



# F5 BIG-IP Misconfigurations

Denis Kolegov

Positive Technologies, Tomsk State University



# #whoami

- Team lead at Positive Technologies Application Firewall Team
- Ex Security Test Engineer at F5 Networks
- Associate professor at Tomsk State University
- <https://twitter.com/dnkolegov>





# Disclaimer

The research is not related to my current job and current employer

The most vulnerabilities were found and fixed during my work at F5 Networks

Some new vulnerabilities have been reported to F5 Networks Platform Security Team





# Links

F5 BIG-IP Security Cheatsheet

<https://github.com/dnkolegov/bigipsecurity>

OWASP Secure Configuration Guide

[https://www.owasp.org/index.php/SCG\\_D\\_BIGIP](https://www.owasp.org/index.php/SCG_D_BIGIP)





# F5 BIG-IP



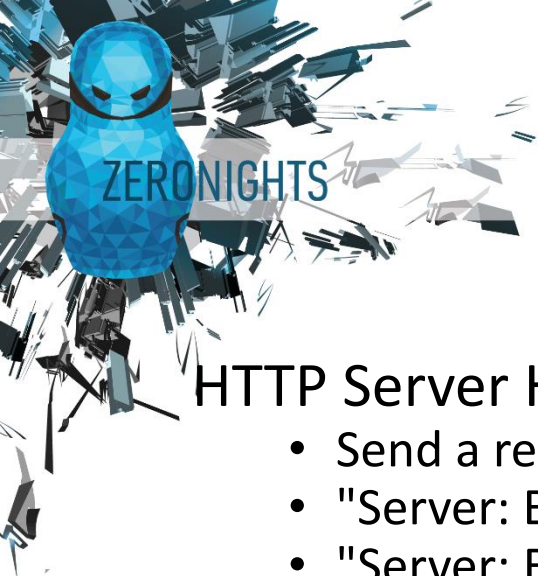
- **Local Traffic Manager (LTM)**
- **Access Policy Manager (APM)**
- Application Security Manager (ASM)
- Application Acceleration Manager (AAM)
- Advanced Firewall Manager (AFM)
- Global Traffic Manager (GTM)
- Link Controller (LC)
- Protocol Security Module (PSM)



# Agenda

- BIG-IP Discovery
  - HTTP Server Header Information Leakage
  - Mass Enumeration using Search Engines
  - Access to Management Interface from Internet
- LTM Information Leakage
  - Management IP-address Disclosure
  - Route Domain Disclosure
  - Persistence Cookie Information Leakage
- APM Attacks
  - Session Exhaustion DoS attack
  - Sandbox Escaping
  - Clickjacking
  - SOP Bypass





# BIG-IP Discovery

## HTTP Server Header

- Send a request to HTTP virtual server
- "Server: BIG-IP" – before 11.4.0
- "Server: BigIP " – after 11.4.0

## Google

- inurl:"tmui/login.jsp"
- intitle:"BIG-IP" inurl:"tmui"
- intitle:"BIG-IP logout page"
- "Thank you for using BIG-IP."

## Shodan

- WWW-Authenticate: Basic realm=BIG-IP
- BIG-IP
- BigIP

## Metasploit

- auxiliary/scanner/http/f5\_mgmt\_scanner







# BIG-IP Discovery

**Request**

Raw Headers Hex

GET / HTTP/1.1  
Host: [REDACTED]

? < + >

**Response**

Raw Headers Hex

HTTP/1.0 302 Found  
Location: https://[REDACTED]  
Server: BIG-IP  
Connection: Keep-Alive  
Content-Length: 0







# BIG-IP Discovery

**Request**

Raw Headers Hex

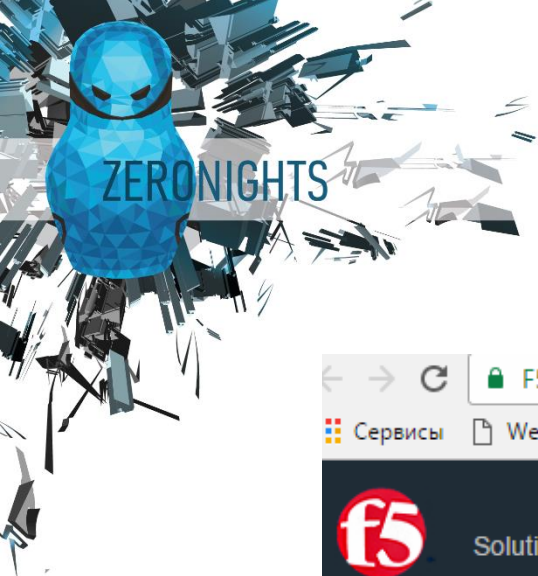
GET / HTTP/1.1  
Host: service [REDACTED] com

