慢速的HTTP拒绝服务攻击

[Slow HTTP Denial of Service Attack]

**漏洞编号：**

**漏洞说明：**

您的Web服务器容易受到慢速HTTP DoS(拒绝服务)攻击。 ? Slowloris和慢速HTTP POST DoS攻击依赖于这样一个情况，即HTTP协议按设计是需要服务器在处理之前完全接收请求。如果HTTP请求未完成，或者传输速率非常低，则服务器会使其资源忙于等待其余数据。如果服务器保持被占用过多资源的状态，则会产生拒绝服务。

**修补建议：**

有关保护Web服务器免受此类攻击的信息，请参阅Web引用。

**影响页面：**

        **http://www.chinagpr.com/**

**技术细节：**

请求信息

应答信息

1 源代码泄露

[Source code disclosure]

**漏洞编号：**CWE-538

**漏洞说明：**

看起来这个脚本的源代码是可用的。此检查使用模式匹配来确定是否在文件中发现服务器端标记。在某些情况下，此警报可能会产生误报。

**修补建议：**

从您的网站删除此文件或更改其权限以删除访问权限。

**影响页面：**

        **http://www.chinagpr.com/phone/member/template/**

**技术细节：**

请求信息

GET /phone/member/template/ HTTP/1.1

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 19:42:53 GMT

Server: Apache

Last-Modified: Mon, 13 Jun 2016 01:41:48 GMT

ETag: "5c06db-2236-5351efddd8f00"

Accept-Ranges: bytes

Vary: Accept-Encoding,User-Agent

Content-Length: 8758

Keep-Alive: timeout=15, max=248

Connection: Keep-Alive

Content-Type: text/html

Original-Content-Encoding: gzip

**低风险**

8 可能的敏感目录

[Possible sensitive directories]

**漏洞编号：**CWE-200

**漏洞说明：**

发现了可能的敏感目录。此目录未直接从网站链接。此检查查找常见的敏感资源，如备份目录，数据库转储，管理页面，临时目录。这些目录中的每一个都可以帮助攻击者更多地了解他的目标。

**修补建议：**

限制对此目录的访问或将其从网站中删除。

**影响页面：**

        **http://www.chinagpr.com/phone/data/sessions/**

**技术细节：**

请求信息

GET /phone/data/sessions/ HTTP/1.1

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 19:23:56 GMT

Server: Apache

Last-Modified: Mon, 13 Jun 2016 01:42:06 GMT

ETag: "5e0613-3-5351efef03780"

Accept-Ranges: bytes

Vary: Accept-Encoding,User-Agent

Content-Length: 3

Keep-Alive: timeout=15, max=208

Connection: Keep-Alive

Content-Type: text/html

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/data/admin/**

**技术细节：**

请求信息

GET /data/admin/ HTTP/1.1

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 17:50:13 GMT

Server: Apache

Last-Modified: Mon, 13 Jun 2016 01:42:12 GMT

ETag: "6004bc-3-5351eff4bc500"

Accept-Ranges: bytes

Vary: Accept-Encoding,User-Agent

Content-Length: 3

Keep-Alive: timeout=15, max=264

Connection: Keep-Alive

Content-Type: text/html

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/data/sessions/**

**技术细节：**

请求信息

GET /data/sessions/ HTTP/1.1

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 17:50:08 GMT

Server: Apache

Last-Modified: Mon, 13 Jun 2016 01:42:06 GMT

ETag: "60048d-3-5351efef03780"

Accept-Ranges: bytes

Vary: Accept-Encoding,User-Agent

Content-Length: 3

Keep-Alive: timeout=15, max=300

Connection: Keep-Alive

Content-Type: text/html

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/includes/FCKeditor/**

**技术细节：**

请求信息

GET /includes/FCKeditor/ HTTP/1.1

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 18:00:31 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Vary: User-Agent,Accept-Encoding