? < + >

**Response**

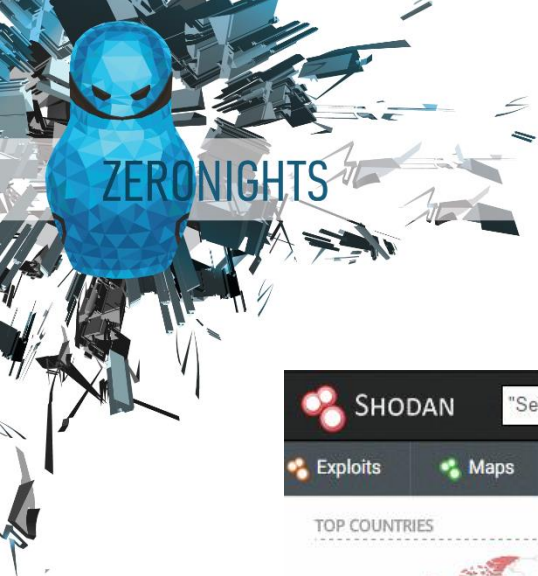
Raw Headers Hex

HTTP/1.1 301 Moved Permanently  
Location: https://service [REDACTED] com/  
Server: BigIP  
Content-Length: 0  
Expires: Wed, 09 Nov 2016 12:10:07 GMT  
Cache-Control: max-age=0, no-cache, no-store  
Pragma: no-cache  
Date: Wed, 09 Nov 2016 12:10:07 GMT  
Connection: keep-alive



# BIG-IP Discovery

F5 Networks Inc [US]   <a href="https://support.f5.com/kb/en-us/products/big-ip_ltm/releases/notes/product/relnote-ltm-11-4-0.html">https://support.f5.com/kb/en-us/products/big-ip_ltm/releases/notes/product/relnote-ltm-11-4-0.html</a>	
Сервисы Web Slice Gallery WebHome < Tools Edit my privacy settings PT Wiki	
f5 Solutions Products Community Support Partners Education About Us	
SUPPORT LOGIN SELF-HELP DOCUMENTATION SERVICES DOWNLOADS	
ID 408080	Changes to LSN pools unrelated to route advertisement no longer stop the advertisement of an LSN pool's LSN prefixes.
ID 408110	For some BIG-IP configurations, big3d can send an improperly formatted error message when responding to iQuery messages from Enterprise Manager or the F5 Management Pack. The error message has been reformatted to be proper XML.
ID 408169	"The following voltage errors are no longer erroneously logged: slot1/hostname emerg system_check[<pid>]: 010d0009:0: Mezzanine 1.0V IDT voltage: voltage (1103) is too high. slot1/hostname emerg system_check[<pid>]: 010d0009:0: Blade 0.75V voltage: voltage (839) is too high."
ID 408198	"1. When should the units get their master keys into sync? When ever a HA pair gets established MasterKey and all the subscribed objects get synced during the first sync and everything is good to go. Only MasterKey gets synced (not the subscribed objects) when the MasterKey is explicitly modified on any of the peer in HA. 2. When should customer have to perform configsync manually on HA Pair? The addition manual sync is required only if someone changes the MasterKey explicitly on any of the peer in an established HA environment in which case we need to explicitly propagates the subscribed objects."
ID 408249	BIG-IP no longer gets into performance degradation situations when tcpdump instances are started and stopped repeatedly.
ID 408276	"We have added a new profile option for http: server-agent-name You can set this to change the name used in the ""Server:"" header in output generated by the BIG-IP system. i.e. root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmsh.profile.http)# modify http server-agent-name TestServer will use ""Server: TestServer"" By default, the server name is ""BigIP"". If you don't want any server header used at all, use an empty string: root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmsh.profile.http)# modify http server-agent-name "" If this is done, then the server header will be elided from BIG-IP-generated content."
ID 408493	"Running the qkview command no longer results in the following error message and core file under rare circumstances: tmstat_subscribe_cols: Assertion 'tmtable->col_count < tmtable->td->cols' failed. Aborted (core dumped)"
ID 408605	No longer floods the log when lacpd drops slow protocols.
ID 408678	Fixed a TMM core seen while handling traffic in a Carrier-Grade NAT configuration.
ID 408753	TMM no longer cores when enabling the dns-cache feature.



# BIG-IP Discovery

[Explore](#)

[Enterprise Access](#)

[Contact Us](#)

TOP COUNTRIES

United States	188,427
United Kingdom	9,805
Germany	9,437
Canada	8,540
Australia	8,268

TOP SERVICES

HTTP	250,347
HTTPS	26,173
444	1,487
HTTPS (8443)	1,026
HTTP (8080)	322

TOP ORGANIZATIONS

Akamai Technologies	18,994
Service-now.com	9,283
Oracle Corporation	6,641
Kronos	4,605
Savvis	3,361

Total results: 281,354

**206.152.14.122**

**Savvis**

Added on 2016-11-08 22:22:43 GMT

United States, Chesterfield

[Details](#)

**SSL Certificate**

Issued By:

- Common Name:

Network Solutions OV Server CA 2

- Organization:

Network Solutions L.L.C.

Issued To:

- Common Name:

\*.ultipro.ca

- Organization:

The Ultimate Software Group

**Supported SSL Versions**

TLSv1, TLSv1.1, TLSv1.2

**BIG-IP logout page**

48.18.229.130

connect.ladrome.fr

**Rhoval SAS**

Added on 2016-11-08 22:22:42 GMT

France

[Details](#)

**SSL Certificate**

Issued By:

- Common Name:

GlobalSign

Organization Validation CA - SHA256 - G2

- Organization:

GlobalSign nv-sa

Issued To:

- Common Name:

\*.ladrome.fr

- Organization:

DEPARTEMENT DE LA DROME

**Supported SSL Versions**

HTTP/1.0 200 OK

Content-Type: text/html

**Server: BigIP**

Connection: Keep-Alive

Content-Length: 812

HTTP/1.1 200 OK

**Server: BigIP**

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

Accept-Ranges: bytes

Connection: Keep-Alive

Date: Tue, 08 Nov 2016 22:22:31 GMT

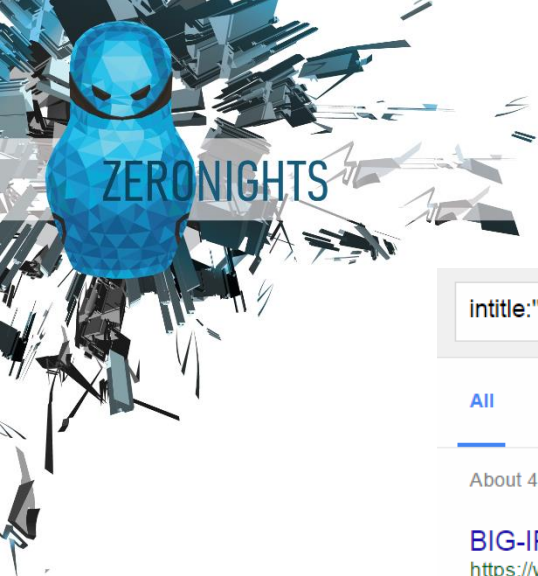
Age: 11082

Content-Length: 5202



X-Frame-Options: DENY

Set-Cookie: MRHSession=deleted;expires=Thu, 01-Jan-1970 00:00:01 GMT;path=/

Set-Co...



# BIG-IP Discovery

[All](#) [Images](#) [Videos](#) [News](#) [Shopping](#) [More ▾](#) [Search tools](#)

About 4,040 results (0.52 seconds)

**BIG-IP logout page**

<https://webmail.health.nsw.gov.au/my.policy> ▾

**BIG-IP logout page - Employee Portal**

<https://employee.hospital.uic.edu/my.policy> ▾

BIG-IP can not find session information in the request. This can happen because your browser restarted after an add-on was installed. If this occurred, click the ...

**BIG-IP logout page - Eastman**

<https://owa.eastman.com/my.policy> ▾

**BIG-IP logout page - F5 DevCentral**

<https://devcentral.f5.com/questions/big-ip-logout-page> ▾

Aug 5, 2015 - When log in, the following error appears Your session could not be established. The session reference number: ##### Access was denied ...