Content-Length: 335

Keep-Alive: timeout=15, max=228

Connection: Keep-Alive

Content-Type: text/html

X-Pad: avoid browser bug

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/uploads/**

**技术细节：**

请求信息

GET /uploads/ HTTP/1.1

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 17:11:43 GMT

Server: Apache

Last-Modified: Mon, 13 Jun 2016 01:41:46 GMT

ETag: "5c0cfc-3-5351efdbf0a80"

Accept-Ranges: bytes

Vary: Accept-Encoding,User-Agent

Content-Length: 3

Keep-Alive: timeout=15, max=184

Connection: Keep-Alive

Content-Type: text/html

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/phone/includes/FCKeditor/**

**技术细节：**

请求信息

GET /phone/includes/FCKeditor/ HTTP/1.1

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 19:36:42 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Vary: User-Agent,Accept-Encoding

Content-Length: 335

Keep-Alive: timeout=15, max=263

Connection: Keep-Alive

Content-Type: text/html

X-Pad: avoid browser bug

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/phone/member/**

**技术细节：**

请求信息

GET /phone/member/ HTTP/1.1

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 17:18:58 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Set-Cookie: DedeUserID=deleted; expires=Mon, 07-Sep-2020 17:18:57 GMT; path=/

Set-Cookie: DedeUserID\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 17:18:57 GMT; path=/

Set-Cookie: DedeLoginTime=deleted; expires=Mon, 07-Sep-2020 17:18:57 GMT; path=/

Set-Cookie: DedeLoginTime\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 17:18:57 GMT; path=/

Vary: User-Agent,Accept-Encoding

Content-Length: 4770

Keep-Alive: timeout=15, max=167

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/phone/data/admin/**

**技术细节：**

请求信息

GET /phone/data/admin/ HTTP/1.1

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 19:24:00 GMT

Server: Apache

Last-Modified: Mon, 13 Jun 2016 01:42:12 GMT

ETag: "5e0624-3-5351eff4bc500"

Accept-Ranges: bytes

Vary: Accept-Encoding,User-Agent

Content-Length: 3

Keep-Alive: timeout=15, max=172

Connection: Keep-Alive

Content-Type: text/html

Original-Content-Encoding: gzip

3 可能的相对路径覆盖

[Possible relative path overwrite]

**漏洞编号：**CWE-20

**漏洞说明：**

此警报需要手动确认。 Gareth Heyes介绍了一种技术，通过覆盖目标文件来利用相对URL的CSS导入。攻击者可以使用此技术诱骗浏览器将HTML页面导入为CSS样式表。如果攻击者可以控制导入的HTML页面的一部分，他可以滥用此问题来注入任意CSS规则。

**修补建议：**

如果可能，建议使用绝对链接进行CSS导入。通过禁止frame元素可以部分地缓解这个问题。要禁止frame元素，请将Web服务器配置为在所有页面上包含X-Frame-Options:deny标头。

**影响页面：**

        **http://www.chinagpr.com/phone/member/resetpassword.php**

**技术细节：**

请求信息

GET /phone/member/resetpassword.php/BbQgw/ HTTP/1.1

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 23:18:33 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Set-Cookie: DedeUserID=deleted; expires=Mon, 07-Sep-2020 23:18:32 GMT; path=/

Set-Cookie: DedeUserID\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 23:18:32 GMT; path=/

Set-Cookie: DedeLoginTime=deleted; expires=Mon, 07-Sep-2020 23:18:32 GMT; path=/

Set-Cookie: DedeLoginTime\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 23:18:32 GMT; path=/

Vary: User-Agent,Accept-Encoding

Content-Length: 4919

Keep-Alive: timeout=15, max=258

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/phone/member/login.php**

**技术细节：**

请求信息

GET /phone/member/login.php/kxXFx/ HTTP/1.1

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 23:15:56 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Set-Cookie: DedeUserID=deleted; expires=Mon, 07-Sep-2020 23:15:55 GMT; path=/

Set-Cookie: DedeUserID\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 23:15:55 GMT; path=/

Set-Cookie: DedeLoginTime=deleted; expires=Mon, 07-Sep-2020 23:15:55 GMT; path=/

Set-Cookie: DedeLoginTime\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 23:15:55 GMT; path=/

Vary: User-Agent,Accept-Encoding

Content-Length: 4792

Keep-Alive: timeout=15, max=258

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/phone/member/reg\_new.php**

**技术细节：**

请求信息

GET /phone/member/reg\_new.php/iNk3r/ HTTP/1.1

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 23:50:38 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Set-Cookie: DedeUserID=deleted; expires=Mon, 07-Sep-2020 23:50:37 GMT; path=/

Set-Cookie: DedeUserID\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 23:50:37 GMT; path=/

Set-Cookie: DedeLoginTime=deleted; expires=Mon, 07-Sep-2020 23:50:37 GMT; path=/

Set-Cookie: DedeLoginTime\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 23:50:37 GMT; path=/

Vary: User-Agent,Accept-Encoding

Content-Length: 8541

Keep-Alive: timeout=15, max=231

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Original-Content-Encoding: gzip

1 没有设置HttpOnly标志的Cookie

[Cookie(s) without HttpOnly flag set]

**漏洞编号：**CWE-16

**漏洞说明：**

此cookie没有设置HTTPOnly标志。使用HTTPOnly标志设置cookie时，它会指示浏览器cookie只能由服务器访问，而不能由客户端脚本访问。这是对会话cookie的重要安全保护。

**修补建议：**

如果可能，您应该为此cookie设置HTTPOnly标志。

**影响页面：**

        **http://www.chinagpr.com/**

**技术细节：**

请求信息

POST /plus/diy.php HTTP/1.1

Content-Type: multipart/form-data; boundary=----------AoB9VYjCxYhz

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 937

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

------------AoB9VYjCxYhz

Content-Disposition: form-data; name="action"

post

------------AoB9VYjCxYhz

Content-Disposition: form-data; name="add"

1

------------AoB9VYjCxYhz

Content-Disposition: form-data; name="dede\_fields"

title,text;lxr,text;tel,text;fax,text;mail,text;add,text;nr,multitext

------------AoB9VYjCxYhz

Content-Disposition: form-data; name="dede\_fieldshash"

9a901f4856de886eeaa77fe6996bc16f

------------AoB9VYjCxYhz

Content-Disposition: form-data; name="diyid"

1

------------AoB9VYjCxYhz

Content-Disposition: form-data; name="do"

2

------------AoB9VYjCxYhz

Content-Disposition: form-data; name="mail"

sample@email.tst

------------AoB9VYjCxYhz

Content-Disposition: form-data; name="nr"

1

------------AoB9VYjCxYhz

Content-Disposition: form-data; name="submit"

submit=提 交

------------AoB9VYjCxYhz

Content-Disposition: form-data; name="title"

Mr.

------------AoB9VYjCxYhz--

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 17:16:28 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

Set-Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd; path=/

Vary: User-Agent,Accept-Encoding

Content-Length: 979

Keep-Alive: timeout=15, max=263

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/**

**技术细节：**

请求信息

GET /phone/view.php?aid=10 HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 18:49:45 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Set-Cookie: DedeUserID=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeUserID\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeLoginTime=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeLoginTime\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Vary: User-Agent,Accept-Encoding

Content-Length: 9253

Keep-Alive: timeout=15, max=286

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/**

**技术细节：**

请求信息

GET /phone/view.php?aid=10 HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 18:49:45 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Set-Cookie: DedeUserID=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeUserID\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeLoginTime=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeLoginTime\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Vary: User-Agent,Accept-Encoding

Content-Length: 9253

Keep-Alive: timeout=15, max=286

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/**

**技术细节：**

请求信息

GET /phone/view.php?aid=10 HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 18:49:45 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Set-Cookie: DedeUserID=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeUserID\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeLoginTime=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeLoginTime\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Vary: User-Agent,Accept-Encoding