**BIG-IP logout page**

<https://www.snap.medxcelglobal.com/> ▾

**BIG-IP logout page - gvb**

<https://in.gvb.nl/my.policy> ▾ [Translate this page](#)

**BIG-IP logout page - click here.**

<https://citrix.brown.edu/my.policy> ▾

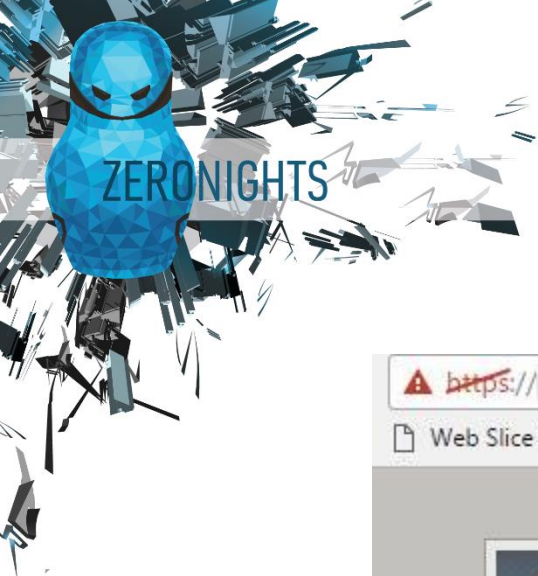
**BIG-IP logout page - Click here**

<https://ra.edwardjones.com/my.logout.php3> ▾

Your session is finished. Logged out successfully. Thank you for using Remote Access! To open a new session, please click here.








# Route Domain Disclosure

https://185.54/tmui/login.jsp

Web Slice Gallery WebHome < Tools < Edit my privacy settin PT Wiki

 IT Agility. Your Way.™

BIG-IP® Configuration Utility  
F5 Networks, Inc.

**Hostname**

**IP Address**

**Username**

**Password**

Log in


Welcome to the BIG-IP Configuration Utility.  
Log in with your username and password using the fields on the left.





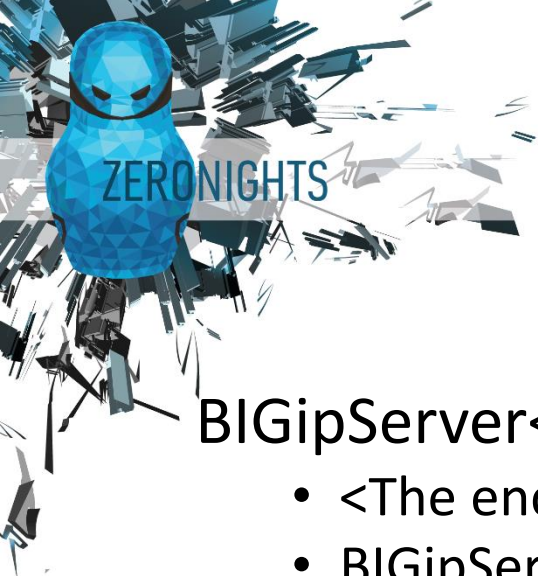
# Management IP-address Disclosure

→ ↻ <https://145.112/tmui/login.jsp>

**BIG-IP Configuration Utility**  
F5 Networks, Inc.

<b>Hostname</b> bigip1	<p>Welcome to the BIG-IP Configuration Utility.</p> <p>Log in with your username and password using the fields on the left.</p>
<b>IP Address</b> 10.0.0.132	
<b>Username</b> <input type="text"/>	
<b>Password</b> <input type="password"/>	
<input type="button" value="Log in"/>	

(c) Copyright 1996-2014, F5 Networks, Inc., Seattle, Washington. All rights reserved.  
[F5 Networks, Inc. Legal Notices](#)



# LTM Persistence Cookies

BIgipServer<pool name> = Encoded value

- <The encoded server IP>.<The encoded server port>.0000
- BIgipServer~DMZ\_V101~web\_443=1677787402.36895.0000
- vi<The full hexadecimal IPv6 address>.<The encoded server port>
- BIgipServer~CORP\_DC1=vi2001011200000000000000000000000030.20480
- rd<The route domain ID>o000000000000000000000000ffff<The hexadecimal representation of the IP address of the pool member>o<The port number>
- BIgipServer~EE\_ORACLE=rd5o000000000000000000000000ffffc0000201o80
- rd<The route domain ID>o<The full hexadecimal IPv6 address>o<The port number>
- BIgipServer~ES~test.example.com=rd3o2001011200000000000000000000000030o80





# LTM Persistence Cookies

## Tools

- Metasploit - auxiliary/gather/f5\_bigip\_cookie\_disclosure
- BeEF - modules/network/ADC/f5\_bigip\_cookie\_disclosure
- Cookie Decipher Tool -  
<https://devcentral.f5.com/wiki/AdvDesignConfig.CookiePersistenceDecipherTool.ashx>

## Protection

- Bad: Cookie renaming
- Good: Cookie encryption



# APM Session Exhaustion DoS Attack

- BIG-IP APM allocates a new session after the first unauthenticated request and deletes the session only if an access policy timeout will be expired
- Metasploit module - `auxiliary/dos/http/f5_bigip_apm_max_sessions`

Settings		
Inactivity Timeout	<input type="text" value="900"/>	seconds
Access Policy Timeout	<input type="text" value="300"/>	seconds
Maximum Session Timeout	<input type="text" value="604800"/>	seconds
Minimum Authentication Failure Delay	<input type="text" value="2"/>	seconds
Maximum Authentication Failure Delay	<input type="text" value="5"/>	seconds
Max Concurrent Users	<input type="text" value="0"/>	
Max Sessions Per User	<input type="text" value="0"/>	
Max In Progress Sessions Per Client IP	<input type="text" value="128"/>	
Restrict to Single Client IP	<input type="checkbox"/>	
Use HTTP Status 503 for Error Pages	<input type="checkbox"/>	



# APM Sandbox Escaping

## APM "Sandbox"

- Vectors (Fixed)
  - `<video src=1 onerror=alert(document.cookie)>`
  - `<img src=1 onerror=result=document.cookie;>`
- BeEF module - `modules/network/ADC/f5_bigip_cookie_stealing`
- New vectors have been reported to F5 Networks Platform Security Team

```
<html>
  <head>...</head>
  <body> == $0
    <script>
      alert( /*F5_*/ F5_Deflate_cookie( /*_5F##*/ document /*F5_*/ ) /*_5F#.cookie#/ )
    </script>
    <!-- ----- -->
    <svg>
      <script>alert(document.cookie)</script>
    </svg>
  </body>
</html>
```



# APM Clickjacking

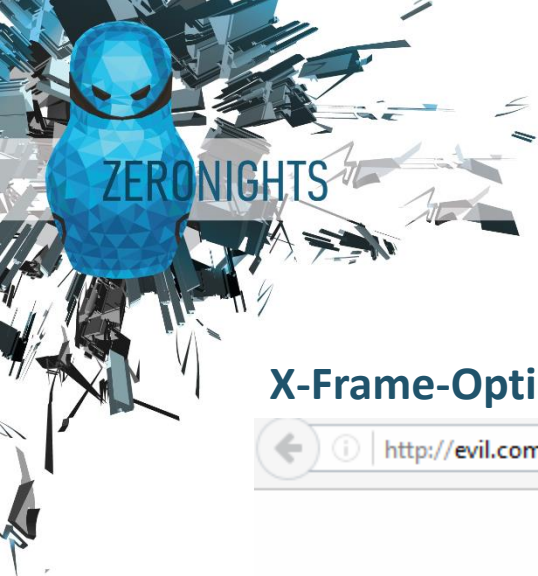
APM ignores application's original Content Security Policy headers

APM removes application's original "X-Frame-Options: sameorigin" header, but accepts "X-Frame-Options: deny"

To protect against classic Clickjacking attack it is necessary to configure LTM iRules

Reproduced on BigIP 12.1.0 build 0.0.1434





# APM Clickjacking

## X-Frame-Options: deny

← ⓘ | http://evil.com/

BIG-IP Portal Access:		Normal access:	
-----------------------	--	----------------	--

## X-Frame-Options: sameorigin

← ⓘ | http://evil.com/

BIG-IP Portal Access:	My X-Frame-Options is SAMEORIGIN!	Normal access:	
-----------------------	-----------------------------------	----------------	--





# Same-Origin Policy Bypass

APM model changes an idea of browser same-origin policy: all applications behind BIG-IP share the same origin `http(s)://bigip:port/`

All real applications origins are HEX-encoded and transmitted via URL path `/f5-w-[HEX-encoded-origin]$$/path`

## Secure configuration

- Services Isolation
- L4/L7 ACL

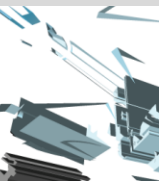
Reproduced on BigIP 12.1.0 build 0.0.1434