Content-Length: 9253

Keep-Alive: timeout=15, max=286

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/**

**技术细节：**

请求信息

GET /phone/view.php?aid=10 HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 18:49:45 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Set-Cookie: DedeUserID=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeUserID\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeLoginTime=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeLoginTime\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Vary: User-Agent,Accept-Encoding

Content-Length: 9253

Keep-Alive: timeout=15, max=286

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Original-Content-Encoding: gzip

1 点击劫持:缺少X-Frame-Options标头

[Clickjacking: X-Frame-Options header missing]

**漏洞编号：**CWE-693

**漏洞说明：**

Clickjacking(用户界面纠正攻击，UI补救攻击，UI纠正)是一种恶意技术，欺骗Web用户点击与用户认为他们点击的内容不同的内容，从而可能泄露机密信息或控制他们的计算机 同时点击看似无害的网页。 服务器没有返回X-Frame-Options标头，这意味着该网站可能面临点击劫持攻击的风险。X-Frame-Options HTTP响应头可用于指示是否应允许浏览器在框架或iframe内呈现页面。站点可以通过确保其内容未嵌入到其他站点中来避免点击劫持攻击。

**修补建议：**

将Web服务器配置为包含X-Frame-Options标头。有关此标头的可能值的更多信息，请参阅Web引用。

**影响页面：**

        **http://www.chinagpr.com/**

**技术细节：**

请求信息

GET / HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 301 Moved Permanently

Date: Tue, 07 Sep 2021 17:07:35 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Location: index.html

Vary: User-Agent,Accept-Encoding

Content-Length: 0

Keep-Alive: timeout=15, max=299

Connection: Keep-Alive

Content-Type: text/html

Original-Content-Encoding: gzip

1 登录页面密码猜测攻击

[Login page password-guessing attack]

**漏洞编号：**CWE-307

**漏洞说明：**

网络开发人员面临的一个常见威胁是一种称为暴力攻击的密码猜测攻击。蛮力攻击是试图通过系统地尝试每种可能的字母，数字和符号组合来发现密码，直到您发现密码为止。正确的组合有效。 ? 此登录页面没有任何防止密码猜测攻击(暴力攻击)的保护。建议在定义的错误密码尝试次数后实施某种类型的帐户锁定。有关修复此问题的详细信息，请参阅Web引用。

**修补建议：**

建议在定义的错误密码尝试次数后实施某种类型的帐户锁定。

**影响页面：**

        **http://www.chinagpr.com/phone/member/index\_do.php**

**技术细节：**

请求信息

POST /phone/member/index\_do.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://www.chinagpr.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 90

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

dopost=login&fmdo=login&gourl=1&keeptime=2592000&pwd=ms4yy4yo&userid=52IPopIo&vdcode=94102

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 19:43:13 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

Set-Cookie: DedeUserID=deleted; expires=Mon, 07-Sep-2020 19:43:12 GMT; path=/

Set-Cookie: DedeUserID\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 19:43:12 GMT; path=/

Set-Cookie: DedeLoginTime=deleted; expires=Mon, 07-Sep-2020 19:43:12 GMT; path=/

Set-Cookie: DedeLoginTime\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 19:43:12 GMT; path=/

Set-Cookie: PHPSESSID=d98477e0c361d15eef1c56b4180d54bf; path=/

Vary: User-Agent,Accept-Encoding

Content-Length: 910

Keep-Alive: timeout=15, max=84

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Original-Content-Encoding: gzip

1 没有安全标志的Cookie设置

[Cookie(s) without Secure flag set]

**漏洞编号：**CWE-16

**漏洞说明：**

此cookie没有设置安全标志。使用安全标志设置cookie时，它会指示浏览器只能通过安全的SSL通道访问cookie。这是会话cookie的重要安全保护。

**修补建议：**

如果可能，您应该为此cookie设置安全标志。

**影响页面：**

        **http://www.chinagpr.com/**

**技术细节：**

请求信息

GET /phone/view.php?aid=10 HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 18:49:45 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Set-Cookie: DedeUserID=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeUserID\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeLoginTime=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeLoginTime\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Vary: User-Agent,Accept-Encoding

Content-Length: 9253

Keep-Alive: timeout=15, max=286

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/**

**技术细节：**

请求信息

GET /phone/view.php?aid=10 HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 18:49:45 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Set-Cookie: DedeUserID=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeUserID\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeLoginTime=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeLoginTime\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Vary: User-Agent,Accept-Encoding

Content-Length: 9253

Keep-Alive: timeout=15, max=286

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/**

**技术细节：**

请求信息

GET /phone/view.php?aid=10 HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 18:49:45 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Set-Cookie: DedeUserID=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeUserID\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeLoginTime=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeLoginTime\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Vary: User-Agent,Accept-Encoding

Content-Length: 9253

Keep-Alive: timeout=15, max=286

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/**

**技术细节：**

请求信息

GET /phone/view.php?aid=10 HTTP/1.1

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 18:49:45 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Set-Cookie: DedeUserID=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeUserID\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeLoginTime=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Set-Cookie: DedeLoginTime\_\_ckMd5=deleted; expires=Mon, 07-Sep-2020 18:49:45 GMT; path=/

Vary: User-Agent,Accept-Encoding

Content-Length: 9253

Keep-Alive: timeout=15, max=286

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Original-Content-Encoding: gzip

**影响页面：**

        **http://www.chinagpr.com/**

**技术细节：**

请求信息

POST /plus/diy.php HTTP/1.1

Content-Type: multipart/form-data; boundary=----------AoB9VYjCxYhz

Referer: http://www.chinagpr.com/

Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Content-Length: 937

Host: www.chinagpr.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

------------AoB9VYjCxYhz

Content-Disposition: form-data; name="action"

post

------------AoB9VYjCxYhz

Content-Disposition: form-data; name="add"

1

------------AoB9VYjCxYhz

Content-Disposition: form-data; name="dede\_fields"

title,text;lxr,text;tel,text;fax,text;mail,text;add,text;nr,multitext

------------AoB9VYjCxYhz

Content-Disposition: form-data; name="dede\_fieldshash"

9a901f4856de886eeaa77fe6996bc16f

------------AoB9VYjCxYhz

Content-Disposition: form-data; name="diyid"

1

------------AoB9VYjCxYhz

Content-Disposition: form-data; name="do"

2

------------AoB9VYjCxYhz

Content-Disposition: form-data; name="mail"

sample@email.tst

------------AoB9VYjCxYhz

Content-Disposition: form-data; name="nr"

1

------------AoB9VYjCxYhz

Content-Disposition: form-data; name="submit"

submit=提 交

------------AoB9VYjCxYhz

Content-Disposition: form-data; name="title"

Mr.

------------AoB9VYjCxYhz--

应答信息

HTTP/1.1 200 OK

Date: Tue, 07 Sep 2021 17:16:28 GMT

Server: Apache

X-Powered-By: PHP/5.2.17

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

Set-Cookie: PHPSESSID=6b8b0750f44bf788ba31182daab7f0cd; path=/

Vary: User-Agent,Accept-Encoding

Content-Length: 979

Keep-Alive: timeout=15, max=263

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Original-Content-Encoding: gzip



**网站总体情况评价** ——————————————————————————————

63

通过本次安全检测在被扫描的网站中发现严重的安全漏洞。

安全情况**一般**

网站的安全漏洞能够直接被攻击者利用。基于测试的结果，我们建议立 即对网站的安全漏洞进行修补，同时对网站服务器进行WEBSHELL检测及系统 后门排查，避免入侵者对服务器的权限获取后造成网站篡改、服务器宕机等 情况发生。