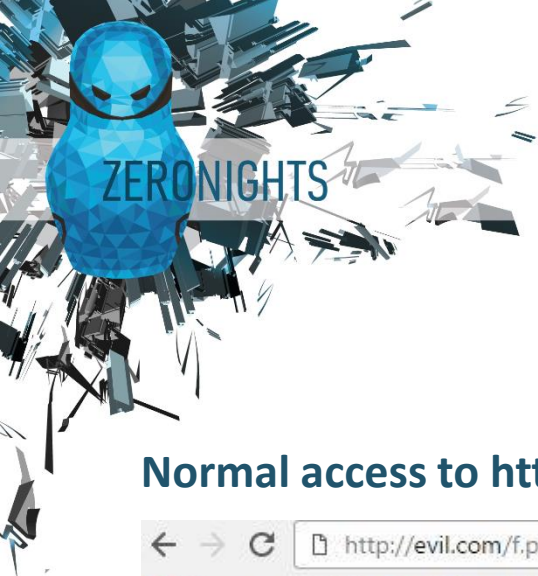


# Same-Origin Policy Bypass

```
<html>
<body>
<p>Frame: http://goodsite.com</p>
<iframe src="http://goodsite.com/secret.php" name="if"></iframe>
<script>
  var f = document.getElementsByName("if")[0];
  f.onload = function(){
    var a=fr.contentDocument;
    var b = a.getElementById("secretform");
    console.log(b);
  }
</script>
</body>
</html>
```

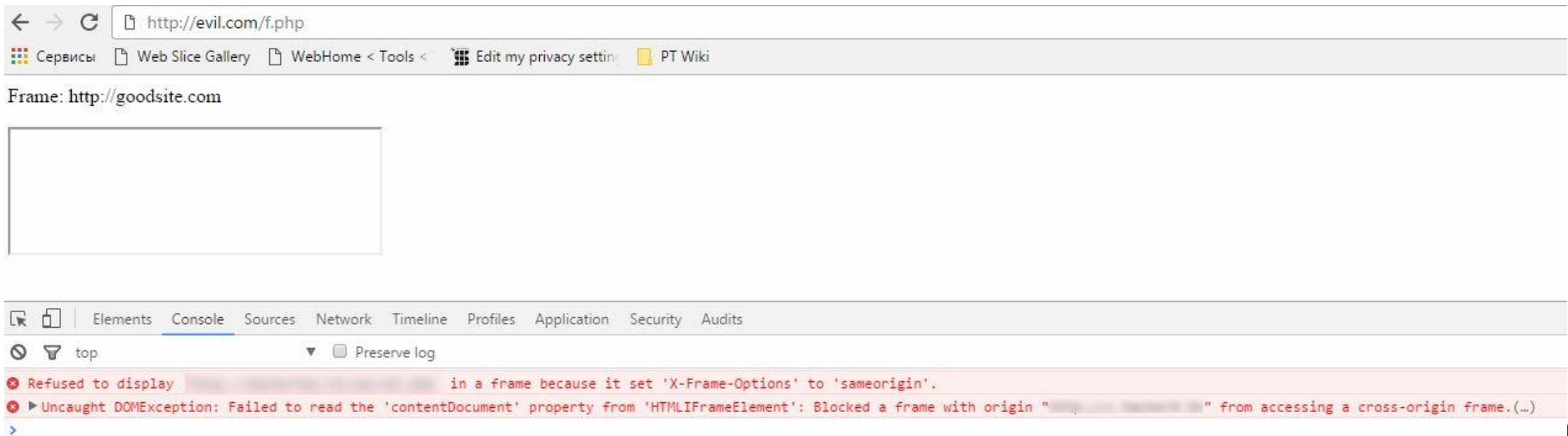






# Same-Origin Policy Bypass

Normal access to <http://goodsite.com> from <http://evil.com>





# Same-Origin Policy Bypass

Access to <http://goodsite.com> from <http://evil.com> via BigIP Portal Access



Frame: <http://goodsite.com>





# Links

F5 BIG-IP Security Cheatsheet

<https://github.com/dnkolegov/bigipsecurity>

OWASP Secure Configuration Guide

[https://www.owasp.org/index.php/SCG\\_D\\_BIGIP](https://www.owasp.org/index.php/SCG_D_BIGIP)





# Thank You!!!