**网站总体安全建议** ——————————————————————————————

73

1. **对已有的安全措施加固**
* 安全产品

从对服务器系统的探测得出只开放了特定应用的端口，这可能是因为利 用防火墙等防护设备做了一定程度的安全策略，很大程度上提高了安全性。

* 安全补丁

通过安全漏洞扫描，没有发现任何应用层和系统层的安全漏洞，管理人 员应该为系统更新了关键补丁，避免了系统存在大量补丁级漏洞的风险。从 这一点上来看补丁及时更新的工作是非常有意义的，能够一定程度的降低风险。

1. **安全意见**

经过本次远程安全测试，发现被检测系统中存在一些安全问题或者隐 患，因此在本节中，建议采用如下方式修补这些问题。对于无法马上得到解 决的问题，也将提出相应的解决建议供您参考。

* 及时安装最新的安全补丁

及时安装最新的安全补丁。这有助于解决已知的一些安全漏洞，提高系 统的安全性。使得攻击者即使绕过防火墙进入了系统也无法轻易入侵内部主机。

* 进行系统级的安全加固配置

对操作系统和应用系统本身进行安全加固可以大大提高系统的抗攻击的 能力。例如，设置合理的口令策略、进行文件系统的访问控制、以及网络访问控制等等。

* Web 安全编程

即使有客户端验证，也不要相信客户端的输入！

请求URL的参数部分；

HTML表单通过POST或GET请求提交的数据；

在客户端临时保存的数据（也就是Cookie）；

数据库查询。

* SQL注入防范

SQL注入可能会查看、修改或删除数据库条目和表，是WEB应用中最直接 的攻击方式，因此SQL注入防范至关重要。解决办法是建议对需要交互、需 要提交用户名或密码的页面，对用户的输入过滤所有以下字符：

[1] |（竖线符号）

[2] & （& 符号）

[3] ;（分号）

[4] $（美元符号）

[5] %（百分比符号）

[6] @（at 符号）

[7] '（单引号）

[8] "（引号）

[9] \'（反斜杠转义单引号）

[10] \"（反斜杠转义引号）

[11] <>（尖括号）

[12] ()（括号）

[13] +（加号）

[14] ,（逗号）

[15] \（反斜杠）

[16]update

[17]delete

[18]insert

[19]drop

[20]truncate

[21]create

[22]count

[23]char

[24]mid

[25]group

[26]union

[27]into

[28]from

[29]select

或者使用asp.net的validaterequest属性进行过滤。

* 跨站脚本攻击防范

跨站脚本攻击可能会窃取或操纵客户会话和 cookie，它们可能用于模 仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务。解决办法是建议对提交的URL过滤所有以下字符：

[1] |（竖线符号）

[2] & （& 符号）

[3];（分号）

[4] $（美元符号）

[5] %（百分比符号）

[6] @（at 符号）

[7] '（单引号）

[8] "（引号）

[9] \'（反斜杠转义单引号）

[10] \"（反斜杠转义引号）

[11] <>（尖括号）

[12] ()（括号）

[13] +（加号）

[14] CR（回车符，ASCII 0x0d）

[15] LF（换行，ASCII 0x0a）

[16] ,（逗号）

[17] \（反斜杠）

[18] script

[19] onload

[20] onmouseover

或使用asp.net的validaterequest属性进行过滤。

* 定期进行安全审计

虽然在本次检测中发现了这些问题，并且相信这些安全隐患能够在短时 间内解决。但仍然建议定期进行类似的安全审计，保障不断发展的动态网络 的持续安全。

* 安全复检

在修复此次发现的安全漏洞并完成系统及应用的安全加固后，建议再次 进行安全检测，以校验评估安全状态，并确保无其他安全问题存在。

* 购买安全产品

由于技术的发展，不断有新的攻击方法出现，仅仅有防火墙是不够的。 很多攻击是管理员无法防范到的，建议购进第三方的入侵保护系统和WAF防 火墙等安全设备来保护您的网络。

**联系我们** ——————————————————————————————————

83

卫士通信息产业股份有限公司　安全服务事业部

地址：北京市丰台区总部基地18区6号楼

电话：010-57533275、010-57533276